

Practical Paranoia

macOS 10.12 Sierra

Security Essentials

- The Easiest
- Step-By-Step
- Most Comprehensive
- Guide To Securing Data and Communications
- On Your Home and Office macOS Computer

Marc L. Mintz, MBA-IT, ACTC, ACSP

Practical Paranoia: macOS 10.12 Security Essentials for Home and Business
Marc Mintz

Copyright © 2016 by Marc Louis Mintz.

Notice of Rights: All rights reserved. No part of this document may be reproduced or transmitted in any form by any means without the prior written permission of the author. For information on obtaining permission for reprints and excerpts, contact the author at marc@mintzit.com, +1 888.479.0690.

Notice of Liability: The information in this document is presented on an *As Is* basis, without warranty. While every precaution has been taken in the preparation of this document, the author shall have no liability to any person or entity with respect to any loss or damage caused by or alleged to be caused directly or indirectly by the instructions contained in this document, or by the software and hardware products described within it. It is provided with the understanding that no professional relationship exists and no professional security or Information Technology services have been offered between the author or the publisher and the reader. If security or Information Technology expert assistance is required, the services of a professional person should be sought.

Trademarks: Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the author was aware of a trademark claim, the designations appear as requested by the owner of the trademark. All other product names and services identified in this document are used in editorial fashion only and for the benefit of such companies with no intention of infringement of trademark. No such use, or the use of the trade name, is intended to convey endorsement or other affiliation within this document.

Editions: 1.0 8/2016 • 1.0.1 8/2016 • 1.0.2 9/2016 • 1.1 9/2016

Cover design by Ed Brandt

Student Edition:

ISBN-10: 1535579323

ISBN-13: 978-1535579322

Instructor Edition:

ISBN-10: 1537025864

ISBN-13: 978-1537025865

Dedication

*To Candace,
without whose support and encouragement
this work would not be possible*

Contents At A Glance

Dedication	3
Contents At A Glance	5
Contents In Detail	7
1 Thank You For Reading Practical Paranoia!	17
2 Introduction	19
3 Data Loss.....	31
4 Passwords.....	59
5 System and Application Updates	107
6 User Accounts.....	119
7 Storage Device.....	149
8 Sleep and Screen Saver.....	161
9 Malware.....	169
10 Firewall.....	191
11 Firmware Password	205
12 Lost or Stolen Device	211
13 Local Network.....	227
14 Web Browsing.....	275
15 Email.....	363
16 Apple ID and iCloud.....	453
17 Documents	477
18 Voice, Video, and Instant Message Communications	525
19 Internet Activity.....	549
20 When It Is Time To Say Goodbye.....	607
21 Miscellaneous.....	617
22 The Final Word.....	625
Mintz InfoTech, Inc. macOS Security Checklist.....	627
Change History.....	633
Index	635
Mintz InfoTech, Inc. when, where, and how you want IT	641
Practical Paranoia Security Essentials Workshops & Books.....	643

Contents In Detail

Dedication	3
Contents At A Glance	5
Contents In Detail	7
1 Thank You For Reading Practical Paranoia!	17
2 Introduction	19
2.1 Who Should Study This Course.....	20
2.2 What is Unique About This Course and Book.....	21
2.3 Why Worry?	23
2.4 Reality Check	24
2.5 About the Author.....	26
2.6 Practical Paranoia Updates.....	27
2.7 Practical Paranoia Book Upgrades	28
2.8 Practical Paranoia Kindle Updates	29
3 Data Loss.....	31
3.1 The Need for Backups	32
3.1.1 Assignment: Format the Backup Drive for Time Machine or Carbon Copy Cloner	36
3.1.2 Assignment: Configure Time Machine	40
3.1.3 Assignment: Integrity Test the Time Machine Backup	42
3.1.4 Assignment: Install and Configure Carbon Copy Cloner.....	43
3.1.5 Assignment: Run the First Clone Backup	49
3.1.6 Assignment: Integrity Test the Clone Backup	53
3.2 Review Questions.....	57
4 Passwords.....	59
4.1 The Great Awakening.....	60
4.2 Passwords	61
4.2.1 Assignment: Create a Strong User Account Password.....	63
4.3 Keychain	68
4.3.1 Assignment: View an Existing Keychain Record	71
4.4 Challenge Questions	74
4.4.1 Assignment: Store Challenge Q&A In the Keychain	74
4.4.2 Assignment: Access Secure Data From Keychain	77

Contents In Detail

4.5	Harden the Keychain.....	80
4.5.1	Assignment: Harden the Keychain with a Different Password.....	81
4.5.2	Assignment: Harden the Keychain with an Automatic Timed Lock.....	83
4.6	Synchronize Keychain Across macOS/OS X, and iOS Devices.....	86
4.6.1	Assignment: Activate iCloud Keychain Synchronization.....	86
4.7	LastPass.....	92
4.7.1	Assignment: Install LastPass	92
4.7.2	Assignment: Use LastPass to Save Website Authentication Credentials	101
4.7.3	Assignment: Use LastPass to Auto Fill Website Authentication .	102
4.8	Review Questions.....	105
5	System and Application Updates	107
5.1	System Updates	108
5.1.1	Assignment: Configure Apple System and Application Update Schedule	109
5.2	Manage Application Updates with MacUpdate Desktop.....	111
5.2.1	Assignment: Install and Configure MacUpdate Desktop	111
5.2.2	Assignment: Application Updates with MacUpdate Desktop	115
5.3	Review Questions.....	117
6	User Accounts.....	119
6.1	User Accounts	120
6.2	Never Log In as an Administrator	122
6.2.1	Assignment: Enable the Root User.....	122
6.2.2	Assignment: Login as the Root User	126
6.2.3	Assignment: Change the Root User Password	127
6.2.4	Assignment: Disable the Root User.....	127
6.2.5	Assignment: Create an Administrative User Account	127
6.2.6	Assignment: Change from Administrator to Standard User.....	129
6.2.7	Application Whitelisting and More With Parental Controls	131
6.2.8	Assignment: Configure a Managed with Parental Controls Account	132
6.2.9	Assignment: View Parental Controls Logs.....	143
6.3	Policy Banner.....	145
6.3.1	Assignment: Create a Policy Banner	145
6.4	Review Questions.....	147

Contents In Detail

7	Storage Device.....	149
7.1	Block Access to USB, FireWire, or Thunderbolt Storage Devices	150
7.1.1	Assignment: Disable USB, FireWire, and Thunderbolt Storage Device Access	150
7.1.2	Assignment: Re-enable USB, FireWire, and Thunderbolt Storage Device Access	151
7.2	FileVault 2 Full Disk Encryption	152
7.2.1	Assignment: Boot Into Target Disk Mode	153
7.2.2	Assignment: Boot Into Recovery HD Mode	153
7.2.3	Assignment: Boot Into Single-User Mode	154
7.2.4	Assignment: Enable and Configure FileVault 2	155
7.3	FileVault Resistance to Brute Force Attack.....	158
7.4	Remotely Access and Reboot a FileVault Drive	159
7.4.1	Assignment: Temporarily Disable FileVault.....	159
7.5	Review Questions.....	160
8	Sleep and Screen Saver.....	161
8.1	Require Password After Sleep or Screen Saver	162
8.1.1	Assignment: Require Password After Sleep or Screen Saver	162
8.2	Review Questions.....	167
9	Malware.....	169
9.1	Anti-Malware.....	170
9.1.1	Assignment: Install and Configure Bitdefender	174
9.2	Review Questions.....	190
10	Firewall.....	191
10.1	Firewall	192
10.1.1	Assignment: Activate the Firewall	193
10.1.2	Assignment: Close Unnecessary Ports.....	196
10.2	Review Questions.....	203
11	Firmware Password	205
11.1	EFI Chip	206
11.1.1	Assignment: Create a Firmware Password.....	206
11.1.2	Assignment: Test the Firmware Password	207
11.1.3	Assignment: Remove Firmware Password.....	207
11.2	Review Questions.....	209
12	Lost or Stolen Device	211
12.1	Find My Mac.....	212

Contents In Detail

12.1.1 Assignment: Activate and Configure Find My Mac	212
12.1.2 Assignment: Use Find My Mac from a Computer.....	218
12.1.3 Assignment: Use Find My Mac From an iPhone or iPad	222
12.2 Review Questions.....	225
13 Local Network.....	227
13.1 Ethernet Broadcasting	228
13.2 Ethernet Insertion	229
13.3 Wi-Fi Encryption Protocols	230
13.4 Routers: An Overview	232
13.4.1 Assignment: Determine Your Wi-Fi Encryption Protocol.....	233
13.4.2 Assignment: Secure an Apple Airport Extreme Base Station.....	235
13.4.3 Assignment: Non-Apple Wireless Router Wi-Fi Encryption.....	239
13.5 Use MAC Address to Limit Wi-Fi Access.....	243
13.5.1 Assignment: Restrict Access by MAC Address to Apple Airport	244
13.5.2 Assignment: Restrict Access by MAC Address to a Non-Apple	
Router	251
13.6 Router Penetration.....	260
13.6.1 Assignment: Verify Apple Airport Port Security Configuration .	261
13.6.2 Assignment: Verify Non-Apple Airport Router Security	
Configuration	266
13.7 Review Questions.....	273
14 Web Browsing.....	275
14.1 HTTPS	276
14.1.1 Assignment: Install HTTPS Everywhere	278
14.2 Choose a Browser.....	282
14.3 Private Browsing	283
14.3.1 Assignment: Safari Private Browsing	283
14.3.2 Assignment: Firefox Private Browsing	284
14.3.3 Assignment: Google Chrome Incognito Mode	286
14.4 Secure Web Searches	289
14.4.1 Assignment: Make DuckDuckGo Your Safari Default Search	
Engine.....	289
14.4.2 Assignment: Make DuckDuckGo Your Firefox Default Search	
Engine.....	290
14.4.3 Assignment: Make DuckDuckGo Your Chrome Default Search	
Engine.....	291

Contents In Detail

14.5	Clear History.....	292
14.5.1	Assignment: Clear the Safari History.....	292
14.5.2	Assignment: Clear the Firefox Browsing History.....	293
14.5.3	Assignment: Clear the Chrome History	294
14.6	Browser Plug-Ins.....	296
14.6.1	Assignment: Install Trafficlight Plug-In for Safari.....	296
14.6.2	Assignment: Install Trafficlight Plug-In for Google Chrome	298
14.6.3	Assignment: Install Plug-Ins for Firefox	300
14.6.4	Assignment: Find and Remove Extensions From Safari.....	302
14.6.5	Assignment: Find and Remove Extensions From Google Chrome.....	303
14.6.6	Assignment: Find and Remove Add-Ons From Firefox	304
14.6.7	Assignment: Secure the Safari Browser	306
14.6.8	Assignment: Secure the Firefox Browser.....	307
14.6.9	Assignment: Secure the Chrome Browser.....	308
14.7	Fraudulent Websites	309
14.7.1	Assignment: Warn When Visiting a Fraudulent Website in Safari	313
14.7.2	Assignment: Warn When Visiting a Fraudulent Website in Chrome.....	313
14.7.3	Assignment: Warn When Visiting a Fraudulent Website in Firefox.....	314
14.8	Do Not Track.....	316
14.8.1	Assignment: Enable Do Not Track In Safari.....	316
14.8.2	Assignment: Enable Chrome Do Not Track	317
14.8.3	Assignment: Enable Firefox Do Not Track	323
14.9	Adobe Flash and Java	327
14.9.1	Assignment: Configure Adobe Flash Automatic Updates.....	327
14.9.2	Assignment: Configure Oracle Java for Automatic Updates.....	329
14.10	Web Scams	333
14.11	Tor	336
14.11.1	Assignment: Install Tor for Anonymous Internet Browsing.....	338
14.11.2	Assignment: Configure Tor Preferences	349
14.12	Onion Sites and the Deep Web	360
14.13	Review Questions.....	361
15	Email.....	363

Contents In Detail

15.1	The Killer App	364
15.2	Phishing.....	365
15.3	Email Encryption Protocols.....	367
15.4	TLS and SSL With Mail App	368
15.4.1	Assignment: Configure Email to Use TLS or SSL	368
15.5	HTTPS With Web Mail.....	373
15.5.1	Assignment: Configure Web Mail to Use HTTPS	373
15.6	End-To-End Secure Email With ProtonMail	374
15.6.1	Assignment: Create a ProtonMail Account	375
15.6.2	Assignment: Create and Send an Encrypted ProtonMail Email ..	380
15.6.3	Assignment: Receive and Respond to a ProtonMail Secure Email.....	383
15.7	End-To-End Secure Email With GNU Privacy Guard.....	388
15.7.1	Assignment: Install GPG and Generate a Public Key	389
15.7.2	Assignment: Add Other Email Addresses to a Public Key	395
15.7.3	Assignment: Install a Friend's Public Key	401
15.7.4	Assignment: Configure GPGMail Preferences	403
15.7.5	Assignment: Encrypt and Sign Files with GPGServices	405
15.7.6	Assignment: Send a GPG-Encrypted and Signed Email	409
15.7.7	Assignment: Receive a GPG-Encrypted and Signed Email.....	411
15.8	End-To-End Secure Email With S/MIME.....	414
15.8.1	Assignment: Acquire a Free Class 1 S/MIME Certificate	415
15.8.2	Assignment: Acquire a Class 3 S/MIME Certificate for Business Use	421
15.8.3	Assignment: Purchase a Class 3 S/MIME Certificate for Business Use	430
15.8.4	Assignment: Download and Install a Business S/MIME Certificate.....	441
15.8.5	Assignment: Exchange Public Keys with Others.....	445
15.8.6	Assignment: Send S/MIME Encrypted Email.....	448
15.9	Closing Comments on Encryption and the NSA	450
15.10	Review Questions.....	451
16	Apple ID and iCloud	453
16.1	Apple ID and iCloud	454
16.1.1	Assignment: Create an Apple ID	455
16.1.2	Assignment: Implement Apple ID Two-Step Verification	465

Contents In Detail

16.2	Review Questions.....	476
17	Documents	477
17.1	Document Security	478
17.2	Password Protect a Document Within Its Application	479
17.2.1	Assignment: Encrypt an MS Word Document.....	479
17.3	Encrypt a PDF Document.....	482
17.3.1	Assignment: Convert a Document to PDF for Password Protection.....	482
17.4	Encrypt a Folder for Only macOS/OS X Use.....	485
17.4.1	Assignment: Create an Encrypted Disk image	485
17.5	Encrypt a Folder for Cross Platform Use with Zip.....	488
17.5.1	Assignment: Encrypt a File or Folder using Zip.....	488
17.5.2	Assignment: Open an Encrypted Zip Archive.....	489
17.6	Cross-Platform Document Encryption.....	490
17.6.1	Assignment: Install FUSE for OS X.....	491
17.6.2	Assignment: Download VeraCrypt	495
17.6.3	Assignment: Configure VeraCrypt.....	499
17.6.4	Assignment: Create a VeraCrypt Container	505
17.6.5	Assignment: Mount an Encrypted VeraCrypt Container	517
17.7	Review Questions.....	523
18	Voice, Video, and Instant Message Communications	525
18.1	Voice, Video, and Instant Messaging Communications	526
18.2	HIPAA Considerations	528
18.3	Wire	529
18.3.1	Assignment: Install Wire	529
18.3.2	Assignment: Invite People to Wire	534
18.3.3	Assignment: Import Contacts Into Wire.....	539
18.3.4	Assignment: Secure Instant Message a Wire Friend.....	540
18.3.5	Assignment: Secure Voice Call a Wire Friend.....	544
18.3.6	Assignment: Video Conference With a Wire Friend	547
18.4	Review Questions.....	548
19	Internet Activity.....	549
19.1	VPN–Virtual Private Network.....	550
19.2	Gateway VPN	551
19.3	VPNArea	555
19.3.1	Assignment: Create a VPNArea Account	555

Contents In Detail

19.3.2 Assignment: Install VPNArea Chameleon.....	558
19.3.3 Assignment: Install Viscosity for VPNArea.....	569
19.3.4 Assignment: Create a Viscosity VPN Internet Connection.....	570
19.3.5 Assignment: Disconnect your Viscosity VPN Internet Connection	572
19.3.6 Assignment: Configure Viscosity OpenVPN Utility	572
19.4 Mesh VPN.....	575
19.5 LogMeIn Hamachi.....	576
19.5.1 Assignment: Create a LogMeIn Hamachi Account	576
19.5.2 Assignment: Add Users to a Hamachi VPN Network.....	589
19.5.3 Assignment: File Sharing Within a Hamachi VPN Network.....	599
19.5.4 Assignment: Screen Share Within Hamachi VPN	601
19.5.5 Assignment: Exit the Hamachi VPN Network	603
19.6 Resolving Email Conflicts with VPN	605
19.7 Review Questions.....	606
20 When It Is Time To Say Goodbye.....	607
20.1 Preparing a Computer for Sale or Disposal.....	608
20.2 Secure Erase a Storage Device	609
20.2.1 Assignment: Secure Erase a Storage Device	609
20.3 Review Questions.....	615
21 Miscellaneous.....	617
21.1 Date and Time Settings	618
21.1.1 Assignment: Configure Date & Time	619
21.2 Hardware Components.....	621
21.3 National Institute of Standards and Technology (NIST)	623
21.3.1 NIST-Specific Security Settings	623
22 The Final Word.....	625
Mintz InfoTech, Inc. macOS Security Checklist.....	627
Change History.....	633
Index	635
Mintz InfoTech, Inc. when, where, and how you want IT	641
Practical Paranoia Security Essentials Workshops & Books.....	643

Practical Paranoia

macOS 10.12 Sierra

Security Essentials

Marc L. Mintz, MBA-IT, ACTC, ACSP

1 Thank You For Reading Practical Paranoia!

Dear reader,

Thank you for getting this far into this book. Although I can't promise it will be as easy getting all the way through as it was to here, I do promise this is the easiest and most comprehensive book in this category that you can buy.

When I wrote the first edition of Practical Paranoia, I received many emails and calls from instructors, students, and fans thanking me for the book. In truth, over half of this book came out of the questions and insights provided by the readers themselves. I love the feedback. I invite you to write to me at marc@mintzit.com, and to visit me at <https://mintzit.com/>.

I also ask a favor. Please write a review of *Practical Paranoia*. Loved it, hated it, what worked for you, what you would like to see added or changed—I both enjoy and value your feedback.

Reviews can be difficult to come by these days. You, the reader, have the power now to make, break, and shape the evolution of a book. If you have the time, please visit my author page on Amazon.com¹. Here you can find all of my books, and leave a review.

Thank you so much for reading Practical Paranoia, and for spending time with me.

Warmly,

A handwritten signature in black ink that reads "Marc L. Mintz". The signature is fluid and cursive, with "Marc L." on top and "Mintz" on the bottom, enclosed in a small circle.

¹ <https://www.amazon.com/author/marclmintz>

2 Introduction

Just because you're paranoid doesn't mean they aren't after you.

–Joseph Heller¹, *Catch-22*

Everything in life is easy—once you know the how.

–Marc L. Mintz²

¹ https://en.wikipedia.org/wiki/Joseph_Heller

² <https://mintzit.com/>

2.1 Who Should Study This Course

Traditional business thinking holds that products should be tailored to a laser-cut market segment. Something like: *18-25-year-old males, still living at their parents' home, who like to play video games, working a minimum-wage job.* Yup, we all have a pretty clear image of that market segment.

In the case of this course, the market segment is *all users of macOS and OS X computers.* Really! From my great-Aunt Rose who is wrestling with using her first computer, to the small business, to the IT staff for major corporations and government agencies.

Even though the military may use better security on their physical front doors—MP's with machine guns protecting the underground bunker—compared to a residential home with a Kwikset deadbolt and a neurotic Chihuahua, the steps to secure macOS for home and business use are almost identical for both. There is little difference between *home-level security* and *military-grade security* when it comes to this technology.

The importance of data held in a personal computer may be every bit as important as the data held by the CEO of a Fortune 500. The data is also every bit as vulnerable to penetration.

2.2 What is Unique About This Course and Book

Practical Paranoia: macOS 10.12 Security Essentials is the first comprehensive macOS security book written with the new to average user in mind—as well as the IT professional. The steps outlined here are the same steps used by my consulting organization when securing systems for hospitals, government agencies, and the military.

By following the easy, illustrated, step-by-step instructions in this book, you will be able to secure your computer to better than National Security Agency (NSA) standards.

Hardening your computer security will help your business protect the valuable information of you and your customers. Should your computer work include HIPAA, SEC, or legal-related information, to be in full compliance with regulations it is likely that you will need to be using at least OS X 10.8, and I recommend macOS 10.12 or higher.

For those of you caught up in the ADHD epidemic, do not let the number of pages here threaten you. This book really is a quick read because it has lots of actual screenshots. Written for use in our *Practical Paranoia: Security Essentials Workshops* as well as for college classroom and self-study, this book is the ultimate step-by-step guide for protecting the new macOS user who has no technical background, as well as for the experienced IT consultant. The information and steps outlined are built on guidelines, policies & procedures, and best practices from Apple, the NSA, NIST, US-CERT, and my own 30 years as an IT and Apple consultant, developer, technician and trainer. I have reduced dull background theory to a minimum, including only what is necessary to grasp the need-for and how-to.

The organization of this book is simple. We provide chapters representing each of the major areas of vulnerability, and the tasks you will do to protect your data, device, and personal identity.

Although you may jump in at any section, I recommend you follow the sequence provided to make your system as secure as possible. Remember, the bad guys will not attack your strong points. They seek out your weak points. Leave no obvious weakness and they will most likely move on to an easier target.

2 Introduction

To review your work using this guide, use the *Mintz InfoTech Security Checklist* provided at the end of this book.

Theodore Sturgeon, an American science fiction author and critic, stated: *Ninety percent of everything is crap*³. Mintz's extrapolation of Sturgeon's Revelation is: *Ninety percent of everything you have learned and think to be true is crap*.

I have spent most of my adult life in exploration of how to distill what is real and accurate from what is, well, Sturgeon's 90%. The organizations I have founded, the workshops I've produced, and the *Practical Paranoia* book series all spring from this pursuit. If you find any area of this workshop or book that you think should be added, expanded, improved, or changed, I invite you to contact me personally with your recommendations.

³ https://en.wikipedia.org/wiki/Sturgeon%27s_law

2.3 Why Worry?

In terms of network, Internet, and data security, macOS users must be vigilant because of the presence of malware⁴ such as viruses, Trojan horses, worms, phishing, and key loggers impacting our computers. Attacks on computer and smartphone users by tricksters, criminals, and governments are on a steep rise. In addition to macOS-specific attacks, we are vulnerable at points of entry common to all computer users, including Flash, Java, compromised websites, and phishing, as well as through simple hardware theft. How bad is the situation?

- According to a study by Symantec, an average enterprise-wide data breach has a recovery cost of \$5 million.
- According to the FBI, 2 million laptops are stolen or lost in the U.S. each year.
- Of those 2 million stolen or lost, only 3% ever are recovered.
- Out of the box, an macOS computer can be broken into—bypassing password protection—in less than 1 minute.
- The typical email is clearly readable at dozens of points along the Internet highway on its trip to the recipient. Most likely, that email is read by somebody you don't know.
- A popular game played by high school and college students is *war driving*: the act of driving around neighborhoods to find Wi-Fi networks, geographically marking the location for others to use and break into.
- The Cyber Intelligence Sharing and Protection Act (CISPA)⁵ allows the government easy access to all your electronic communications. PRISM⁶ allows government agencies to collect and track data on any American device.

The list goes on, but we have lives to live and you get the point. It is not a matter of *if* your data will ever be threatened. It is only a matter of *when*, and how often the attempts will be made.

⁴ <http://en.wikipedia.org/wiki/Malware>

⁵ http://en.wikipedia.org/wiki/Cyber_Intelligence_Sharing_and_Protection_Act

⁶ [http://en.wikipedia.org/wiki/PRISM_\(surveillance_program\)](http://en.wikipedia.org/wiki/PRISM_(surveillance_program))

2.4 Reality Check

Nothing can 100% guarantee 100% security 100% of the time. Even the White House and CIA websites and internal networks have been penetrated. We know that organized crime, as well as the governments of China, North Korea, Russia, Great Britain, United States, and Australia have billions of dollars and tens of thousands of highly skilled security personnel on staff looking for *zero-day exploits*⁷. These are vulnerabilities that have not yet been discovered by the developer. As if this is not enough, the U.S. government influences the development and certification of most security protocols. This means that industry-standard tools used to secure our data often have been found to include vulnerabilities introduced by government agencies.

With these odds against us, should we just throw up our hands and accept that there is no way to ensure our privacy? Well, just because breaking into a locked home only requires a rock through a window, should we give up and not lock our doors?

Of course not. We do everything we can to protect our valuables. When leaving on vacation we lock doors, turn on the motion detectors, notify the police to prompt additional patrols, and stop mail and newspaper delivery.

The same is true with our digital lives. For the very few who are targeted by the NSA, there is little that can be done to completely block them from reading your email, following your chats, and recording your web browsing. But you can make it extremely time and labor intensive.

For the majority of us not subject to an NSA targeted attack, we are rightfully concerned about our digital privacy being penetrated by criminals, pranksters, competitors, nosy people, as well as about the collateral damage caused by malware infestations.

You *can* protect yourself, your data, and your devices from such attack. By following this book, you should be able to secure fully your data and your first

⁷ [https://en.wikipedia.org/wiki/Zero-day_\(computing\)](https://en.wikipedia.org/wiki/Zero-day_(computing))

2 Introduction

device in two days, and any additional devices in a half day. This is a very small price to pay for peace of mind and security.

Remember, penetration does not occur at your strong points. A home burglar will avoid hacking at a steel door when a simple rock through a window will gain entry. A strong password and encrypted drive by themselves do not mean malware can't slip in with your email, and pass all of your keystrokes – including usernames and passwords – to the hacker.

It is imperative that you secure all points of vulnerability.

- Note: Throughout this book we provide suggestions on how to use various free and for-fee applications to help enforce your protection. Neither Marc L. Mintz nor Mintz InfoTech, Inc. receives payment for suggesting them. We have used them with success, and thus feel confident in recommending them.

2.5 About the Author

Marc Louis Mintz is one of the most respected IT consultants and technical trainers in the United States. His technical support services and workshops have been embraced by hundreds of organizations and thousands of individuals over the past 3 decades.

Marc holds an MBA-IT (Masters of Business Administration with specialization in Information Technology), Chauncy Technical Trainer certification, Post-Secondary Education credentials, and over a dozen Apple certifications.

Marc's enthusiasm, humor, and training expertise have been honed on leading edge work in the fields of motivation, management development, and technology. He has been recruited to present software and hardware workshops nationally and internationally. His technical workshops are consistently rated by seminar providers, meeting planners, managers, and participants as *The Best* because he empowers participants to see with new eyes, think in a new light, and problem solve using new strategies.

When away from the podium, Marc is right there in the trenches, working to keep client Android, iOS, macOS, and Windows systems securely connected.

The author may be reached at:

Marc L. Mintz

Mintz InfoTech, Inc.

1000 Cordova Pl

#842

Santa Fe, NM 87505

+1 888.479.0690

Email: marc@mintzIT.com

Web: <https://mintzIT.com> • <http://thepracticalparanoid.com>

2.6 Practical Paranoia Updates

Information regarding IT security changes daily, so we offer you newsletter, blog and Facebook updates to keep you on top of everything.

Newsletter

Stay up to date with your Practical Paranoia information by subscribing to our free weekly newsletter.

1. Visit <https://mintzIT.com>
2. Scroll to the bottom of the home page to the *Newsletter Signup* form.
3. Complete the form, and then click the *Sign Up* button.

Blog

Updates and addendums to this book also will be included in our free *Mintz InfoTech Blog*. Go to: <https://mintzit.com>, and then select the *Blog* link.

Facebook

Updates and addendums to this book also will be found in our *Practical Paranoia Facebook Group*. Go to <https://www.facebook.com/groups/PracticalParanoia/>

2.7 Practical Paranoia Book Upgrades

We are constantly updating *Practical Paranoia* so that you have the latest, most accurate resource available. If at any time you wish to upgrade to the latest version of *Practical Paranoia* at the lowest price we can offer:

1. Tear off the front cover of *Practical Paranoia*.
2. Make check payable to Mintz InfoTech for \$30.
3. Send front cover, check, and mailing information to:
Mintz InfoTech, Inc.
1000 Cordova Pl
#842
Santa Fe, NM 87505
4. Your new copy of *Practical Paranoia* will be sent by USPS. Please allow up to 4 weeks for delivery.

2.8 Practical Paranoia Kindle Updates

We are constantly updating *Practical Paranoia* so that you have the latest, most accurate resource available. If at any time you wish to update to the latest Kindle version of *Practical Paranoia* at no cost:

1. Delete the copy of *Practical Paranoia* currently installed on your Kindle device.
2. Download the current edition of *Practical Paranoia*.

3 Data Loss

Weather forecast for tonight: Dark.

—George Carlin¹

I know, you want to jump right into cyber security and harden your awesome macOS computer. Sorry to be a Debbie Downer², but there is a very real risk of losing data in the process of some of the work ahead of us. Because of this, we must begin our exciting journey into the heart of security with drudgery—backing up your computer.

¹ https://en.wikipedia.org/wiki/George_Carlin

² https://en.wikipedia.org/wiki/Debbie_Downer

3.1 The Need for Backups

Data loss is a very real fact of life. It is not a matter of if you will experience data loss, just a matter of when, and how often. Only a small percentage of computer users back up on a regular basis. I suspect these are the folks who have experienced catastrophic data loss and never want a repeat.

There are many sources of data loss. The top contenders include:

- Computer theft
- Power surges
- Power sags
- Sabotage
- Fire
- Water damage. I personally have had 3 clients who have lost computers due to cats or dogs marking their territory, and my own cat took out a \$4,000 monitor with nothing more than a hairball.
- Entropy / aging of the drive
- Malware
- Terrorist activities
- Criminal activities
- Static electricity
- Physical shock to the drive (banging the computer, dropping, etc.)

Best Practice³ calls for three backups:

- **One full backup onsite.** This allows for almost immediate recovery of lost or corrupted documents, or full recovery of the OS, applications, and documents in the event of complete loss of the hard drive.

³ https://en.wikipedia.org/wiki/Best_practice

- **One full backup offsite.** This is your *Plan B* in the event of a catastrophic loss of both the computer and the onsite backup. This typically takes the form of fire or theft.
- **One Internet-based backup.** This is your OMG, what do I do now? fallback plan. Many people substitute the Internet backup for the offsite. A potential problem is that your Internet backup may take several days to weeks to download.

Onsite Full Backup with Time Machine

macOS comes with the most advanced backup software for any computer—Time Machine. Time Machine has several advantages over other options, including:

- Free
- Highly reliable and stable
- Low resource requirements
- Maintains document versioning. With each run Time Machine will back up the latest version of your documents, while maintaining all prior versions as well
- Runs in the background every hour without user intervention
- Works with Migration Assistant (part of the standard macOS installation) to replicate the last backup to another Macintosh.
- Does backup to a FireWire, Thunderbolt, or USB drive attached locally, to an Apple Airport Extreme Base station, or a computer running macOS Server or OS X Server
- Can create an encrypted backup to a locally attached drive (macOS 10.12 and above, Mac OS X 10.7 and above, macOS 10.12 and above), or to a drive attached to an Airport Extreme or macOS Server (10.12 and above) or OS X Server (10.8 and above)

As a general rule, the backup drive should be at least double the size of your data, preferably quadruple. This allows for future growth and the maintenance of long-term document versioning.

Although FireWire drives typically cost \$20-\$50 more than USB, and Thunderbolt \$40 more than FireWire, that extra cost will be paid back with interest in the event you ever need to use the backup. FireWire drives outperform USB 2-4 fold, and Thunderbolt drives are a bit faster than FireWire. When recovering a Terabyte or more of data, speed will lessen the pain.

Onsite Full Backup with Carbon Copy Cloner

As great as Time Machine is, there is one critical area in which it fails—it does not create a bootable clone. A bootable clone is an exact duplicate of the original drive. This is where Carbon Copy Cloner comes in.

The need for a bootable clone backup becomes clear when you have a hard drive failure. Without a bootable clone, the recovery process looks like this:

1. Call a technician for assistance or rush to the store to buy a new drive.
2. Remove the old drive, install the new drive.
3. Install macOS.
4. Install all updates.
5. Use Migration Assistant to copy over the latest backup from Time Machine.
6. Get back to work—4 to 8 hours after the crash.

With a bootable clone, the recovery process looks like this:

1. Restart your Mac with the option key held down. This triggers the Start Manager, allowing you to select from which drive to boot.
2. Select the bootable clone drive as your boot drive.
3. Get back to work—5 minutes after the crash.
4. Call a technician for assistance. Let them know there is no rush.
5. At a time that is convenient (and not on overtime) the problem drive is replaced and all data copied over.

So why use Time Machine? It is the fastest and easiest way to recover lost or damaged documents.

Internet-Based Data Backup

There are several great and unique advantages to Internet-based backups:

- If a small black hole opens up devouring your computer, backup and offsite backup, your Internet backup will always be waiting for you. Think disaster recovery after a multi-block explosion, terrorist activity that prevents access to either the computer or off-site location.
- Should you find yourself far away from your computer, as long as you have any computer, your data can be accessed.
- A few of the Internet-based options now include sharing access to any documents that have been backed up.

When looking for the right Internet-based backup service, in addition to cost, features, company and software stability, keep an eye out for document versioning. You want your service to keep at least one month of document versions. In the event that you accidentally delete a document, it will remain on the server for at least a month, or if a document corrupts, you want to be able to go back to a previous (presumably not corrupted) version.

My personal favorites include:

Backblaze⁴. Easy to use, very fast uploads, rock solid stable, 30-day document versioning, backs up all user accounts.

Carbonite⁵. Fast uploads, rock solid stable, limited document versioning, backs up all user accounts. 30-day document versioning, family and business accounts make it easier to administer multiple computers.

CrashPlan⁶ for home and **CrashPlan Pro**⁷-my only choice for business. Fast upload, rock solid stable, document versioning, lifetime document versioning, individual and business accounts. Can meet your HIPAA or SEC compliance needs.

⁴ <http://www.backblaze.com>

⁵ <http://www.carbonite.com>

⁶ <http://www.crashplan.com>

⁷ <http://www.crashplan.com>

3.1.1 Assignment: Format the Backup Drive For Time Machine or Carbon Copy Cloner

Redundancy calls for two on-site backups. My preference is to use two tools, one for each backup—Time Machine and Carbon Copy Cloner.

In this assignment, you will format a drive for use with either. If you will be following my approach and have two backups, repeat this process with each of two drives.

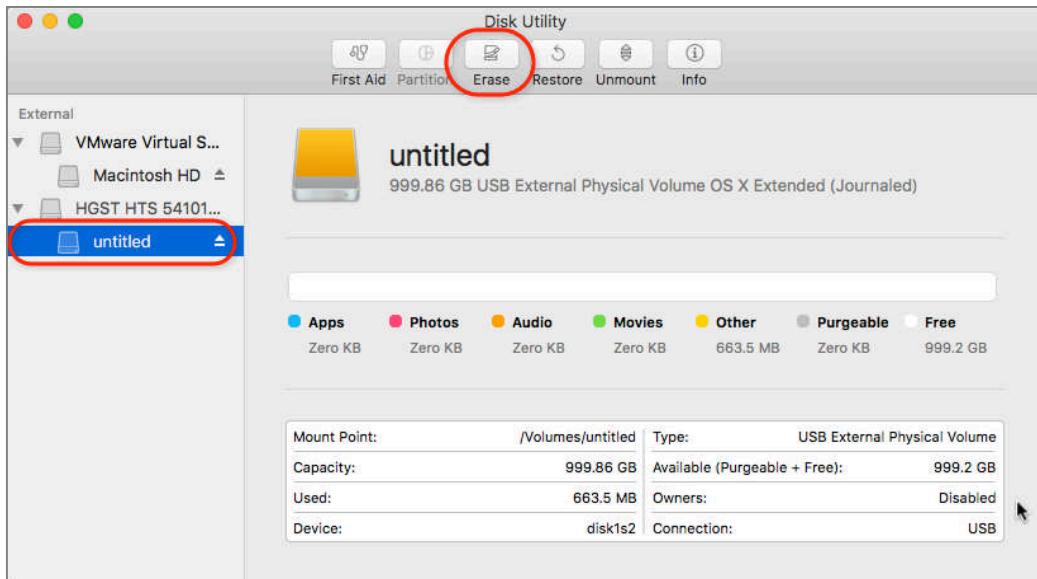
1. Purchase an external hard drive that has at least four times the capacity of the data to be held on the host computer. We strongly recommend purchasing a drive with FireWire 800, USB 3, or Thunderbolt. Although you pay up to \$50 extra upfront, these drives are significantly faster than those with FireWire 400 or USB 2. That speed makes a huge difference as you are sweating blood trying to recover your data.
2. Connect the new drive to your computer.
3. Open Disk Utility, located in your */Applications/Utilities* folder.

Change Volume format to OS X Extended (Journaled)

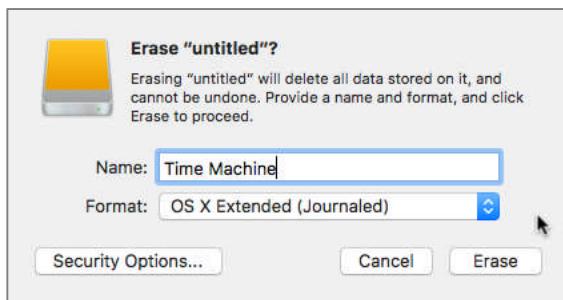
It is most likely the drive you have purchased is in either FAT or NTFS format. To be used by Time Machine (or Carbon Copy Cloner), the format of the volume will need to be OS X Extended (Journaled).

3 Data Loss

4. Select the indented name of the drive, and then select the *Erase* button in the tool bar.



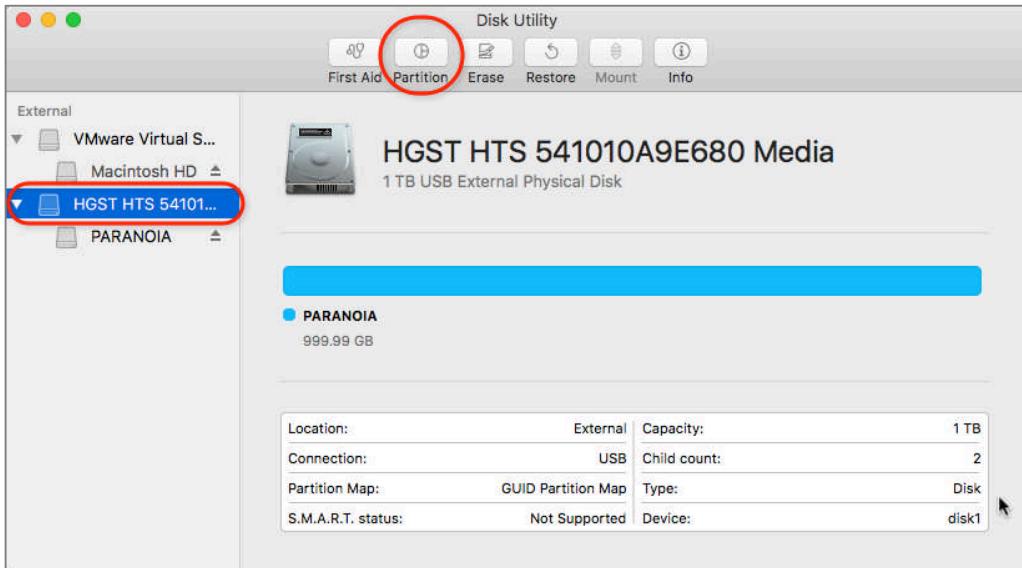
- a. In the *Name* field, enter the name you want displayed for this drive
- b. In the *Format* field, select *OS X Extended (Journaled)*, and then select the *Erase* button.



5. If you see a pop-up window asking if you want to use this drive for Time Machine, click *Don't Use* (we aren't done yet.)
6. In the volume format window, select the *Done* button.

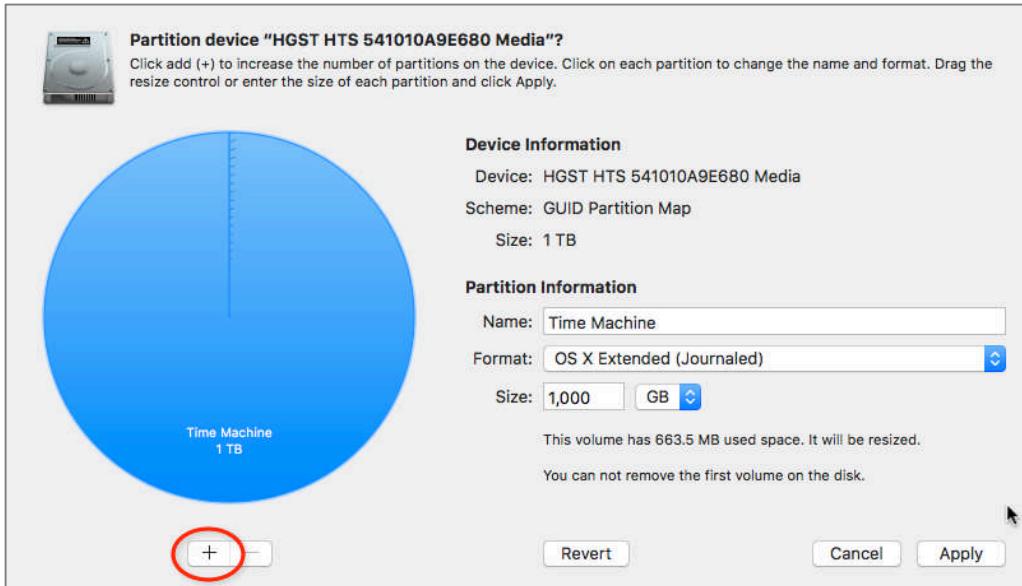
Format the drive for GUID partition

7. Select the out dented hard drive name from the sidebar (the out dented name is the physical drive, while the indented name(s) is/are the partition or volume.) Then select the *Partition* tab.

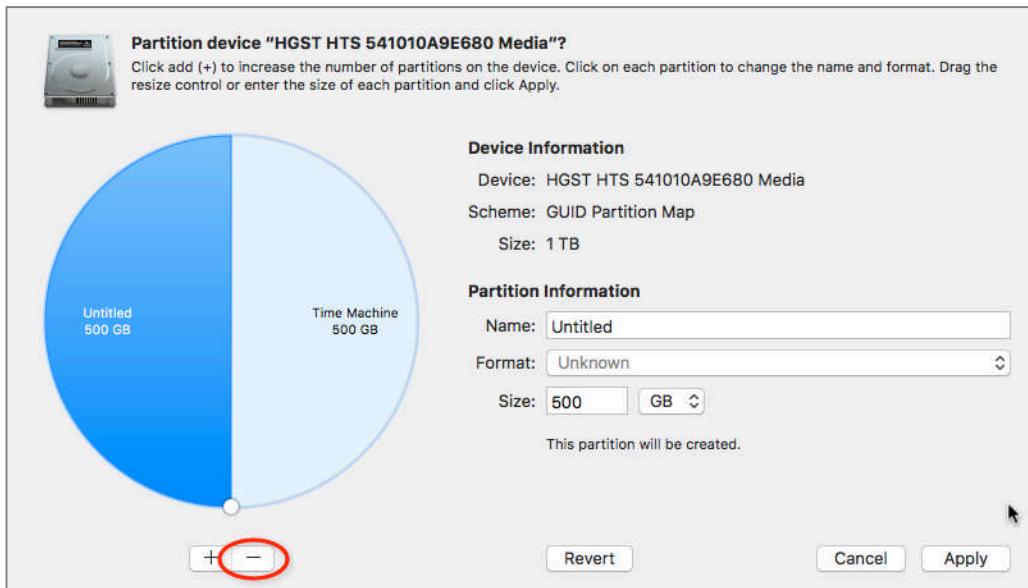


3 Data Loss

8. The *Partition Device* pane will open. Select the + (add volume) button.



9. This will create an additional volume on the drive. Select the new volume, and then click the - (delete volume) button.



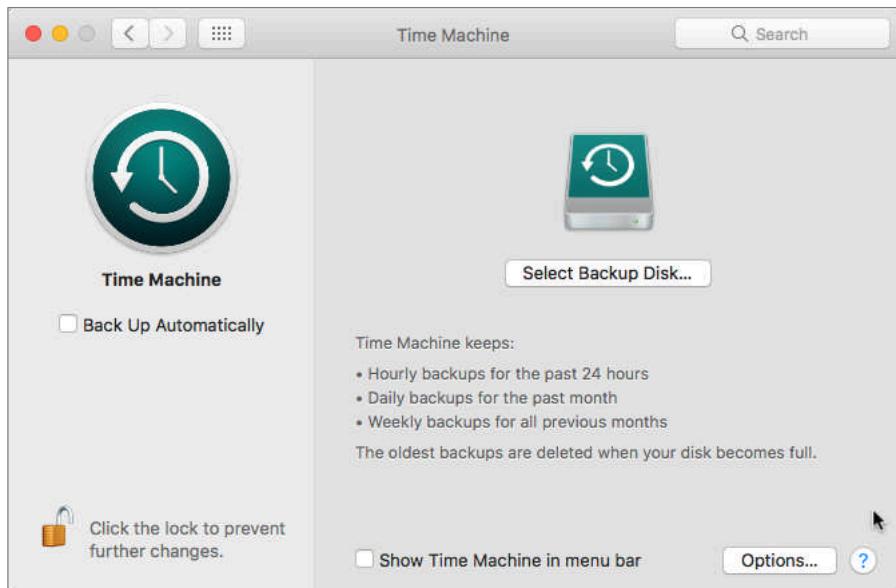
10. Click the *Apply* button.

The formatting process will begin. Depending on the size and speed of the drive, and the speed of the computer, this may take from a few seconds to a few minutes. When complete, the drive is ready for use.

3.1.2 Assignment: Configure Time Machine

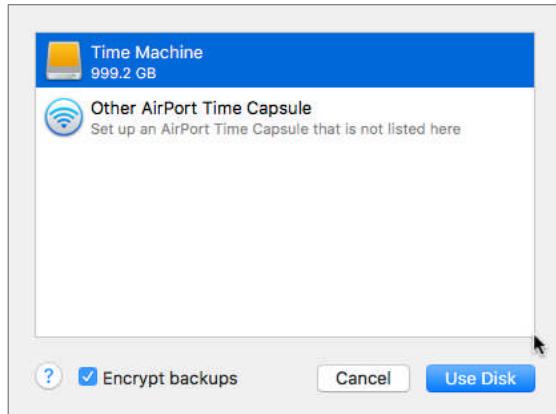
Although Time Machine is designed to auto-configure, that doesn't mean it has auto-configured correctly. To manually configure Time Machine:

1. Attach your Time Machine drive. If you have followed the steps above, it is already attached and mounted.
2. Open *Apple menu > System Preferences > Time Machine*. Enable the *Back Up Automatically* checkbox.



3 Data Loss

3. All drives available to serve as backup drives appear. Select your Time Machine drive, enable the *Encrypt backups* checkbox, and then select the *Use Disk* button.



4. In the *Backup password* field, enter a password to encrypt the backup drive. I recommend using your account login password for your computer. Enter it again in the *Verify password* field. In the *Password hint* field, enter a character or two as it is required to have an entry, but, come on, a hint? *Really*?! Then select the *Encrypt Disk* button.



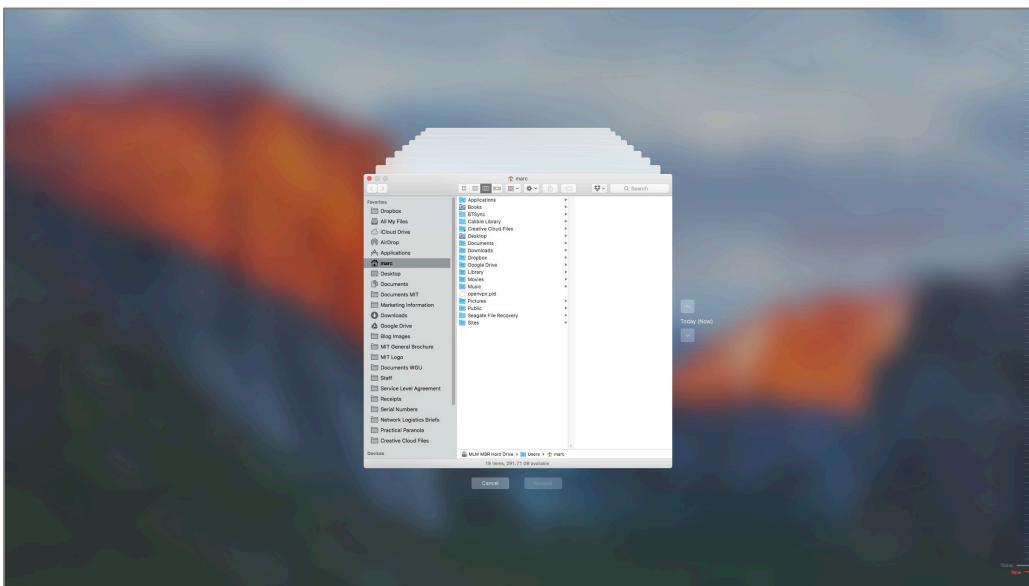
5. Quit System Preferences.

Time Machine will automatically start to back up to this drive within the hour.

3.1.3 Assignment: Integrity Test the Time Machine Backup

To test your Time Machine backup, you need to enter Time Machine, and then verify the existing backups. If you have a portable Mac, it is likely that you have two different backups—one on your Time Machine drive, and the other on your laptop itself. The local backups are created when Time Machine auto launches but does not find the Time Machine drive connected, so it backs up to the laptop drive itself. You can see the two backups in the Time Machine window. Backups to the Time Machine drive have purple tick marks, local backups have white tick marks.

1. From the menu bar, select the *Time Machine* icon > *Enter Time Machine* menu.
2. When in Time Machine, look to the right hand edge of your screen. If you see a series of tick marks that display date and time as the cursor moves over them, Time Machine has performed backups.
3. Verify the latest time stamp (at the bottom) is current.



Congratulations! You have verified your Time Machine backup is working properly.

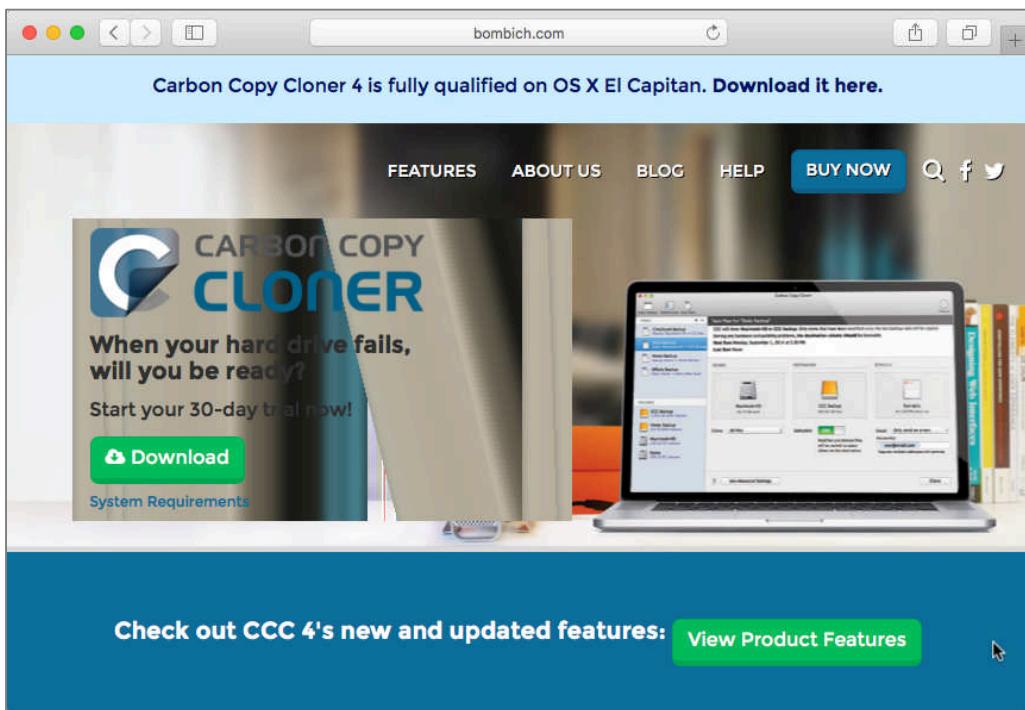
3.1.4 Assignment: Install and Configure Carbon Copy Cloner

In this assignment, you will download, install, and then configure Carbon Copy Cloner to create bootable clone backups of your boot drive.

Prerequisite: You must have a hard drive at least twice the size of your data, formatted as OS X Extended (Journaled).

Download Carbon Copy Cloner

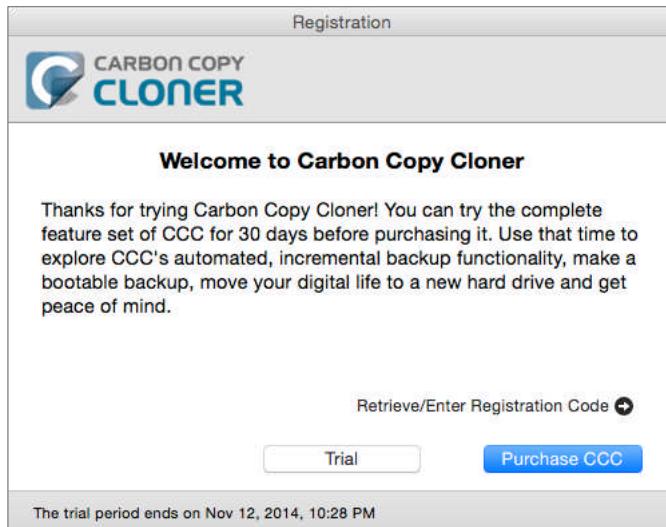
1. Open a web browser and go to <http://bombich.com>.



2. Select the *Download* button. Carbon Copy Cloner will download. This will be a time-limited full version. Should you wish to purchase CCC, you can do so from within the application.

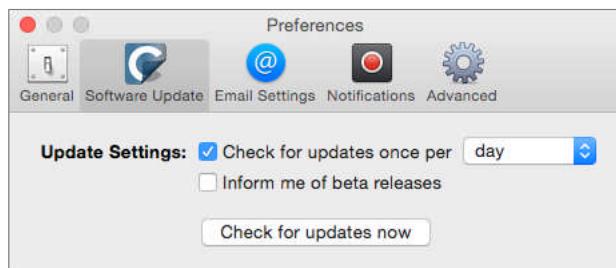
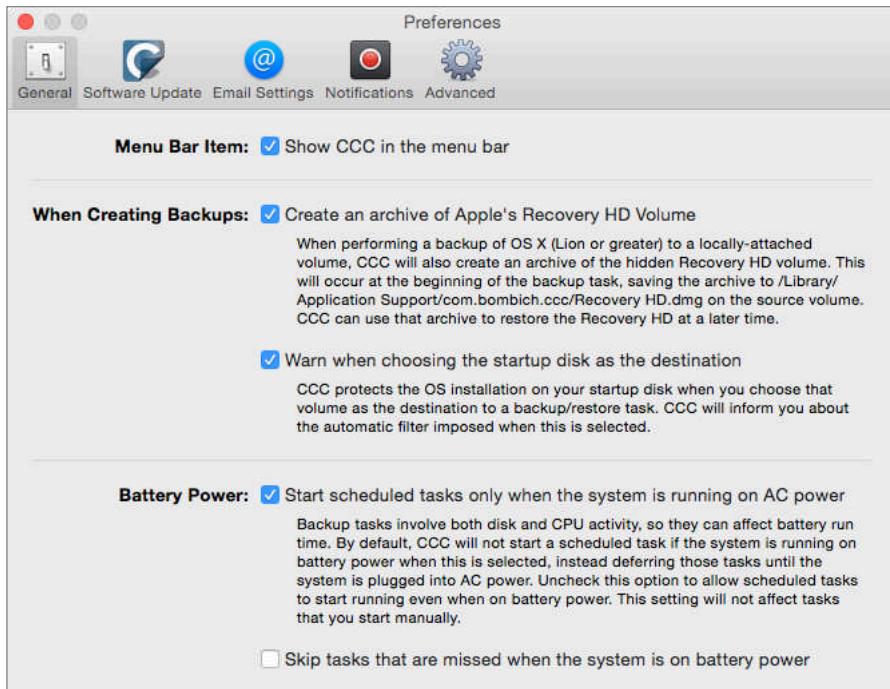
Install Carbon Copy Cloner

3. Launch Carbon Copy Cloner. If you see a license agreement, select *OK*. At the welcome window, select the *Trial* button.

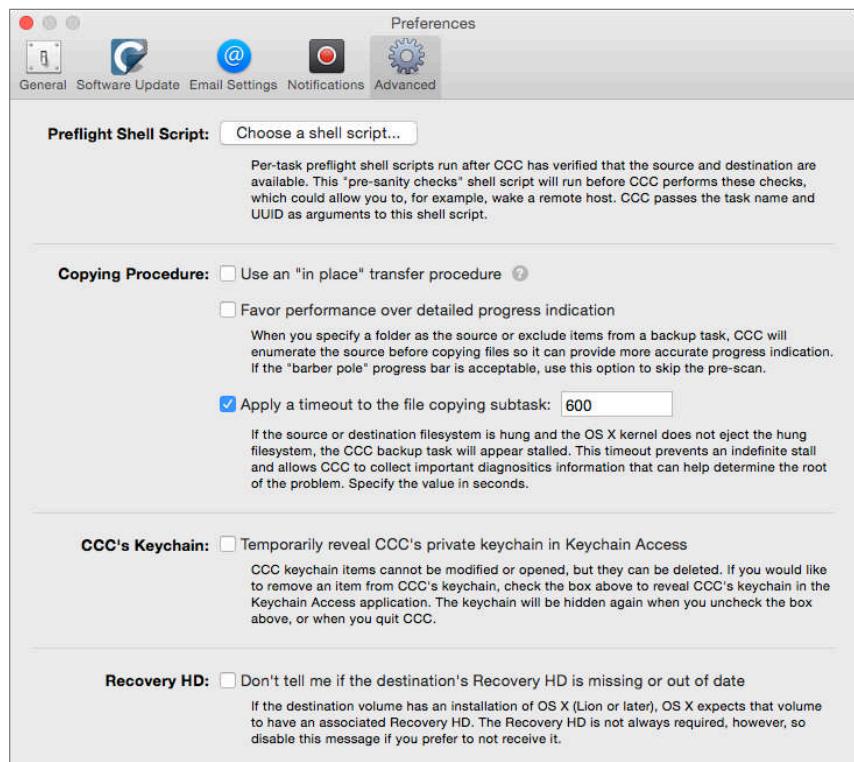
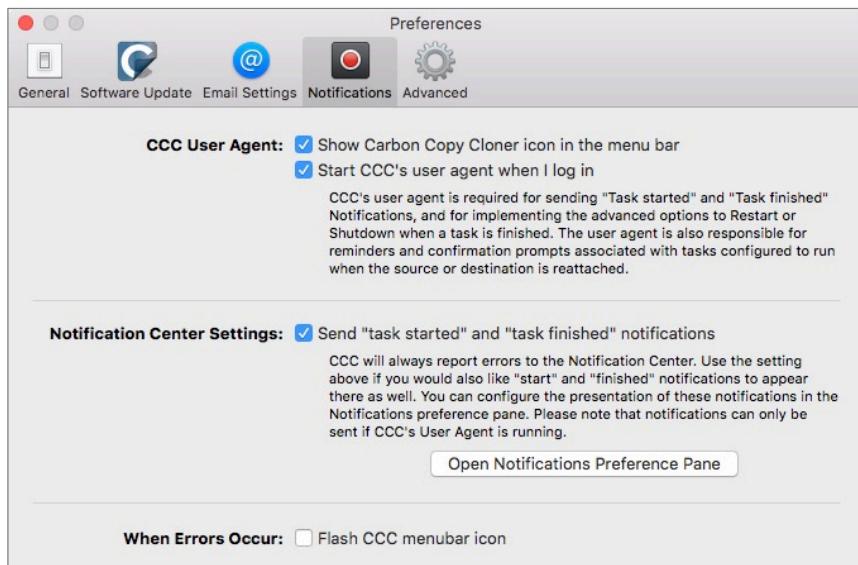


3 Data Loss

4. The main window opens. It's always a bright idea to configure an application's preferences before having it do heavy lifting. Select the *Carbon Copy Cloner* menu > *Preferences*. Configure each of the preference windows as below.

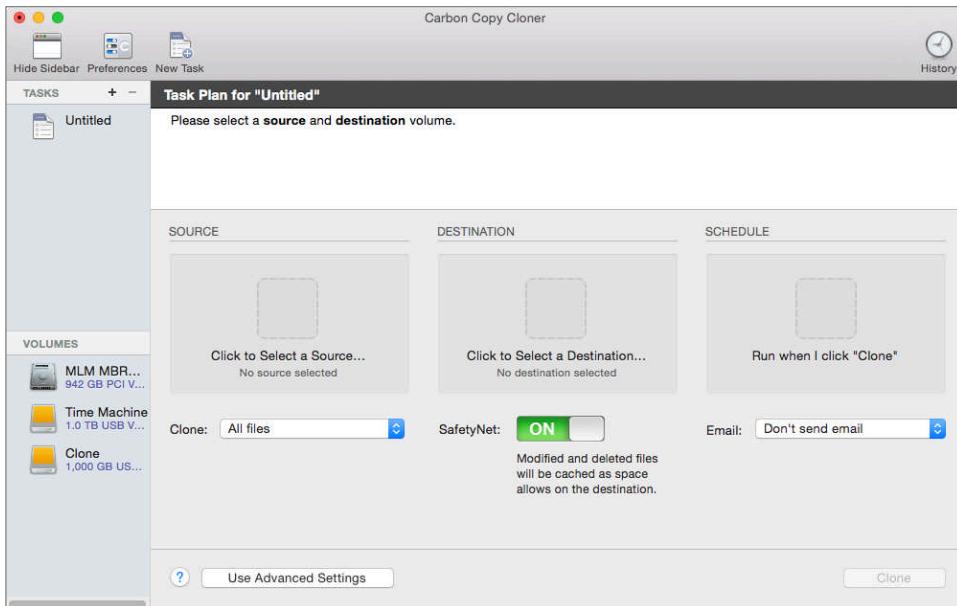


3 Data Loss



3 Data Loss

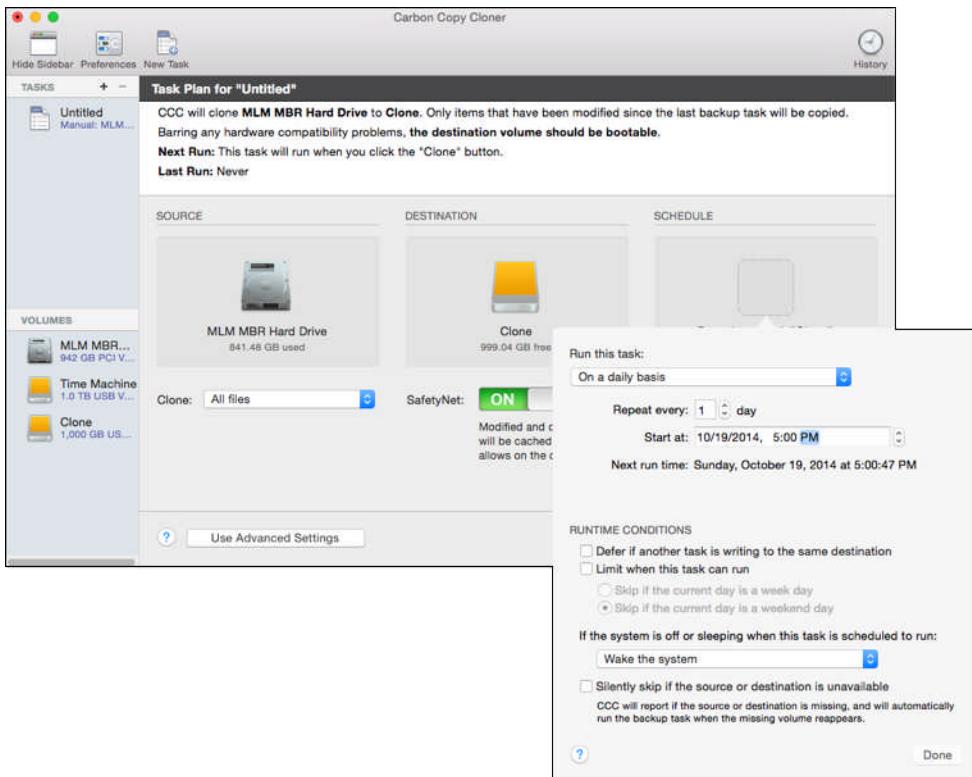
5. Close the *preferences* window.
6. Back at the main window, from the tool bar select the *Show Sidebar* button. The sidebar will slide out.



7. From the *Source* area, select the *Click to select a Source* icon, and then select your internal boot hard drive.
8. From the *Destination* area, select the *Click to Select a Destination* icon, and then select the Clone drive.

3 Data Loss

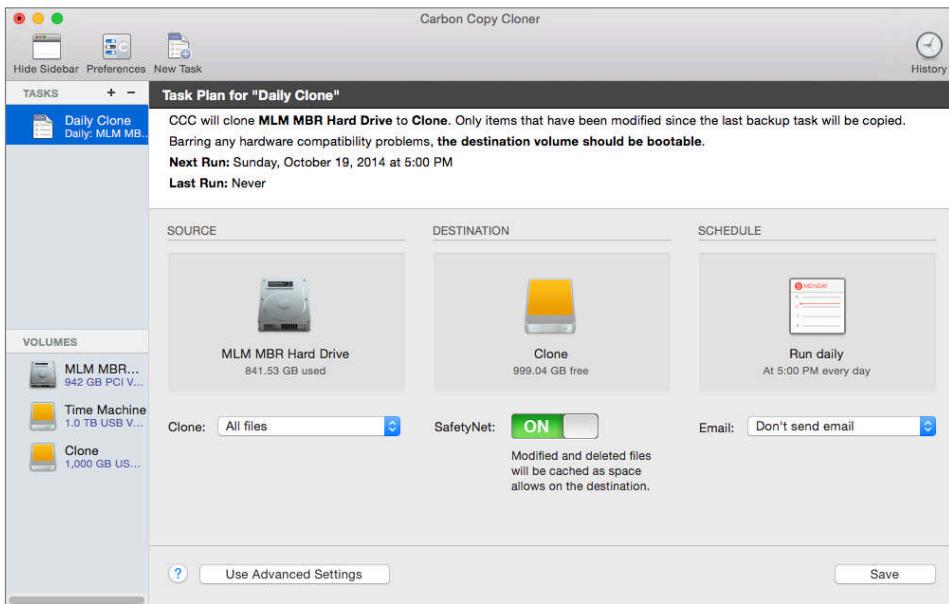
9. From the *Schedule* area, select the icon, configure as below, and then select the *Done* button.



10. At the main window, in the sidebar, double-click on *Untitled* task, and then rename to *Daily Clone*.

3 Data Loss

11. Select the *Save* button. Your configuration should look like this:

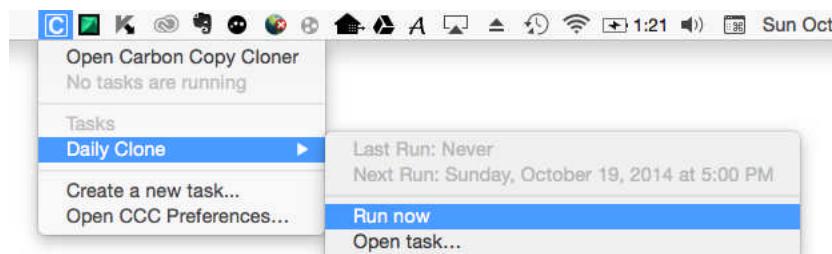


3.1.5 Assignment: Run the First Clone Backup

To test your Carbon Copy Cloner script, you will manually trigger the first backup. It is also necessary to have an initial backup in order to create a Recovery HD partition onto the drive (required to boot from an encrypted drive), and to then encrypt the drive.

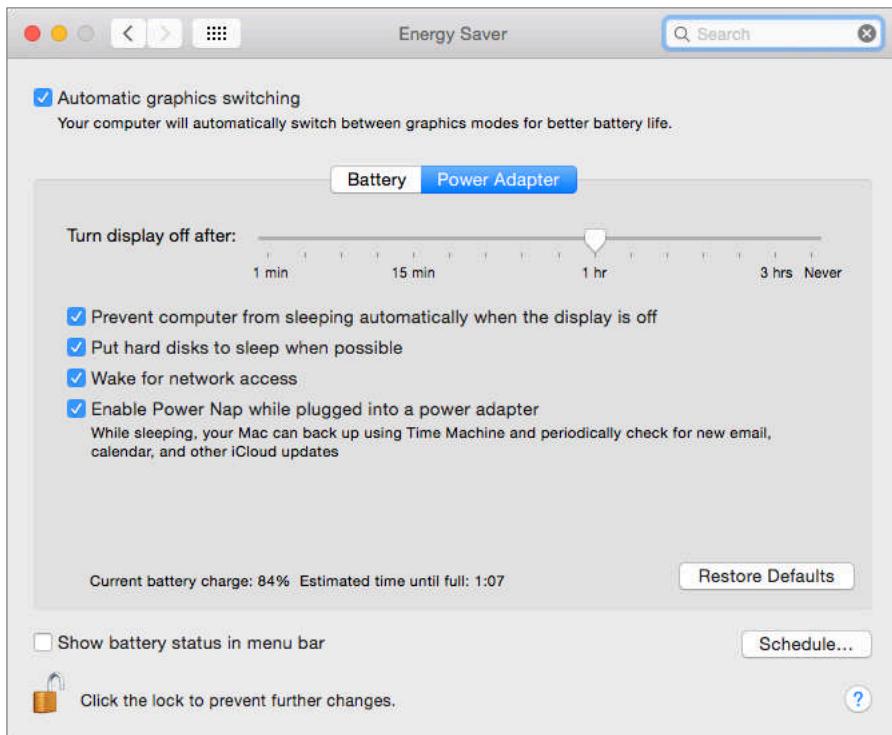
Run the first clone backup.

1. From the *Carbon Copy Cloner* menu icon, select *Daily Clone > Run Now*.



3 Data Loss

2. Depending on the speed of your computer and the size of the source drive, the first backup may take from 1-12 or more hours. Make certain that your computer will not go into sleep mode during the backup by selecting the *Apple* menu > *System Preferences* > *Energy Saver*. Although it is ok to have your monitor go to sleep, your system must not. Configure your preferences so the system will not sleep.



3. Close System Preferences.

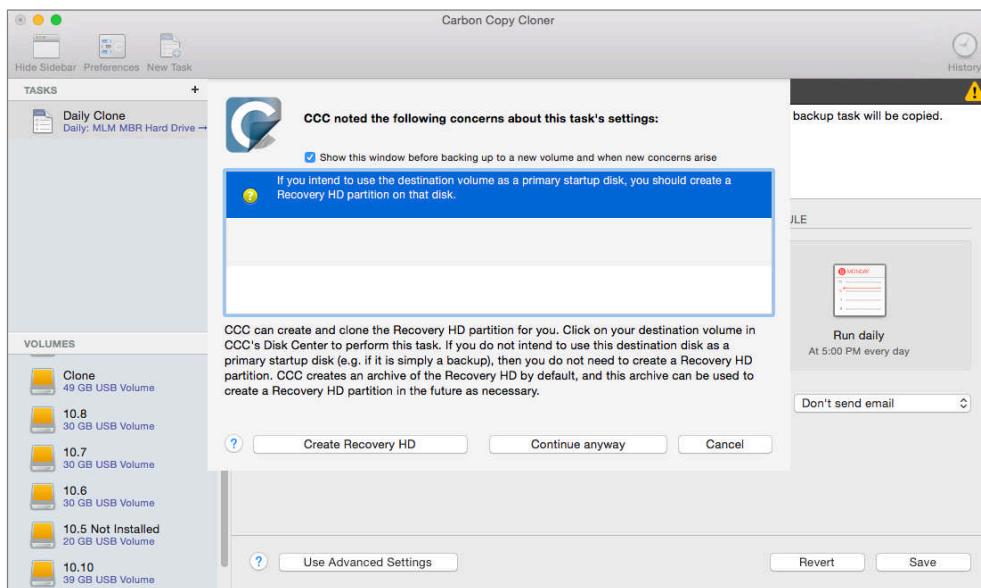
Add a Recovery HD to your Clone Backup.

In order to have FileVault 2 encryption on a boot volume, it is necessary to add a hidden Recovery HD volume to the drive. The macOS installer performs this task behind the scenes when installing macOS onto a drive. But as you aren't "installing" macOS on the clone, Carbon Copy Cloner will do this for you.

4. Open Carbon Copy Cloner.

3 Data Loss

5. From the side bar, select the Clone volume. If you have added the Clone volume as the Destination volume, a window will appear recommending that you create a Recovery HD on this volume. Select the Create Recovery HD button.



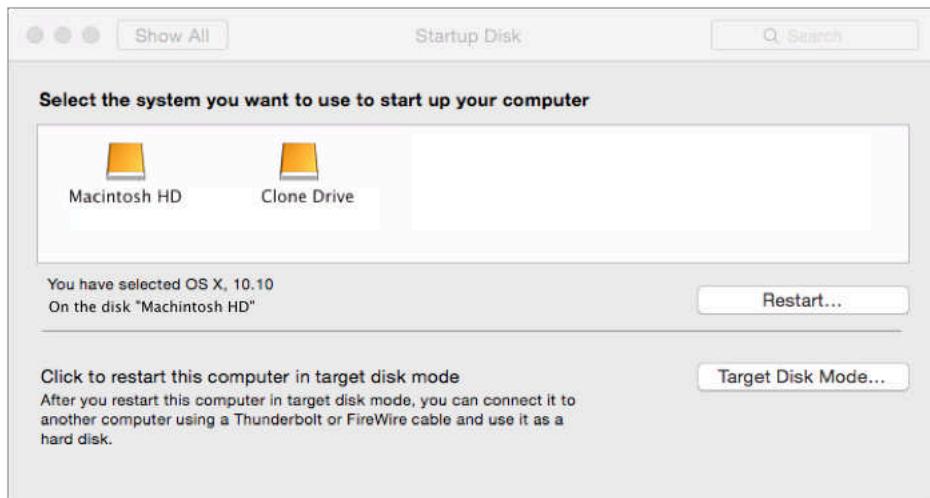
6. This process takes only a minute. When complete, return to the main window.

Encrypt the Clone Backup

If an unauthorized person gains access to your clone backup, they will have full access to all of your data unless the data is encrypted. The process of encrypting the clone drive is identical to configuring FileVault 2 on the system drive.

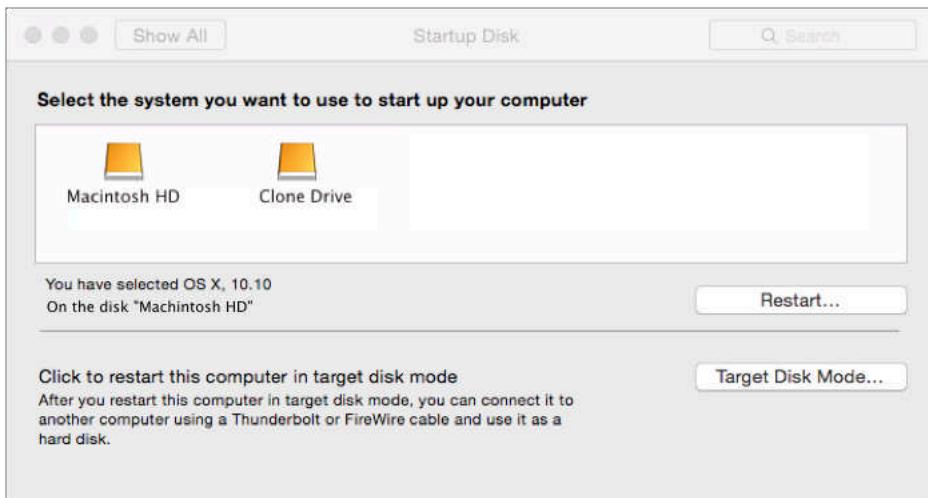
7. Complete at least one full back up to the clone drive.
8. Restart your computer, booting from the clone drive.
9. Open *Apple* menu > *System Preferences* > *Startup Disk*.
10. Click the Lock icon and authenticate as an administrator.
11. Select the clone drive.

12. Click the *Restart...* button. Your computer will restart, booting into the clone backup.



13. Once back at the desktop, start the encryption process for the clone drive by opening *Apple* menu > *System Preferences* > *Security & Privacy* > *FileVault* tab.
14. Click the Lock icon and authenticate as an administrator.
15. Click the *Turn On FileVault* button.
16. Follow the on-screen instructions.
17. Record the FileVault 2 Recovery Key in a secure location. I use the Address Book/Contacts application. The FileVault 2 Recovery Key is a secondary password used to decrypt and access your boot drive in the event the user does not remember their account password, or the account password does not work.
18. Click the *Restart* button. FileVault 2 will restart your computer to the clone drive.
19. When back on the desktop, open *Apple* menu > *System Preferences* > *Startup Disk*.

20. Select your normal system/boot drive, which is by default named *Macintosh HD*.



21. Click the Restart... button. The computer will restart, booting from your normal boot drive.

The encryption process for the clone drive will continue. Depending on the size of the drive, the speed of the computer, and if HDD or SSD, it may take from a few hours to a few days to complete the encryption. Although it is ok to let your computer sleep or turn off, this will delay the encryption process.

3.1.6 Assignment: Integrity Test the Clone Backup

The step missed by almost every user is testing the integrity of the backups. This testing process should be performed every month. Not a bad idea to put it on your calendar for the first workday of the month.

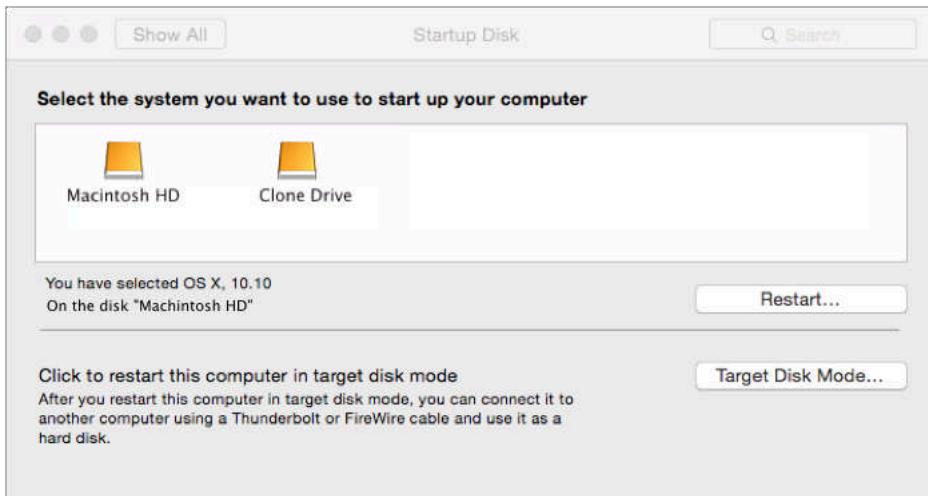
Integrity testing requires that your backup has completed at least one full cycle. If you have just completed the previous exercise, allow 24 hours of uptime before moving on.

To test your bootable clone backup, you need to boot from it, and then verify it has been backing up by looking at the history.

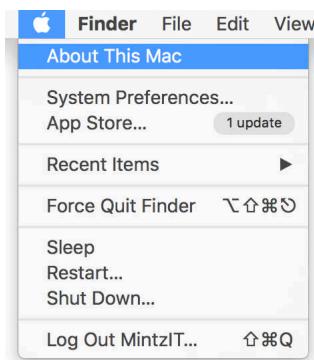
1. Select the *Apple* menu > *System Preferences* > *Startup Disk*.

3 Data Loss

2. Select your clone drive.



3. Click the *Restart* button. Your computer will restart, then boot to the clone drive.
4. Verify that you have booted to the clone drive by selecting the *Apple* menu > *About This Mac*.



3 Data Loss

5. If the *Startup Disk* field lists the name of your clone drive, you know your clone is bootable and you are half way home.

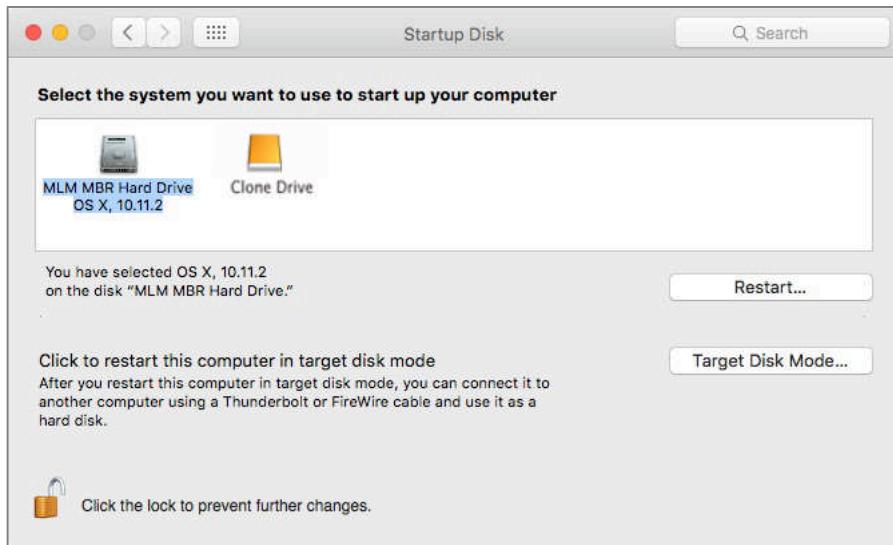


6. Close the *About This Mac* window.
7. Open the clone drive.
8. Open the *CCC Archives* folder.
9. A date and time stamp will label each backup. If the most current date and time stamp is what it should be (as opposed to several days or weeks ago), you are good.



3 Data Loss

10. To restart your Mac into the default boot drive, select the *Apple* menu > *System Preferences* > *Startup Disk*.



11. Select your normal boot drive.
12. Click the *Restart* button. Your computer will restart, and then boot to the normal drive.

Congratulations! You have just verified the integrity of your clone backup.

3.2 Review Questions

1. Best Practices call for how many backups?
2. The benefits of an on-site backup are _____.
3. The benefit of an off-site backup is _____.
4. What application is used to format a storage device, and where is it located?
5. What application can be used to create bootable clone backups?
6. What is the backup software included with macOS?

4 Passwords

For a people who are free, and who mean to remain so, a well-organized and armed militia is their best security.

–Thomas Jefferson¹

Knowledge, and the willingness to act upon it, is our greatest defense.

–Marc L. Mintz²

¹ https://en.wikipedia.org/wiki/Thomas_Jefferson

² <https://mintzit.com/>

4.1 The Great Awakening

In June 2013, documents of NSA origin were leaked to The Guardian newspaper³. The documents provided evidence that the NSA was both legally and illegally spying on United States citizens' cell phone, email, and web usage. These documents, while causing gasps of outrage and shock by the general public, revealed little that those of us in the IT field already did not know/suspect for decades: every aspect of our digital lives is subject to eavesdropping.

The more cynical amongst us go even further, stating that *everything* we do on our computers *is* recorded and subject to government scrutiny.

But few of us have anything real to fear from our government. Where the real problems with digital data theft come from are local kids hijacking networks, professional cyber-criminals who have fully automated the process of scanning networks for valuable information, competitors/enemies and malware that finds its way into our systems from criminals, foreign governments, and our own government.

The first step to securing our data is to secure our computers and mobile devices. Remember, we are not in Kansas anymore.

³ https://en.wikipedia.org/wiki/NSA_warrantless_surveillance_controversy

4.2 Passwords

We all know we need passwords. Right? But do you know that *every* password can be broken? Start by trying *a*. If that does not work, try *b*, and then *c*. Eventually, the correct string of characters will get you into the system. It is only a matter of time.

Way back in your great-great-great grandfather's day, the only way to break into a personal computer was by manually attempting to guess the password. Given that manual attempts could proceed at approximately 1 attempt per second, an 8-character password became the standard. With a typical character set of 24 (a-z) this created a possibility of 24^8 or over 100 billion possible combinations. The thought that anyone could ever break such a password was ridiculous, so your ancestors became complacent.

This is funny when you consider that research has shown that the majority of passwords can be guessed. These passwords include: name of spouse, name of children, name of pets, home address, phone number, Social Security number, and main character names from Star Trek and Star Wars (would I kid you?). Most computer users are unaware that what they thought was an obscure and impossible-to-break password actually could be cracked in minutes.

It gets worse. A while back the first hacker wrote password-breaking software. Assuming it may have taken 8 CPU cycles to process a single attack event, on an old computer with a blazing 16 KHz CPU that would equate to 2,000 attempts per second. This meant that a password could be broken in less than 2 years. Yikes.

IT directors took notice.

So down came the edict from the IT Director that we *must* create *obscure* passwords: strings that include upper and lower case, numeric, and symbol characters. But in many cases this actually was a step backward. Since a computer user could not remember that their password was 8@dC%Z#2, the user often would manually record the password. That urban legend of leaving a password on a sticky note under the keyboard? I have seen it myself more than a hundred times.

Come forward to the present day. A current quad-core Intel i7 with freely available password-cracking software can make over 10 billion password attempts per second. Create an army of infected computers called a botnet to do your dirty work⁴ and you can likely achieve over a hundred trillion attempts per second, unless your system locks out the user after x number of failed log on attempts.

What does this mean for you? The typical password using upper and lower case, number, and symbol now can be cracked with the right tools in under than 2 minutes. If using just a single computer to do the break in, make that a week. Don't believe it? Take a look at the *haystack*⁵ search space calculator.

If we use longer passwords, we can make it too time consuming to break into our system, so the bad guys will move on to someone else.

But you say it is tough enough to remember 8 characters, impossible to remember more?

This is true, but only if we keep doing things as we have always done before. Since virtually all such attacks are now done by automated software, it is only an issue of length of password, not complexity. So, use a passphrase that is easy to remember, such as, "Rocky has brown eyes" (which at 100 trillion attempts per second could take over 1,000,000,000,000,000 centuries to break – provided Rocky is not the name of your beloved pet and thus more guessable).

How long should you make your password, or rather, passphrase? As of this writing, Microsoft's Security Chief recommends a minimum of 14 characters. US-CERT currently recommends at least 15. Cisco recommends at least 24. My recommendation to clients is a minimum of 15, in an easy-to-remember, easy-to-enter phrase.

In addition to password length, it is critical to use a variety of passwords. In this way, should a bad person gain access to your Facebook password, that password cannot be used to access your bank account.

Yes, pretty soon you will have a drawer full of passwords for all your different accounts, email, social networks, financial institutions, etc. How to keep all of

⁴ <http://en.wikipedia.org/wiki/Botnet>

⁵ <https://www.grc.com/haystack.htm>

them organized and easily accessed amongst all of your various computers and devices? More on that later in the *LastPass* section of this *Password* topic.

4.2.1 Assignment: Create a Strong User Account Password

There is no universally-accepted definition of a *strong password*. US-CERT recommends at least 15 characters, Microsoft recommends at least 14 characters, and Cisco recommends at least 24. For our purposes and for the purposes of this workshop and book, a minimum of 15 characters is the definition of strong password.

As password cracking is now done through automated software, complexity isn't nearly as important as it was when humans were attempting the crack. This is to say that a password of 11111111111111 is about as secure as f^w1&%Ge0*\$W18. I recommend using a passphrase—easy to remember, easy to enter, at least 14 characters. For example, *I love brown eyes* is an excellent password.

In this assignment, you will create a strong password.

1. Think up a password for yourself that is consists of at least 15 easy-to-remember and easy-to-enter characters.
2. Test how difficult it is to break your password by visiting haystack
<https://www.grc.com/haystack.htm>.
3. Create an account password for yourself that is consists of at least 15 easy-to-remember and easy-to-enter characters.

4 Passwords

4. Test how difficult it is to break your password by visiting haystack at <https://www.grc.com/haystack.htm>.

GRC's Interactive Brute Force Password "Search Space" Calculator
(*NOTHING* you do here ever leaves your browser. What happens here, stays here.)

No Uppercase 16 Lowercase No Digits 3 Symbols 19 Characters

this is my password

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+33 = 59
Search Space Length (Characters):	19 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	4,504,143,715,596,357,284,195,985,482,676,599
Search Space Size (as a power of 10):	4.50×10^{33}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	1.43 billion trillion centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	14.32 trillion centuries
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	14.32 billion centuries

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

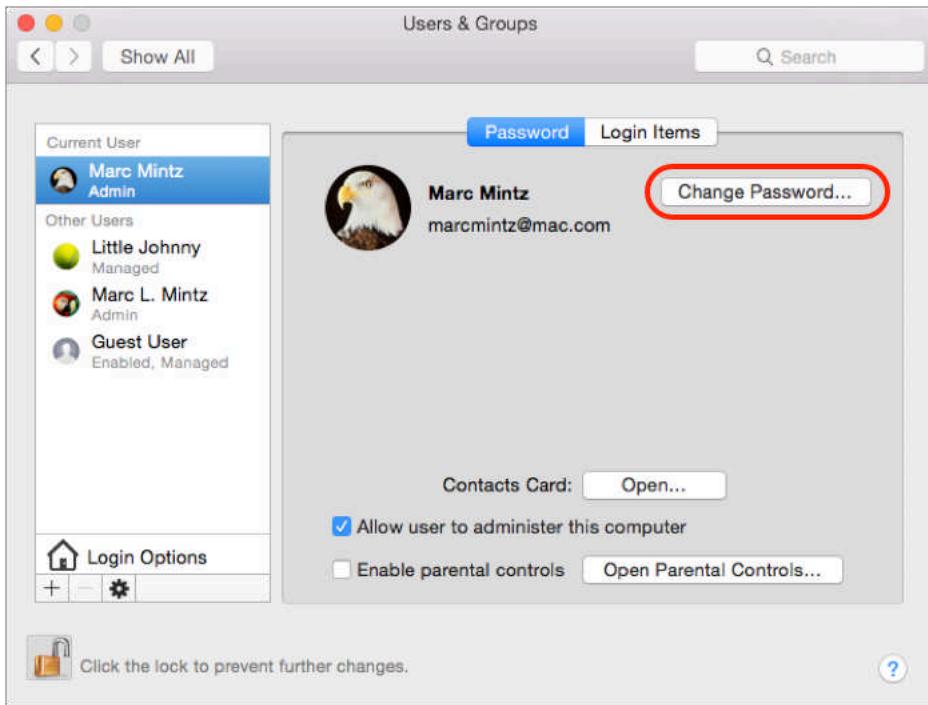
5. If your password does not meet your or your organization's strength requirements, edit it until it does.
6. Record your new password in a way that you can find when you need it.
7. Exit the browser.

Change Your Old Password to the Strong Password:

8. Log in to your computer using your user account.
9. Click on *Apple* menu > *System Preferences* > *Users and Groups*.

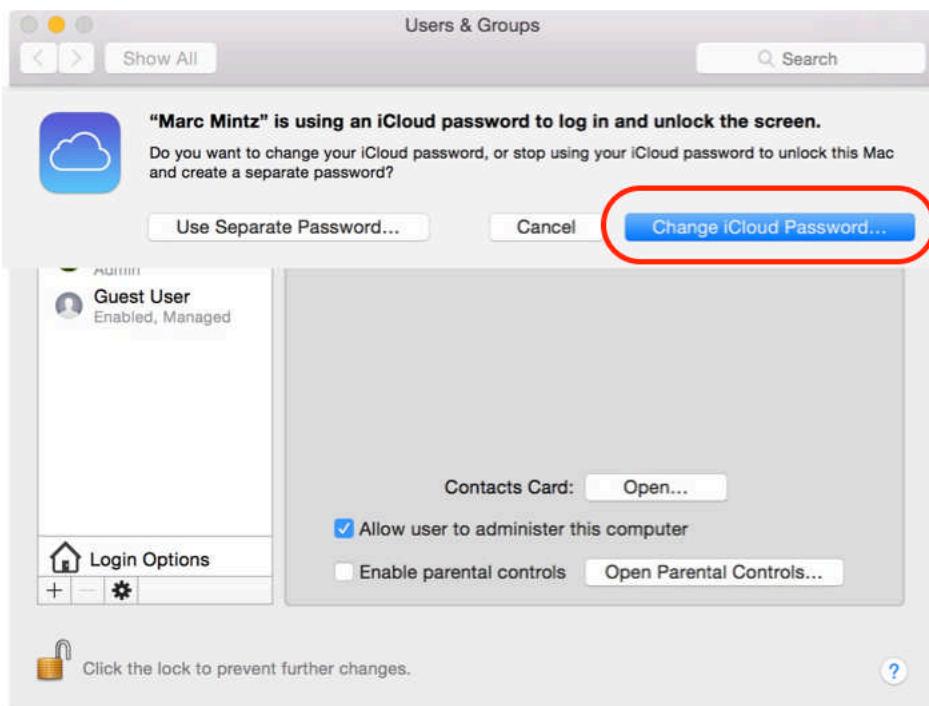
4 Passwords

10. Select the Change Password button:



- Note: When changing a user/login password, if at all possible, the change should be made while logged in with that user account. Doing so will simultaneously change the *Keychain* password to match. The Keychain stores usernames and passwords. When changing the user/login password in any other way, the Keychain password remains unchanged. If the user doesn't then know the password to the Keychain, it is impossible to ever open again, and all stored passwords will be lost. More on Keychain later.
11. By default your login password is set the same as your iCloud password. You will be asked if you want to *Use Separate Password...*, or to *Change iCloud Password...*
- a. Synchronizing the iCloud and login password makes remembering both easier, and accessing your iCloud data from a new computer easier, but it also presents a roadblock to login should the Apple authentication servers be offline (as has happened at least once).

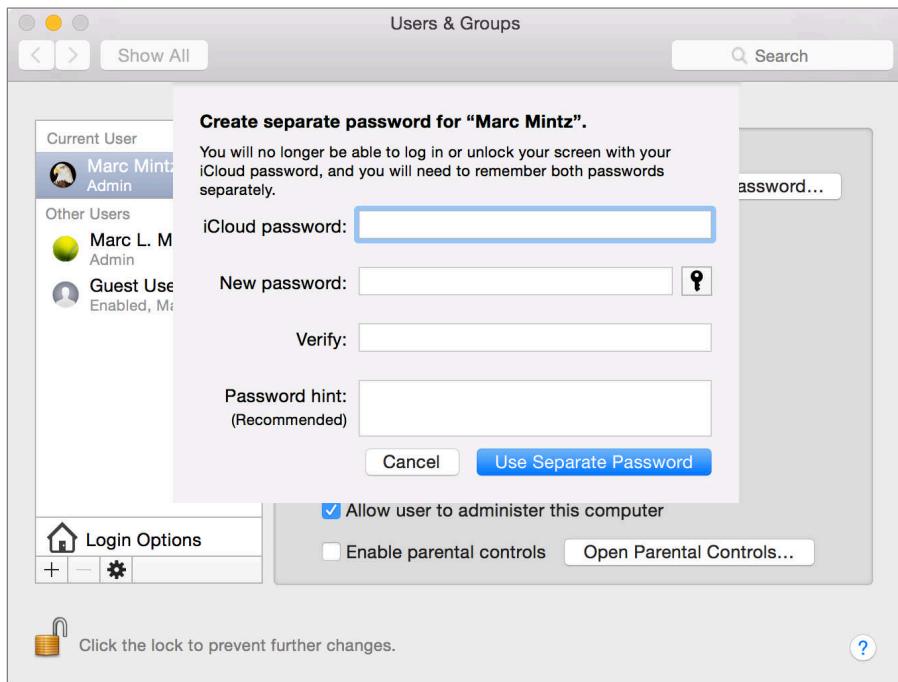
4 Passwords



- b. If you select Change iCloud Password, a browser opens to the My Apple ID page at Apple so that you may manage your ID.

4 Passwords

- c. If you select *Use Separate Password*, the *Create separate password for <user name>* window appears so that you may create a password. At the prompt, enter your *iCloud password*, *New password*, *Verify* your new password, and then select the *Use Separate Password* button:



12. Quit System Preferences.

Your new, strong password now is in effect.

4.3 Keychain

In our grandparents' day, life was so much simpler. I'm not talking about politics or sociology, but, well... to give an example: My grandfather had four keys in his pocket at all times: one for home, one for the car, and the other two he could never remember what for.

In today's world, the realm of keys has expanded into the digital world. You now have keys or passwords for logging on to your computer, your phone, your tablet, your email, many of the websites you visit, Wi-Fi access points, servers, your frequent flyer account, etc. In my case, I have 857 passwords in use. I know because they are all neatly stored in a database so that I don't have to remember them.

Unfortunately for most of us, our "keys" are not very well organized, so when we need to access our mail from another computer, or order a book on Amazon, we are stuck.

By default, your Mac stores most usernames and passwords used to access Wi-Fi networks, servers, other computers, and websites. The exceptions are usually websites that are programmed specifically so they do not have credentials saved. These are typically financial institutions.

The built-in tools that store this information automatically can also be used to manually store any text-based data. This includes credit card information, software serial numbers, challenge Q&A, offshore banking information, etc.

Your Mac has two locations to store keys:

- Safari, which stores only credentials for websites visited with Safari.
- Keychain database, which stores username, password, and URL for websites which request authentication, Wi-Fi networks, servers, other computers you access, email accounts, and encrypted drives.

Keychain is what interests us here.

Let's take the case of visiting a website that requires a username and password, connecting to another computer or server, or performing some other action that

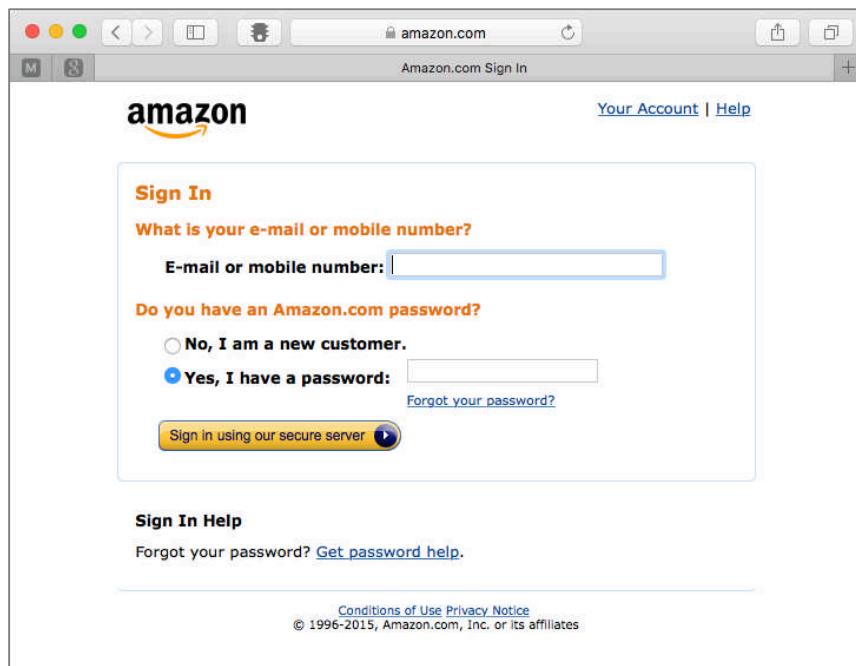
4 Passwords

triggers an authentication request. The following are the steps as they typically occur:

1. A prompt appears requesting a username and password.
 - Typical default authentication window for a server:



- Typical authentication window for a website:

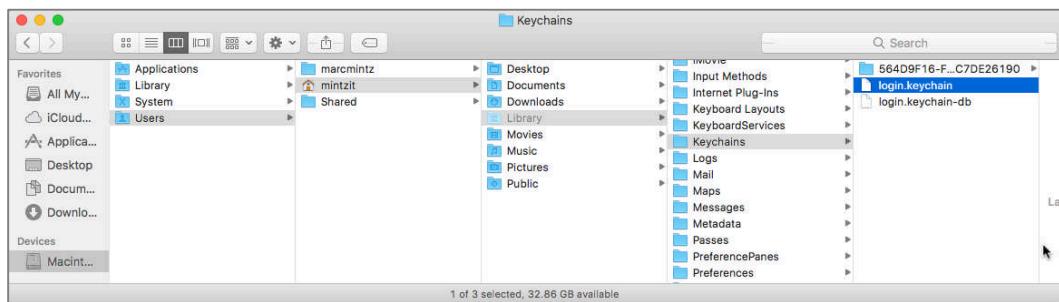


4 Passwords

2. Enter your username and password. In most cases there is a checkbox to *Remember this password in my Keychain*. Enable that checkbox, and then click Enter or Continue.
3. The website takes you to the appropriate secured page or the other computer mounts a drive on your Mac.

Behind the curtain, your Mac has copied your username and password into the Keychain database, named *Login.Keychain*.

This database is located in your Home *Library/Keychains* folder. The database is military grade AES 256 bit encrypted, safe from prying eyes.



The next time you visit this same website or server, the steps change somewhat:

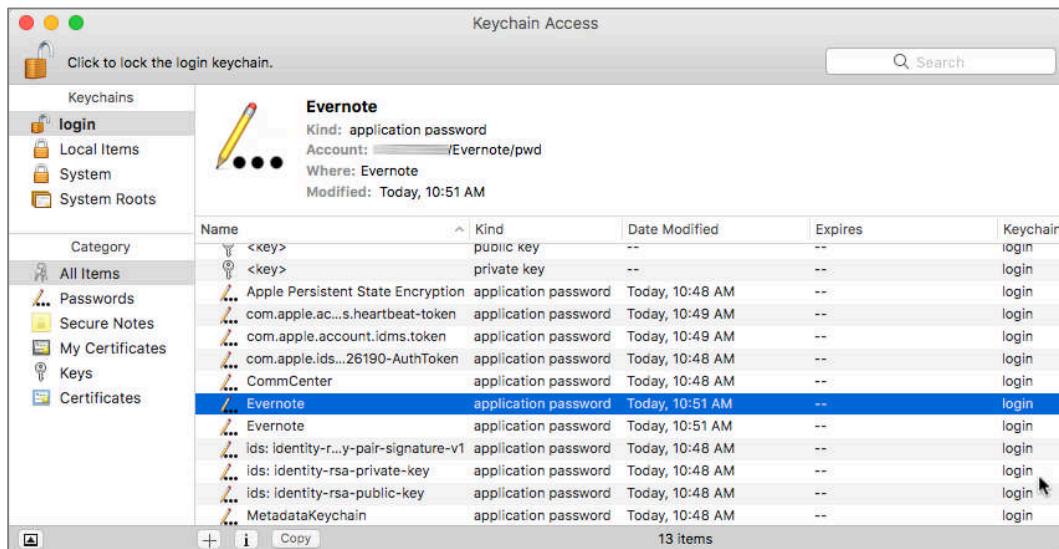
1. You surf to the website or select a server to access.
2. A prompt appears requesting a username and password.
3. Behind the scenes your web browser or Finder asks: “Has the Keychain stored the credentials for this site or server?”
4. A query is made of the Keychain database based on the URL of the site or the name of the server.
5. If Keychain has stored the username and password associated with the URL or server (it has), the credentials are automatically copied/pasted into the *username* and *password* fields.
6. Select *Enter*.
7. The website takes you to the appropriate secured page or the server share point mounts.

Note that you did not need to know your credentials—Keychain did it all for you. macOS ships with a tool allowing the user full access to the database, named *Keychain Access*, located in the /Applications/Utilities folder.

4.3.1 Assignment: View an Existing Keychain Record

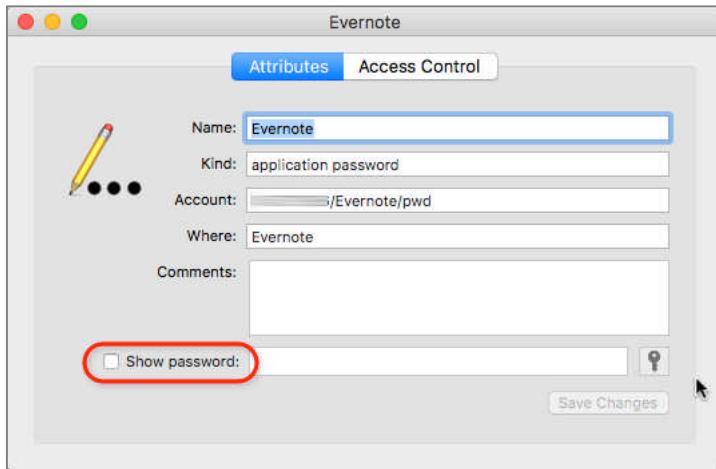
Perhaps a trusted visitor needs access to your Wi-Fi network, and you have forgotten the password to that network. The Keychain database has it stored, you just need to look for it. In this assignment, you will examine a record in the Keychain.

1. Launch *Keychain Access* (located in /Applications/Utilities/).
2. From the sidebar, in the *Keychains* field, select log in. This is the database that holds your secure information.
3. From the sidebar, in the *Category* field, select *All Items*.
4. In the center, main area of the window, double-click on the *target record*, in this example, *Evernote*.

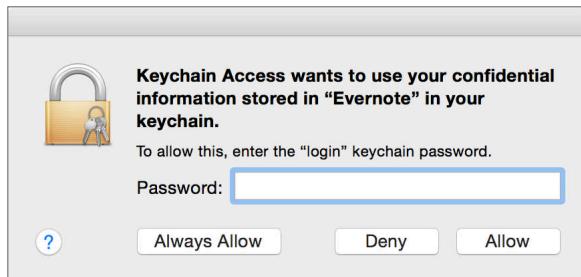


4 Passwords

5. In this example, it is *Evernote*. The records *Attributes* window will open. At the bottom of the *Attributes* window you will see *Show Password*. Enable the checkbox. This will open the authentication window.

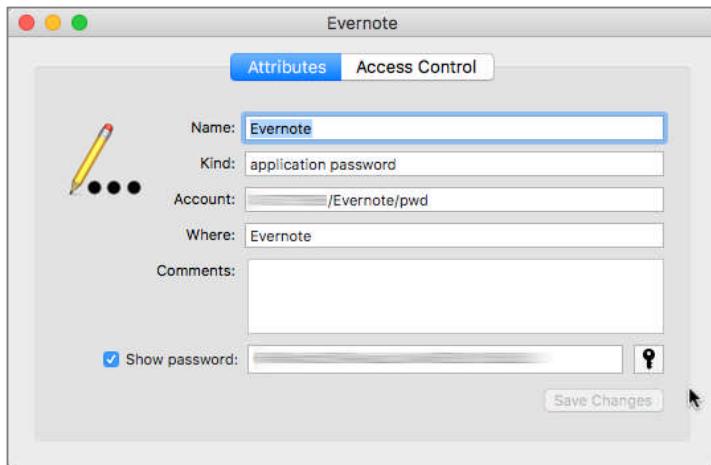


6. At the prompt, enter your Keychain password. By default, this is the same as your user account password. This will authorize Keychain to show you the password. Then click the *Allow* button.



4 Passwords

7. The *Show Password* field will now display the needed password.



8. Quit Keychain Access.

4.4 Challenge Questions

A Challenge Question is a way for websites to authenticate who you claim to be when you contact support because of a lost or compromised password.

For example, when registering at a website you may see: *Question – Where did your mother and father meet?*

The problem with this strategy is that most answers easily are discovered with an Internet search of your personal information, or a bit of social engineering.

The solution is to give bogus answers. For example, my answer to the question, *Where did your mother and father meet?* may be: *1954 Plymouth back seat*. It would not be possible for a hacker to discover this answer, as it is completely bogus. My mother tells me it was really a 1952 Dodge.

Unless you are some type of savant, there is no way you will remember the answers to your challenge questions. But, there is no need to remember. We already have a built-in utility that is highly secure and designed to hold secrets such as passwords—Keychain Access!

Although Keychain can automatically record and auto fill usernames and passwords, it will require manually entering other data such as challenge Q&A.

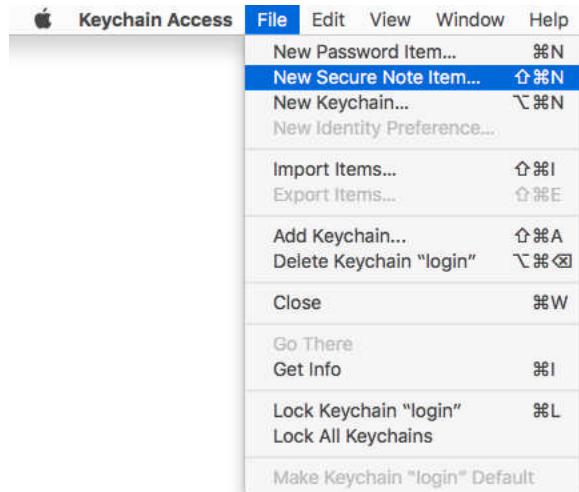
4.4.1 Assignment: Store Challenge Q&A In the Keychain

In this assignment you will manually store the challenge Q&A for a pretend website, myteddybear.com.

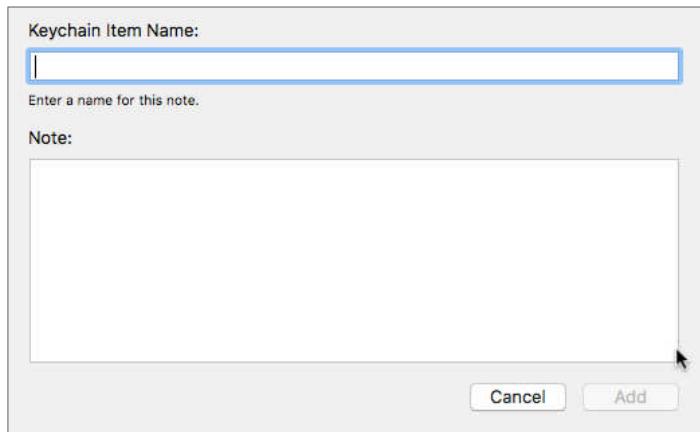
1. Open *Keychain Access.app*, located in */Applications/Utilities*.

4 Passwords

2. Select the Keychain Access *File* menu > *New Secure Note item...*



3. The Keychain *Item Name* window appears.

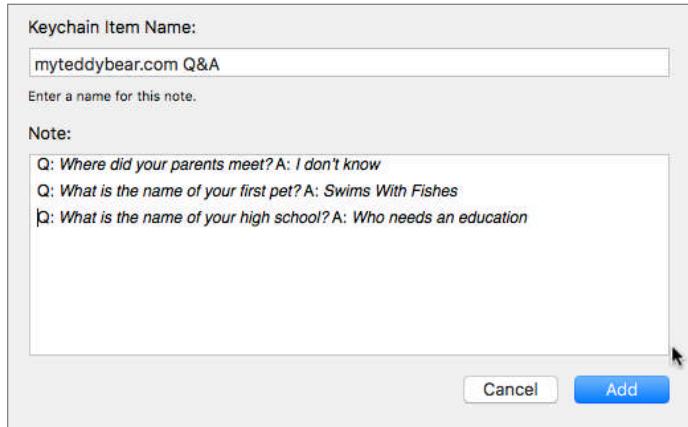


4. In the *Keychain Item Name* field, enter: *myteddybear.com Q&A*.
5. In the *Note* field, enter:
Q: Where did your parents meet? A: I don't know

4 Passwords

Q: What is the name of your first pet? A: Swims With Fishes

Q: What is the name of your high school? A: Who needs an education



6. Select the *Add* button.
7. You will find your new Secure Note within all of your other Keychain items.

Name	Kind	Date Modified	Expires	Keychain
Apple Persistent State Encryption	application password	Today, 10:48 AM	--	login
com.apple.ac...s.heartbeat-token	application password	Today, 10:49 AM	--	login
com.apple.account.idms.token	application password	Today, 10:49 AM	--	login
com.apple.ids...26190-AuthToken	application password	Today, 10:48 AM	--	login
CommCenter	application password	Today, 10:48 AM	--	login
Evernote	application password	Today, 10:51 AM	--	login
Evernote	application password	Today, 10:51 AM	--	login
ids: identity-r...y-pair-signature-v1	application password	Today, 10:48 AM	--	login
ids: identity-rsa-private-key	application password	Today, 10:48 AM	--	login
ids: identity-rsa-public-key	application password	Today, 10:48 AM	--	login
MetadataKeychain	application password	Today, 10:48 AM	--	login
myteddybear.com Q&A	secure note	Today, 11:16 AM	--	login
Safari Session State Key	application password	Today, 10:54 AM	--	login

8. Quit Keychain Access.

Your challenge questions and answers are now securely stored.

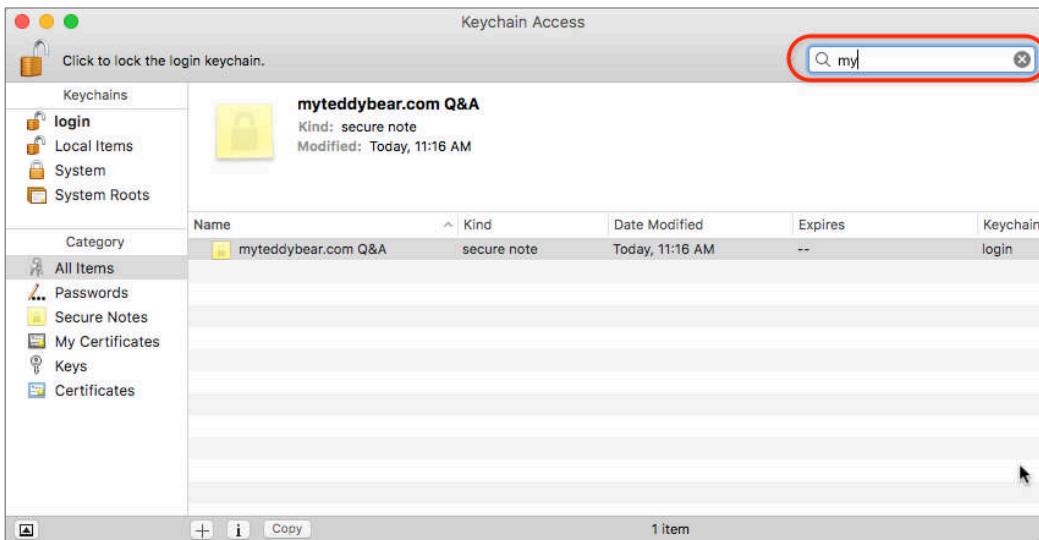
4.4.2 Assignment: Access Secure Data From Keychain

There may come a time that you forget your password to myteddybear.com. A call to technical support with a request to either retrieve or reset your password is met with a challenge question. If you are like me, your synapses holding that memory have long died out.

But, no worries! You do remember that you have the habit of storing all of your important data securely in your Keychain.

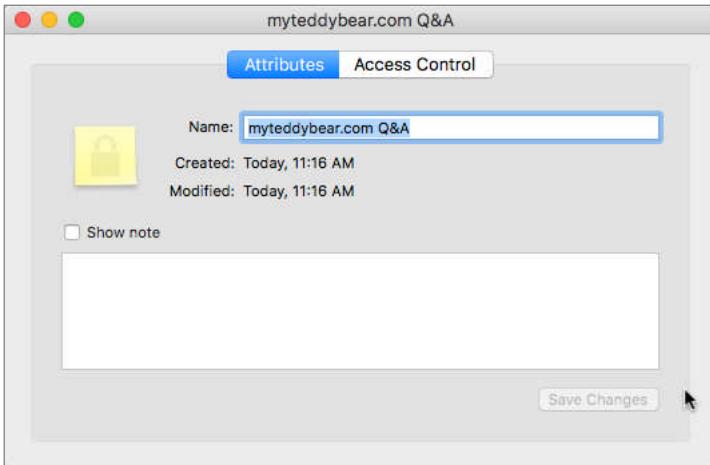
In this assignment you retrieve your challenge Q&A for myteddybear.com.

1. Open Keychain Access.app, located in */Applications/Utilities*.
2. Click in the *search* field at the top right corner of the *Keychain Access* window.
3. Enter: *myteddybear*. As you type, only those records matching your search string appear, until only the proper record shows.

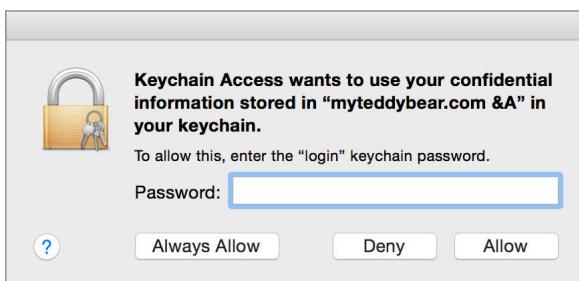


4 Passwords

- Double-click on the myteddybear.com record to open it. Your password is not initially displayed. This is intentional, doubly protecting your data.

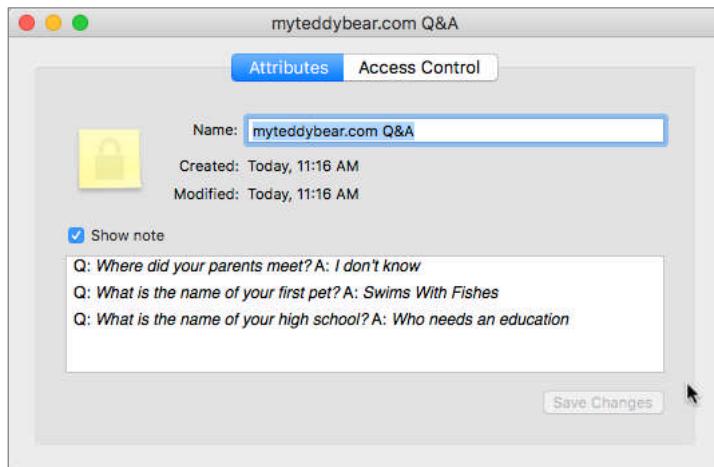


- Enable the *Show note* checkbox.
- You are prompted to enter your Keychain password. By default, this is the same as your log in password. Enter your Keychain password, and then click either the *Always Allow*, or *Allow*, button. By selecting *Always Allow*, you will not be asked to verify your Keychain password for this record in the future. If you select *Allow*, you have access to your data, but you will be prompted for your Keychain password in the future.



4 Passwords

7. After selecting either *Always Allow* or *Allow*, you see your challenge Q&A.



8. Close the window and Quit *Keychain Access*.

4.5 Harden the Keychain

The work we have done so far in Keychain Access is all that is necessary for almost every environment. Some situations call for even greater levels of security—think military bases, the computer used by the CEO, and my aunt Rose who needs to protect her secret recipe for kosher raisin noodle Koogle.

There are two options to further protect the Keychain, which may be used separately or in tandem:

- Change your Keychain password to be different than your log in password
- Have your Keychain automatically log off after X minutes of inactivity.

By default your Keychain password matches your log in password. With this configuration, in the process of logging in to your computer the Keychain is automatically unlocked. If you give your Keychain a different password, it will remain locked after log in. Where you see this is when you attempt to access a website or connect with another computer and you have the authentication credentials stored in Keychain. Instead of auto filling as usual, you are prompted to enter the password for the Keychain. This unlocks the Keychain, allowing it to continue the auto fill process.

By default the Keychain remains unlocked as long as the user remains logged in. There is also the option to set the Keychain to automatically lock after a specified amount of inactivity time.

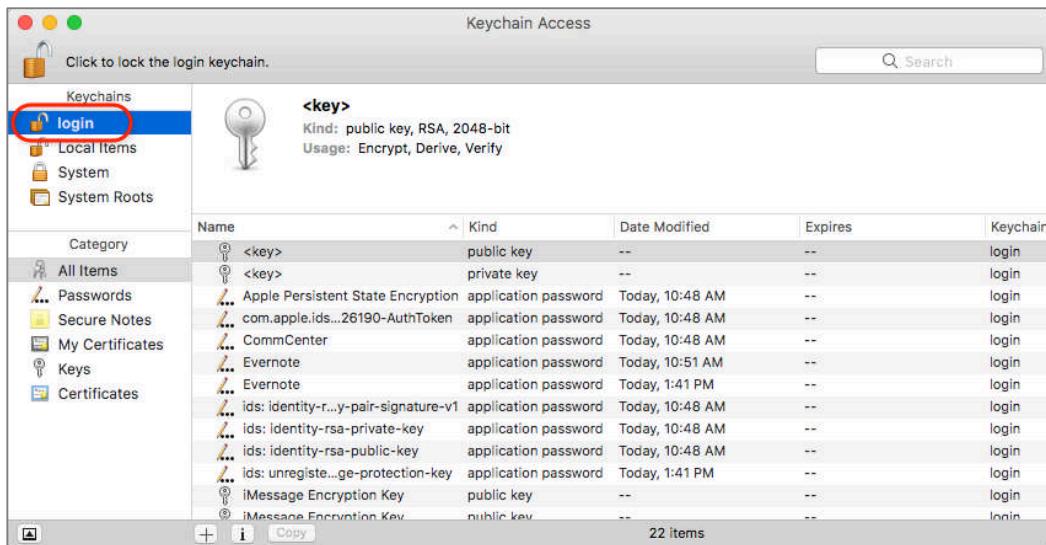
Let's say Keychain Access to automatically lock the Keychain after 5 minutes of inactivity. Upon log in, if the Keychain password is the same as the log in password, the Keychain will unlock and remain unlocked for 5 minutes. If you need an auto fill from data held in Keychain after that 5 minutes, you are prompted for the Keychain password. If within 5 minutes another auto fill is needed, the data is pulled from Keychain automatically. But when 5 minutes or more has passed, the Keychain will lock automatically.

4.5.1 Assignment: Harden the Keychain with a Different Password

By default the Keychain password is the same as the user login password. Under this condition, the Keychain automatically unlocks when the user logs in. An additional layer of security may be gained by giving Keychain a different password. If this is done, the Keychain remains locked at login. When called upon to provide a password, it prompts the user for the Keychain password so that it may unlock.

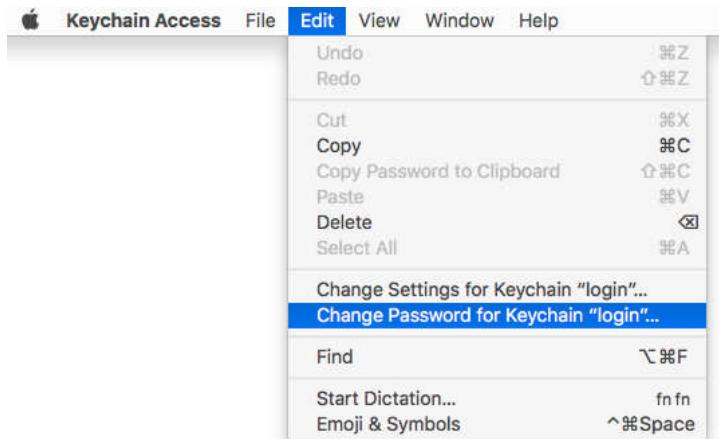
In this assignment, you give your Keychain a password different than your user account login password.

1. Open Keychain Access.app, located in */Applications/Utilities*. From the top of the sidebar, select the *login* keychain.

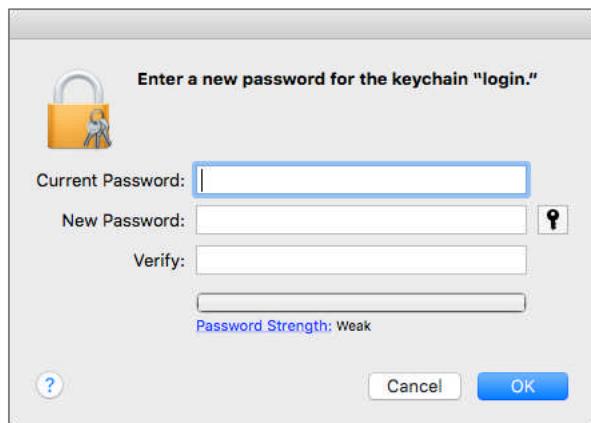


4 Passwords

2. Select the Keychain *Edit* menu > *Change Password for Keychain "login"*.



3. This opens the Enter a new password for the *Keychain "login"* window. Enter the following:



- In the *Current Password* field, enter your current Keychain password. By default, this is your user account log in password.
 - In the *New Password* and *Verify* fields, enter your new strong password for Keychain. Write it down so it is not forgotten. I keep this in my Address Book / Contacts application.
4. Select the *OK* button.

5. Select the Lock icon in the top left corner of the Keychain Access window.
This locks the log in Keychain.

6. Quit Keychain Access.

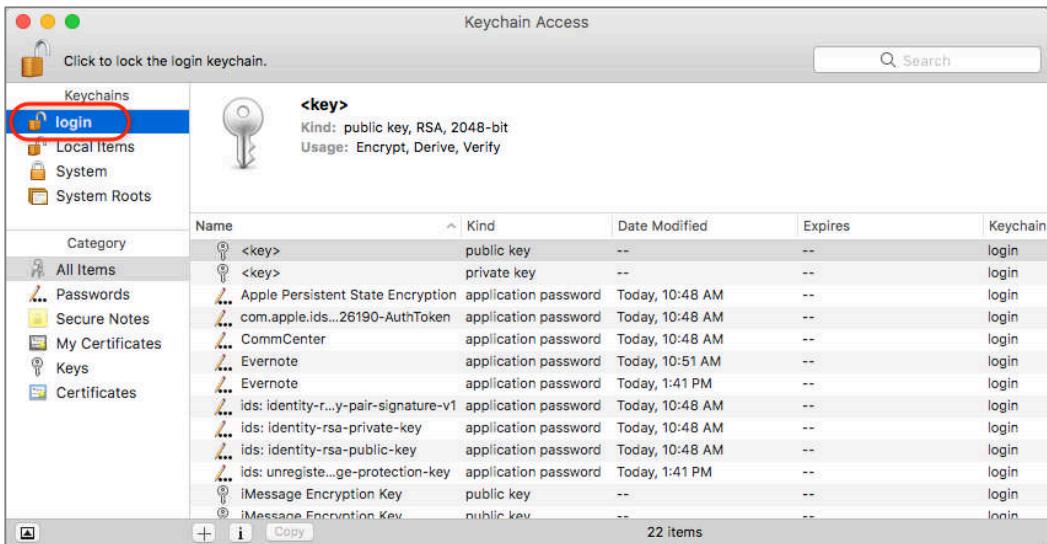
Because your login Keychain now has a different password than your user account password, it will not automatically unlock when you log in to your computer. Attempting to access the Keychain through *Keychain Access* requires that you manually unlock it. Also, the first time that an autofill is attempted, you are prompted to enter the Keychain password.

7. If you do not wish to have a hardened Keychain, repeat steps 1–9, changing the password back to your user account password.

4.5.2 Assignment: Harden the Keychain with an Automatic Timed Lock

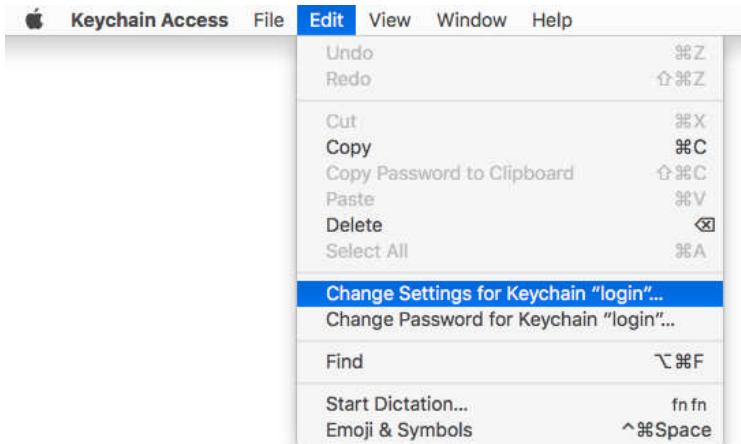
In this assignment, you give your Keychain a timeout to automatically lock after it has not been used for 1 minute.

1. Open Keychain Access, located in */Applications/Utilities*. From the top of the sidebar, select the *login* keychain.

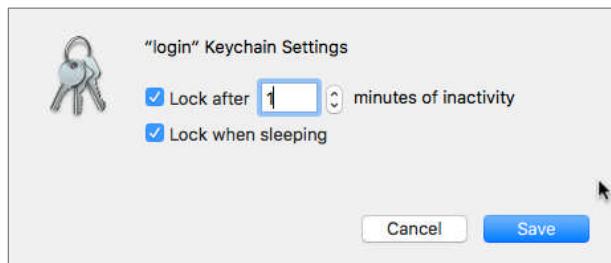


4 Passwords

2. Select the Keychain Access *Edit* menu > *Change Settings for Keychain "login."*



3. The *Login Keychain Settings* window will open. Configure as follows:



- Enable the *Lock after ____ minutes of inactivity* checkbox, and then set this to 1 minute.
 - Enable the *Lock when sleeping* checkbox.
4. Select the *Save* button.
 5. Quit Keychain Access.
 6. Sit on your thumbs for 60 seconds—time enough for the Keychain to lock.
 7. Open a browser and visit a website or connect to another computer on your network that you frequent with a password that otherwise auto fills. You find you now are prompted to enter the password for the Keychain it to open.

8. If you do not need a hardened Keychain, repeat steps 1–3, and then when the *Login Keychain Settings* window appears, disable the checkboxes. Then select the *Save* button.
9. Quit Keychain Access.

Your Keychain will now automatically lock, preventing anyone from accessing all of your passwords should you step away from your desk with your system awake and no screen saver in place.

4.6 Synchronize Keychain Across macOS/OS X, and iOS Devices

Perhaps like me, you have a need to access most of these passwords and challenge answers anywhere, anytime. When I have my computer with me, no worries. But what if I don't? It would be a rare event indeed for me to be without my computer or my iPhone, so I keep my Keychain on my iPhone as well.

If you have upgraded to macOS 10.12 or higher, OS X 10.9 or higher, and iOS 7 or higher, Apple has you handled. With the most recent incarnations of both operating systems, Apple has added *Keychain* to the iCloud synchronization scheme. This allows your Keychain database to be synchronized between all of your computers, iPhones, and iPads.



4.6.1 Assignment: Activate iCloud Keychain Synchronization

Synchronizing your Keychain with iCloud allows all of your macOS 10.12 and higher, OS X 10.9 and higher, and iOS 7 and higher devices share your keychain.

4 Passwords

In this assignment you will enable iCloud Keychain synchronization.

This assignment assumes that you have configured Apple ID 2-step authentication. If you have not yet done this, please skip to chapter 15, *Assignment: Implement Apple ID Two-Step Verification*.

1. Open the *Apple* menu > *System Preferences* > *iCloud*.

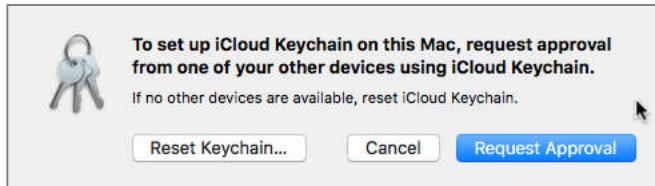


2. Select the *Keychain* checkbox. The *Enter your Apple ID password to setup iCloud Keychain* dialog box appears.
3. Enter your Apple ID password, and then select the *OK* button.

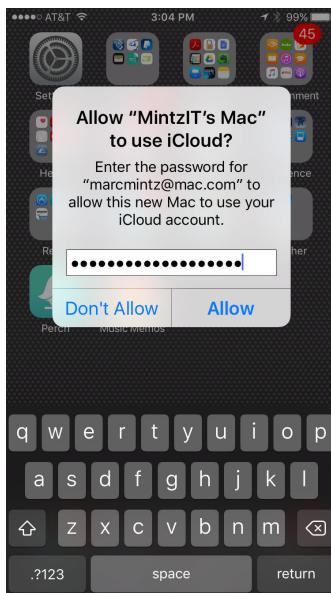


4 Passwords

4. If you have previously created a 2-step verification for your Apple ID, the *Keychain Setup* dialog box opens. Select the *Request Approval* button.

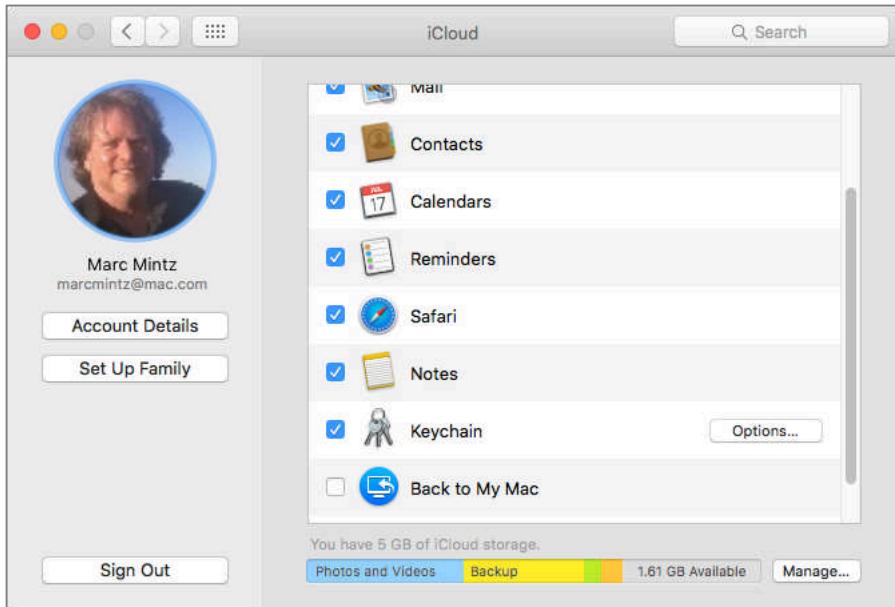


5. A request will be sent to the other devices currently approved on your account to approve this device. Enter your Apple ID password, and then click *Allow*.



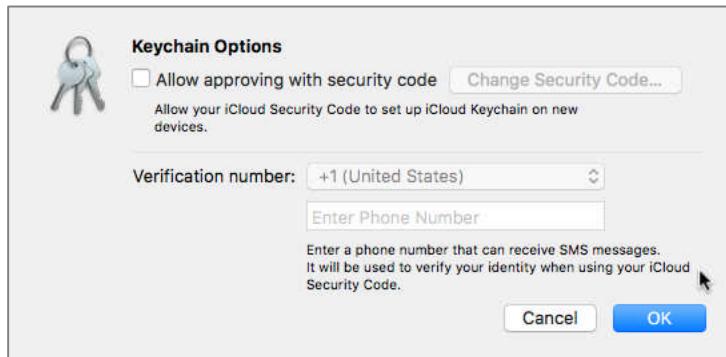
4 Passwords

6. Go back to *System Preferences*, and notice that the *Keychain* is now enabled.



Further secure your keychain:

7. In the *iCloud Preferences*, select the Keychain *Options* button.
8. The *Keychain Options* window opens:

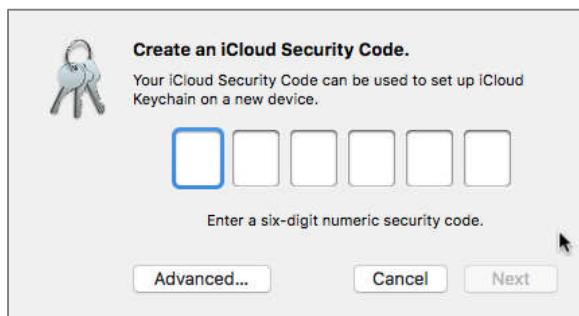


9. Enable the *Allow approving with security code* checkbox.

4 Passwords

10. The *Create an iCloud Security Code* window opens. Enter a 6-character code that can be used to enable your other Apple devices to share and synchronize Keychains, and then select the *Next* button.

- Notes: If you would like a more complex code, you can select the *Advanced...* button instead.



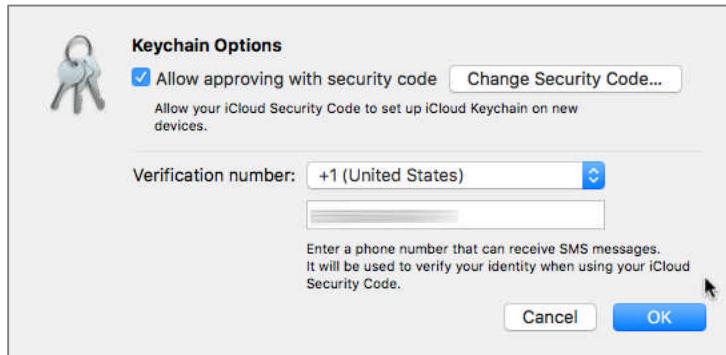
11. The same security window appears again to verify your security code. Reenter the code, and then select the *Next* button.

12. The *Enter a phone number that can receive SMS messages* window opens. This will be used by Apple to verify your identity when using the security code. Enter your phone number, and then select the *Done* button.



4 Passwords

13. You are returned to the *Keychain Options* window. Select the *Done* button.



14. At the *Enter your Apple ID password to update your account settings* window, enter your Apple ID password, and then select the OK button.



15. *Quit System Preferences*.

Your Keychain on this computer will now synchronize automatically with your iCloud account, and therefore with all other OS X, macOS, and iOS devices synchronizing on the same account.

4.7 LastPass

A great solution to the problem of password management is *LastPass*⁶.

There are two important advantages of LastPass:

1. You no longer have to concern yourself with Internet passwords—the correct response becomes automatic. LastPass will keep your Internet passwords available in each of your browsers.
2. Stores and share your passwords with all of your devices—even across operating systems. It also securely stores manually entered data such as challenge questions.

LastPass provides the following solutions:

- Provides free (ad supported) and premium (no ads) options
- Automatically remembers your Internet passwords, fully encrypted
- Auto fills web-based forms and authentication fields
- Stores notes and challenge questions and answers (Q&A), fully encrypted
- Synchronizes across multiple browsers
- Synchronizes across multiple computers
- Synchronizes across Android, BlackBerry, iOS, Linux, macOS, OS X, Windows
- Automatically generates very strong passwords, which since you do not need to remember them, provide even greater online security.

4.7.1 Assignment: Install LastPass

In this assignment you will download and install LastPass on your macOS computer. The free version works indefinitely across computers, but to

⁶ <http://www.LastPass.com>

synchronize with mobile devices beyond the 14-day trial requires upgrading to *LastPass Premium*.

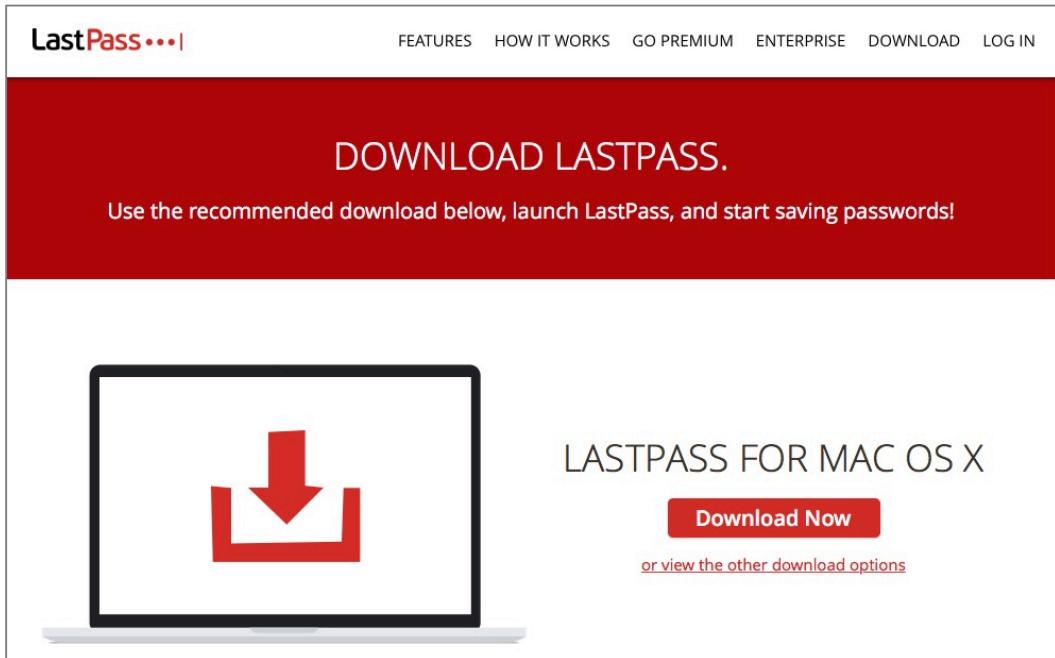
Download the LastPass Multi-Browser Installer

1. Using your browser, surf to *LastPass* at <https://LastPass.com>. Select the *Navigation bar > DOWNLOAD* button.

The screenshot shows the LastPass website homepage. At the top, there's a navigation bar with links for FEATURES, HOW IT WORKS, GO PREMIUM, ENTERPRISE, DOWNLOAD, and LOG IN. Below the navigation, a large banner features the text "SIMPLIFY YOUR LIFE." and a subtext: "LastPass remembers your passwords so that you can focus on the more important things in life." A red button labeled "Get LastPass Free" is prominent. To the right of the text, there are images of various devices (laptop, tablet, smartphone) displaying the LastPass interface. Below this section, there are two promotional boxes: one for "LastPass Premium" featuring a circular icon with a lock and a double arrow, and another for "LastPass Enterprise" featuring a circular icon with multiple human figures connected by lines. Both boxes contain descriptive text and a red "Go Premium" or "Start a Trial" button.

4 Passwords

2. In the *Download LastPass* page, select the *Download Now* link.



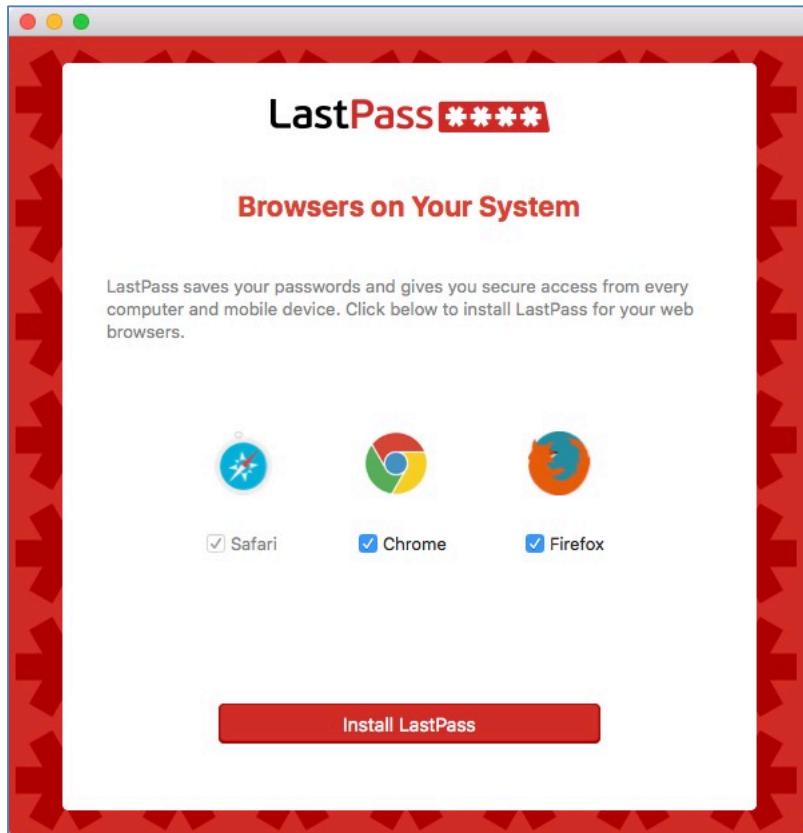
3. LastPass will download.

Install LastPass for Safari

4. Once the installer has downloaded, double-click to launch it.

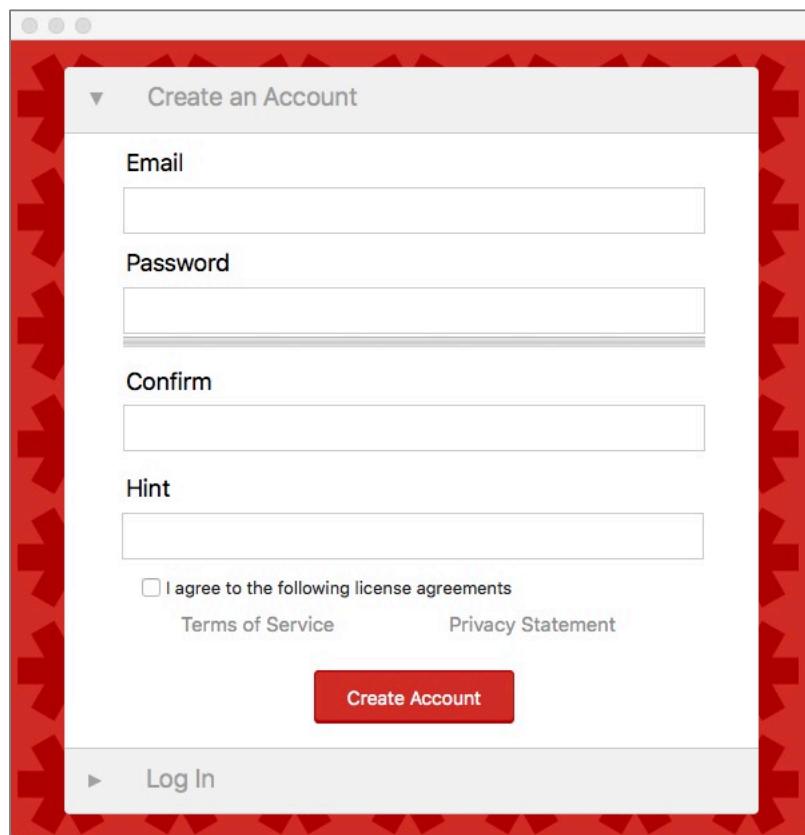
4 Passwords

5. The LastPass installer determines which browsers are installed, and enables the installation of the LastPass extension for each. Select the *Install LastPass* button.



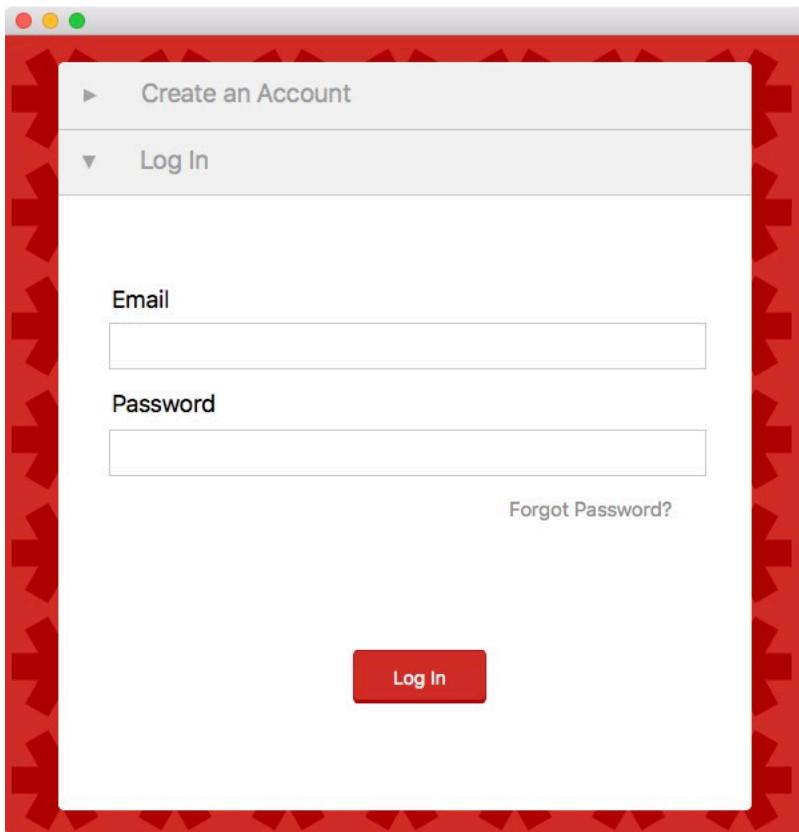
4 Passwords

6. If you have not yet created a LastPass account, do so now by filling out the *Create an Account* window. If you do have a LastPass account, skip to the next step.



4 Passwords

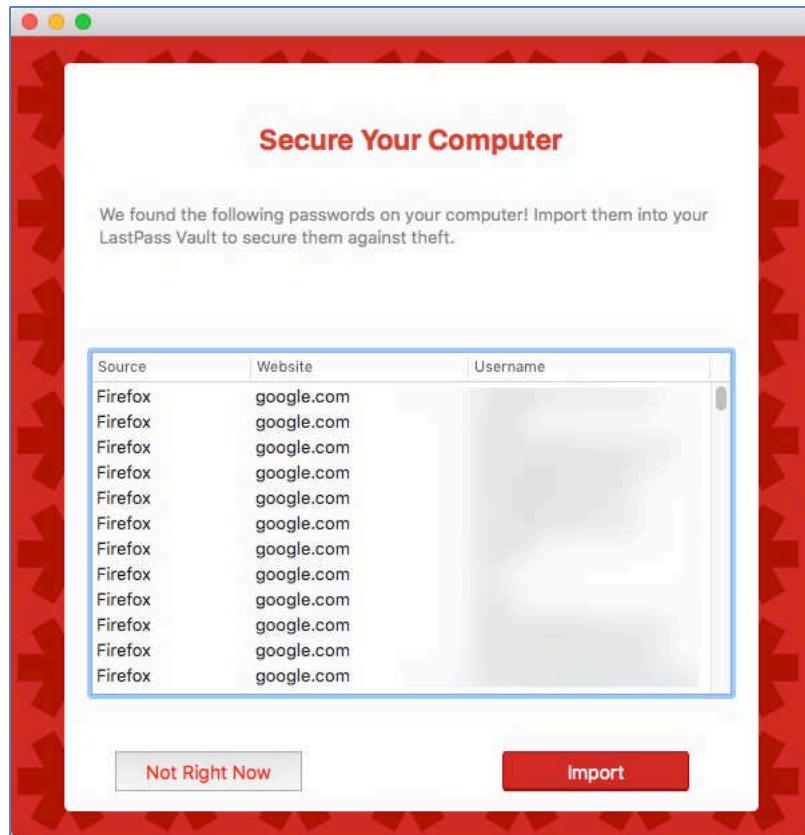
7. If you have a LastPass account, click the *Log In* button, enter your *Email* and *Password*, and the select the *Log In* button.



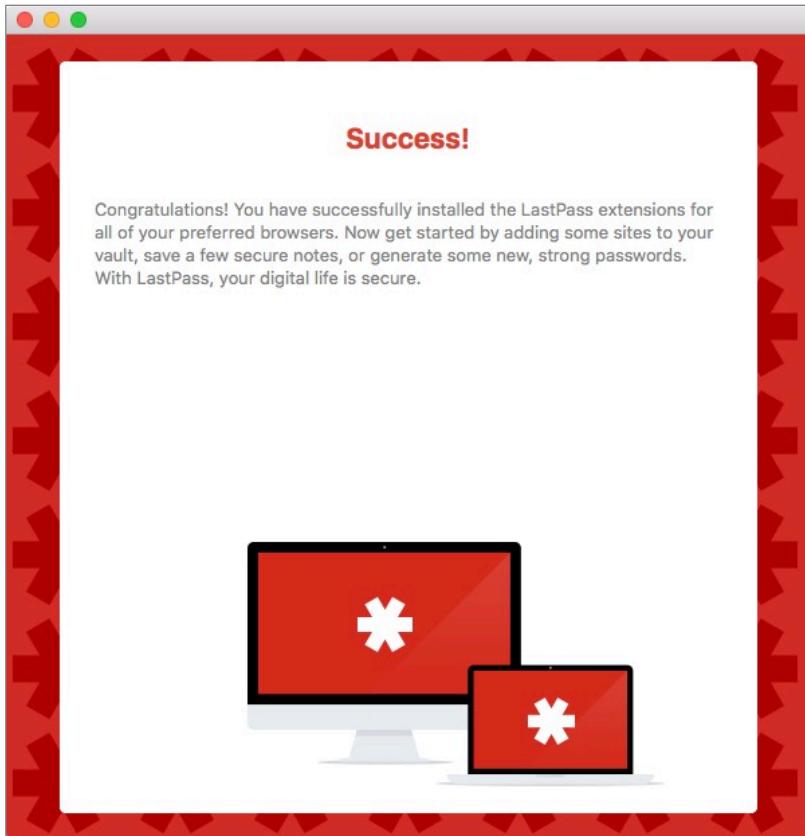
8. At the *Secure Your Computer* window, LastPass will prompt for your OK to import passwords found in your Keychain. It is fine to authorize this. Be

4 Passwords

forewarned that you will need to give an *Allow* click for each and every credential imported.

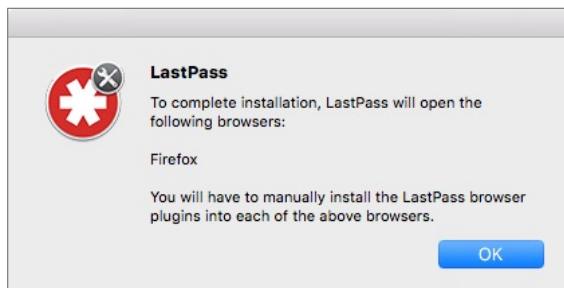


9. When done, you are greeted with the *Success* window. LastPass is now installed in Safari and Google Chrome (if they are present on your computer).



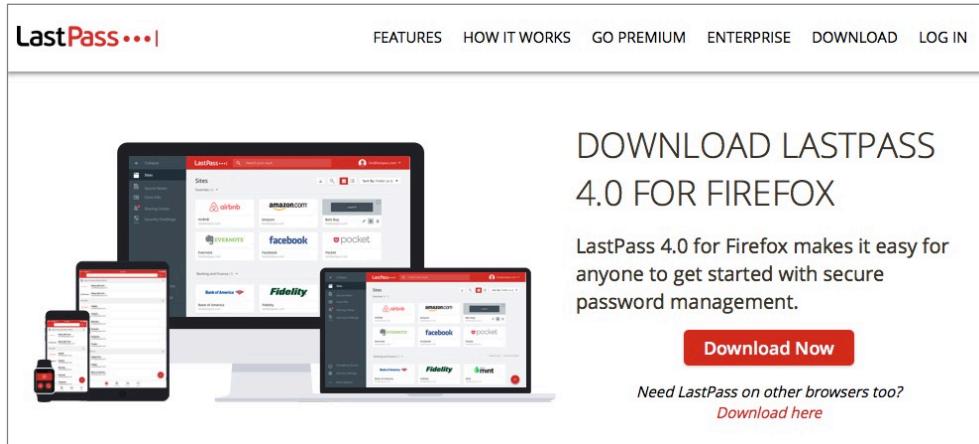
Install LastPass for Firefox

10. Close the *Success* window by clicking the red close gel button. An alert gives you a glimpse into your immediate future. Select the *OK* button.

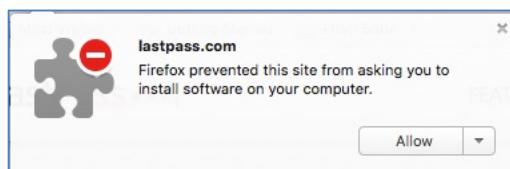


4 Passwords

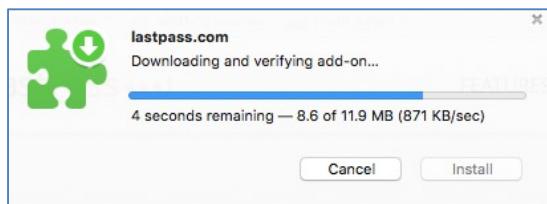
11. If you have Firefox installed, it will launch, prompting to install the LastPass plug-in. Select the *Download Now* button.



12. The plug-in will download. Click the *Allow* button to allow installation.
13. At the Firefox prompt, select the *Allow* button.



14. LastPass will begin downloading into Firefox. When complete, select the *Install* button.

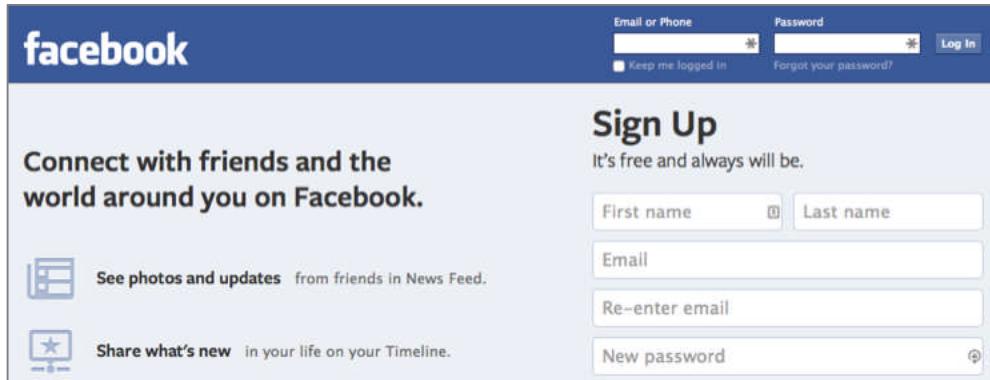


LastPass is now installed in Firefox.

4.7.2 Assignment: Use LastPass to Save Website Authentication Credentials

Once you have LastPass installed, it's time to put it to use. In this assignment you will use LastPass to store the user name and password for Facebook.

1. Use your browser to visit Facebook <https://facebook.com>.

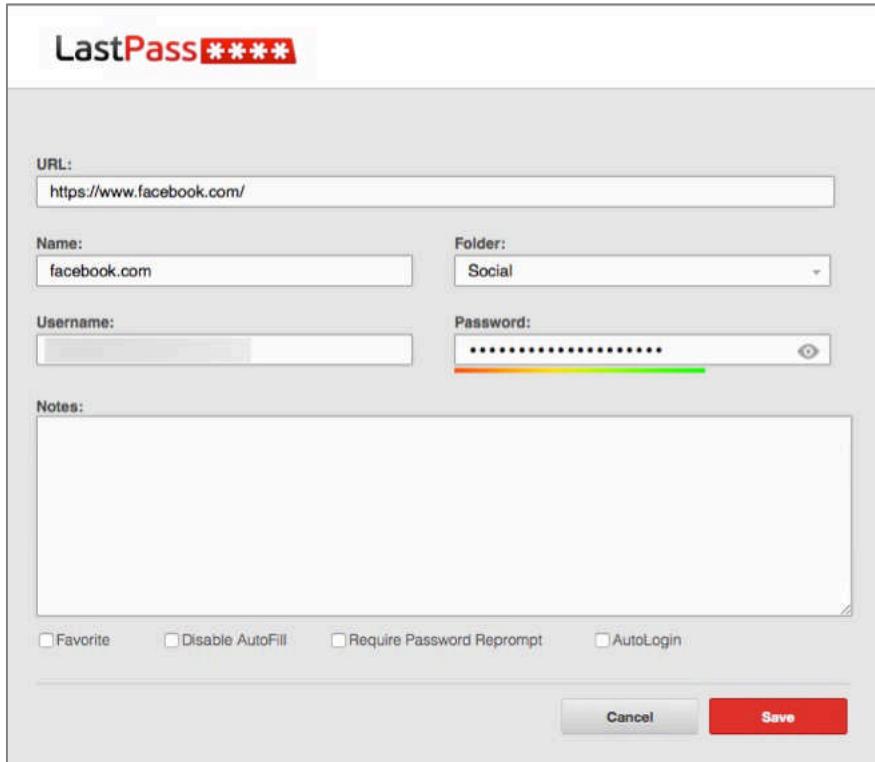


2. As this is the first time you have visited Facebook since installing LastPass, your log in credentials have not yet been stored in LastPass. Enter your Email or Phone and Password information, and then select the *Log in* button.
3. LastPass will detect that there is a form on this page, and present an option to remember your credentials. This will appear just under the navigation bar. Select the *Save Site* button.



4 Passwords

4. The LastPass *Form Fill* web page for this site will open. Configure to taste (in most cases, no edits are necessary), and then select the *Save* button. This will return you to the Facebook page.



5. Quit your web browser.

Your Facebook account credentials are now stored in LastPass, so you do not need to remember them.

4.7.3 Assignment: Use LastPass to Auto Fill Website Authentication

When LastPass has saved user name and password information for a site, you will never need to manually enter that information again. For this assignment, you will revisit Facebook and allow LastPass to enter our credentials.

4 Passwords

1. Launch your browser and surf to *Facebook* at <https://facebook.com>. Take note that your authentication credentials have been automatically entered for you by LastPass.

The screenshot shows the Facebook sign-up page. At the top, there's a blue header bar with the Facebook logo. Below it, the main title is "Sign Up" with the subtext "It's free and always will be." On the left, there's a large button with the text "Connect with friends and the world around you on Facebook." Below this, there are two sections: "See photos and updates from friends in News Feed." and "Share what's new in your life on your Timeline." To the right, there are four input fields: "First name" and "Last name" (both with placeholder text), "Email" (placeholder text), "Re-enter email" (placeholder text), and "New password" (placeholder text). At the very top of the page, the "Email or Phone" field contains "marcmintz@gmail.com" and the "Password" field contains a masked password. There are also "Log In" and "Forgot your password?" links.

2. Quit your browser.

You have just successfully proved that LastPass is saving your credentials.

4.8 Review Questions

1. What are the minimum number of characters recommended for a password by US-CERT?
2. What is one website that can be used to test the strength of a password?
3. In which system preference can the login password be changed?
4. When changing a user login password, why is it best to do so only when logged in as that user account?
5. Where does macOS store most passwords?
6. What application is used to access the Keychain?
7. What are two ways to harden the security of the Keychain?
8. What System Preference is used to synchronize the Keychain between a user's macOS/OS X and iOS devices?
9. What is the minimum macOS version needed to synchronize the Keychain?
10. What is the minimum OS X version needed to synchronize the Keychain?
11. What is the minimum iOS version needed to synchronize the Keychain?
12. Challenge questions should typically have a truthful answer. (True or False)

5 System and Application Updates

Every new beginning comes from some other beginning's end.

—Seneca¹, Roman philosopher, statesman, and dramatist

¹ https://en.wikipedia.org/wiki/Seneca_the_Elder

5.1 System Updates

The majority of computer and mobile device users simply fail to update their systems. In most cases they give the reason that updates slow down the computers, or they are concerned about introducing instability to their computers.

It is occasionally true that updates introduce instability—but it is far more likely that not updating will create greater instability.

More important is that many updates actually are about patching vulnerabilities and security holes in the system. Fixing these security issues is so important that US-CERT (Homeland Security division responsible for cyber terrorism and IT security) strongly recommends that all users update all computers and mobile devices within 48 hours of an update release.

There are fundamentally three reasons for updates and upgrades:

- **Bug fixes.** All software and hardware have bugs. We simply never will be rid of them. Developers do want to squash as many as possible so that you are so happy with their product and will continue to pay for upgrades.
- **Monetization.** Updates to operating systems and applications almost always are free, or included in the price of the original purchase. Upgrades typically are for fee. But developers will include significant new features in an upgrade to encourage the market to purchase, so the developers can afford to stay in business.
- **Security patches.** Although rarely talked about, one of the most important reasons for an update is to patch newly discovered security holes. Without the update, your computer may be highly vulnerable to attack.

It is for this last reason alone that I implore clients to be consistent with the update process.

To protect your computer from security holes in the operating system, it is critical to check for updates daily. Fortunately, we can automate this process.

5.1.1 Assignment: Configure Apple System and Application Update Schedule

In this assignment you will automate the process of updating the macOS operating system, as well as Apple software.

1. Open *Apple* menu > *System Preferences* > *App Store*. Configure as shown below:



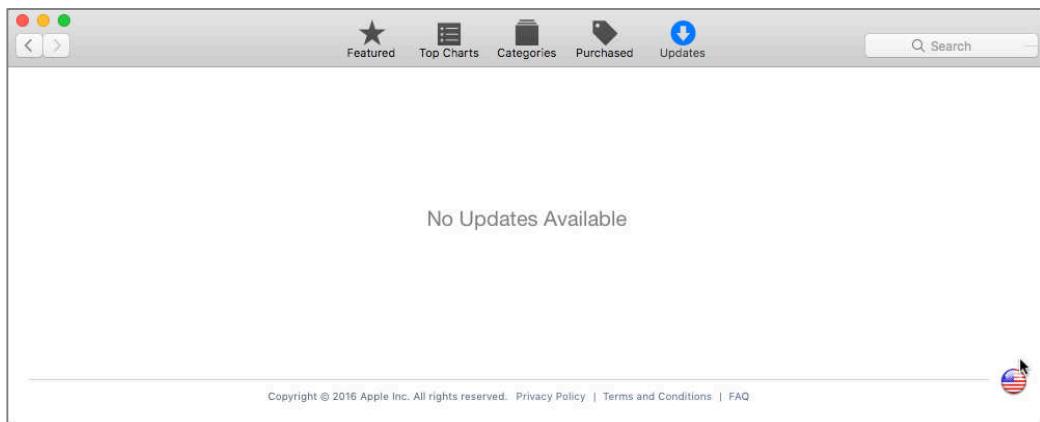
- Enable *Automatically check for updates*. That is why we are here!
- Enable *Download newly available updates in the background*. With this option active, the updates are downloaded without you knowing it. An alert will appear telling you updates are ready to be installed. Installation will start immediately upon you clicking *OK* or *Install*.

5 System and Application Updates

- Enable *Install system data files and security updates*. I cannot imagine why you would not want to have the most current macOS anti-malware installed.
 - Enable *Automatically download apps purchased on other Macs*. If you own multiple macOS or OS X machines, and have the same Apple ID in use for the Mac App Store on each, this will automatically install applications on this Mac even if they were purchased on one of the others.
2. Close System Preferences.
 3. When new system or Apple software updates are available, the *App Store Dock* icon will display a red dot with the number of updates available.



4. Select the *App Store* icon to launch the App Store Application. Select the *Updates* button in the navigation bar to display the available updates. Depending on your Internet connection speed, this may take several minutes to display.



5. Select the *Update All* button to download and install all available updates.
6. Quit the App Store application.

Your macOS system and Apple Store applications will now automatically alert you when updates are available.

5.2 Manage Application Updates with MacUpdate Desktop

macOS, Apple applications, and apps downloaded from the Apple App Store can be updated through the App Store app. Although some other applications have built-in automatic updating, it is still not the norm. Also, system preferences, plug-ins, and other software do not typically automatically update.

Recently, Adobe Flash and Oracle Java have been used by criminal elements to gain control over computers to access user data. Apple has taken the offensive by blocking older susceptible versions from running on macOS and OS X 10.7 and higher. There are many other software points that have been, can, and will be exploited. It is critical to keep all of your software up-to-date so that security holes can be secured.

As the typical user has over 100 applications, plug-ins, extensions, etc., by far the fastest, easiest, and most cost-effective way to do this is to automate the process using MacUpdate Desktop² (\$20/year license).

5.2.1 Assignment: Install and Configure MacUpdate Desktop

In this assignment you will download, install, and configure MacUpdate Desktop.

² <http://www.macupdate.com/desktop>

5 System and Application Updates

1. Open a browser to surf to the *MacUpdate* home page at <https://macupdate.com>.

The screenshot shows the MacUpdate website homepage. At the top, there's a navigation bar with links for "MacUpdate", "Promo", "Desktop", and a search bar labeled "Search Mac Apps". To the right of the search bar is a button that says "How many outdated apps are on your Mac?" with a "FIND OUT" button next to it. There's also a "Sign in or create" link. Below the navigation, there's a large promotional banner for "Copy music & playlists from your iPhone & iPad to your Mac" with a "Download" button. The main content area features the text "MacUpdate simplifies finding, buying and installing apps for your Mac". A dropdown menu under "These Mac apps are great for" shows "replacing Adobe CC". Below this are icons for several apps: Pixelmator, Sketch, Affinity Photo, Vector Icon Box, Affinity Designer, Sparkle, MyBrushes, Super Vectorizer, and a "+5 more" link.

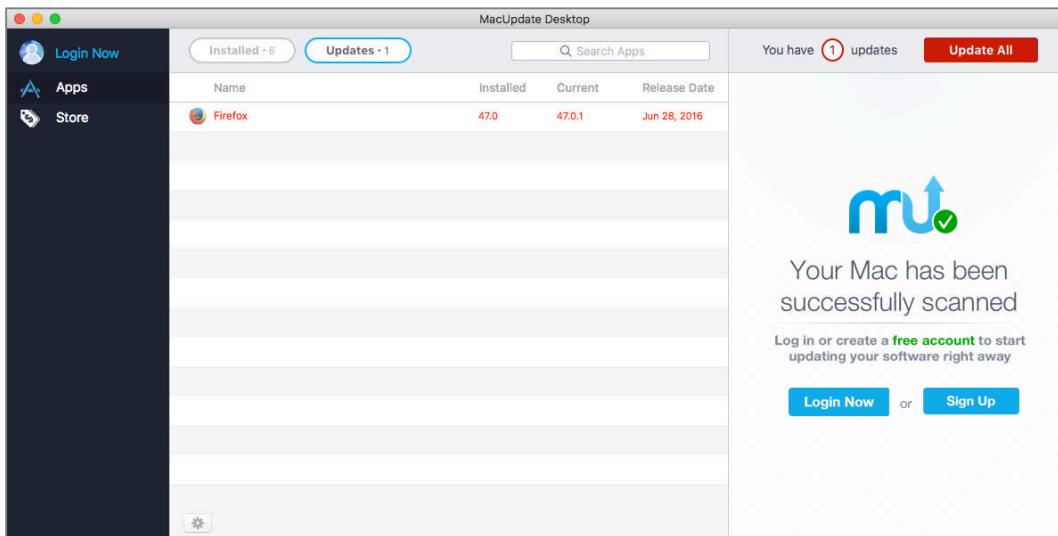
2. Select the *Desktop* button at the top of the page. The *MacUpdate Desktop 6* page opens.

The screenshot shows the MacUpdate Desktop 6 page. At the top, it has the same navigation bar as the home page. The main title is "MacUpdate Desktop 6" with the subtitle "Mac app installs & updates made easy". On the left, there's a "Get started, it's freemium!" section with input fields for "First name", "Last name", "Email address", and "Password", followed by a "Download Now" button. On the right, there's a "MacUpdate Desktop" window showing a list of installed applications with their versions and update status. One application, Spotify, is highlighted with a "Watch Video" button. A sidebar for Spotify provides information about the service and its features.

- a. Enter your First name.
- b. Enter your Last name.
- c. Enter your Email address.

5 System and Application Updates

- d. Create a Password.
3. Select the *Download Now* button. Then select the *10-day free trial Download Now* button.
4. MacUpdate Desktop will begin to download. The default location is your Downloads folder.
5. Drag the MacUpdate Desktop.app into the Applications folder.
6. From the Applications folder, locate and launch *MacUpdate Desktop*. The app will open.

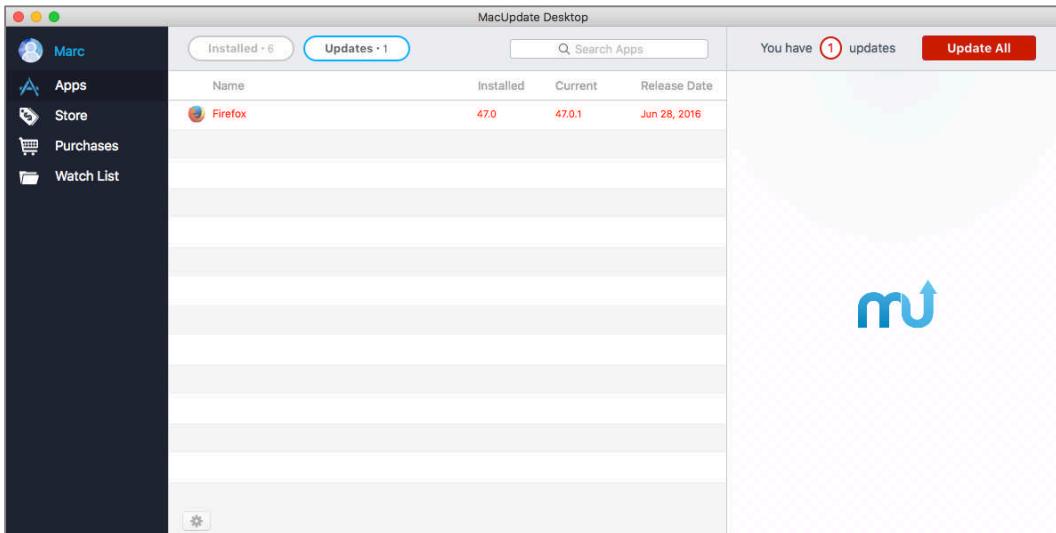


7. Click the *Login Now* button. The *Login to your MacUpdate account* dialog opens. Enter the *Email address* and *Password* used when downloading the app, and then click the *Login Now* button.

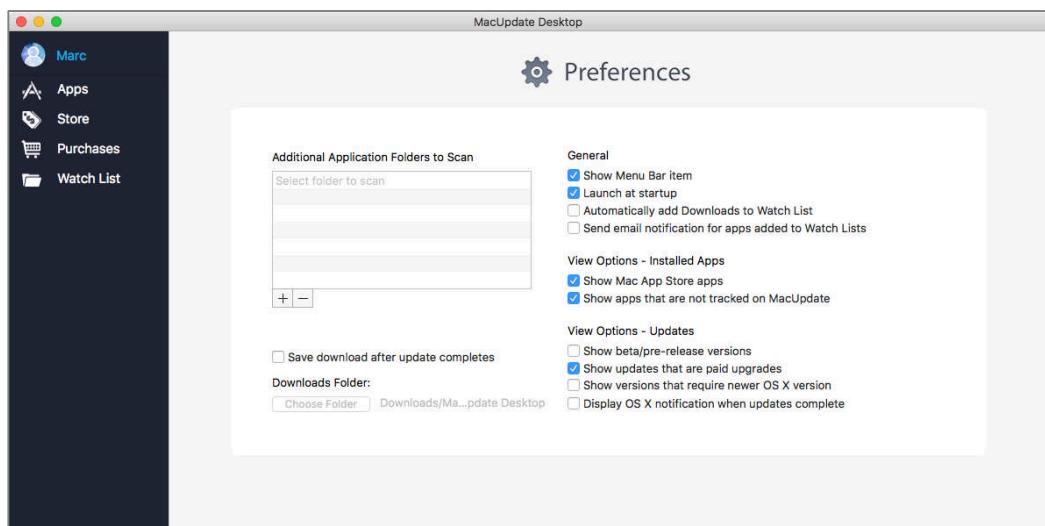
A screenshot of the "Login to your MacUpdate account" dialog. It features a "mu" logo at the top left. Below it is the text "Login to your MacUpdate account". To the right is a form with two input fields: "Email address" and "Password". Underneath the password field is a link "Forgot your password?". To the right of the password field is a blue "Login Now" button. At the bottom right of the dialog is a link "Don't have an account? Create one now."

5 System and Application Updates

8. It will automatically scan your computer for all installed applications, check for any available updates, and then display them for you. Available updates will appear in red.



9. Select the *MacUpdate Desktop* menu > *Preferences*. Configure the main window as below:



10. Quit MacUpdate Desktop to save your preferences.

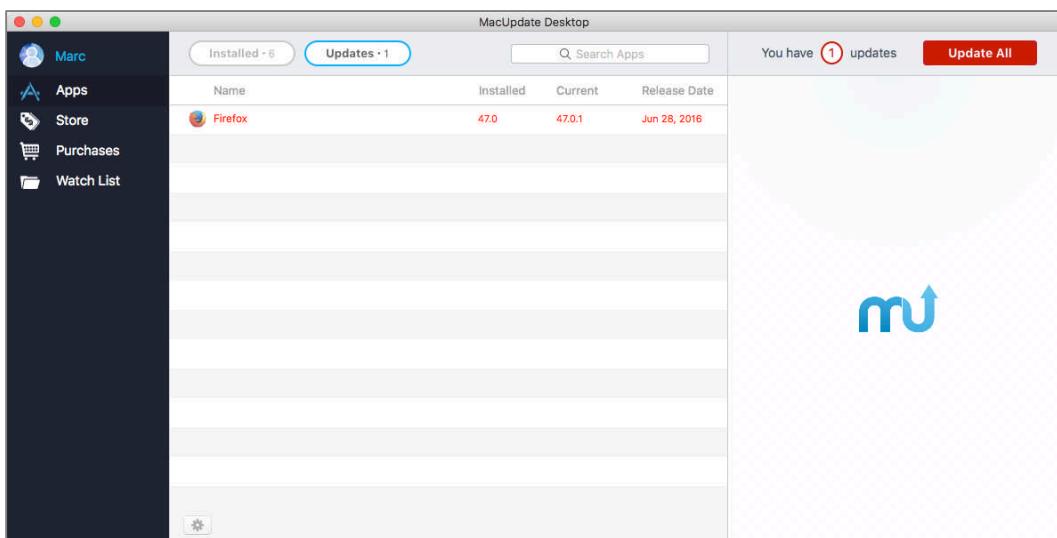
5 System and Application Updates

You have successfully installed and configured MacUpdate Desktop on your computer.

5.2.2 Assignment: Application Updates with MacUpdate Desktop

Once you have MacUpdate Desktop installed and configured, it will notify you daily of available Apple and third-party application updates. In this exercise, we use MacUpdate Desktop to manually scan, download, and install updates.

1. From the *Applications* folder, launch MacUpdate Desktop. It will automatically begin scanning for available updates.
2. From the sidebar, select *Apps*.
3. Select the *Apps* menu > *Check for Updates*.
4. Select the *Updates* button in the navigation bar. This will filter out any applications that don't have updates. Then select the *Name* column to sort alphabetically:



5 System and Application Updates

5. From the top right corner of the windows, select *Update All* to, well, download and install all updates.
 - Note: If you prefer to hand-select which updates to install, double-click the target update from the main window.
6. Most updates require authorization to install. At the prompts, enter an administrator name and password.
7. When all desired updates are complete, Quit MacUpdate Desktop.

Can it get any easier or faster than this?

5.3 Review Questions

1. US-CERT recommends installing updates within _____ hours of release.
2. Name the three fundamental reasons for updates and upgrades: _____.
3. System and many application updates and upgrades can be configured from the _____ System Preference.
4. Apple and most 3rd-party application updates and upgrades can be automatically reviewed and downloaded using the _____ application.

6 User Accounts

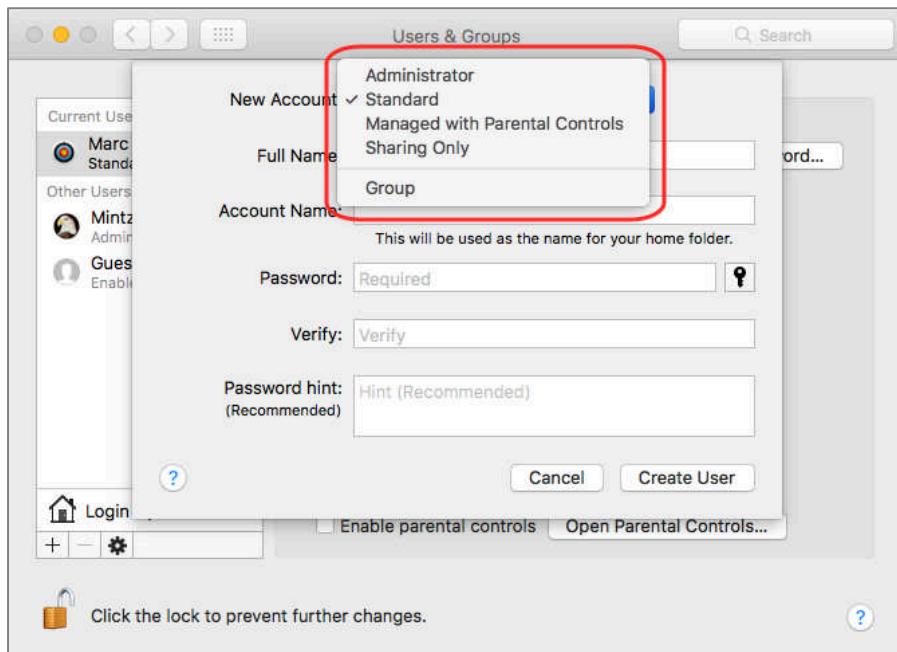
Those who desire to give up freedom in order to gain security will not have, nor do they deserve, either one.

—Benjamin Franklin¹

¹ https://en.wikipedia.org/wiki/Benjamin_Franklin

6.1 User Accounts

macOS allows six different types of user accounts, each with its own pros and cons, powers and limitations. Most of these may be designated from the *Users & Groups System Preference*.



- **Root.** The Root account cannot be created or enabled from System Preferences. There can be one, and only one root account ever on any computer. Root is the ultimate lord over the system, with unquestioned power and control. If root does something dangerous—say, issues a command to erase the entire drive—the system will not even issue a *Danger, Will Robinson* alert, it will simply dutifully erase the drive. Root is present out of the box, but is disabled by not having a password assigned. It would be rare to ever need to enable the root user, as any administrator account can assume the powers of root.
- **Administrator.** There must always be at least one, and may be an unlimited number of administrators, or administrative user accounts, each having identical power over the computer. What makes an Administrator unique

above the Standard, Sharing, and Guest user accounts are its abilities to: Create new user accounts, delete user accounts, modify the contents of restricted folders (System, Library, Applications), authorize the installation or removal of applications and system updates, and take on the powers of root from the command line by issuing *sudo* and *su* commands.

- **Standard.** There can be an unlimited number of Standard accounts. This is the recommended account level for most users working locally on the computer. Standard accounts can open and work without limitations with any application installed on your Mac. The advantage of working as a Standard account is that it is not possible to damage the operating system or applications.
- **Managed with Parental Controls.** This account is typically a Standard account that has had Parental Controls assigned to it. Parental Controls further restrict the powers of the account by limiting: Access to specific applications, access to specific websites or any adult site, who can communicate with the user via Apple Mail and Messages/iChat, the hours for which the user may stay logged in, etc. Although this account level was originally intended to protect children from the darker areas of the Internet, and the computer from the children, it is a powerful tool for use with employees (guess how many billions of dollars a year in wasted productivity are spent on Facebook?)
- **Sharing Only.** There can be an unlimited number of Sharing Only accounts. This type of account cannot log in locally to the computer. The only access is via the network and file sharing. It is highly useful if you need to work with someone else on the same network and share files with them. This allows them to access your computer and files over the network, but only those files.
- **Guest.** There is only one Guest account. With Guest enabled, anyone may access your computer, either locally or via file sharing over the network. The Guest only has access to folders and files that have been shared as either read or read & write for everyone. If a Guest logs in locally, any documents the Guest creates and saves in the Guest home folder are deleted upon log off. Unless you are certain of your file-sharing configuration, it is unsecure to allow Guest access.

6.2 Never Log In as an Administrator

Maybe it is the human condition. We want power, authority, and more power! This carries over into how we log in to the computer. Everyone wants to be the administrator of his or her computer! Apple enables this. When the owner of a new Mac boots up for the first time, that person is prompted to create a user account, which is by default an administrator account.

But this is bad juju.

If you have the bad luck of launching a malware attack on your computer (most often unknowingly) while you are logged in as an administrator, the malware will take on your user account power. This means the malware has full control and power over the computer—including all other user accounts. Yikes.

On the other hand, if you have the same lousy luck to launch a malware attack while logged in as a non-administrative user, the malware will typically take on your non-admin power. Under this scenario, the malware has full control over your home folder and nothing else.

I can hear the wailing from here: *But I need to be an administrator. How else will I be able to install software and updates, and perform maintenance?*

Fear not. In macOS you do not need to be logged in as an administrator to perform administrator tasks (adding/deleting user accounts, installing/updating the system and applications, and running system diagnostic and repair utilities). You can be logged in with any type of user account. You only need to authenticate with an administrator name and password when prompted.

To do this, you need to have an administrative user account on the computer, but log in with a non-admin (standard) user account. Then when you are prompted for an admin name and password while performing admin duties, just enter them.

6.2.1 Assignment: Enable the Root User

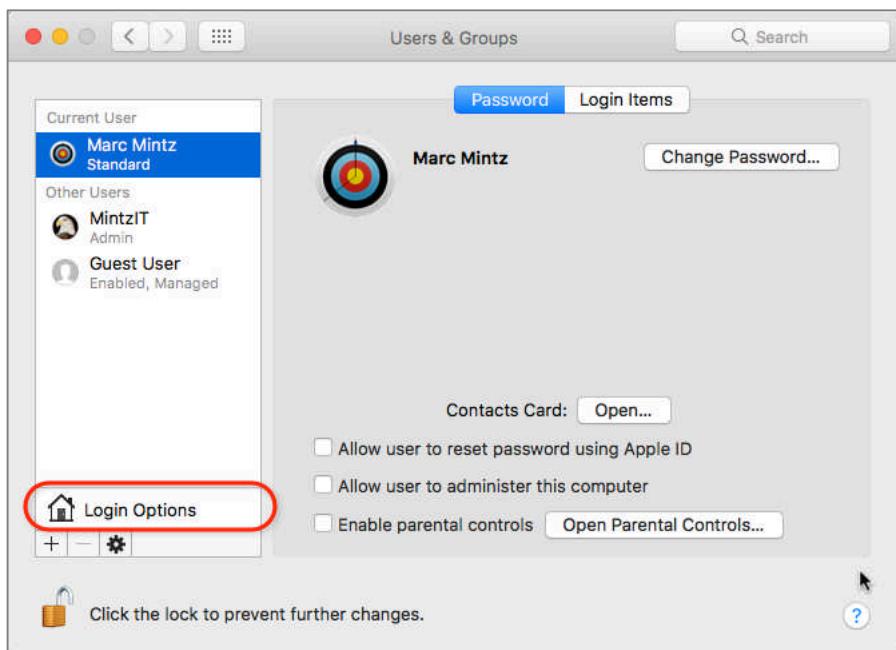
As mentioned earlier, the root user account is present right out of the box, but it is disabled. The way Apple has disabled the account is by not assigning a password. That's right—all that is needed to enable root is to assign the account a password!

6 User Accounts

Before jumping in and assigning a password, give thought to why you want to enable root. Any administrative account can assume the powers of root whenever needed. I've also seen far too many users send their data to the cornfield when logged in as root and then making a simple keystroke error.

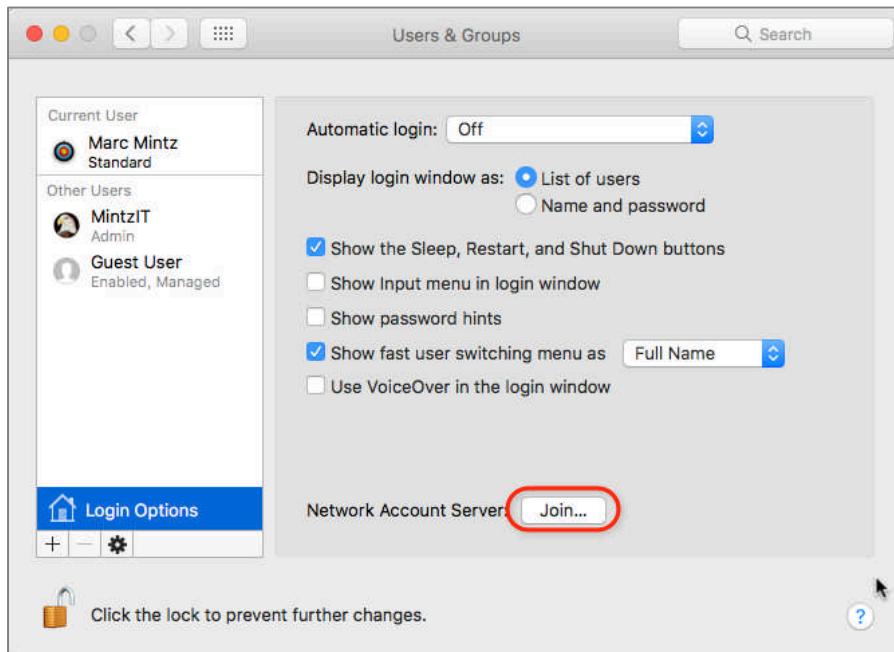
However, if you would like to experiment with root powers, here we go...

1. Select *Apple* menu > *System Preferences* > *Users & Groups*.
2. Authenticate.
3. Select the *Login Options* button.

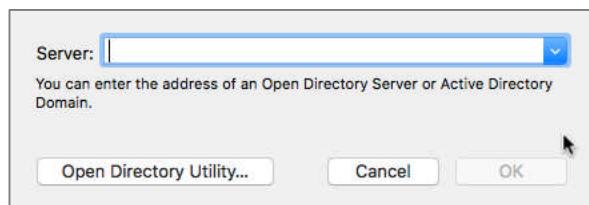


6 User Accounts

4. Select the *Network Account Server: Join or Edit button*.

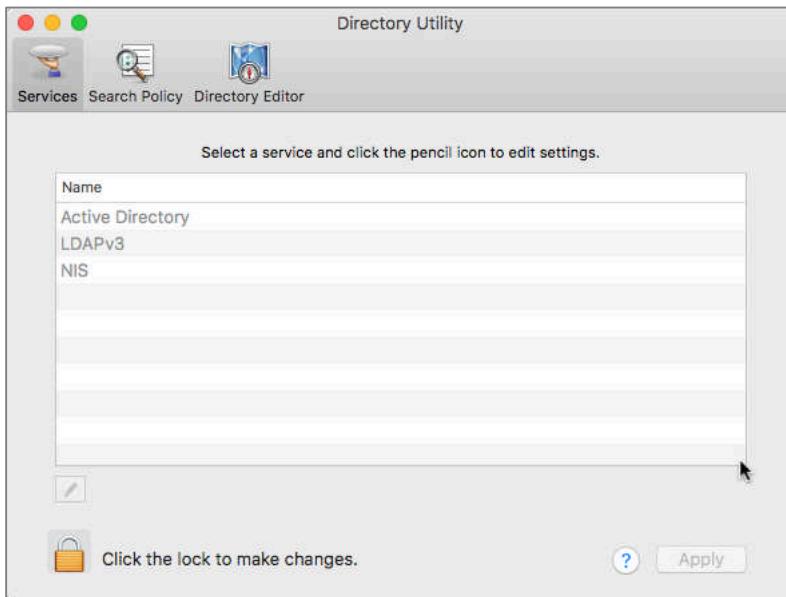


5. Select the *Open Directory Utility* button.

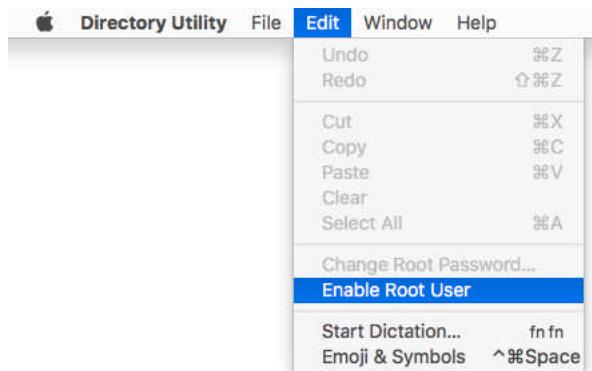


6 User Accounts

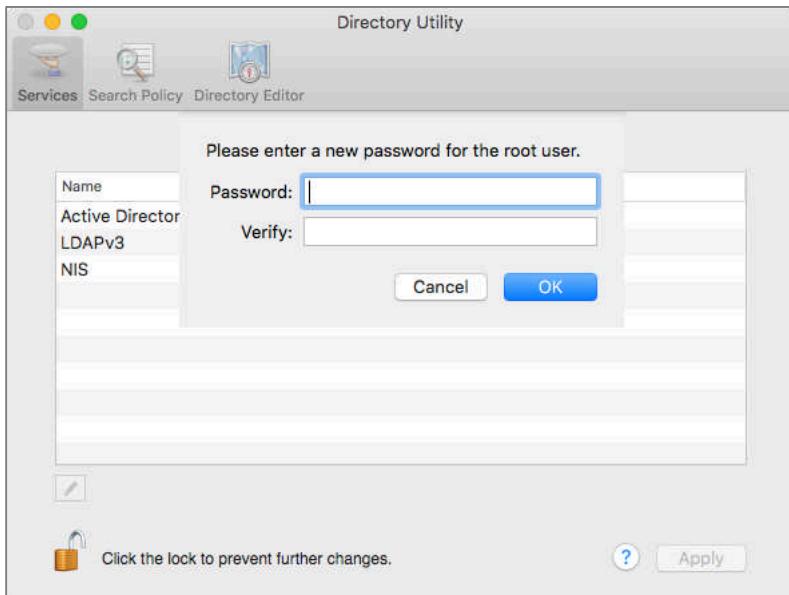
6. Click the lock icon, and then authenticate with administrator credentials.



7. Select the *Edit* menu > *Enable Root User*.



8. In the *Please enter a new password for the root user* window, create a strong password.



9. Quit Directory Utility.
10. Quit System Preferences.

Root was on the computer from the moment the system was installed. Giving root a password enabled it.

6.2.2 Assignment: Login as the Root User

To see how the macOS landscape appears to root user, it's easiest to simply log in as root.

1. Log out of the current user account.
2. At the Login Window, log in as *root*. If you don't see the *root* user, select *Other...* From here you may enter the username "root", and the password you assigned for root.
3. Once at the Desktop, navigate to the */Users/<username>* folders. Notice that you are able to access any user folder with read and write permissions.

4. To log out, select the *Apple* menu > *Log Out*.
5. At the *Login Window*, log in with your standard account.

6.2.3 Assignment: Change the Root User Password

1. Select *Apple* menu > *System Preferences* > *Users & Groups*.
2. Authenticate.
3. Select the *Network Account Server Join* or *Edit* button.
4. Authenticate.
5. Select the *Edit* menu > *Change Root Password*.
6. Enter a strong password
7. Quit Directory Utility.
8. Quit System Preferences.

6.2.4 Assignment: Disable the Root User

1. Select *Apple* menu > *System Preferences* > *Users & Groups*.
2. Authenticate.
3. Select the *Network Account Server Join* or *Edit* button.
4. Authenticate.
5. Select the *Edit* menu > *Disable Root User*.
6. Quit Directory Utility.
7. Quit System Preferences.

6.2.5 Assignment: Create an Administrative User Account

One of the most important rules in IT security is to log in with a non-administrative account, not an administrative account. However, the very first account created when you initially boot up your computer *is* an administrator!

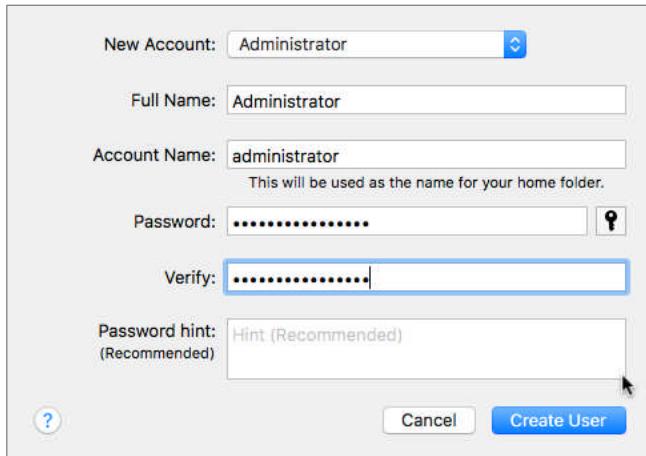
6 User Accounts

In this assignment, you will create an administrative user account on the computer. In the next assignment, you will change your own account to a standard user account so that you will no longer be in violation of this rule.

1. Log in to the computer with your normal administrator account.
2. Open *Apple menu > System Preferences > Users & Groups*. Click the *Lock* icon in the bottom left corner, and then authenticate with an administrator name and password.



3. Click the + (*add user*) button at the bottom of the side bar. The *Create a New Account* window will open.



- From the *New Account* pop-up menu, select *Administrator*.
 - In the *Full Name* field, enter “Administrator”.
 - In the *Account Name* field, enter “administrator”.
 - In the *Password* field, enter a strong password.
 - In the *Verify* field, reenter the strong password.
 - I’m not fond of entering anything in the *Password Hint* field, as this will be of assistance to hackers as well.
4. When done, click the *Create User* button. You are returned to the *Users & Groups* preference.
 5. *Quit* System Preferences.

You have successfully created a new administrator account.

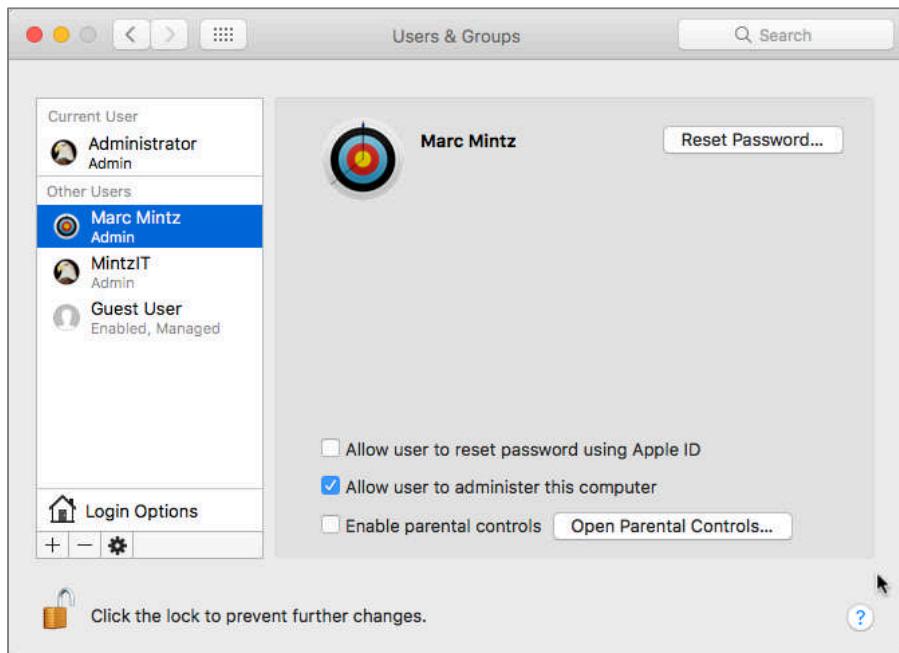
6.2.6 Assignment: Change from Administrator to Standard User

In the previous assignment, you created an administrative user account whose name and password can be used when needed. In this assignment, you change

6 User Accounts

your own account to a standard user account, which will remain your regular log in account.

1. Log out of your account.
2. Log in as the new administrator account.
3. Select the *Apple* menu > *System Preferences* > *Users & Groups*.
4. Unlock the Lock icon, and authenticate with administrator credentials.
5. Select your account in the side bar.
6. Disable the *Allow user to administer this computer* check box:



7. You receive a prompt informing you that the change will take place after a restart. Select the *OK* button.
8. Select *Apple* menu > *Restart*.
9. Log in with your everyday account (now a Standard account).

Whenever you need to perform administrative tasks, use the name and password of the new administrator account you have just created. No need to login as an administrator!

6.2.7 Application Whitelisting and More With Parental Controls

In 2014, Target, Home Depot, and other major retailers were hacked for their customer databases. Although there were multiple breakdowns in the security protocols of these organizations, one step would likely have prevented all of them—*Application whitelisting*. This same strategy should be used by both home and business systems to help secure computer systems.

Application whitelisting is a process that allows only authorized applications to run on a computer, blocking any executable that is not on the list. This is a vital ingredient to system security because even the very best anti-malware catches only 99.9% of the *known* bugs. And what if your computer is penetrated by *unknown* malware? Anti-malware is of no use here. However, if your computer has application whitelisting in place, the unknown malware is blocked from executing! In macOS, *Parental Controls* can be used to perform application whitelisting.

Parental Controls allow an Administrator to restrict access to specific applications and services to a non-administrative user account. As the name implies, this feature was originally intended as a way for parents to better manage their children's account. It also has its place in the business setting by restricting specific applications (disallowing Spotify, etc.), restricting access to specific websites (pornography, Facebook, etc.), or allowing access to the account only during work hours.

Once Parental Controls has been used to implement application whitelisting, it will be necessary for the administrator to be available for a brief time while the unintended consequences shake out. It is common for some permitted applications to require the use of a restricted application or process. An administrator will need to be available to provide authorization.

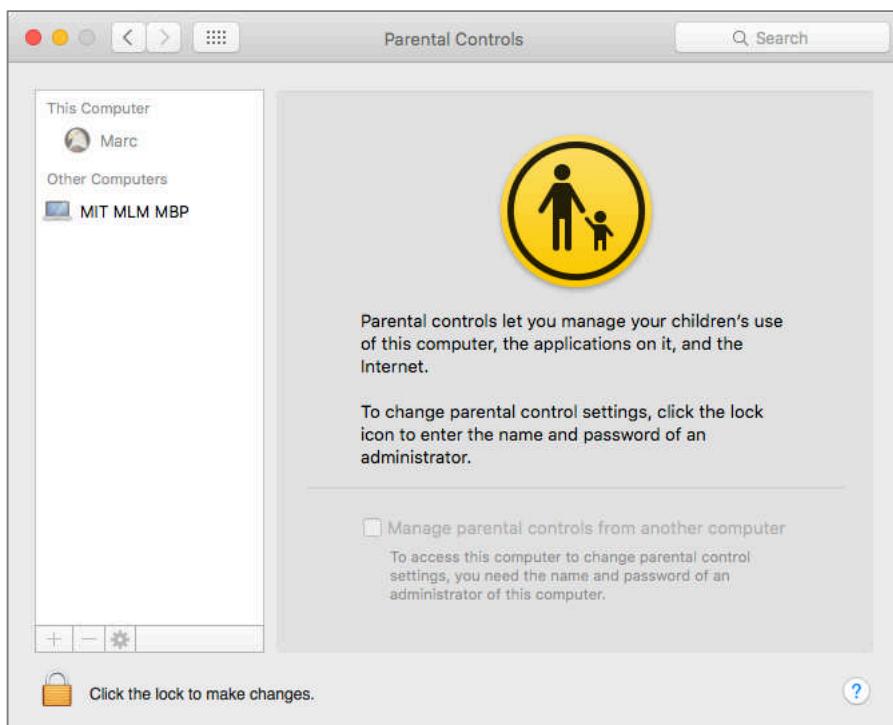
Once Parental Controls are established for a user account, the account is referred to as *Managed with Parental Controls*, or as a *managed* account. Only non-administrative accounts may be managed. If creating a new user account, it can be

initially setup as *Managed with Parental Controls*. If the account already exists as a Standard account, it can be converted to managed. The *Guest* account can also have parental controls assigned.

6.2.8 Assignment: Configure a Managed with Parental Controls Account

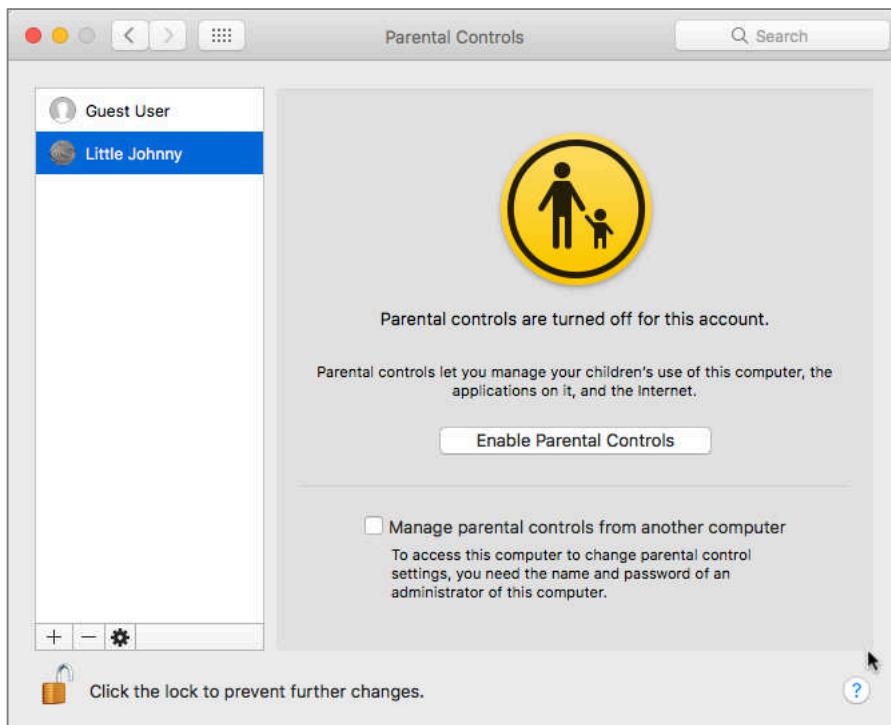
For this assignment you will configure your own account to have the added security of application whitelisting. These same steps should be taken for all non-administrative accounts on your computer, and all computers in your household or business. Understand that best practices holds that *all* of your non-administrative accounts should have application whitelisting enabled—and that you never login with an administrative account.

1. On the computer hosting the user account to be managed, open *Apple menu > System Preferences > Parental Controls*.



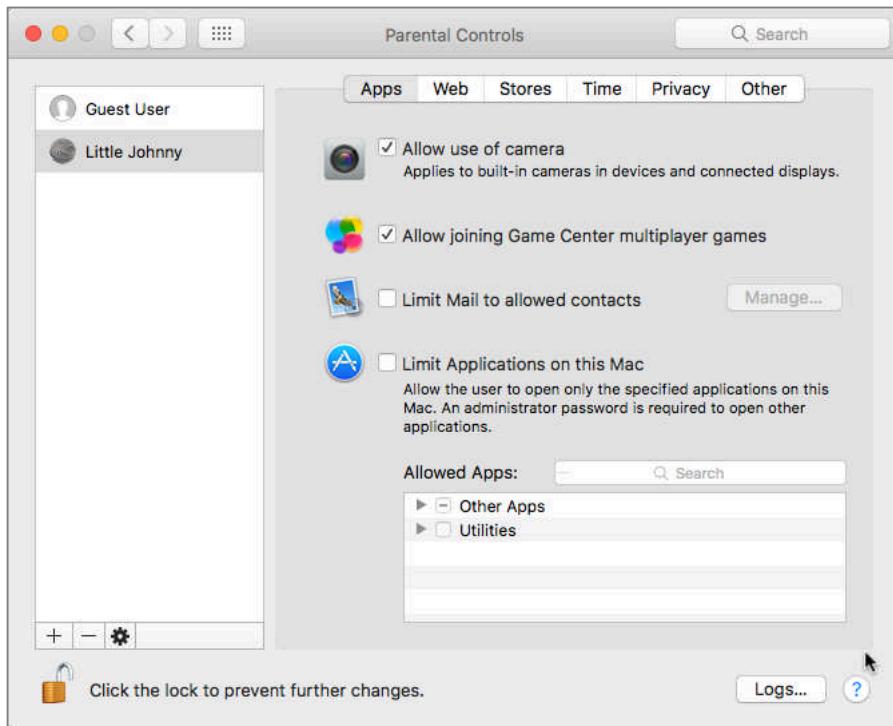
6 User Accounts

2. Select the *Lock* icon to authenticate as an administrator.
3. In the sidebar select the target account to manage, and then select the *Enable Parental Controls* button.
 - Note: If you want to manage parental controls from another computer on the same network, enable the *Manage parental controls from another computer* checkbox.



6 User Accounts

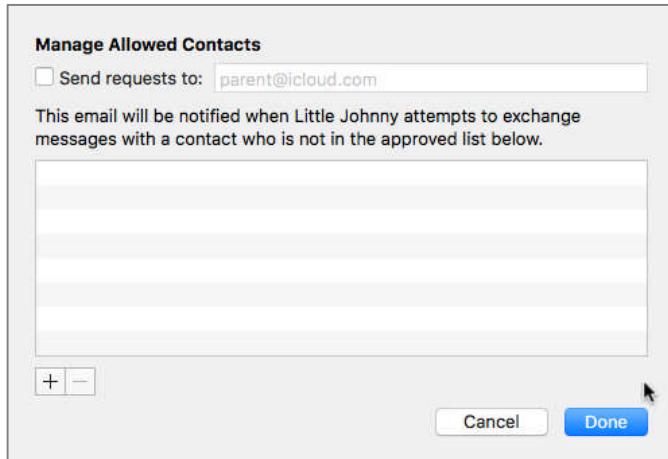
4. The *Parental Controls* System Preference pane opens. Unlock the pane.



- *Allow use of camera* is self-explanatory.
- *Allow joining Game Center multiplayer games* is self-explanatory.

6 User Accounts

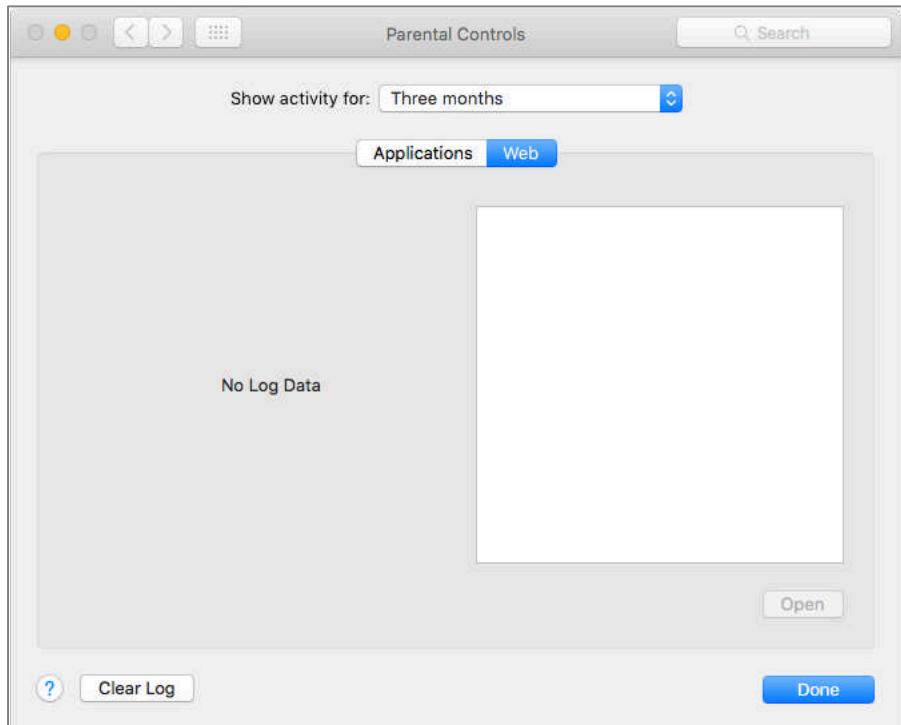
- *Limit Mail to allowed contacts* helps to prevent unknown and unwanted people from exchanging email with the user. Selecting the *Manage* button opens a configuration window for this option.



- *Limit Applications on this Mac* activates application whitelisting. It allows picking which specific applications the account will have access.
5. Expand *Other Apps*. Enable the checkbox for applications this account needs, but do not enable the *Other Apps* checkbox as this will allow any application to run. Keep in mind we are attempting to prevent unwanted malware from launching.
 6. Expand the Utilities checkbox. Pick which utilities should be allowed access by this user.

6 User Accounts

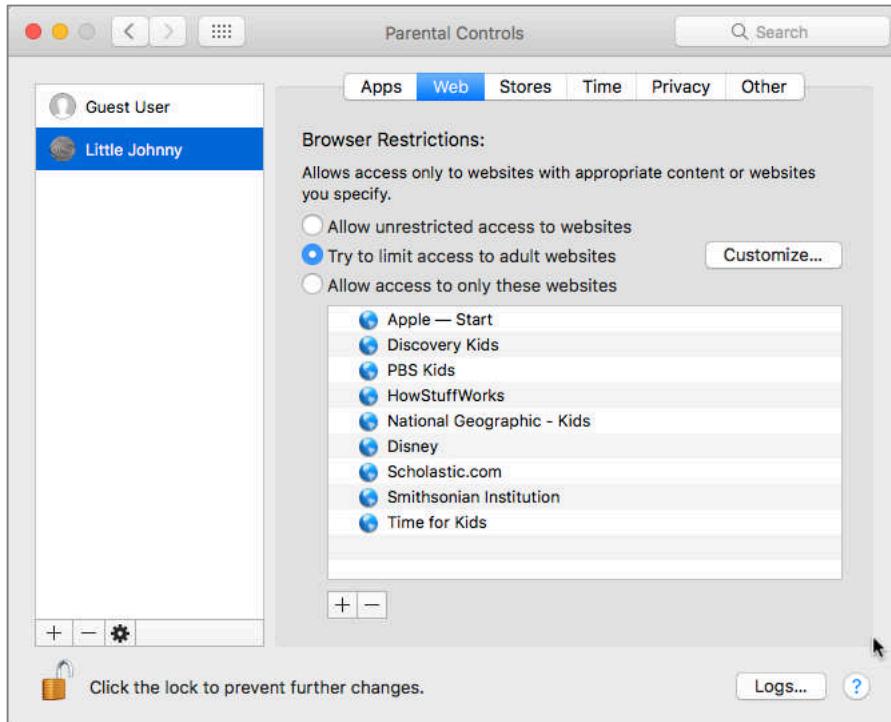
7. By selecting the *Logs* button, the administrator is able to view the activities of the managed user. Logs may be viewed from any other computer on the same network.



8. Select the *Done* button to return to Parental Controls.

6 User Accounts

- Select the *Web* tab to view the managed web options.

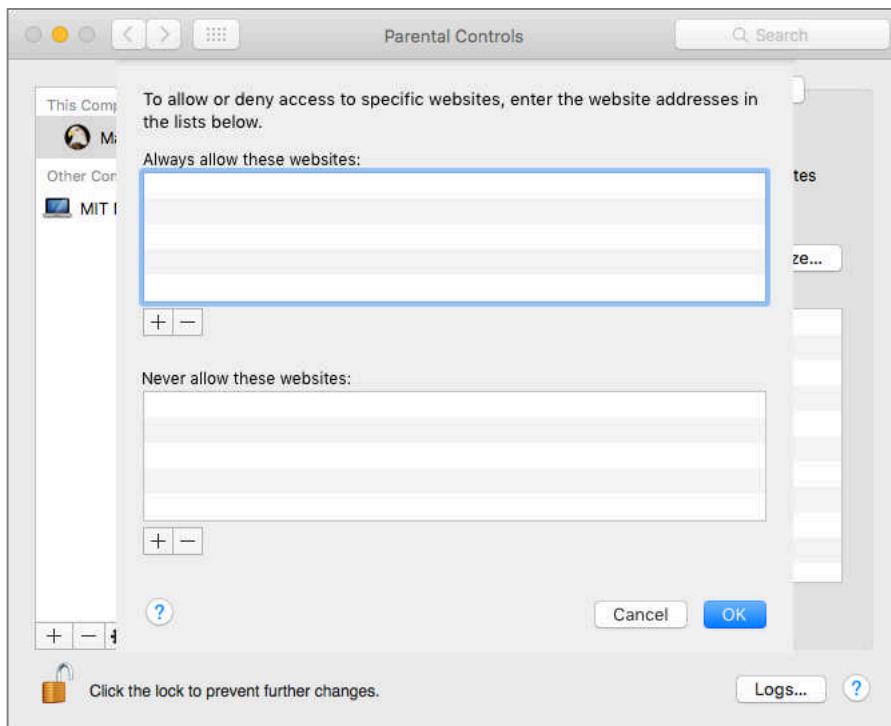


- *Allow unrestricted access to websites* eliminates any filtering of website access. Less than 5% of the businesses with which we hold an initial consult restrict web use. This is due primarily from leadership not understanding the consequences of doing so. According to a recent salary.com survey² 64% of employees visit non-work related websites *every day*. This is a costly misuse of company resources. It is also a significant source of malware infections. We do not recommend this option without a demonstrated business need.
- *Try to limit access to adult websites automatically* is our recommendation for business environments. Selecting the *Customize* button opens the

² <http://www.salary.com/wasting-time-at-work-2012/>

6 User Accounts

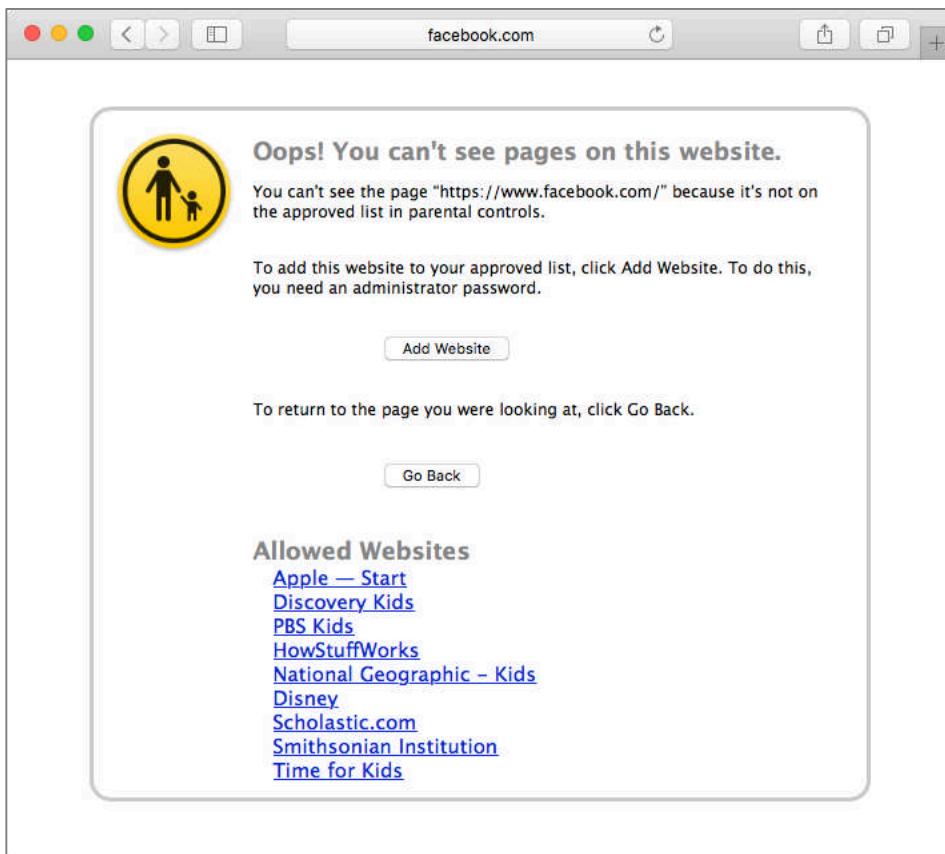
configuration window. When done looking it over, select the OK button to return to Parental Controls.



- *Allow access to only these websites* is the most restrictive, and may find its niche with young children.
- If the user attempts to visit a site that is restricted, they receive notice of such. If the user has access to administrative credentials, or if an

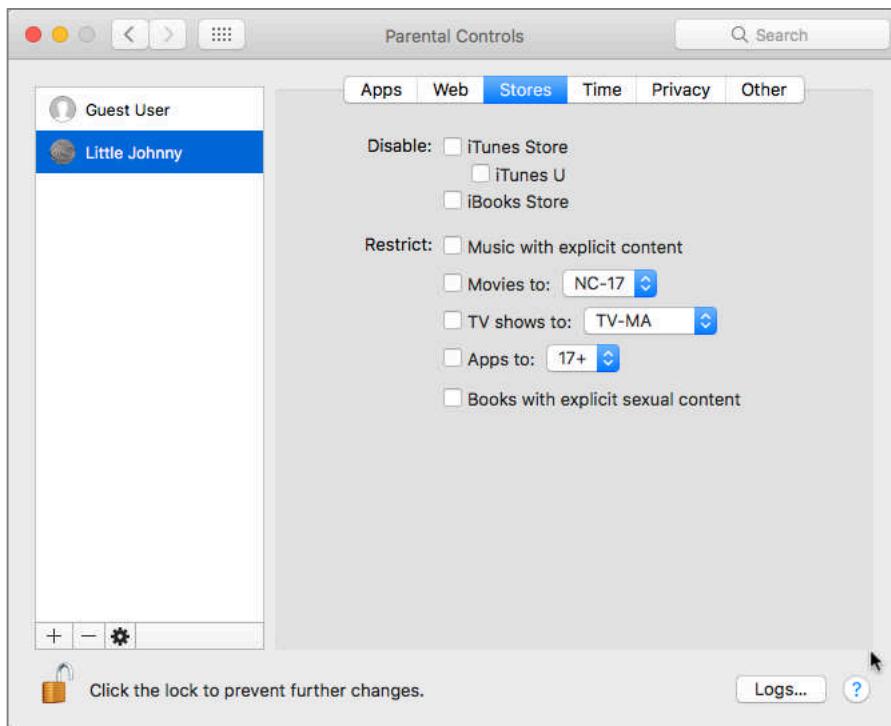
6 User Accounts

administrative user is available, selecting the *Add Website* button will make this website accessible.



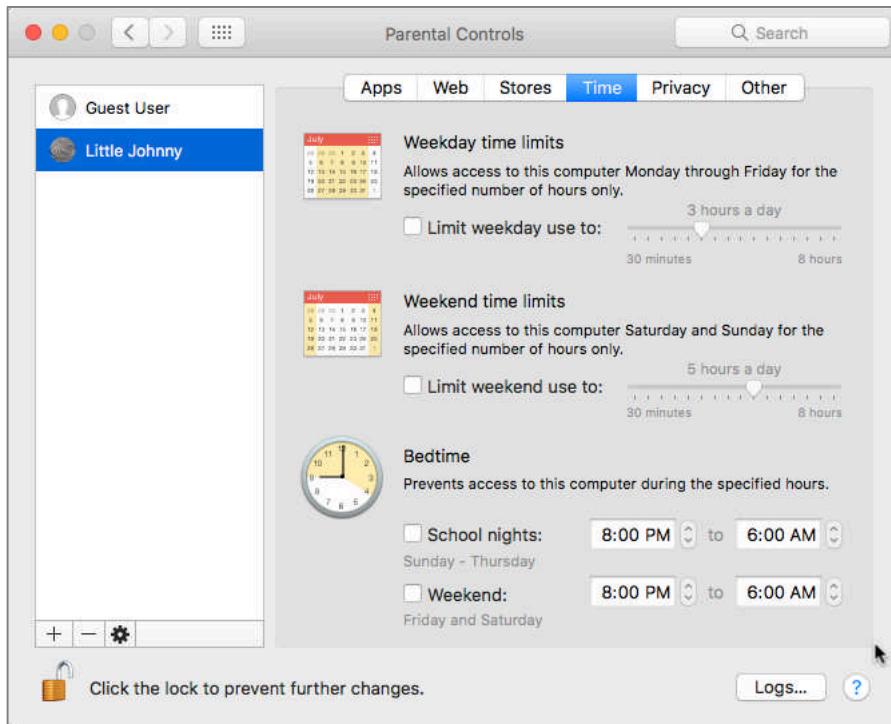
6 User Accounts

10. Selecting the *Stores* tab allows configuring access to all the various Apple commercial offerings.

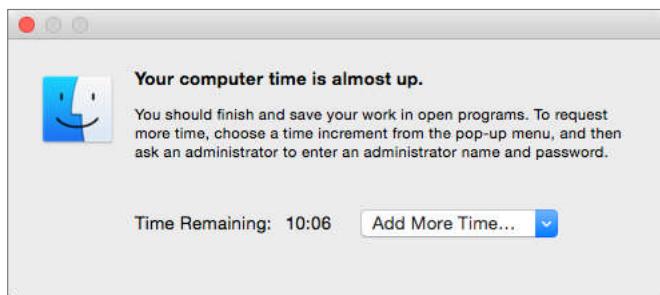


6 User Accounts

11. Selecting the *Time* tab allows configuration of when the account is able to use the computer:

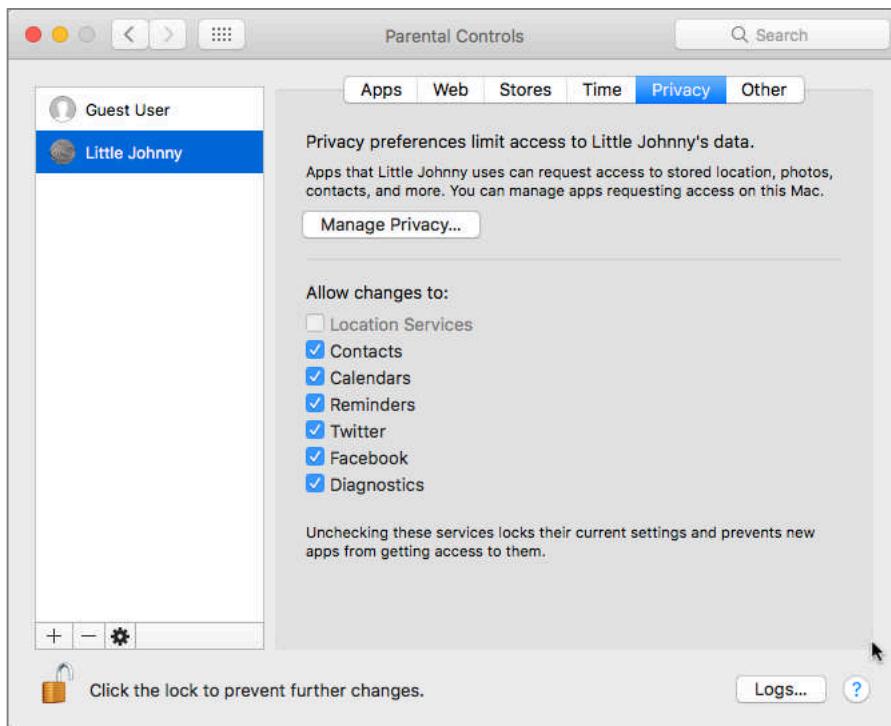


- As the end of their time approaches, an alert appears, allowing any administrative user to extend the managed user time for this session only:



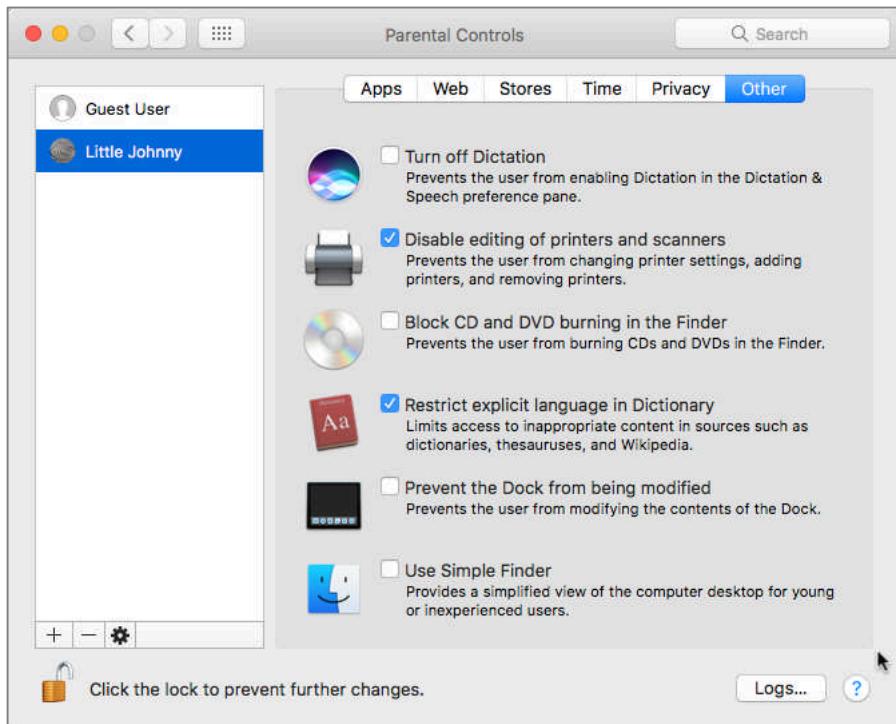
6 User Accounts

12. Selecting the *Privacy* tab allows configuration of privacy settings for this account.



6 User Accounts

13. Selecting *Other* allows configuration of the odds and ends.



14. Quit System Preferences.

You have successfully created a Managed user account with Parental Controls.

6.2.9 Assignment: View Parental Controls Logs

If the managed user has an account on the same computer as the administrator, viewing the logs is just a couple of clicks away:

1. Log in as the administrator.
2. Select the *Apple* menu > *System Preferences* > *Parental Controls*.
3. Click the *Lock* icon and then authenticate as an administrator.
4. Select the targeted managed account.
5. Select the *Logs* button.

6. In the *Logs* window, you can choose to view the *Websites Visited*, *Websites Blocked*, *Applications*, and *Messages*. When selecting the specific log files, each event is listed individually, along with time stamps. In the case of websites, they will be grouped by category.
7. *Quit Parental Controls*.
8. Take your sweet time torturing the managed user with the knowledge you have gleamed about them.

Viewing the logs from another macOS computer on the same network is almost identical. The only difference is that when opening *Parental Controls* on your own Mac to view the logs of the managed user on the remote Mac, you will see the user account under *Other Computers*.

6.3 Policy Banner

Within some organizations, the legal department specifies that there must be a *Policy Banner* present at startup. This will alert any would-be hackers or criminals that proceeding into the computer is considered a criminal offense. It is possible having a policy banner in place may prevent the “I didn’t know I was doing anything wrong” defense in court.

6.3.1 Assignment: Create a Policy Banner

In this assignment you will create a policy banner that will display upon startup.

1. Log in with an administrative account.
2. Open a word processor or text editor that is capable of creating a plain text (.txt) or rich text (.rtf) file format.
3. Create a new document with the specifics required for your policy banner. A sample policy banner is listed below:

*** WARNING***

This is a <organization name> computer system. <Organization name> computer systems are provided for processing of official <organization name> information only. All data contained on this system is owned by the <organization name> and may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel.

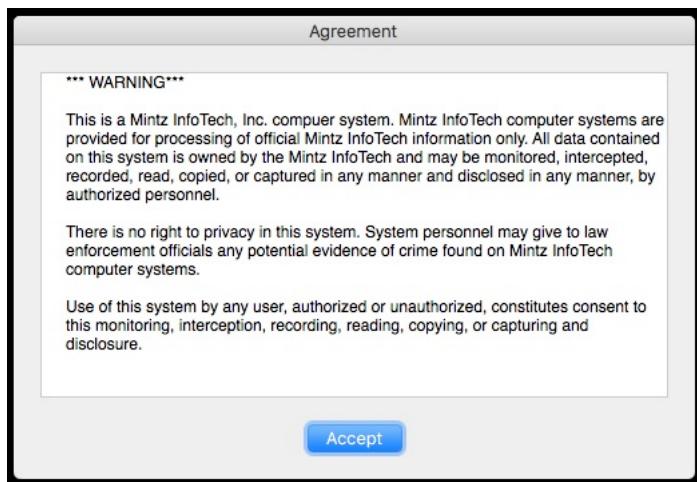
There is no right to privacy in this system. System personnel may give to law enforcement officials any potential evidence of crime found on <organization name> computer systems.

Use of this system by any user, authorized or unauthorized, constitutes consent to this monitoring, interception, recording, reading, copying, or capturing and disclosure.

4. Save the file as *PolicyBanner* in either .txt or .rtf, to the Desktop.
5. Drag and drop the PolicyBanner file into the */Library/Security* folder.
6. At the prompt, enter your administrator credentials to authorized the copy.
7. Open Terminal to adjust permissions so that Everyone (Other) has read and execute privileges. Enter:
 - For .txt: `sudo chmod o+rwx /Library/Security/PolicyBanner.txt`
 - For .rtf: `sudo chmod -R o+rwx /Library/Security/PolicyBanner.rtf`
8. At the prompt, enter your password.
9. Quit Terminal.

Test the Policy Banner

10. Restart.
11. Before the login window, you should see the policy banner appear:



12. Select the *Accept* button.
13. Continue log in as normal.

6.4 Review Questions

1. Name the six different types of user accounts available in macOS.
2. The maximum number of Root accounts available on macOS is _____.

3. By default, is Root enabled or disabled?

4. Which user accounts may assume the powers of Root?

5. In what ways are Administrator accounts different than the Standard, Sharing, and Guest accounts?

6. How many Guest accounts are available on macOS?

7. Root may be enabled from the _____ System Preference.

8. The first user account to be created is a(n) _____.

9. Application Whitelisting can be enabled with _____.

10. A policy banner must be named _____ or _____.

11. A policy banner must be located _____.

7 Storage Device

I am disturbed by how states abuse laws on Internet access. I am concerned that surveillance programs are becoming too aggressive. I understand that national security and criminal activity may justify some exceptional and narrowly tailored use of surveillance. But that is all the more reason to safeguard human rights and fundamental freedoms.

–Ban Ki-moon¹, Secretary General of the United Nations

¹ https://en.wikipedia.org/wiki/Ban_Ki-moon

7.1 Block Access to USB, FireWire, or Thunderbolt Storage Devices

In some environments, it is appropriate to block access to USB, FireWire, or Thunderbolt storage devices. This may be required so that users cannot copy sensitive data. There are two ways to accomplish this:

- Disable the software controlling USB, FireWire, or Thunderbolt storage devices. Advantages: Free, takes a minute to accomplish. Disadvantages: Difficult to undo, impacts all users equally.
- Install a utility to control access. We recommend *DeviceLock*². Advantages: Granular control over any storage device from thumb drive to iPhone, controllable user by user. Disadvantages: Must be run from a Windows computer to control macOS, OS X and Windows clients.

7.1.1 Assignment: Disable USB, FireWire, and Thunderbolt Storage Device Access

Within a few rarified, high-security environments, it is necessary to ensure that users are unable to use USB or FireWire storage devices. This can be accomplished by removing the drivers for such devices

1. Log in as Root.
2. Navigate to the */System/Library/Extensions* folder.
3. Rename *IOUSBMassStorageClass.kext* to *IOUSBMassStorageClass.kext.disabled*.
4. Rename *IOFireWireSerialBusProtocolTransport.kext* to *IOFireWireSerialBussProtocolTransport.kext.disabled*.
5. Rename *IOThunderboltFamily.kext* to *IOThunderboltFamily.kext.disabled*.
6. Reboot.

² <http://www.devicelock.com>

7. Connect either a USB or FireWire storage device to the computer. Note that it will not mount, and that no user has access.

You have successfully blocked any user on this computer (including yourself, all administrators, and even root) from being able to “steal” data from this computer onto any USB, FireWire, or Thunderbolt storage device.

7.1.2 Assignment: Re-enable USB, FireWire, and Thunderbolt Storage Device Access

1. Log in as Root.
2. Navigate to the */System/Library/Extensions* folder.
3. Rename *IOUSBMassStorageClass.kext.disabled* to *IOUSBMassStorageClass.kext*.
4. Rename *IOFireWireSerialBusProtocolTransport.kext.disabled* to *IOFireWireSerialBussProtocolTransport.kext*.
5. Rename *IOThunderboltFamily.kext.disabled* to *IOThunderboltFamily.kext*.
6. Reboot.
7. Connect either a USB, FireWire, or Thunderbolt storage device to the computer. Note that it will now mount, and all users have access.

You have successfully returned your computer to default functionality.

7.2 FileVault 2 Full Disk Encryption

Strong passwords keep the network and Internet-based password attacks at bay, but should someone have physical access to your computer, they may be able to perform a brute force attack on your login password.

Prior to Mac OS X 10.7, the system included home directory encryption using *FileVault*, now referred to as *Legacy FileVault*. This was enabled on a user-by-user basis.

Starting with Mac OS X 10.7, and continuing with macOS, we now have FileVault 2³ (normally referred to as simply *FileVault*), which enables military-grade full disk encryption. With FileVault configured, your drive has a secure wall around it that can only be penetrated by entering an account password.

Once FileVault has been enabled, it may take 1–5 days for the encryption to complete on a spinning hard disk drive, as little as 30 minutes on a Solid State Drive or Flash Drive. During this time, you can continue working normally, although your computer may be sluggish as it is doing both your work and the encryption process.

Enabling FileVault has an additional advantage: Boot time keyboard commands require authenticating at the Login Window. This has significance for three keyboard commands.

Target Disk Mode

Target Disk Mode (TDM) allows booting with macOS functionally disabled, with only Firewire and Thunderbolt active for storage devices. This effectively turns the computer into an external drive that can connect via Firewire or Thunderbolt.

Recovery HD Mode

Recovery HD Mode allows booting into the otherwise invisible Recovery HD partition, to perform directory repair with Disk Utility, reinstall macOS, enable Firmware password, etc.

Single-User Mode

³ <http://en.wikipedia.org/wiki/FileVault>

Single-User Mode allows booting into a command line state, prior to loading of Open Directory (the database holding all user accounts) and the entire OS. In this state, only the Root user account is active, hence the term *Single-User Mode*.

7.2.1 Assignment: Boot Into Target Disk Mode

In this assignment you will boot into Target Disk Mode (TDM).

1. Power off your computer.
2. Power on your computer, and then immediately (before the appearance of the Apple logo) hold down the *T* key, and keep held down.
3. If your computer does not have FileVault enabled, skip to step 4. If FileVault is enabled:
 - a. The login window will appear.
 - b. Release the *T* key.
 - c. Select your account, enter your password, and then tap the Return/Enter key.
4. The Firewire or Thunderbolt icon will appear moving around your screen. You are now in TDM.
5. To verify this, you may connect your computer to another Mac via Firewire or Thunderbolt, and it will mount on the other computer.
6. To exit TDM, press and hold the power button to power off, and then power on as normal.

7.2.2 Assignment: Boot Into Recovery HD Mode

In this assignment you will boot into Recovery HD Mode.

1. Power off your computer.
2. Power on your computer, and then immediately (before the appearance of the Apple logo) hold down the *cmd + R* keys, and keep held down.

3. If your computer does not have FileVault enabled, skip to step 4. If FileVault is enabled:
 - a. The Login Window appears.
 - b. Release the cmd + R keys.
 - c. Select your account, enter your password, and then tap the Return/Enter key.
4. The Recovery HD home screen will appear, displaying a list of available *Utilities*.
 - a. If you wish, you may experiment with the various utilities.
5. To exit Recovery HD Mode, select the *Apple* menu > *Restart*.

7.2.3 Assignment: Boot Into Single-User Mode

In this assignment you will boot into Single-User Mode.

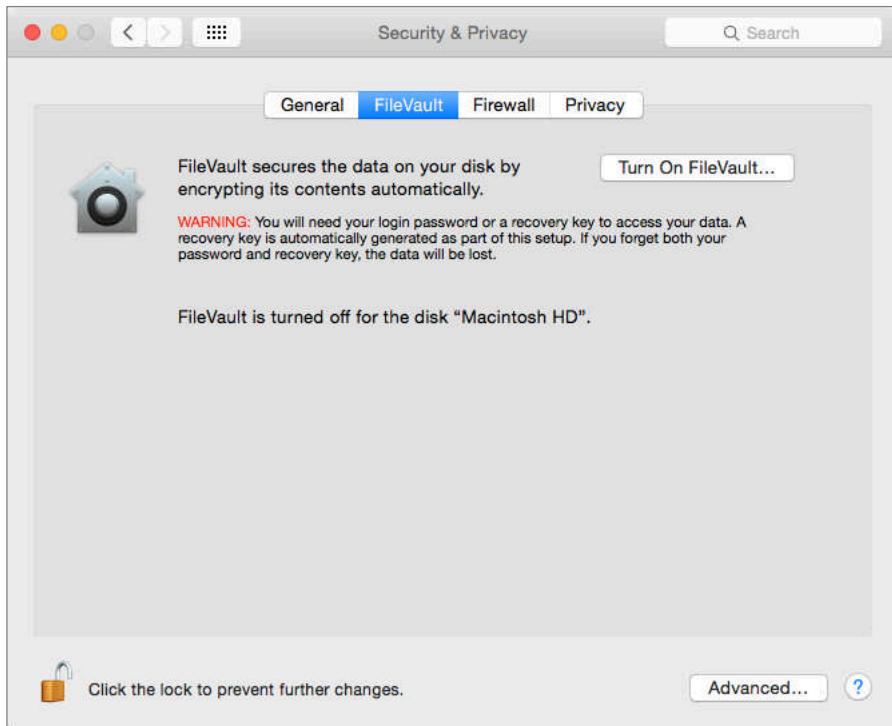
1. Power off your computer.
2. Power on your computer, and then immediately (before the appearance of the Apple logo) hold down the cmd + S keys, and keep held down.
3. If your computer does not have FileVault enabled, skip to step 4. If FileVault is enabled:
 - a. The Login Window appears.
 - b. Release the cmd + S keys.
 - c. Select your account, enter your password, and then tap the Return/Enter key.
4. The Single-User Mode screen will appear, displaying a list all of the commands and activity that is occurring.
5. Within a minute or so the scrolling list of activity will stop at a command line prompt. If you are familiar with Linux, Unix, or the bash shell, you can issue commands and look around the drive from here .

6. To exit Single-User Mode, enter *exit* at the prompt, and then tap the Return/Enter key. The system will continue to the normal login window.

7.2.4 Assignment: Enable and Configure FileVault 2

In this assignment you will enable full disk encryption using FileVault 2.

1. Open *Apple menu > System Preferences > Security & Privacy*, and then select the *FileVault* tab.



2. Unlock the *FileVault* lock icon.
3. Select the *Turn On FileVault...* button.

4. A dialog box appears to select using either your iCloud account or a recovery key to unlock the disk in the event your login password is forgotten.



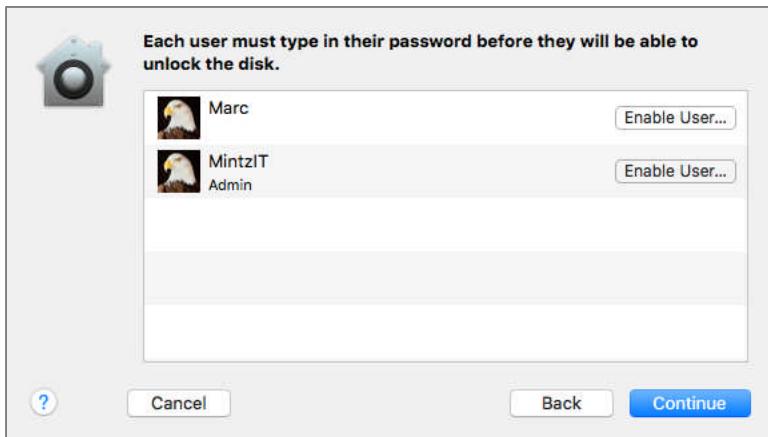
- Selecting *Allow my iCloud account...* allows you to use your iCloud account password to be used, and then select the *Continue* button.
- Selecting *Create a recovery key...* presents a randomly generated password. Store this key in a secure location. I recommend in your Address Book / Contacts application, and then select the *Continue* button.



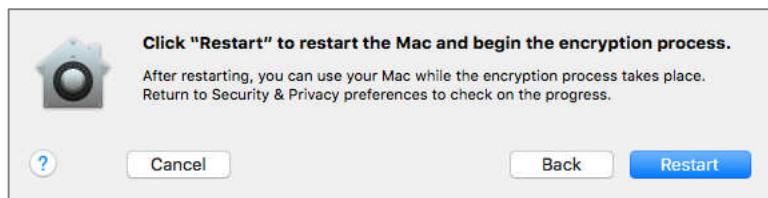
5. If there are multiple user accounts on this machine, you are asked to enable the user accounts that are to be allowed to unlock the encrypted boot drive to boot up. For each of these accounts, click the *Enable User...* button, and enter the account password. (Users that have not been enabled can still access their

7 Storage Device

accounts via *Fast User Switching* after the drive is unlocked by one of the authorized accounts.) Then click *Continue*.



6. Select the Restart button to restart the Mac and begin the encryption process.



7. When your Mac returns to the Desktop, the *Security & Privacy* preference window will reopen, providing a progress indicator for the encryption process. You may close this window if desired.

The encryption process may take as little as an hour (small flash drive in a MacBook Air), or more than a day (4TB hard disk drive in an older, slower computer.) Though encryption will start again after the computer has been sleeping or turned off, to have it complete faster, set *Energy Saver* System Preferences to *Never Sleep*.

Enabling FileVault 2 is only half of the solution. The other half is to enable the Firmware Password. More on that later.

7.3 FileVault Resistance to Brute Force Attack

Apple claims there is no back door or golden key to FileVault 2. If there is a way to hack into a FileVault-protected volume, only one group is laying claim to it.

*Passware*⁴ says their software is capable of breaking into a FileVault 2 drive in 40 minutes. The author has not tested this claim.

It is recommended that in addition to using FileVault to encrypt the drive, the EFI chip (firmware chip) on the motherboard also have a password in place. More on that later.

⁴ <https://www.passware.com/>

7.4 Remotely Access and Reboot a FileVault Drive

When a drive is protected with FileVault, remote support that requires a reboot may become an issue. The reason is that the macOS will reboot into an encrypted mode, which most remote support software cannot communicate with. So, once the technician has rebooted the machine, they have lost control over it.

A workaround for this situation is to temporarily disable FileVault. This can be done using the Terminal to enter the appropriate command.

7.4.1 Assignment: Temporarily Disable FileVault

In this assignment, you will temporarily disable FileVault during a macOS restart. This will allow remote support software to regain control over the computer after a restart.

- Prerequisite: The computer must have the Root user account enabled, and you must know the Root password.
1. Login to an administrative account.
 2. Open Terminal.app.
 3. Enter the command: `sudo fdesetup authrestart`
 4. At the authentication prompt, enter your administrative password.
 5. At the prompt: *Enter a password for '/', or the recovery key*, enter the Root password.
 6. The computer will restart with FileVault disabled.
 7. At the login screen, enter your *user name* and *password*.
 8. On the next boot, FileVault will be enabled.

7.5 Review Questions

1. To disable access to USB, Firewire, or Thunderbolt storage devices, the kext files may be removed or renamed from which folder?
2. Explain the fundamental difference between the original FileVault (now called Legacy FileVault), and FileVault 2 (now called FileVault).
3. FileVault 2 may be enabled from which System Preference?
4. Describe how to enable Single-User Mode.
5. What does Single-User Mode do?
6. Describe how to enable Target Disk Mode.
7. What does Target Disk Mode do?
8. Describe how to enable Recovery HD Mode.
9. What does Recovery HD Mode do?

8 Sleep and Screen Saver

Do not take life too seriously. You will never get out of it alive.

—Elbert Hubbard¹, American writer, publisher, artist, and philosopher

¹ https://en.wikipedia.org/wiki/Elbert_Hubbard

8.1 Require Password After Sleep or Screen Saver

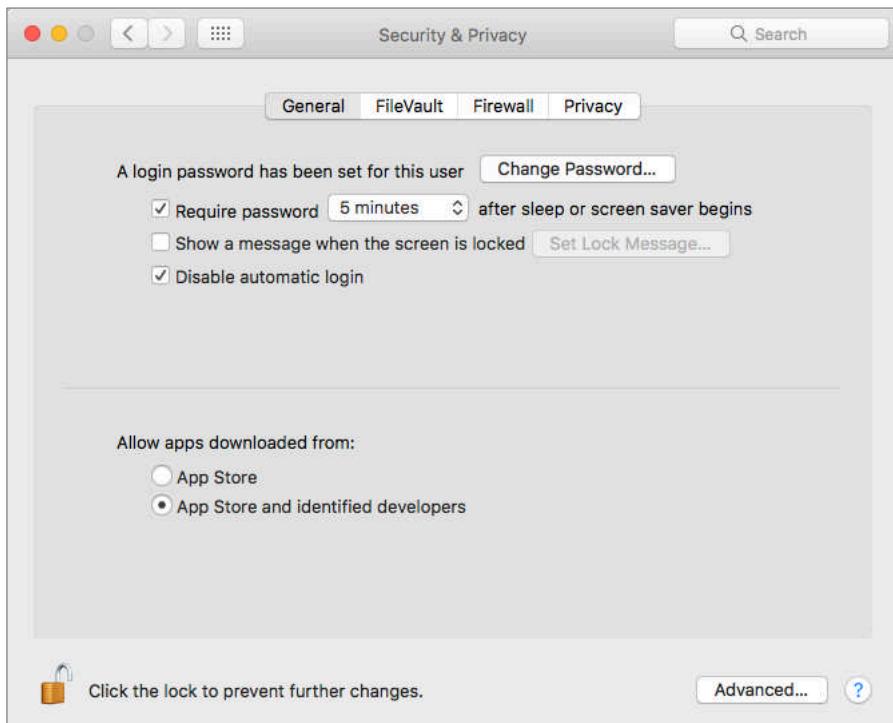
When not using a powered-on computer, by default it will remain on. It is a trivial task for someone else to sit down in front of the computer and access all your data.

To help prevent this, configure your computer to lock down after a short period of inactivity (5-15 minutes), or upon command.

8.1.1 Assignment: Require Password After Sleep or Screen Saver

In this assignment, we will configure the computer to go into screen saver mode after 5 minutes of inactivity, and to require entering a password to remove the screen saver.

1. Open *Apple menu > System Preferences > Security & Privacy > General tab.*

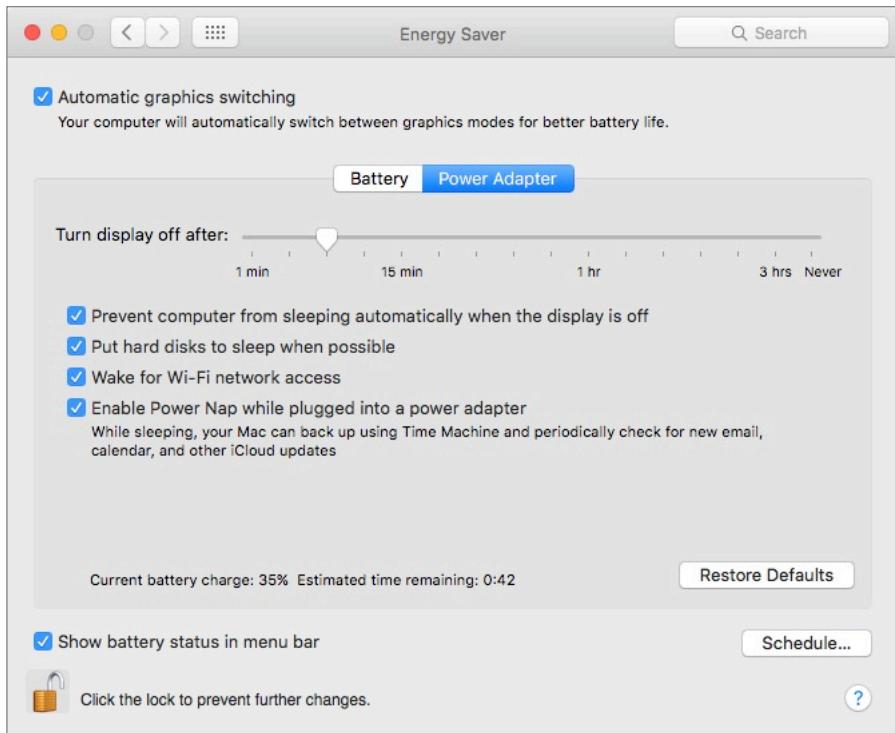


2. Click the Lock icon, and then authenticate as an administrator.
3. Enable and then set the *Require password* after sleep or screen saver begins to 5 seconds. This provides a time buffer in the event your computer goes to sleep while you are at it. All you need do is move the mouse to wake it up within 5 seconds.
4. Enable *Disable automatic login*. How many nights of sleep will you lose should a thief take your computer, and all that is needed to access your data is to power it on?
5. Configure *Allow apps downloaded from*:
 - *Mac App Store*. This is the most secure setting. Apple performs diagnostics on apps sold through the App Store to verify being free from malicious code. It is also the most restrictive, as not all apps are available from the App Store.
 - *Mac App Store and identified developers*. Though less secure than the previous setting, it is better than the proverbial stick in the eye. This allows apps from developers that are a member of the Apple Developer Connection² to run on your computer. Though Apple has not vetted their software, at least you know they haven't been exiled by Apple for distributing malicious code.
6. From the toolbar, select the *Show All* button, and then select the *Energy Saver* preference.

² <https://developer.apple.com>

8 Sleep and Screen Saver

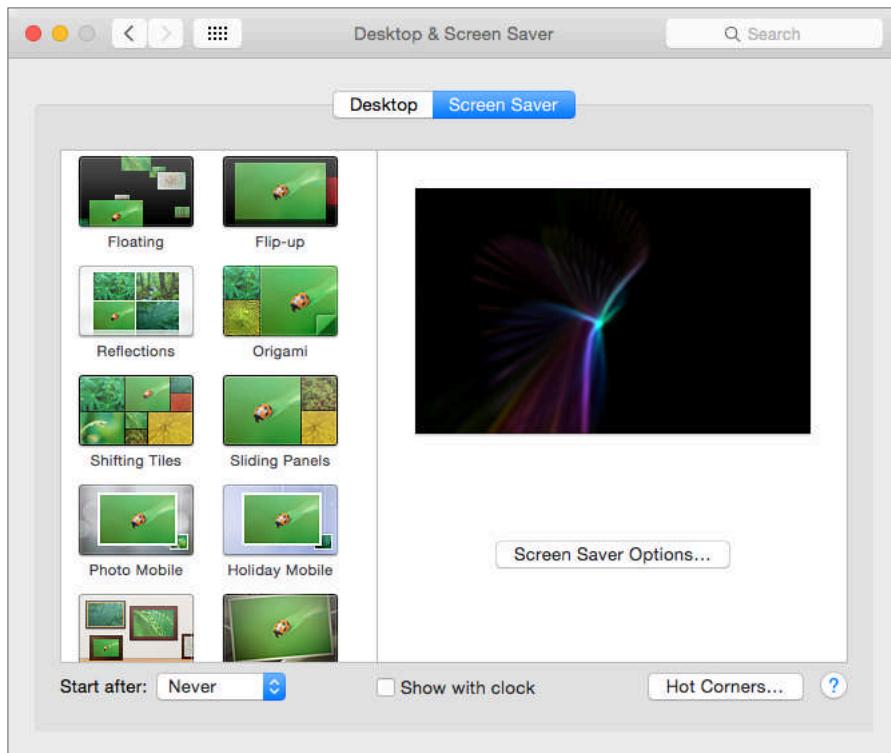
7. Set *Display sleep* to 5 minutes. This provides a minimal window of opportunity for someone to view your screen or gain access to your system should you step away from your computer.



8. From the toolbar, select the *Show All* button.

8 Sleep and Screen Saver

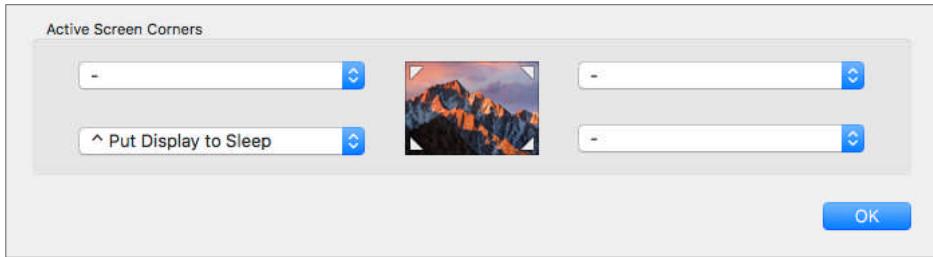
9. Select the *Desktop & Screen Saver* preference, and then the *Screen Saver* tab.



10. Select the *Hot Corners* button.
11. Select one of the four corners pop-up menus, and then select either *Put Display to Sleep* or *Start Screen Saver*. Either option will immediately put your

computer into lock down mode the moment your cursor is pushed to that corner. Then select the *OK* button.

- Note: In the example below I held down the Control key while making my corner selection, which is reflected in the image.



12. Quit System Preferences.
13. Test your new setting by pushing your cursor into that corner. Leave the cursor there for 5 or more seconds, and then move the cursor. You should be presented with an authentication screen.
 - Note: If following my example of holding down the Control key while creating the setting, you will need to hold down the Control key when moving the cursor to the corner.
14. Enter your password to unlock your computer and return to work.

You have successfully enabled lockdown of your system with sleep or screensaver.

8.2 Review Questions

1. Where can you configure requiring a password after sleep or screen saver?

9 Malware

Behind every great fortune lies a great crime.

–Honore de Balzac¹, 19th-century novelist and playwright

¹ https://en.wikipedia.org/wiki/Honoré_de_Balzac

9.1 Anti-Malware

Most people know this category of software as Antivirus, but there are so many other nasty critters out there (worms, Trojan horses, phishing attacks, malicious scripts, spyware, etc.) that the overarching term “Anti-Malware” is more accurate.

Depending on how one chooses to measure, there are from 500,000–40,000,000 malware² in the field that impact Windows. Currently there are fewer than 300 that specifically target macOS, but this number pales compared to the malware that impacts Windows, macOS and OS X through scripts, Adobe Flash, Java, JavaScript, malicious websites, email phishing, etc.

macOS and OS X 10.7 and higher includes several automatically updating system-level architectures designed to help prevent malware from getting a foothold. Although Apple has done a good job here, they can do better. These invisible utilities only protect against known macOS/OS X malware, and Apple has been slow to update when new malware shows up.

Should we care about Windows malware? Yes. Not that Windows-specific malware will hurt you. Well, it will if you have Boot Camp or any virtual machine running another OS. But it is probable that at some point you will inadvertently pass windows malware along to a friend or business associate that is using Windows. Imagine how your relationship will change should an email from you take down a friend’s computer, or a customer’s entire network.

It is for these reasons that I strongly recommend the installation of quality anti-malware on all macOS machines. This raises the question of how to know that an anti-malware is quality software? We go by the results of independent testing organizations. These include AV TEST³ and ICSA Labs⁴. One of the most recognized is AV Comparatives⁵ (AVC). Although no testing organization tests all of the 100+ anti-malware products on the market, AVC tests the major players at least a few times each year against a wide range of the current bugs. The results of

² <http://en.wikipedia.org/wiki/Malware>

³ <https://www.av-test.org/en>

⁴ <https://www.icsalabs.com/technology-program/anti-virus>

⁵ <http://av-comparatives.org>

their Windows anti-malware product tests are made public on their website⁶. The report on macOS/OS X anti-malware product tests is also available⁷.

In their most recent testing of macOS/OS X anti-malware products, most of the tested software caught all of the OS X malware. So the deciding factors come down to ease of use, resource utilization (impact on computer performance), and ability to catch Windows malware.

The only product we currently recommend for macOS/OS X and Windows home and business users is Bitdefender⁸. This is due to their first-rate ability to recognize and remove macOS/OS X and Windows malware, simple interface, low impact on computer performance, and macOS, OS X, and Windows versions are available. If you have more than a few computers, you can upgrade to their business version which can be centrally administered from a cloud-based console. This option is called *Gravity Zone*.

For macOS users running Windows in Boot Camp or in a Virtual Machine environment such as VMware Fusion or Parallels, you will also need a Windows anti-malware product. Though Microsoft provides a free option, by most independent testing reports, it is capable of catching only 80% of known malware. This is about the same as leaving for vacation after locking the front door, but leaving the back door wide open.

⁶ <http://www.av-comparatives.org/comparatives-reviews/>

⁷ <http://www.av-comparatives.org/mac-security-reviews/>

⁸ <http://www.bitdefender.com/>

9 Malware

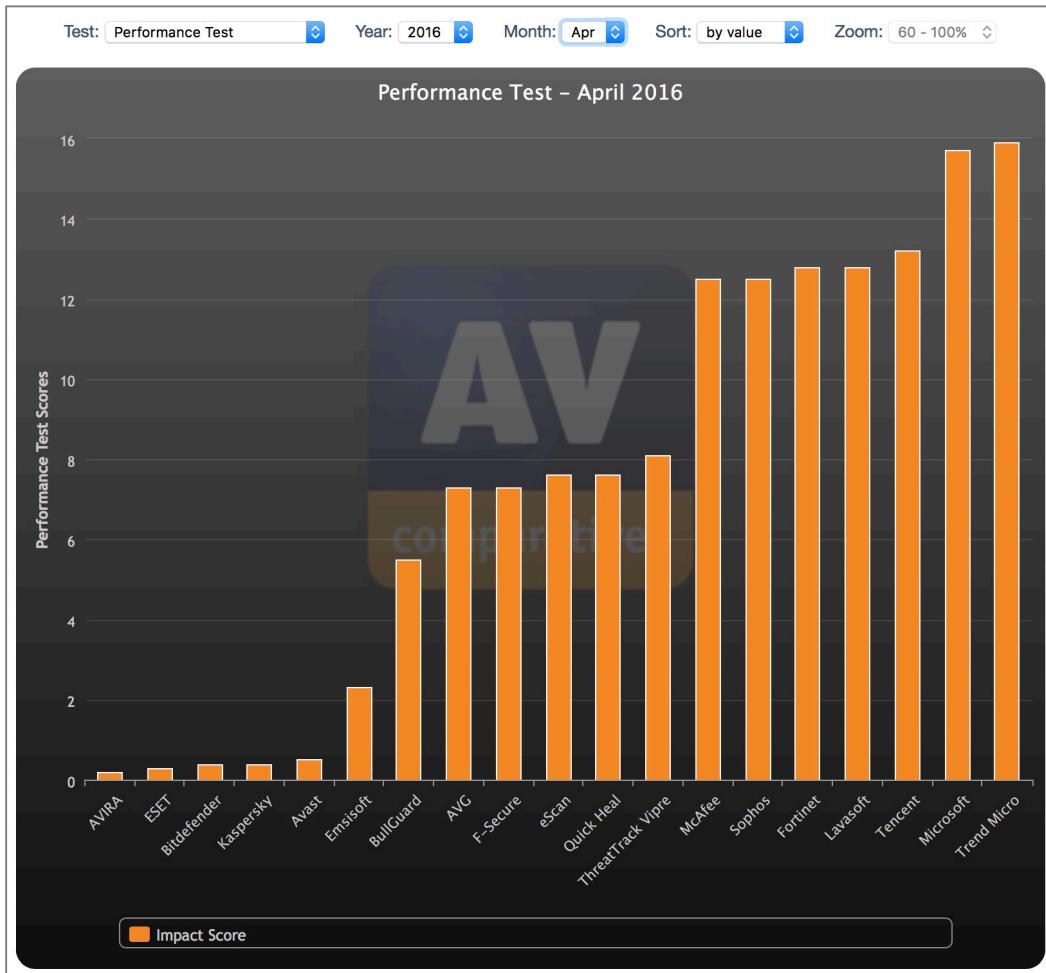
Turning to AVC for guidance, here is their chart on effectiveness of catching and removing malware from Windows:



As of this writing, the top contenders for effectiveness at 100% are Bitdefender, Vipre, and Trend Micro. But effectiveness isn't the only important measurement. In this same chart we can see false-positives. It's a sad day when a clean file is flagged as infected and then automatically trashed. Of the leading brands, only Bitdefender and Kaspersky, have zero false positives, with Avira at one.

9 Malware

Another vital measurement is performance—the impact the anti-malware has on overall performance of your computer. Anti-malware should use as little system resources as possible.



AV-Comparatives performs separate testing for macOS/OS X anti-malware products⁹. For reasons only known to the organization, they do not conduct as

⁹ http://www.av-comparatives.org/wp-content/uploads/2015/07/avc_mac_2015_en.pdf

thorough testing for the macOS/OS X products as they do for Windows. A summary of product testing is provided by AV-Comparatives below.

Product	Mac Malware Protection (105 recent samples)	Windows Malware Detection (1,000 most-prevalent samples)
Avast Free Mac Security	100%	100%
AVG AntiVirus for Mac	100%	100%
AVIRA Free Antivirus for Mac	99%	100%
Bitdefender Antivirus for Mac	99%	100%
ESET Cyber Security Pro	100%	100%
F-Secure SAFE for Mac	100%	28%
Intego Mac Premium Bundle X8	100%	50%
Kaspersky Internet Security for Mac	100%	100%
Kromtech MacKeeper	98%	97%
Sophos Anti-Virus for Mac	100%	100%

As with any research, don't use just one set of data points. The "winners" and "losers" will jostle for position on a monthly basis.

9.1.1 Assignment: Install and Configure Bitdefender

In this assignment, you will download, install, and configure Bitdefender Antivirus for Mac.

- Note: If you have more than a few computers, or are running business computers, I strongly recommend you seek out a Bitdefender partner for assistance to set up a Gravity Zone account.

Download Bitdefender Antivirus for Mac

1. Using your favorite browser, visit *Bitdefender.com*.

9 Malware

2. In the navigation bar, click *Home Users > Bitdefender Antivirus for Mac*.

The screenshot shows the Bitdefender website's main navigation bar at the top, featuring links for Resource Center, Support, Company, and Login to Central. Below the navigation bar, there are three dropdown menus: Home Users, Business Solutions, and Partners. A search icon is also present.

The main content area is divided into several sections:

- Solutions**: Includes links for Bitdefender BOX (internet of things), Bitdefender Total Security, Multi-Device 2016, Bitdefender Internet Security 2016, Bitdefender Antivirus Plus 2016, Compare solutions, Bitdefender Security for Windows 10, Bitdefender Family Pack 2016, Bitdefender Mobile Security, and Bitdefender Antivirus for Mac. There is also a link to View all solutions.
- Useful links**: Includes Compare solutions, Trial Downloads, and links for Already a customer? (Renew & Upgrade, Login to Central, Home Users Support).
- Bitdefender services**: Includes Tech Assist: Live services performed by experts, Bitdefender Install & SetUp, Bitdefender PC Optimizer, Bitdefender Virus & Spyware Removal, and Bitdefender System Repair. There is also a link to View all services.
- Toolbox**: Includes links for Free Antivirus, Free Online Virus Scanner, Antivirus Free for Android, and Free Virus Removal Tools.

A sidebar on the right side of the page features several vertical panels with text and icons:

- our digital life
- ulti-device!
- for Mac
- der Box
- o your comfort zone

At the bottom of the page, there is a promotional banner for Bitdefender BOX, which is described as "Security for your Internet of Things". It includes a "LEARN MORE" button and an image of various IoT icons like a smart lock, a monitor, and a shield.

3. Select the *Try a 30-Day Trial Now* link.

The screenshot shows the Bitdefender Antivirus for Mac product page. At the top, there's a navigation bar with links for 'Resource Center', 'Support', 'Company', 'Login to Central', and language selection ('EN'). Below the navigation is a shopping cart icon showing '0' items and a globe icon for international access. The main content features a large image of the Bitdefender Antivirus for Mac software box, which has a futuristic, glowing blue and purple wolf head design. To the right of the box, the product name 'Bitdefender ANTIVIRUS FOR MAC' is displayed in large, bold letters, with the tagline 'Absolute Protection. Designed for Mac.' underneath. A list of features is shown with checkmarks:

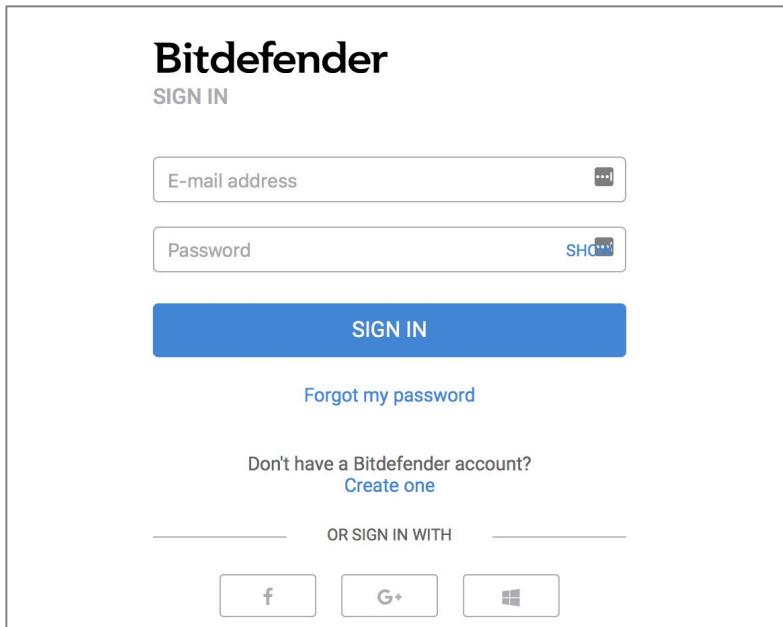
- Blocks and removes annoying adware
- Zero negative impact on speed
- Provides non-stop protection with Bitdefender Autopilot™
- Secures your online shopping experience
- Protects against Mac and PC malware
- Delivers 24/7 Cloud-based guard duty

On the right side, there are dropdown menus for 'Number of MACs' (set to 'up to 3 Mac') and 'Validity' (set to '1 Year'). Below these is a total price of '\$59.95'. A prominent orange 'BUY NOW' button is at the bottom, with the note 'Tax Included' underneath it.

4. Enter your email address, and then click the *Activate Your Free Trial* button.

This screenshot shows the trial activation page for Bitdefender Antivirus for Mac. On the left, there's a form to enter an email address, with a note that users will receive installation steps via email. Below the form is a green button labeled 'ACTIVATE YOUR FREE TRIAL'. On the right, a red banner says 'You've Just Unlocked An Offer For Our Trial Users'. Below the banner, a large offer is presented: 'Buy 1 Year and Get 1 Year FREE!'. There's an image of the software box again, and a green 'GET IT NOW' button. A small note at the bottom right mentions a '30 day money back guarantee'.

5. Check your email for the link from Bitdefender. Click the link to authenticate. You will be taken to the Bitdefender Central to login. Enter your email address and password, and then click the *Sign In* to login.

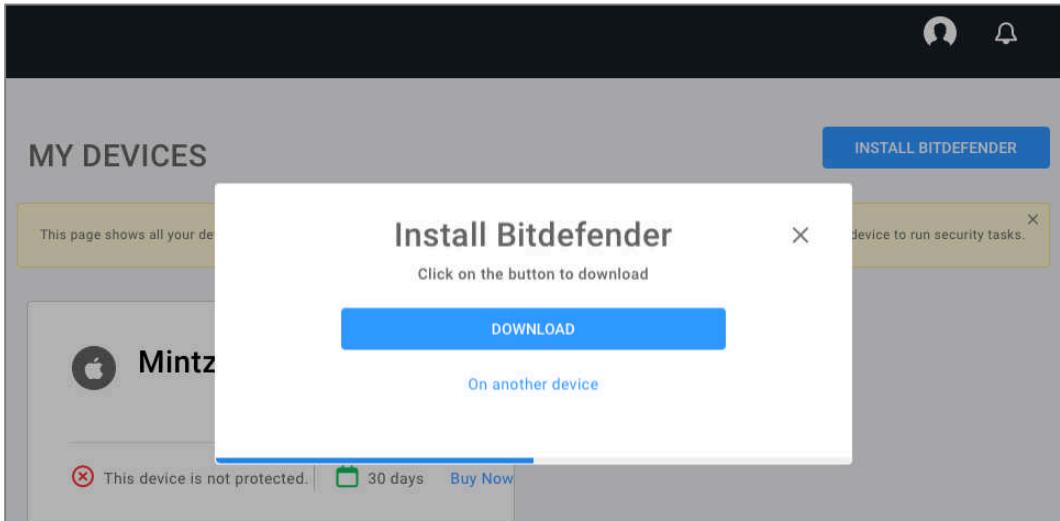


6. At the *My Devices* window, click the *Install Bitdefender* button.

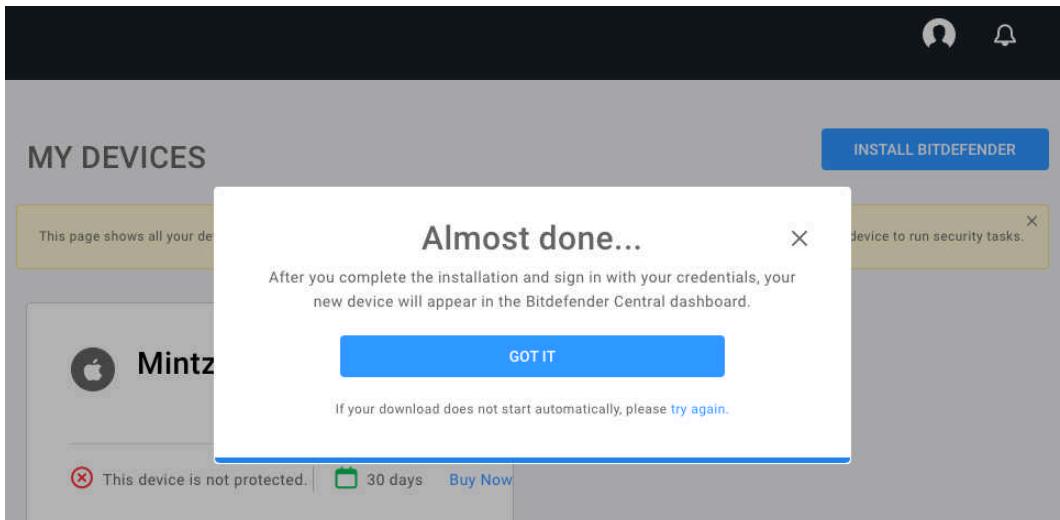
A screenshot of the Bitdefender Central 'MY DEVICES' section. At the top, there's a dark header with a menu icon, user profile, and notification bell. Below it, the 'MY DEVICES' title is displayed. On the right, a blue 'INSTALL BITDEFENDER' button is visible. A yellow callout box contains the text: 'This page shows all your devices currently protected by Bitdefender. Add more devices by clicking the top-right button. Click on a device to run security tasks.' Below this, a device card for 'MintzIT's iMac' is shown. The card includes an Apple icon, the device name, a three-dot menu icon, and a status message: 'This device is not protected.' with a red 'X' icon. It also shows a calendar icon with '30 days' and a 'Buy Now' button.

9 Malware

- At the *Install Bitdefender* window, click the *Download* button.

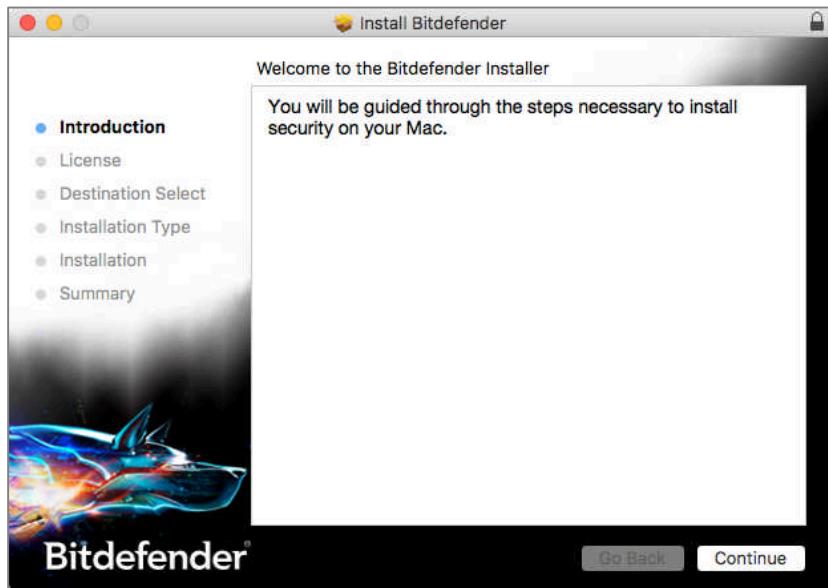


- At the *Almost done...* windows, click the *Got It* button.

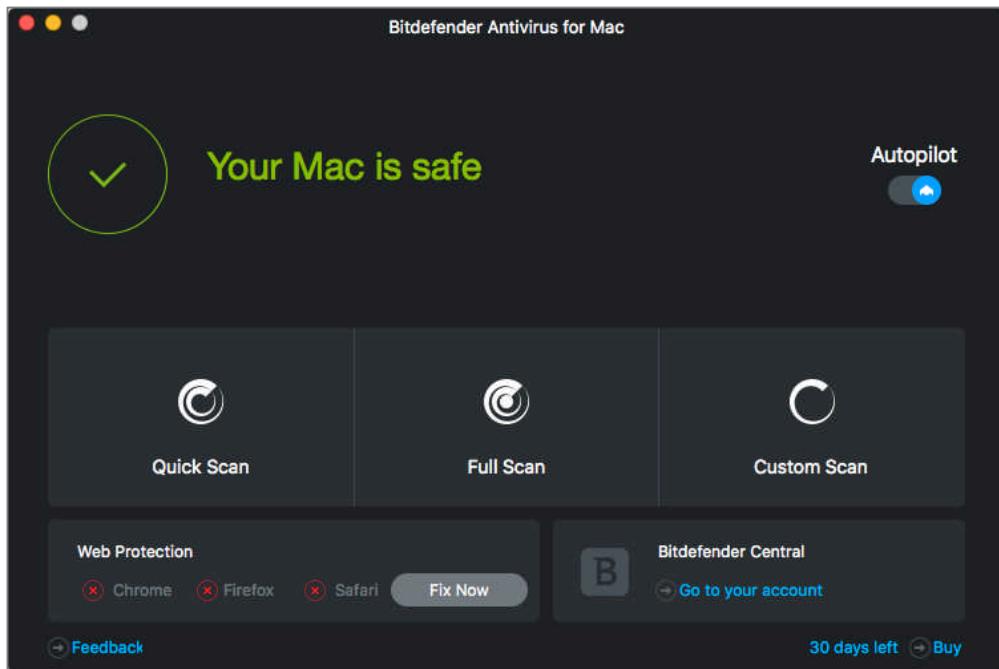


- Double-click the downloaded installer. It will mount and open a virtual disk on your Desktop. Launch the installer.

10. Follow the on-screen instructions to install Bitdefender.

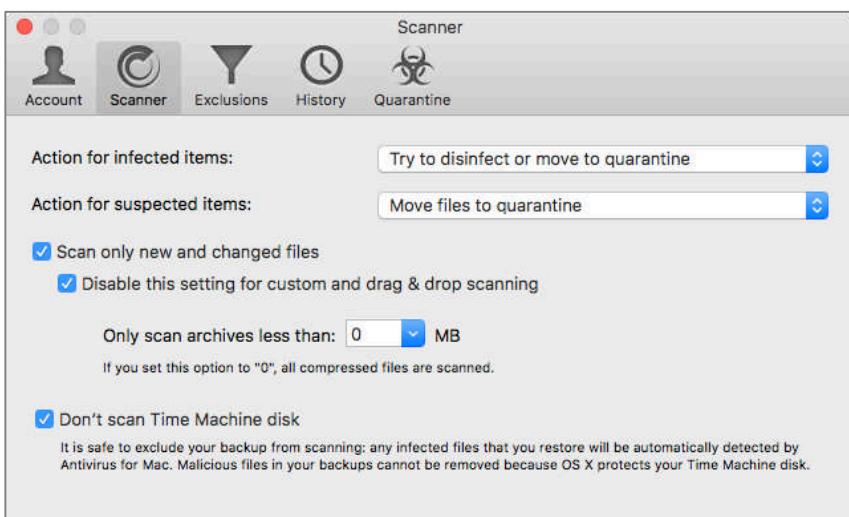
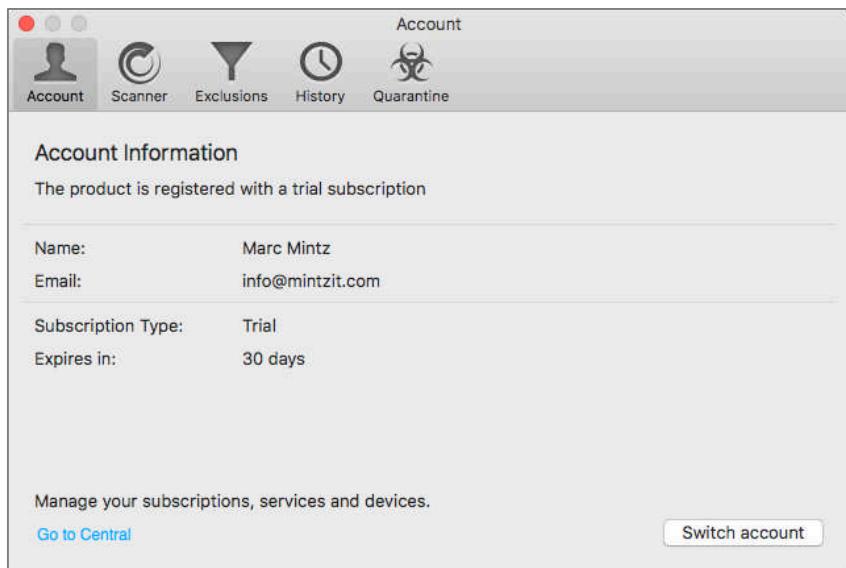


11. Once installed, Bitdefender Antivirus for Mac will open.

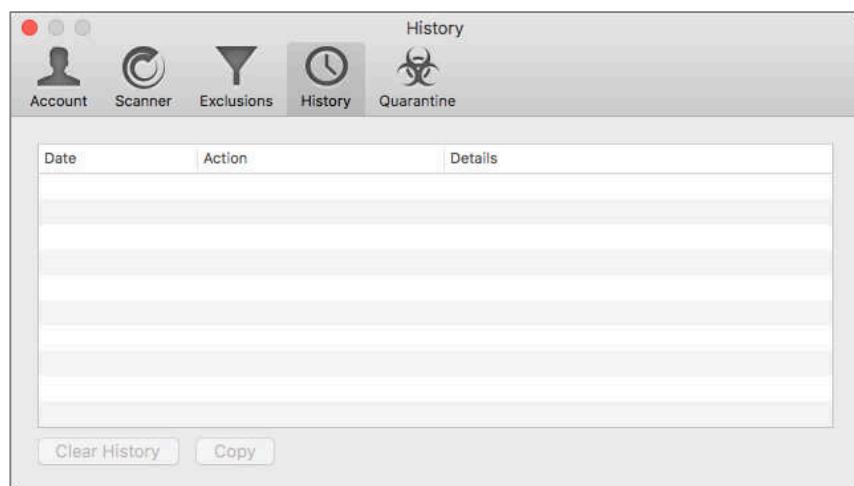
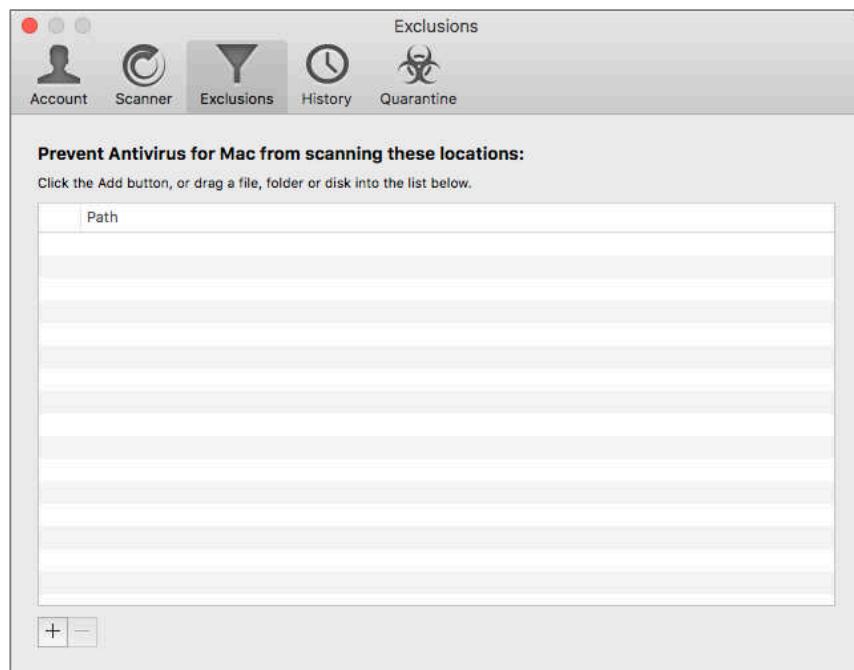


9 Malware

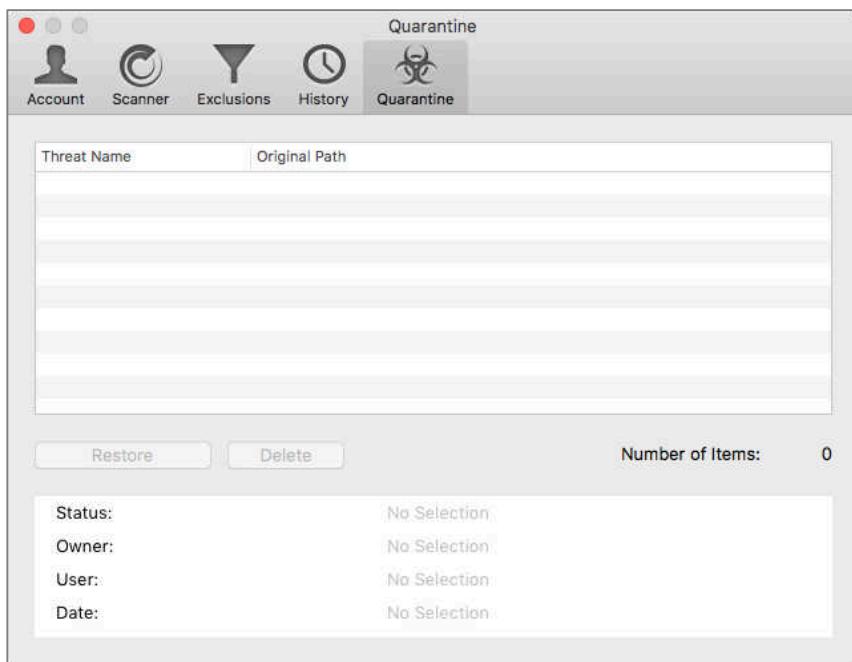
12. To configure, select the *Antivirus for Mac* menu > *Preferences*, and then select *Account* from the toolbar. We recommend the following configurations.



9 Malware

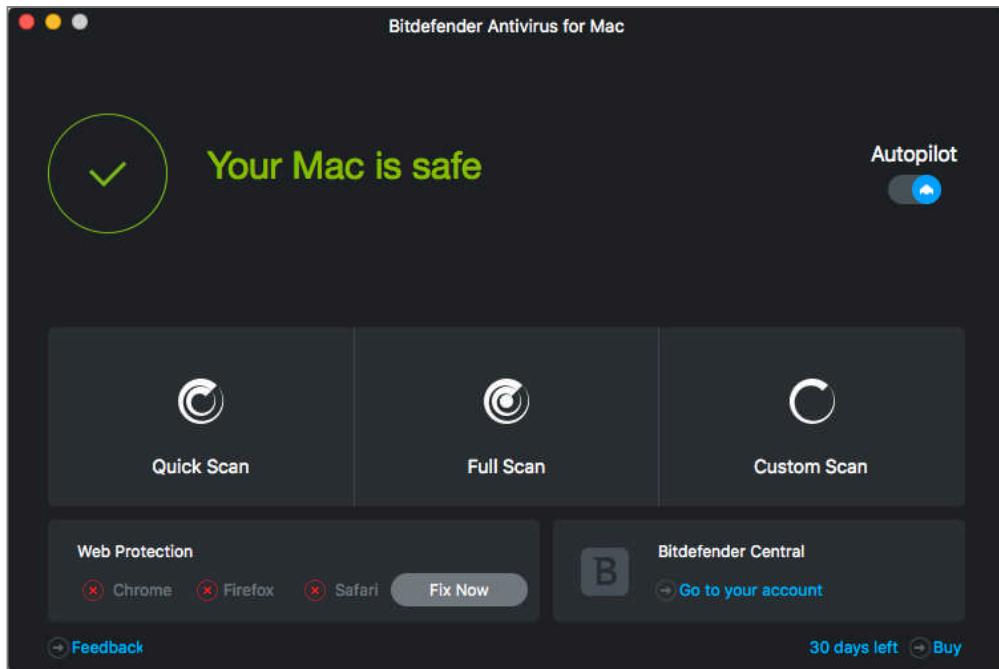


9 Malware

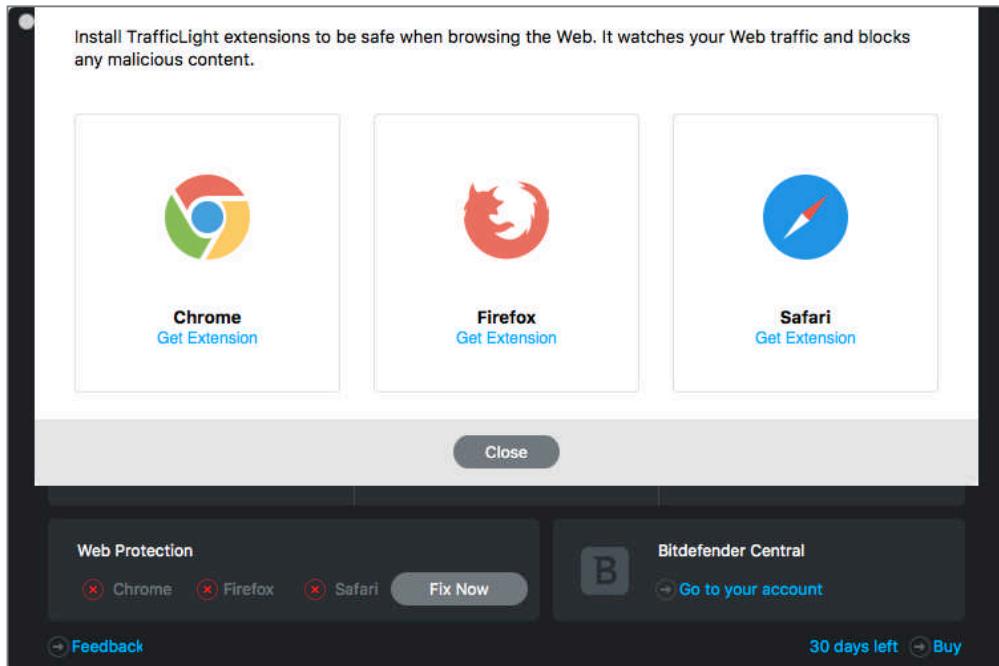


13. Close the *Preferences* window.
14. *Bitdefender Antivirus for Mac* includes *TrafficLight* to watch over your web browsing. *TrafficLight* is also available for free for Safari, Firefox, and Chrome as extensions/plug-ins. It will alert if a site is potentially dangerous, and

inform what is tracking your browsing. To enable *TrafficLight*, select the *Fix Now* button in the bottom left area of the main window.

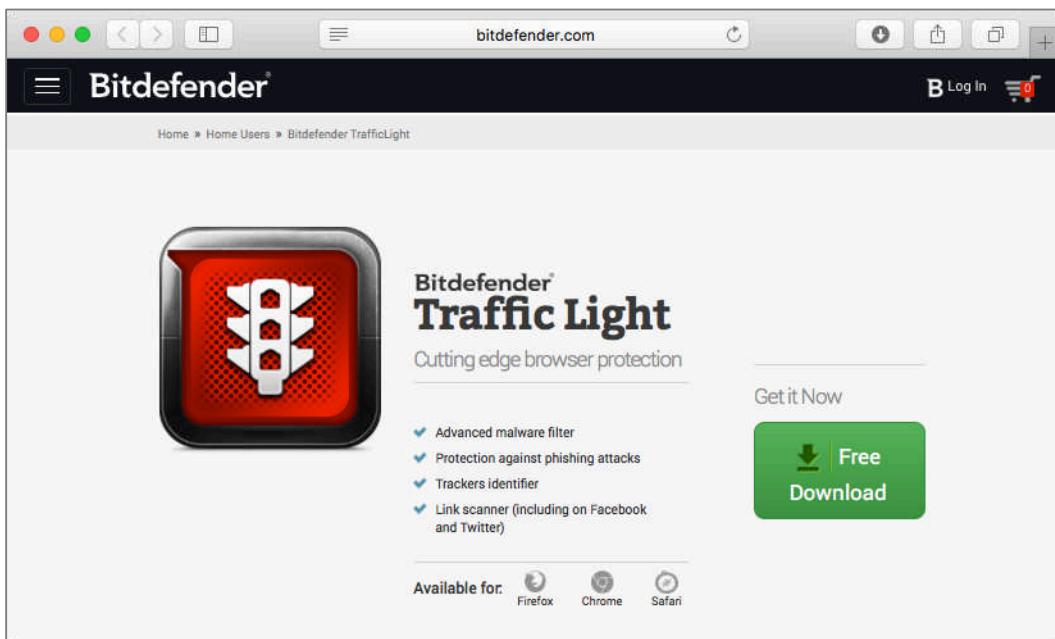


15. *TrafficLight* is an extension available for Safari, Google Chrome, and Firefox. Select the *Get extension* button for each browser you use. First, we will install for Safari. Click the *Safari Get Extension* link.

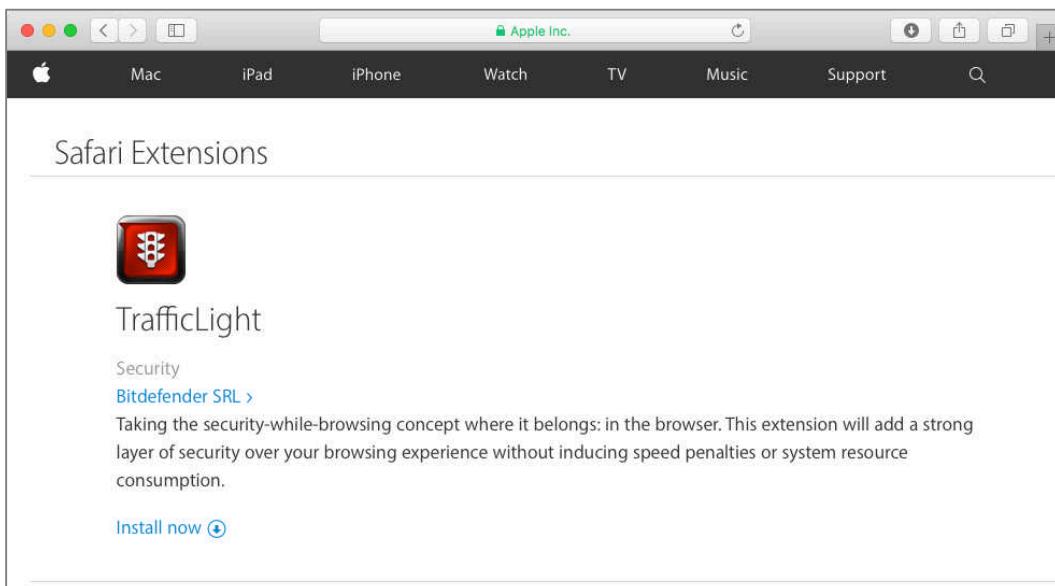


9 Malware

16. From the *TrafficLight* extension webpage, select the *Free Download* button.

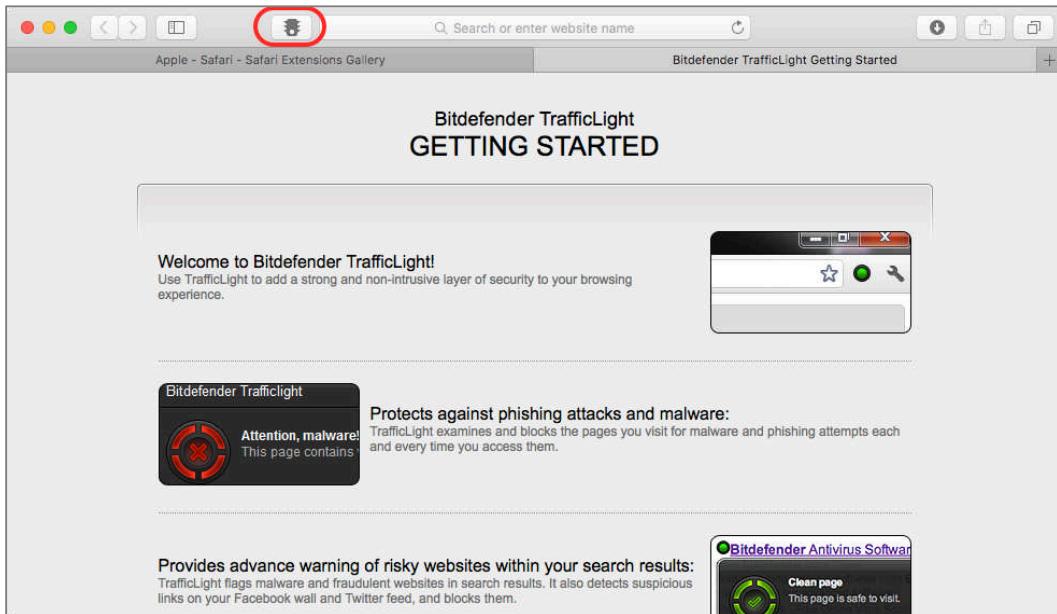


17. At the *Safari Extensions* page, click the *Install Now* link for TrafficLight.



9 Malware

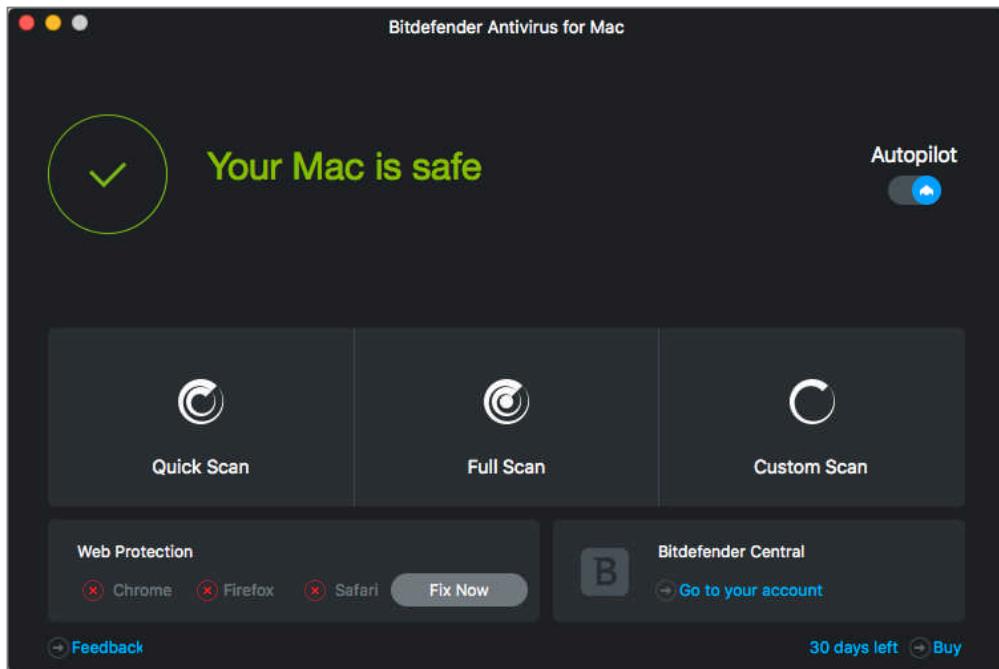
18. TrafficLight will download, install, and then you will be taken to the *Getting Started* page. The TrafficLight icon will display just to the left of the address bar.



19. Repeat these steps for each web browser installed.

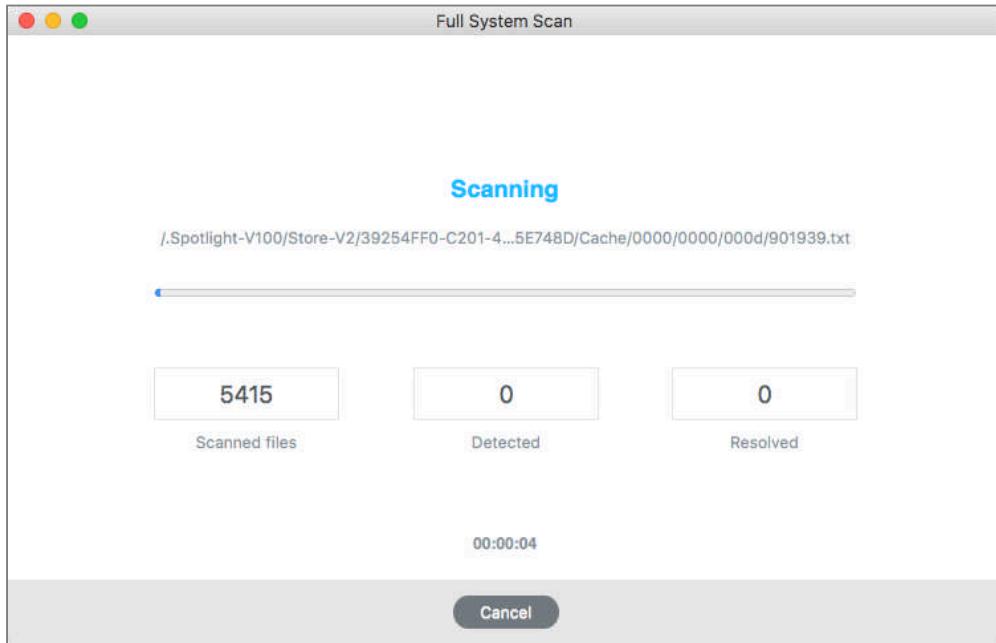
Last step is to perform a full system malware scan. You normally would only need to do this once—right after the first installation of your antivirus software. When this step completes, Bitdefender will scan new files, new emails, and files as they are opened.

20. From the Bitdefender main window, select *Full System Scan*.



9 Malware

21. The *Full System Scan* window opens.



22. When the scan completes, quit Bitdefender.

Congratulations! You have just built a wide moat to keep malware from your computer.

9.2 Review Questions

1. Apple started to include system-level anti-malware beginning with OS X ____.
2. Name a website that independently researches and publishes anti-virus software effectiveness.
3. Name a few of the best anti-virus software for macOS/OS X in terms of both effectiveness and performance, according to this website.

10 Firewall

If you could kick the person in the pants responsible for most of your trouble, you wouldn't sit for a month.

–Theodore Roosevelt¹

¹ https://en.wikipedia.org/wiki/Theodore_Roosevelt

10.1 Firewall

Whenever a computer needs to communicate with the outside world—say, to print, receive or send email, or surf the web—it must *open a door* to that world. In the IT universe this is called *opening a port*.

Ports are numbered from 1–65,535, with at least one port number assigned to any one communication task. For example, when using your browser to visit Google, you enter *https://www.google.com* in the address field. This can be translated into English as: *Using the language of the (secure) Internet (https) I would like to communicate with a server named www, within a domain named google.com.*

The problem is that the www server at Google has 65,535 ports to which it may potentially need to listen. Invisible to the user, :80 is been placed at the end of the address request. This translates into: *And please knock on port 80 (reserved for web server communications) so that www can respond to the web page requests that I send to it.*

To best secure your computer, it is important to only have those ports open that are necessary to perform your work.

The purpose of a firewall² is to block unwanted attempts to get into or communicate with your computer from the network or Internet through your 65,535 ports. It is about as simple as anything gets on a computer, and once activated you likely will never need to know about it again.

To get into your computer or to communicate with it, a few ducks must be lined up.

- Your computer must be on a network with other computers (such as your local area network at home or office, or the Internet).
- You must have a port open. On macOS, ports are opened by enabling sharing services from the Sharing System Preference, and by some applications.
- Lastly, there has to be some process or application listening at the port that can respond. You can open port 80 on a web server, but if the web server

² <http://en.wikipedia.org/wiki/Firewall>

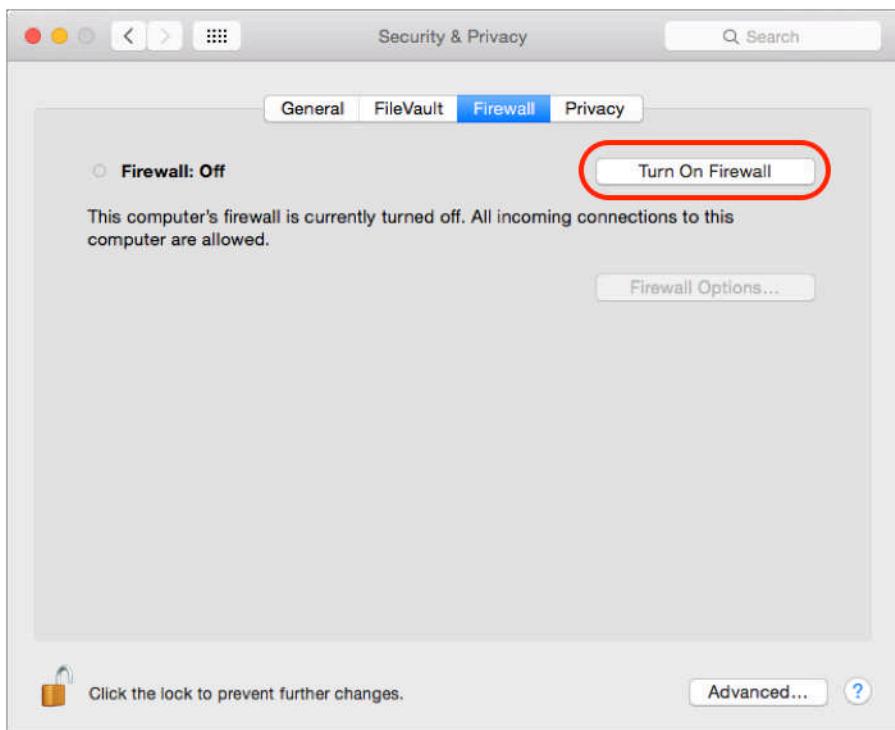
application (typically Apache) hasn't been launched, no amount of your browser screaming at the server will elicit a response.

In macOS, activating the firewall puts guards at the gates to prevent unwanted visitors. The second step is to close those ports whose associated services you don't need. This is accomplished by disabling unnecessary services in *System Preferences > Sharing*.

10.1.1 Assignment: Activate the Firewall

In this assignment you enable the built-in macOS firewall.

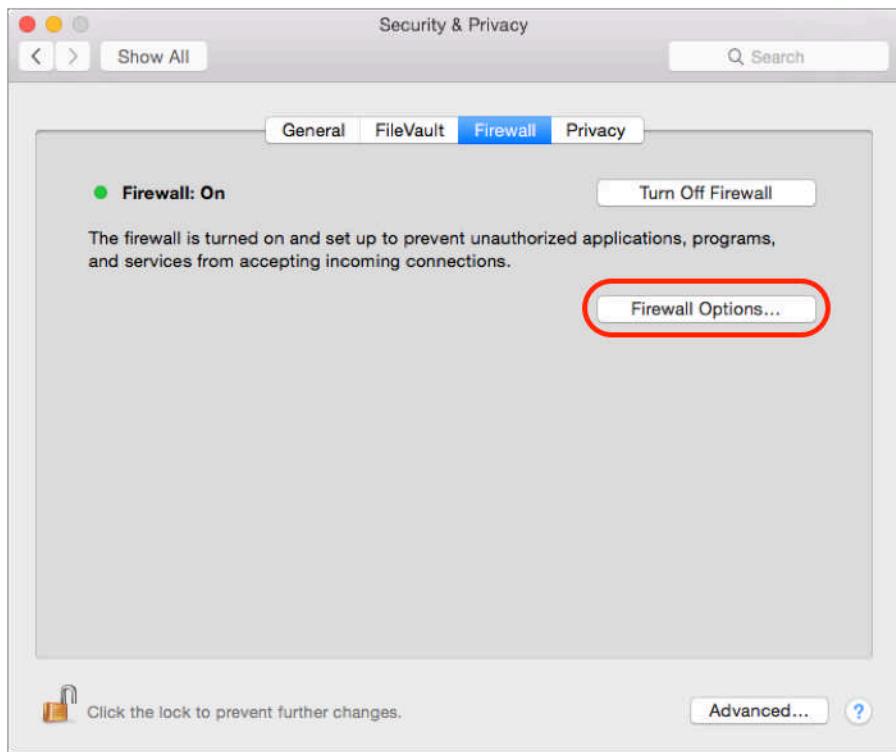
1. Open *Apple menu > System Preferences > Security & Privacy*.



2. Select the *Firewall* tab.
3. Select the Lock icon, and then authenticate as an administrative user.
4. Select the *Turn On Firewall* button.

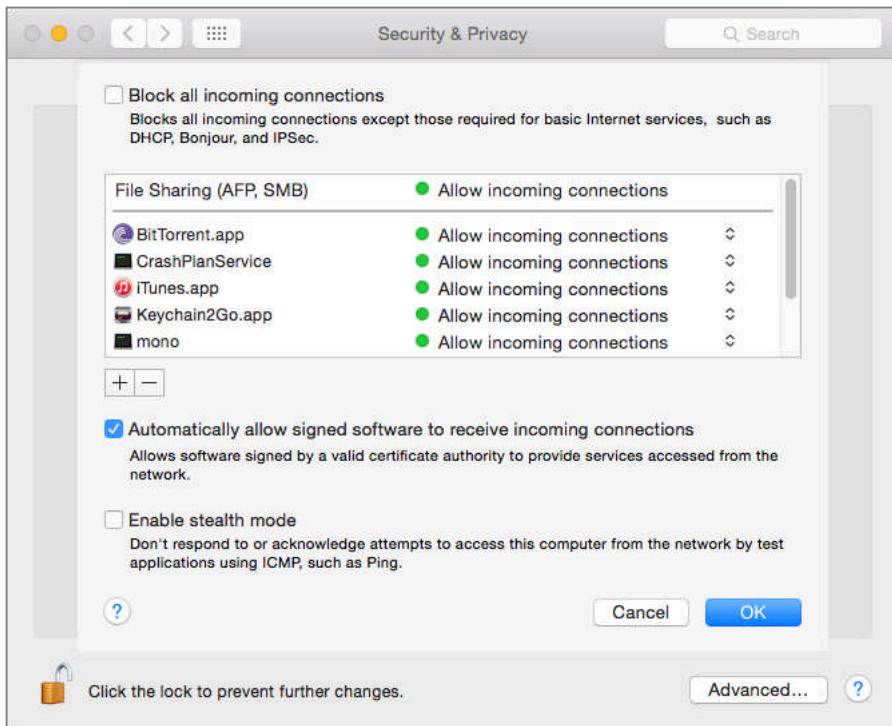
10 Firewall

5. Select the *Firewall Options...* button to further refine the firewall.



10 Firewall

6. The *Firewall Options* window opens.



- Enabling *Block all incoming connections* will effectively close down all but the most essential ports. You still will be able to reach out to initiate communications, such as to surf on a web browser or initiate a call on Skype, but you must do the initiating or others won't get in. Unless you are working in an unusual environment, this step is not necessary.
- In the main body area, you see all of the ports that are open. Above the horizontal line are those ports you opened when enabling items in the Sharing System Preference. Below the line are those ports opened by launching applications that require communication outside of your computer. It is possible that some of these applications have no need for outside communications, in which case you can click on the *Allow incoming connections*, then select *Block incoming connections*.
- *Automatically allow signed software to receive incoming connections* is enabled by default. Applications that are "signed" have special coding that

allows your Mac to determine if it has been damaged or modified from the original in any way. Apple has given its seal of approval to the original as being free of any intrusion software.

- *Stealth mode* can usually be left disabled. Enabling this checkbox will make your Mac unresponsive to Ping and other diagnostic tools. However, enabling this checkbox should have no impact on any aspect of your computer use.
7. Select the *OK* button.
 8. Quit System Preferences.

Congratulations! Your firewall will now be on guard, preventing unwanted penetration of your computer.

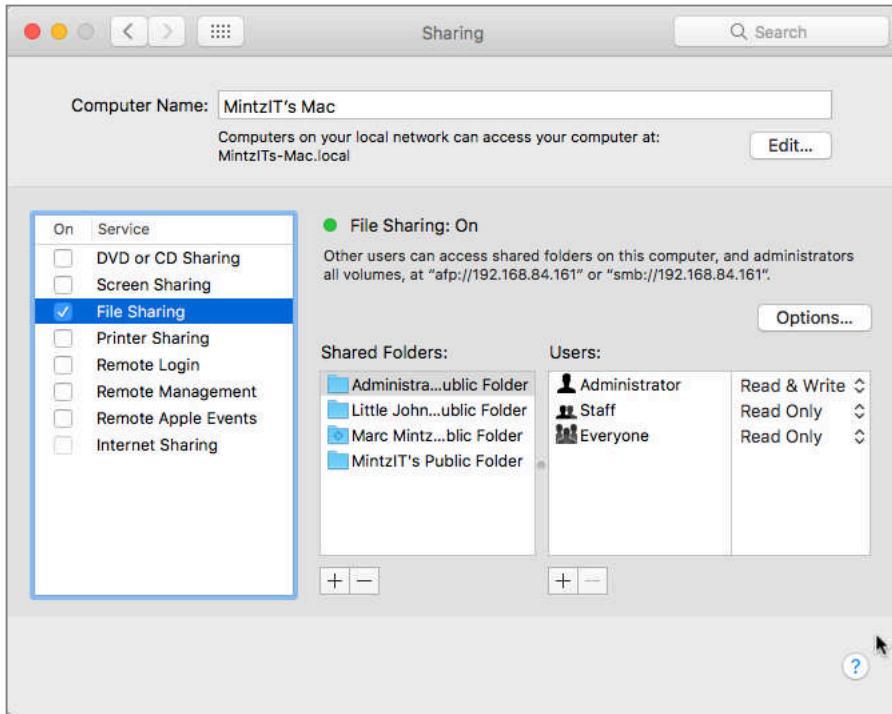
10.1.2 Assignment: Close Unnecessary Ports

In this assignment we will examine our currently open ports, and close those that are not necessary.

1. Open *Apple* menu > *System Preferences*.

10 Firewall

2. Select the *Sharing* preference. The *Sharing* System Preference pane opens.



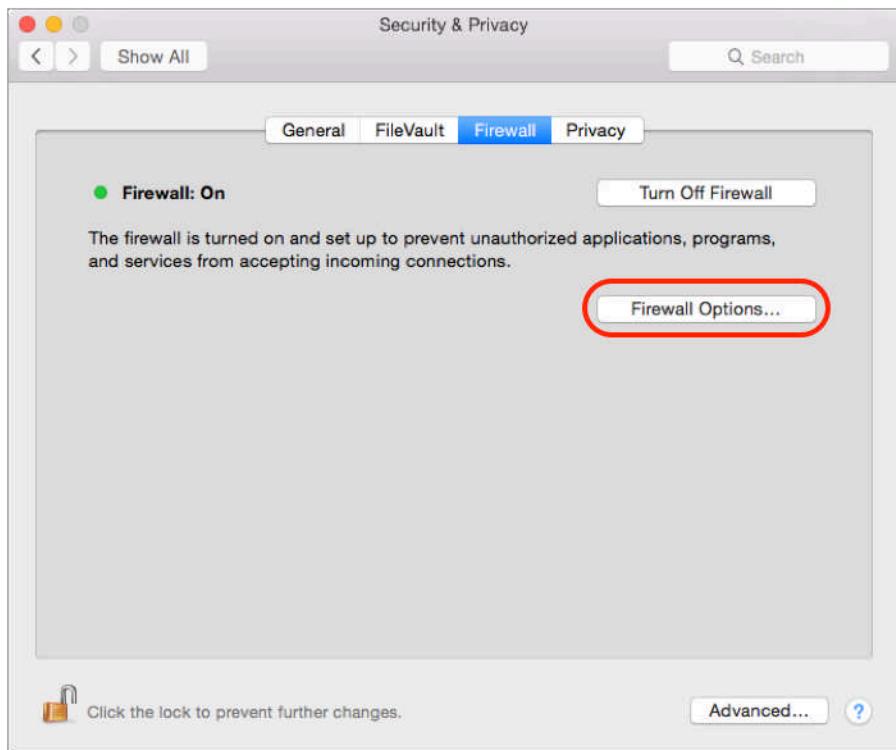
3. As necessary, select the Lock icon, and then authenticate as an administrator.
4. If any of your sharing items are enabled, at least one port has been opened to allow communication for that item.
5. If any currently enabled item is not needed, disable its checkbox.

Check on which, if any, ports are opened via user-launched applications

6. Select the *Show All* (12 dots in a grid) button in the tool bar.
7. Select *Security & Privacy* icon.
8. Select the *Firewall* tab.
9. Click the *Lock* icon, and then authenticate as an administrator.

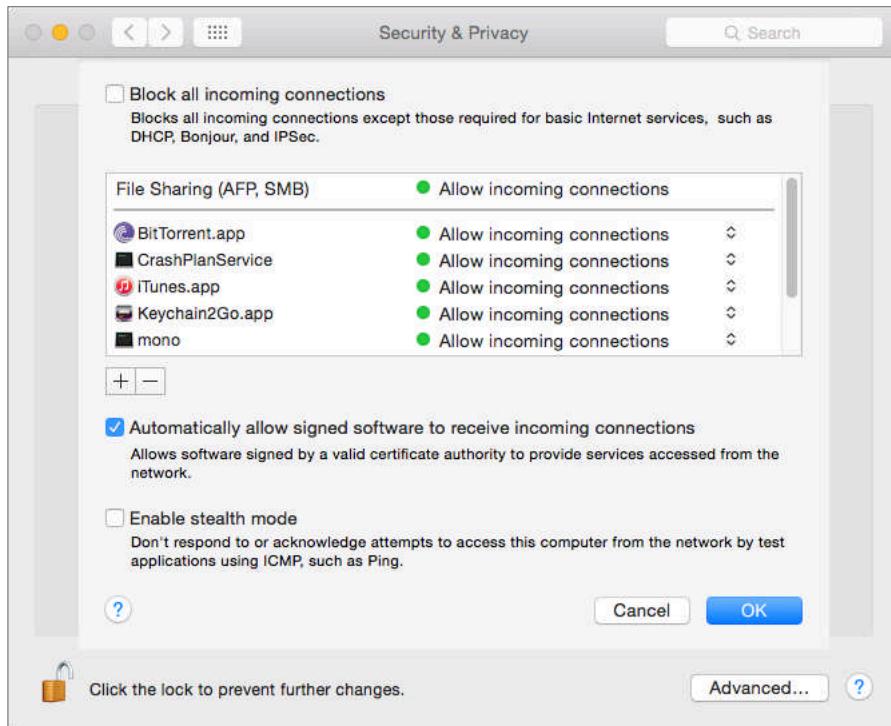
10 Firewall

10. Select the *Firewall Options...* button.



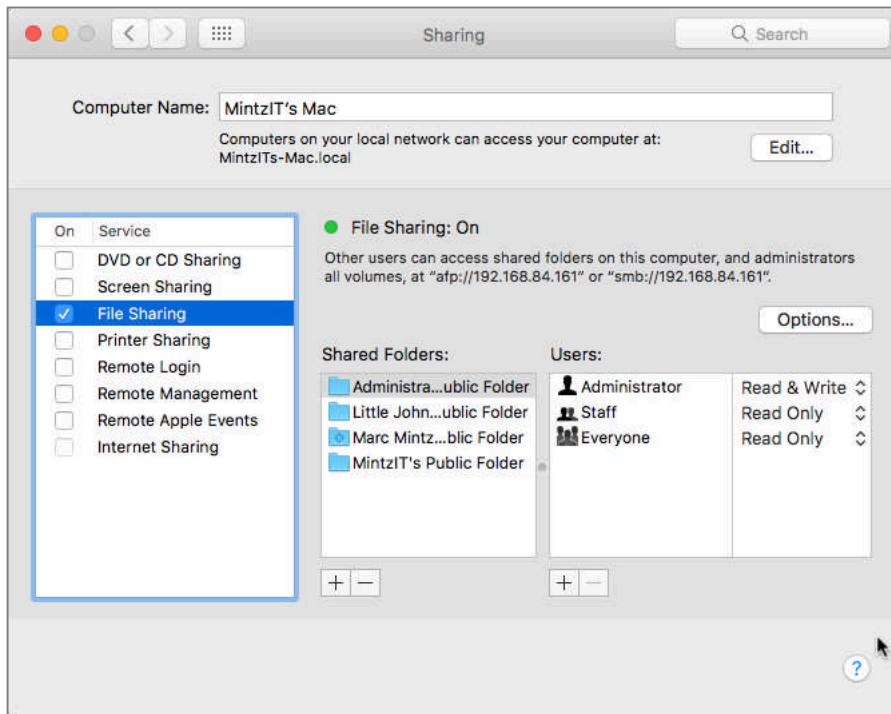
10 Firewall

11. The Firewall Options window opens, displaying all open ports based on the name of the process or application that has opened them. In this example, above the line I have *File Sharing (AFP, SMB)* ports open.



10 Firewall

- This screenshot reflects the *Sharing* preferences that I currently have open, *File Sharing*.

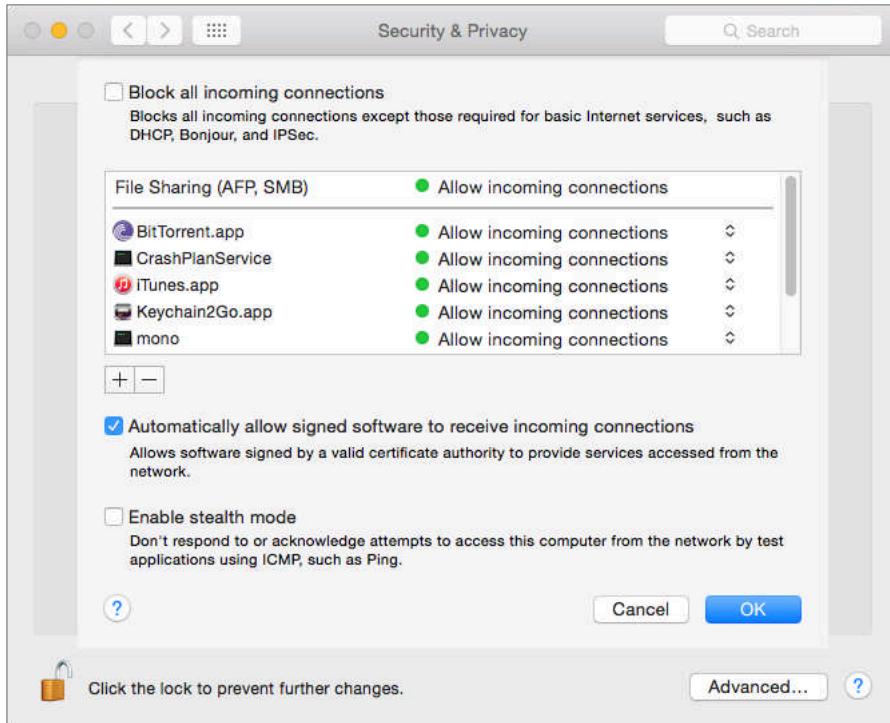


If any of the above the line ports should be closed:

12. Select *System Preferences* > *Sharing*, and then turn off the shared item.

10 Firewall

Below the line are ports opened by some of the applications I have launched.



- BitTorrent (Internet file-sharing service)
- CrashPlanService (Internet backup service)
- iTunes.app (iTunes music store service)
- Keychain2Go.app (Password storage and synchronization service)
- Mono (Part of the ScreenConnect remote support service)

If any of these ports should be closed:

10 Firewall

13. Select the *Allow incoming connections* pop-up menu, and then select *Block incoming connections*.



14. If changes have been made, select the *OK* button.

15. Quit System Preferences.

If any unnecessary port had been opened, you have now closed them, preventing unwanted access.

10.2 Review Questions

1. The macOS firewall is enabled by default. (True or False)
2. Where is the firewall enabled or disabled?
3. When selecting the firewall option to *Block all incoming connections*, are all ports disabled?

11 Firmware Password

I have six locks on my door all in a row. When I go out, I lock every other one. I figure no matter how long somebody stands there picking the locks, they are always locking three.

–Elayne Boosler¹, American comedienne

¹ https://en.wikipedia.org/wiki/Elayne_Boosler

11.1 EFI Chip

Apple computers use a chip on the logic board for part of the boot process. It is named the Firmware chip. Intel-based Macs use the Intel EFI (Extensible Firmware Interface) chip as the firmware chip. This chip has the ability to be password protected. Once done, it is not possible to boot the computer from another source (such as Single User Mode, Target Disk Mode, or another startup disk), or use any startup modifier key without first entering the Firmware Password.

This puts gold plating on your computer security. It is also something to take very seriously. If your Mac was manufactured after January 1, 2010 and you forget your Firmware Password, the only way to unlock the chip is to physically take the computer to an Apple Store where you may be required to present documents proving your legal ownership over the computer. Macs made before this date can have their Firmware Password reset by the following:

1. Shut down the computer.
2. Remove or add RAM.
3. Power on, and then immediately hold down the cmd-opt-p-r keys until the computer reboots. This last process is called *Zapping the PRAM* (Parameter RAM chip.)

The Firmware Password now is erased. Not much security in these older units.

11.1.1 Assignment: Create a Firmware Password

In this assignment you create and install a password on your Firmware chip to add NSA-level security to your computer.

1. Shut down your Mac.
2. Power on.
3. Immediately after pressing the Power button, hold down the cmd-r keys until you see the dark gray Apple logo center screen.

4. At the *Recovery HD* window, select the *Utilities* menu > *Set Firmware Password*.
5. Enter a strong password.
6. Record your password in a secure location. I use the iPhone Contacts as this both synchronizes with my iPhone Contacts, and is accessible from any computer by visiting <https://icloud.com>.
7. Click the *OK* button, returning you to the main Recovery HD screen.
8. Restart your Mac by selecting *Apple* menu > *Restart*.

Congratulations! You have successfully locked down your data from all but perhaps NSA attempts.

11.1.2 Assignment: Test the Firmware Password

In this assignment we will verify that your firmware password is active.

1. Shut down your Mac.
2. Power on your Mac. Immediately after the startup tone, hold down the option key.

Without a firmware password, this startup modifier would put you into *Start Manager Mode*, allowing anyone full access to all of your data by booting from an external drive. But with a firmware password in place you should see a screen requesting the firmware password in order to proceed.

3. Enter your firmware password.
4. Select your normal boot volume and continue startup as normal.

11.1.3 Assignment: Remove Firmware Password

I consider having a firmware password in place as important as the user password. However, there may come a time when removing the Firmware Password is called for (selling the computer is all I can think of.)

11 Firmware Password

In this assignment, you will remove your Firmware Password. If you wish to leave it enabled, skip this assignment.

1. Shut down your Mac.
2. Power on your Mac. Immediately after the startup tone, hold down the option key.
3. At the Firmware Password prompt, enter it.
4. Select the *Utilities* menu > *Set Firmware Password*.
5. Select the *Remove Firmware Password* button.
6. Enter the firmware password.
7. Select the *Remove* button.
8. Select the *Apple* menu > *Restart* to restart the Mac.

11.2 Review Questions

1. What is the name of the logic board chip can be password protected?
2. If the Firmware password is not known, how is it cleared on Macintosh computers manufactured prior to January 1, 2010?
3. If the Firmware password is not known, how is it cleared on Macintosh computers manufactured after January 1, 2010?
4. To create a Firmware password, you must be an administrator. (True or False)

12 Lost or Stolen Device

It takes considerable knowledge just to realize the extent of your own ignorance.

–Thomas Sowell¹, American economist, social theorist, political philosopher, and currently Senior Fellow at the Hoover Institution, Stanford University²

¹ https://en.wikipedia.org/wiki/Thomas_Sowell

² This observation has since been validated in University studies, originally performed by David Dunning and Justin Kruger. It is now referred to as the *Dunning-Kruger effect*. https://en.wikipedia.org/wiki/Dunning-Kruger_effect

12.1 Find My Mac

Millions of computers are stolen each year. If you have followed the steps above to enable *FileVault 2* with strong passwords, as well as a Firmware password, nobody is going to break into your data.

But it would be nice to be able to get your Mac back.

Find My Mac is an option within iCloud accounts that locates your Mac on a web map, often to within 6 feet. You can pass this information along to your local police, allowing them to get a search warrant to the address and recover your property.

With FileVault 2 enabled, the thief won't be able to access your account or data, but if you leave the Guest account active, the thief will be able to boot your computer to the Guest account... All the while Find My Mac is broadcasting the thief's location.

For Find My Mac to function, the following must happen:

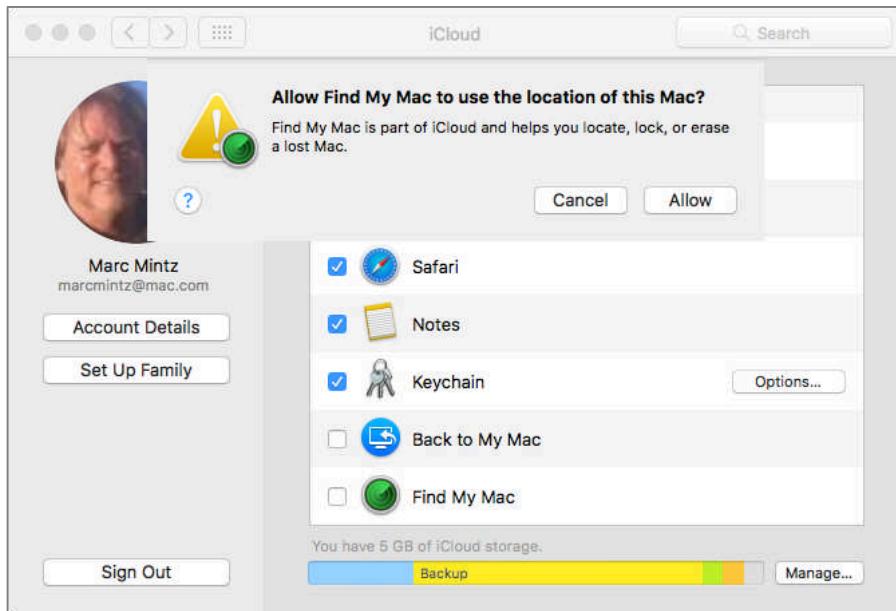
- An iCloud account has been activated.
- Find My Mac has been enabled for the computer.
- The computer is turned on.
- The computer is connected to the Internet via Wi-Fi.

12.1.1 Assignment: Activate and Configure Find My Mac

1. Select the *Apple* menu > *System Preferences* > *iCloud*.
2. If you have not created an iCloud account, select the *Sign In* button and follow the on-screen instructions to create an account.

12 Lost or Stolen Device

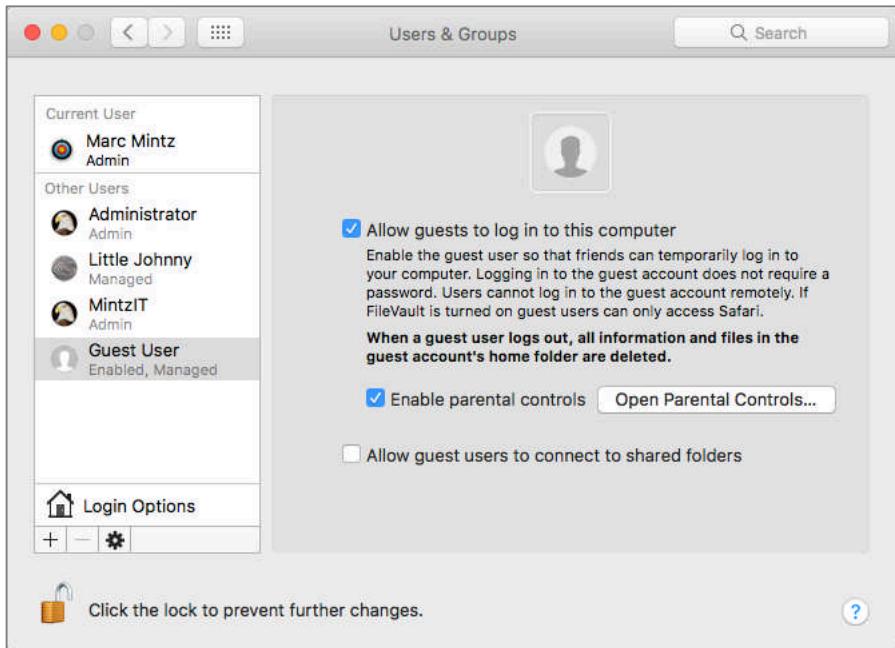
3. Enable the *Find My Mac* checkbox. You will be prompted to *Allow* this function. Earlier OS versions did not present this prompt.



Next we need to allow the Guest account to log in.

4. Open *Apple* menu > *System Preferences* > *Users & Groups*.
5. Select the Lock icon and authenticate as an administrator.

6. From the side bar, select the *Guest User* account. By default, macOS has *Guest User* enabled to log in to this computer. If someone has disabled this option, enable it.

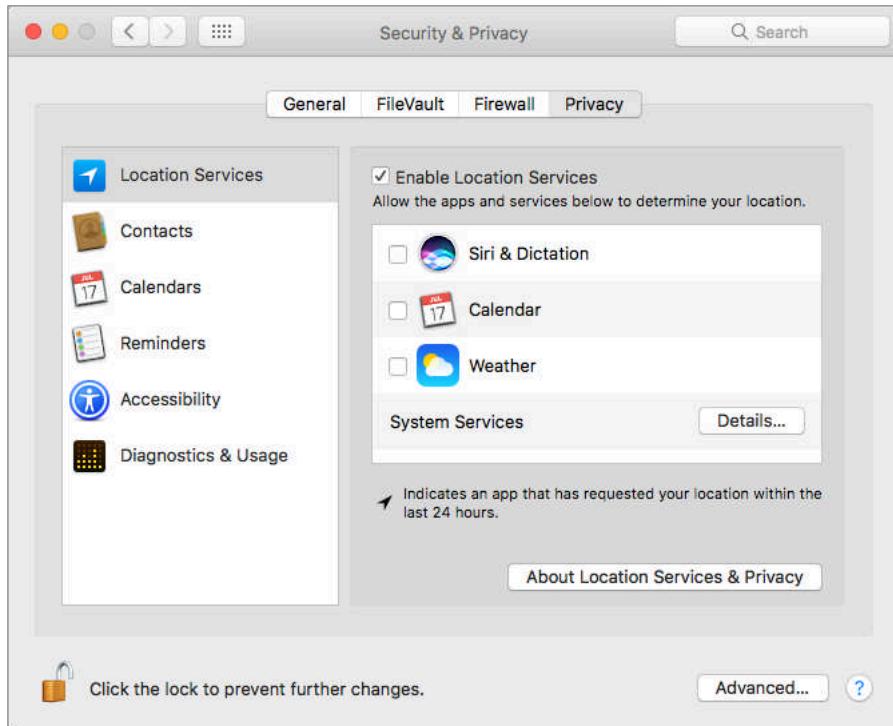


Next step is to ensure that a Guest is unable to modify any security-related System Preferences.

7. Select the *Show All* button.
8. Select the *Security & Privacy* icon.

12 Lost or Stolen Device

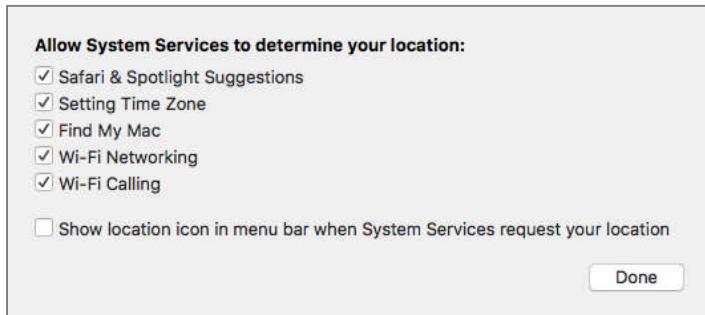
9. Select the *Privacy* tab.



10. Select the Lock icon and authenticate as an administrator.
11. By default, macOS has *Enable Location Services* enabled. If someone has disabled it, enable the checkbox.

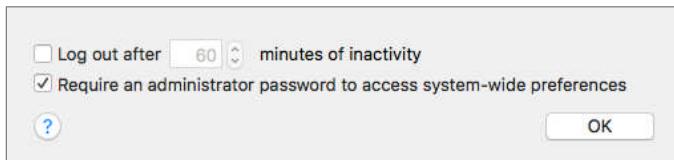
12. Select the *Details* button. At the least, enable the following, and then select the *Done* button:

- *Find My Mac*
- *Wi-Fi Networking*



13. Select the *Advanced* button.

14. Enable *Require an administrator password to access locked preferences*, and then select the *OK* button. This will stop a Guest, as well as other non-administrators, from changing critical system preferences.



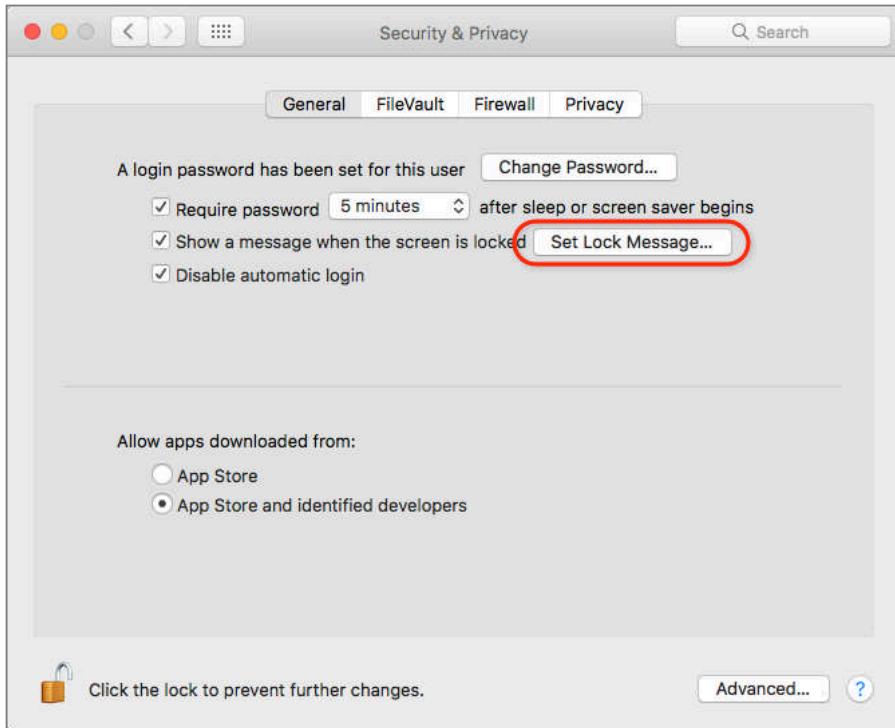
Lastly, in the event that a Good Samaritan finds your computer, let's provide contact information so they can call you to return the computer.

15. Open *Apple* menu > *System Preferences* > *Security & Privacy*.

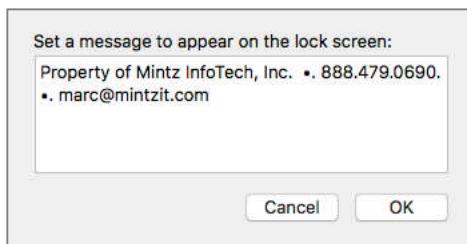
16. Select the *General* tab.

12 Lost or Stolen Device

17. Select the *Set Lock Message...* button.



18. Enter the message to be displayed at the log in screen and screen saver. This will be displayed as one long line, and then select the *OK* button.



19. Quit System Preferences.

Find My Mac is now configured and active. In the event of loss or theft, you have a good chance of locating your computer.

12.1.2 Assignment: Use Find My Mac from a Computer

For the purposes of this assignment, let's assume someone has taken your Mac and we will use Find My Mac to locate it. As there are two ways this can take place depending on the device used, we have two assignments: Locating your stolen Mac using Find My Mac from another computer, and locating your stolen Mac using an iPhone or iPad and the Find iPhone app.

1. Turn your Mac on and log into the only account available to the thief—Guest.
2. Connect to the Internet. Wi-Fi will be more accurate with a location, but Ethernet will sometimes work as well.
3. On another computer (macOS/OS X, or Windows), launch a web browser, visit iCloud at <https://icloud.com>, and then enter your Apple ID and password:
 - If you don't have another computer available, just perform this exercise on your own computer, logged in as Guest:

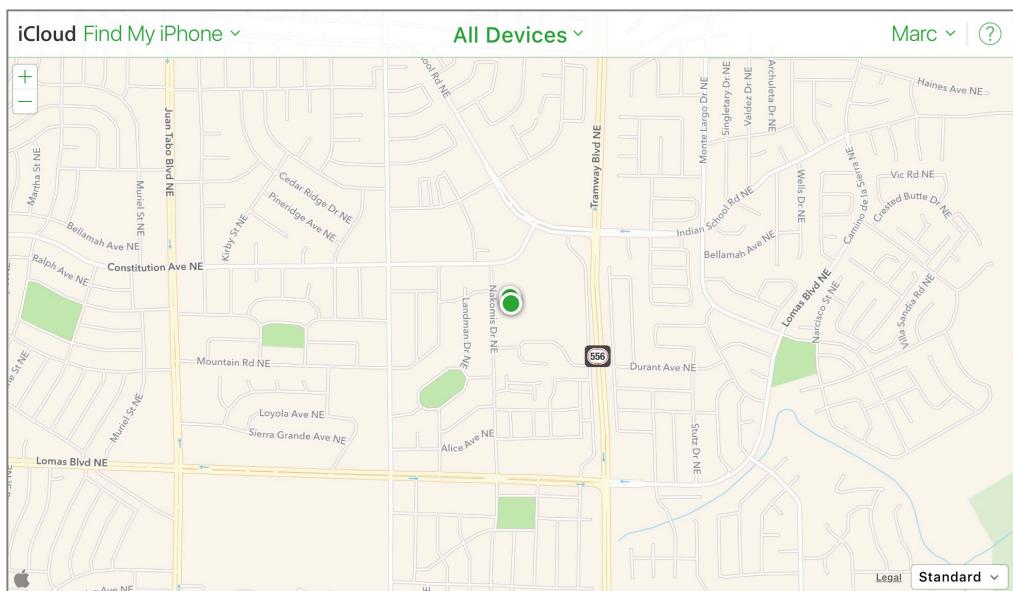


12 Lost or Stolen Device

4. The iCloud desktop will appear. Select the *Find iPhone* button.

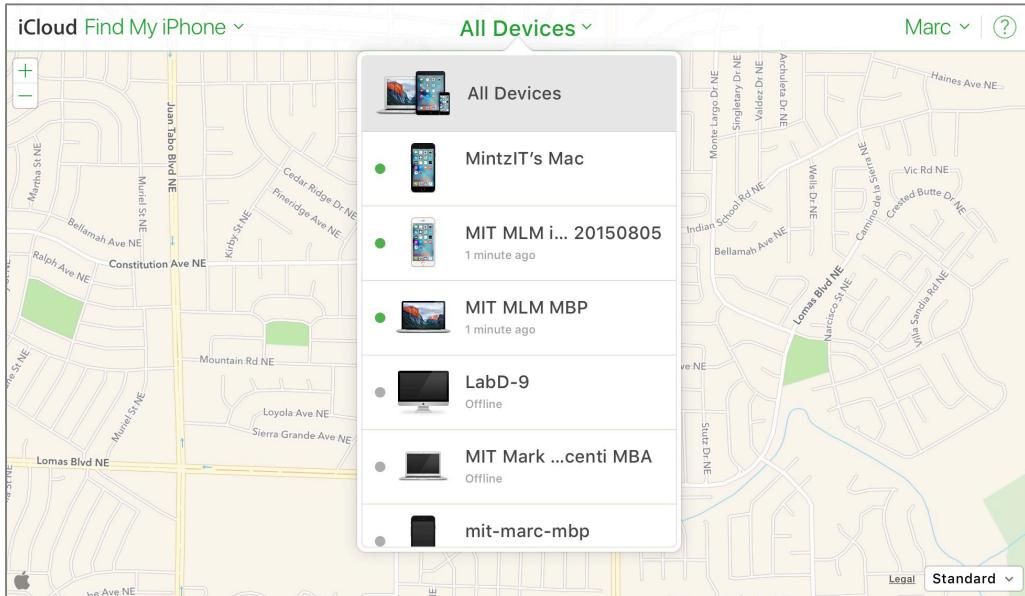


5. At the prompt, enter your iCloud password again.
6. The Find My iPhone map appears.



12 Lost or Stolen Device

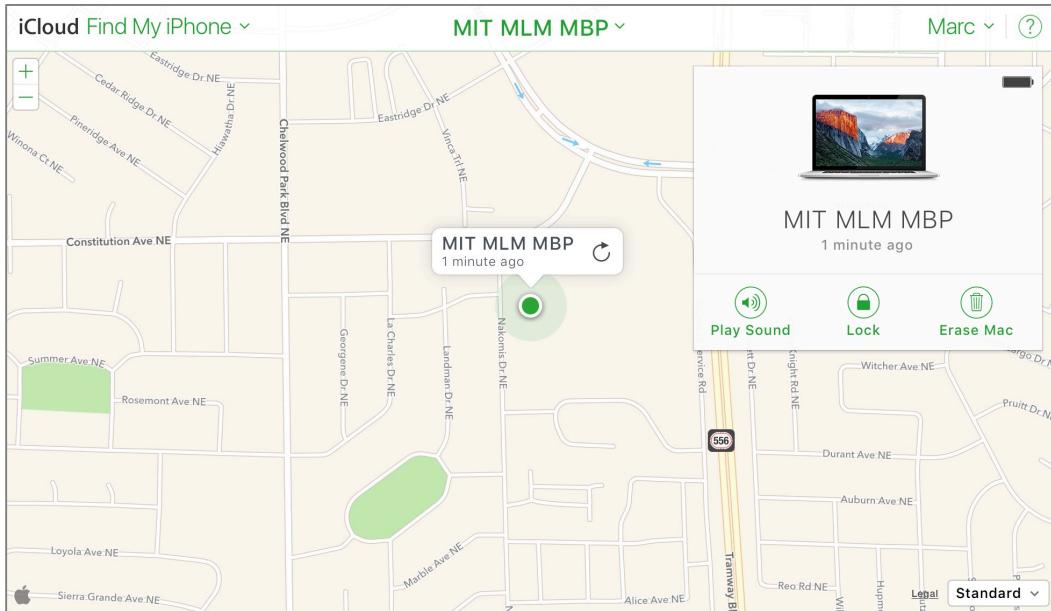
- At top, select the *All Devices* menu. All of your registered devices with Find My Mac and Find My iPhone enabled will appear. If the device is powered on, it will have a green light next to it.



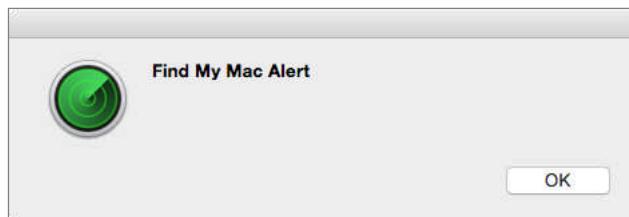
- From the *All Devices*, select the device to be located. Zooming into the map will provide a detailed location.

12 Lost or Stolen Device

9. Once located on the map, a pop-up window with the name of your device will appear. If you wish, you have access to three options.



- *Play Sound*. This will play a “sonar” sound and display an alert window on the device.



- *Lock*. This will lock down your system, preventing any use. I don't recommend either the Play Sound or Lock options, as it will notify the thief that you are tracking them. They may turn off the computer, blocking any future tracking, or worse; destroy the “tracking device.”
- *Erase Mac*. If it is not possible to get prompt police intervention, you have valuable data on the computer, and the thief may have access to a server farm to perform a massive password hack attempt, you may want to

consider simply erasing your Mac. After all, you do have a full current backup, don't you?

12.1.3 Assignment: Use Find My Mac From an iPhone or iPad

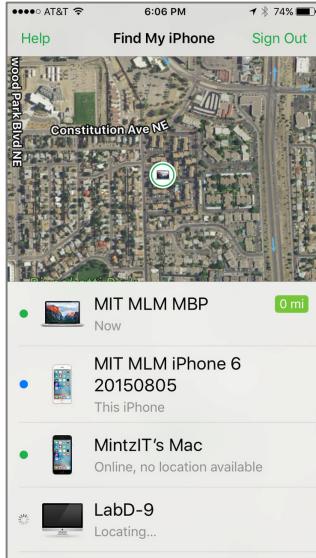
For this assignment we will assume the thief took your only Mac, and you don't have access to another computer. However, you do have access to an iPhone or iPad.

1. If you don't already have the *Find My iPhone* app installed on your device, visit the App Store and download it.
2. Open the *Find My iPhone* app.
3. Enter your *Apple ID* email address and *password*, and then select the *Go* key.

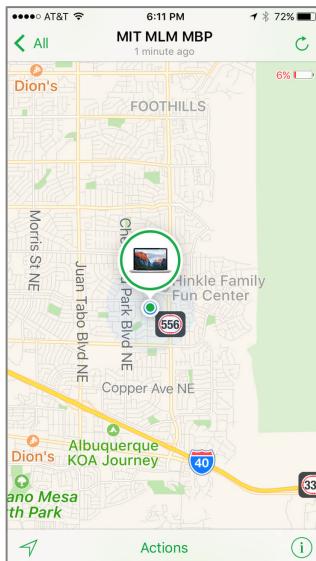


12 Lost or Stolen Device

4. The *Find My iPhone* screen will open. Select the target device to locate.

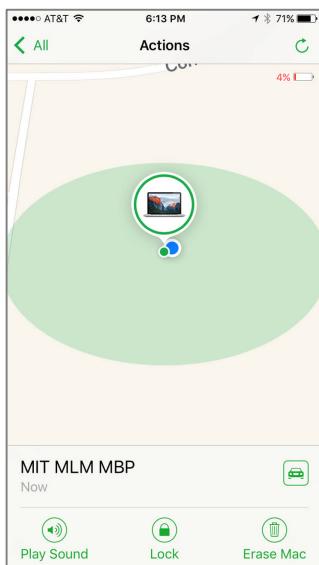


5. The Find My iPhone map will open, displaying the exact last known location for the target device.



12 Lost or Stolen Device

6. Select the device icon. The Info screen will open. From here you may have the device play a sonar sound (I use this at least once a week–my Yellow Lab is obsessed with hiding my iPhone), lock it to prevent any access, or erase the drive.



7. When done, exit the Find My iPhone app.

Hooray! You've found your lost/stolen device.

12.2 Review Questions

1. Find My Mac is enabled by default. (True or False)
2. Should the Guest account be enabled when Find My Mac is active, and why?
3. A lost Mac may be located via Find My Mac only with another macOS/OS X or iOS device. (True or False)

13 Local Network

I am concerned for the security of our great Nation; not so much because of any threat from without, but because of the insidious forces working from within.

—General Douglas MacArthur¹

¹ https://en.wikipedia.org/wiki/Douglas_MacArthur

13.1 Ethernet Broadcasting

It is common wisdom that Ethernet is more secure than Wi-Fi. But as with most things we believe, this is not accurate.

There are two security issues with Ethernet: Broadcasting and Insertion. At the most fundamental level, what is happening when data travels through Ethernet is that electrons are traveling along a metal cable. There are two unintended consequences that occur whenever electrons go for a ride—heat generation, and the creation of an electromagnetic field. For our purposes, heat isn't an issue. But the electromagnetic field is.

Sending data through copper wire effectively turns that wire into a very large antenna that is broadcasting your data through radio waves. If you have the right receiver and translation software, you can easily capture every bit of data being sent and received along that cable.

This vulnerability is not something about which the average person or business would or should be concerned. On the other hand, if you or your business requires the utmost in security, it is mandatory to add encryption to your Ethernet network.

Speaking specifically about macOS, computer-to-computer communications are not encrypted, and so are not recommended. When using computer-to-macOS/OS X Server communications, then all communications are encrypted. For business, this means that users should not do file sharing between themselves, but instead copy any file to the Server for others to copy back to their own computers.

13.2 Ethernet Insertion

You would notice if someone came into your home, plugged a computer into your network, and sat there watching data go by. But in the typical business, nobody would notice.

Ethernet and Wi-Fi networks can be protected from unwanted insertions by implementing the 802.1x protocol (often referred to as RADIUS)

https://en.wikipedia.org/wiki/IEEE_802.1X. This protocol works with both Ethernet and Wi-Fi, mandating that anyone attempting to join the network authenticate with their own personal name and password. This is unlike the typical Wi-Fi authentication that uses the same password for everyone.

To implement 802.1x you need to have either a macOS/OS X, Windows, or Linux Server running within your network, or one of the many other 802.1x appliances that are available. Details on how to configure 802.1x are beyond the scope of this book. Please consult the following for more information:

- *OS X Server Administrator Guide*²
- *Jedda*³
- *OS X Server Essentials 10.11*⁴
- *Microsoft TechNet documentation*⁵

² <https://help.apple.com/advancedserveradmin/mac/>

³ <https://jedda.me/2012/11/configuring-basic-radius-os-108-server/>

⁴ https://www.amazon.com/Support-Essentials-10-11-Supporting-Troubleshooting/dp/013442820X/ref=sr_1_1?ie=UTF8&qid=1468196548&sr=8-1&keywords=OS+X+10.11+server

⁵ <https://technet.microsoft.com/en-us/library/hh831831.aspx>

13.3 Wi-Fi Encryption Protocols

Right out of the box almost all Wi-Fi base stations are insecure. Anyone that can pick up the signal can connect. This allows them not only to use your bandwidth to access the Internet, but also to see all of the other data—such as usernames and passwords—that are travelling on that network. All that is needed to secure your Wi-Fi is to add strong password protection with encryption.

Although cellular networks do use encryption, the protocol in use has been broken for many years, making it easy for a novice hacker to see all the data passing on it. In addition, it is common practice for police and other government law enforcement agencies to set up their own cellular towers with the purpose of harvesting data.

In order to prevent your data from being seen while on a cellular network or an unencrypted Wi-Fi network, it is necessary to use VPN (Virtual Private Network) encryption (more on that later.) If the Wi-Fi network is properly encrypted, you should have little concern over the security and privacy of your data.

Below you will find the brief on each of the Wi-Fi encryption protocols.

- **WEP⁶** (Wired Equivalency Protocol) was the first encryption protocol for Wi-Fi. Introduced in 1999, it was quickly broken, and by 2003 was replaced by WPA and WPA2 (Wi-Fi Protected Access). Any Wi-Fi base station manufactured in the past 5 years will offer WPA and WPA2, in addition to WEP.

There is only one reason to ever use WEP—you simply have no other option. Kids driving by your home can likely break into your WEP network before leaving the block.

- **WPA⁷** (Wi-Fi Protected Access) superseded WEP in 2003. Although it is a great advancement, it too has been broken. As with WEP, the only reason to use WPA is that you have no other option.

⁶ http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

⁷ http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

- **WPA2**⁸ is the only protocol considered secure. WPA2 superseded WPA in 2004. Although in the past year WPA2 has been broken, it is very difficult to do, and with strong passwords or with 802.1x still provides military-grade protection for your wireless networks.

There are two encryption algorithms that can be used—*TKIP* and *AES* (technically known as CCMP, but virtually all vendors refer to it as AES.) TKIP has been compromised and is no longer recommended. If your Wi-Fi device allows the option of AES, use only that. If it only allows for TKIP, trash the unit and purchase a more modern device.

⁸ http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

13.4 Routers: An Overview

The connection point between your Internet Service Provider (ISP) and your Local Area Network (LAN) is most likely a router. A router is a device designed to connect two different types of networks, and provide resources for them to interact.

Common brands of routers include: Cisco, Linksys, Netgear, D-Link, Apple, and the many unbranded devices that Internet Service Providers lease to their customers.

Some newer routers, especially those provided by ISPs are all-in-one units containing several, if not all of the components below:

- **Modem.** The hardware that decodes and modulates the signal from your Internet provider to your cable or telephone jack. This is most likely to be a separate component if more than one device exists for your Internet connection.
- **Router.** A component that runs a specialized program, which allows hundreds of different devices to interact on a network, usually sharing a single IP address to the Internet. Routers use *Network Address Translation* (NAT) to convert and direct Internet traffic from websites to your computer and from your computer to other computers and peripherals on the *Local Area Network* (LAN).
- **Firewall.** Software which inspects data traffic between the internet and internally connected devices
- **Network Switch.** A hardware component that allows multiple devices to be connected simultaneously and interact with the router
- **Access Point.** A hardware component that allows tens or hundreds of wireless (Wi-Fi) devices to connect to it.

Every router has at least some basic security controls built in, including the ability to filter out what it thinks are attempts to hack into your network, and the ability to forward specific types of data packets to a specific computer within your LAN, or to point specific types of data packets to a specific computer on the Internet.

Malware, hackers, criminals, and even some government agencies, sometimes attempt to alter these configurations so that either the malware or the perpetrators have an easier time harvesting your data. Because of this, it is wise to routinely inspect the condition of your router. How often is *routine*? Within larger or security-conscious organizations with high-value data, it is common to have a network administrator dedicated to maintaining watch over the status of network equipment. For a small business or household, once every few months wouldn't be too often.

13.4.1 Assignment: Determine Your Wi-Fi Encryption Protocol

You find yourself at a hotel with Wi-Fi and the need to access the Internet. You have the need to ensure that your data is not intercepted. How do you determine if the Wi-Fi network is using WPA or WPA2 instead of WEP? Just attempt to access the network, and the dialog box will tell what protocol is in use.

For this assignment, take yourself to a location that has an available Wi-Fi network. Your own home will do.

1. From the *Wi-Fi* icon in the menu bar, select the target network.

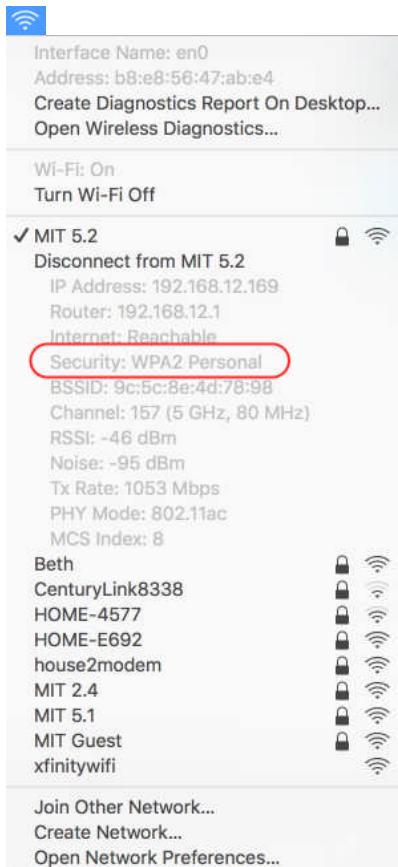


2. The authentication window will appear, requesting authentication and informing you of the security protocol.
 - If it does not appear, either the network does not use encryption, or your Keychain may be storing the password from a previous time you were connected.



If you have already connected to the Wi-Fi network and don't recall which security protocol it uses, you can find it from the Wi-Fi menu icon.

3. Hold down the *Option* key while clicking on the Wi-Fi menu icon. The Wi-Fi submenu will display with expanded information, including the encryption protocol in use, if any.



If the protocol is WPA2, life is all rainbows and unicorns. If it is anything else, *everything* you do on that network is clearly visible to others and I strongly recommend not using this network unless you have installed VPN software to encrypt your Internet traffic (more on this later.)

13.4.2 Assignment: Secure an Apple Airport Extreme Base Station

Every Wi-Fi base station model has its own unique configuration method. We will detail how to configure your Apple Airport Extreme for WPA2 protection. For

this exercise we assume you are on a network with an Apple Airport Extreme base station.

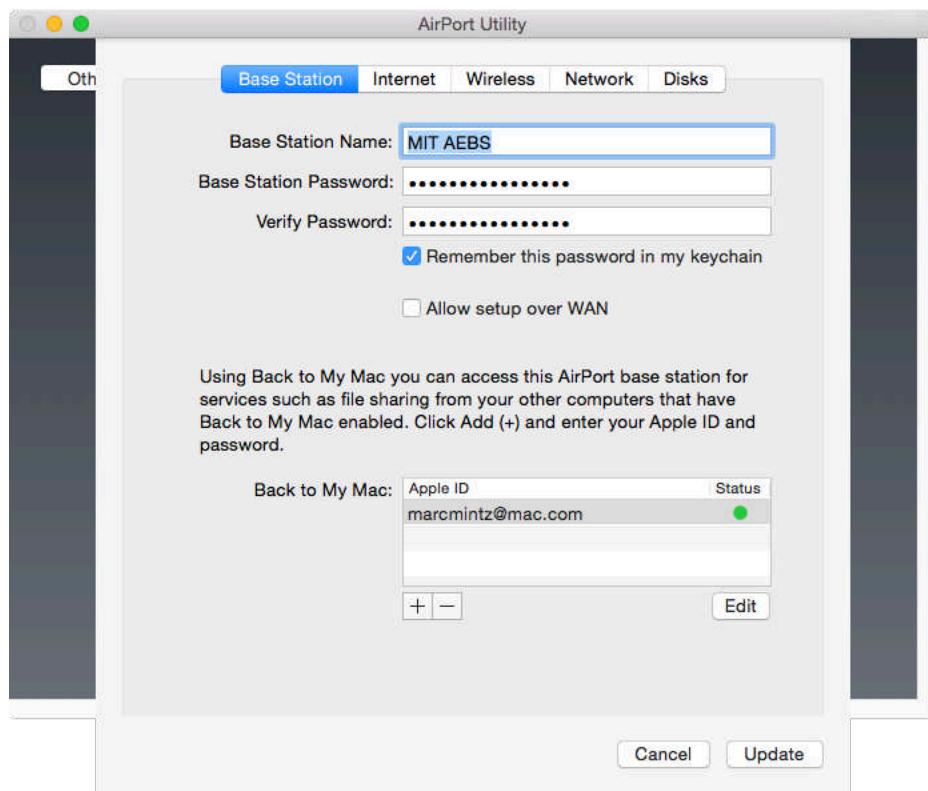
1. Open *Airport Utility.app*, located in your */Applications/Utilities* folder. Select the target base station.
2. The target base station information pane will appear. Select the *Edit* button.



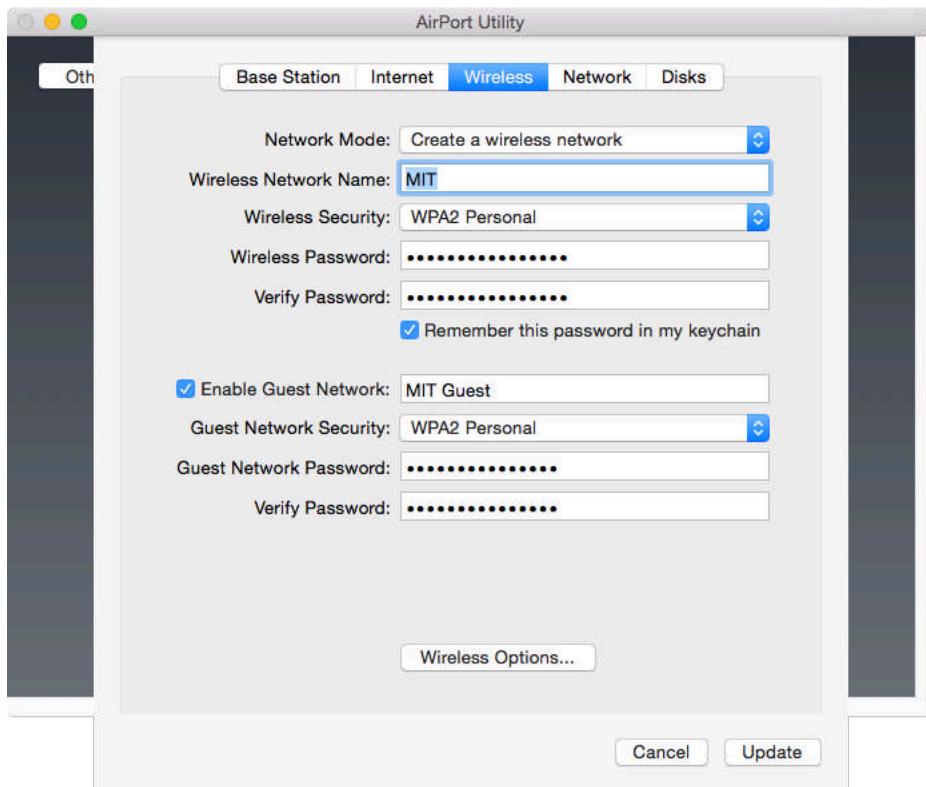
3. If so prompted, enter the administrator name and password for the base station.

13 Local Network

4. Select the *Base Station* tab. Enter a strong administration password here.



5. Select the *Wireless* tab and then configure as follows.



- From the Wireless Security pop-up menu, select *WPA2 Personal*. If you have older wireless equipment, you may need to change this to *WPA/WPA2 Personal* to offer compatibility with your older equipment. Keep in mind that doing so severely compromises your network security.
 - In the *Wireless Password* and *Verify Password* fields, enter a strong password.
6. Click the *Update* button.
7. *Quit* Airport Utility.app.

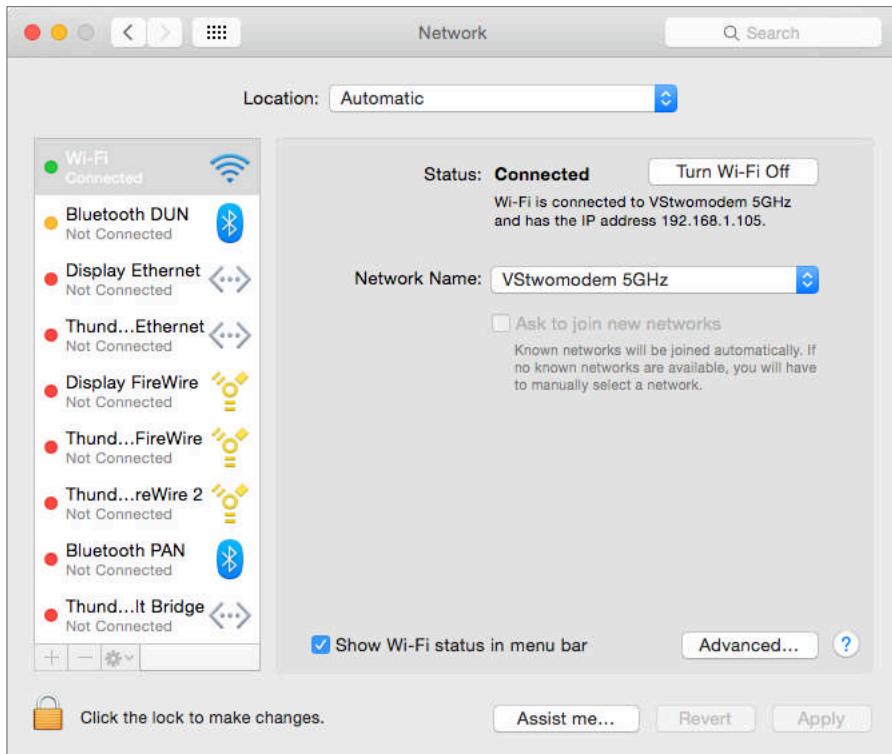
Congratulations! All traffic across your Wi-Fi network is now securely encrypted.

13.4.3 Assignment: Non-Apple Wireless Router Wi-Fi Encryption

Although all Wi-Fi routers or base stations are configured differently, most follow a basic template. In this assignment we will be using an ASUS RT-AC3200. We will assume you are on a network with a similarly managed router.

Find the IP address of your Wi-Fi router.

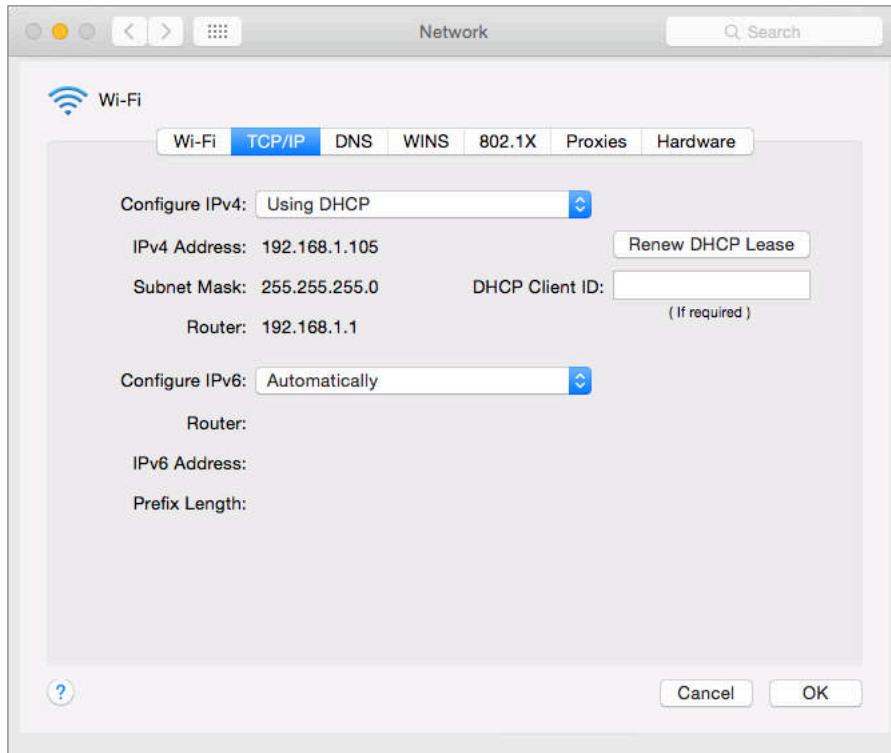
1. Open the *Apple* menu > *System Preferences* > *Network*.



2. If needed, click the lock icon and authenticate as an administrator.
3. Select the *Advanced* button.

13 Local Network

4. Select the *TCP/IP* tab.

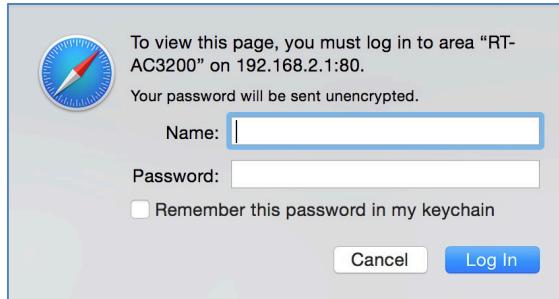


5. About half way down on the left side you will find the *Router* address. This is your Wi-Fi base station or router IP address.
6. Close System Preferences.

Now, on to configuration:

7. Open a web browser.
8. In the URL or Address field, enter the IP address of the Wi-Fi base station or router.

9. At the *Authentication* window, enter the administrator user name and password. This will be the administrator of the router, not of your computer.

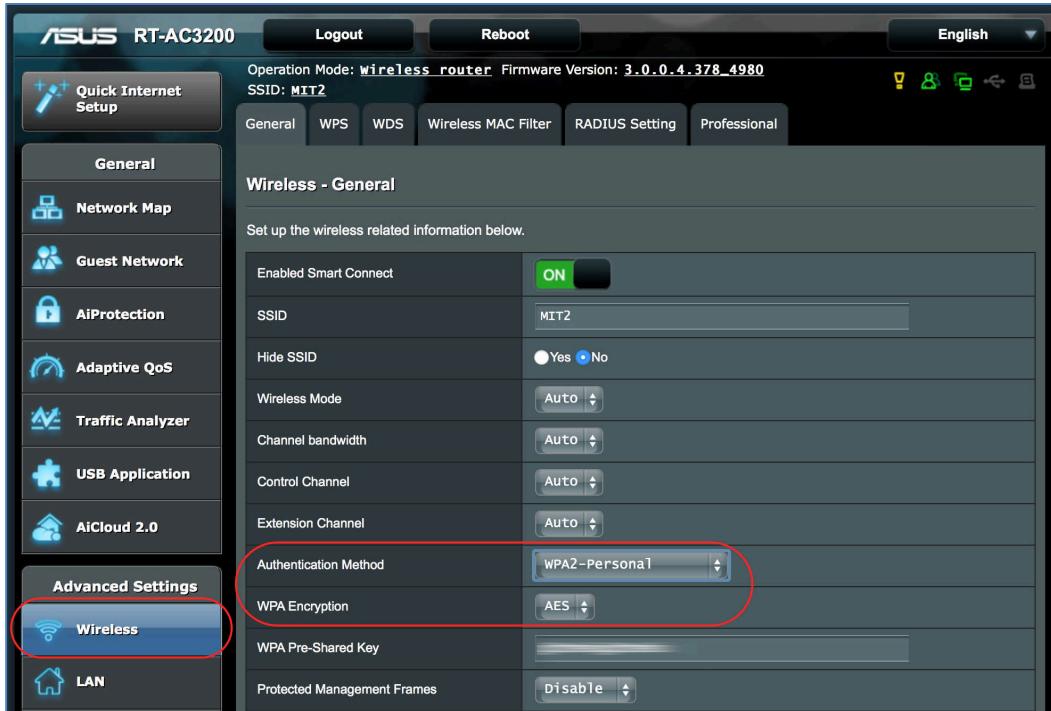


10. The router control panel will appear.



11. From the sidebar, select the *Wireless* button. This will display the options available with your Wi-Fi. Of interest to us now is the *Authentication Method* and *WPA Encryption*. Verify that your Wi-Fi is configured to use the WPA2

protocol. If it isn't, select it now, and then enter your desired strong password to access the network.



- Note: If your router has the option of using either *AES* or *TKIP*, select *AES*. The *TKIP* encryption scheme has been broken and is easily hacked.
- Note: Although the *WPA2 Enterprise* is the strongest security (even higher than *WPA2*), it requires network administrator skills and hardware that are outside the scope of this book.

12. If any changes were made, click the *Apply* button to save the changes.

13. Close the browser window to exit out of your router.

Congratulations! All traffic on your Wi-Fi is now securely encrypted.

13.5 Use MAC Address to Limit Wi-Fi Access

Every device that is capable of connecting to a TCP network has a unique *MAC Address*⁹ (Media Access Control). This address specifies the manufacturer of the device, and a device-specific number. Don't go to sleep on me yet! This MAC address can be used with most Wi-Fi base stations to limit what devices can connect to your network.

Although every Wi-Fi base station has a unique interface to filter by MAC address, they all operate on the same principle—either allow anyone with the proper password to gain access to the network, or allow anyone with the proper password *and* proper MAC address access to the network. In this way, you can easily lock down your Wi-Fi to only approved devices. So even if an employee knows the password, they are unable to connect their iPhone or personal computer to the Wi-Fi unless the MAC address for those devices are on the list.

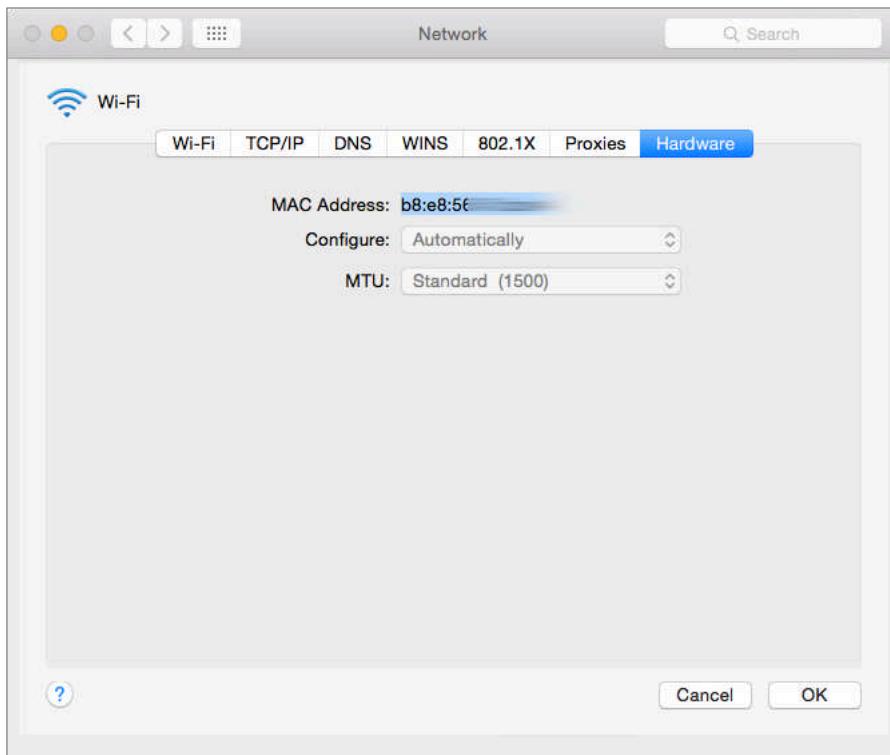
⁹ http://en.wikipedia.org/wiki/MAC_address

13.5.1 Assignment: Restrict Access by MAC Address to Apple Airport

In this assignment we will configure our Apple Airport to allow only desired devices to connect.

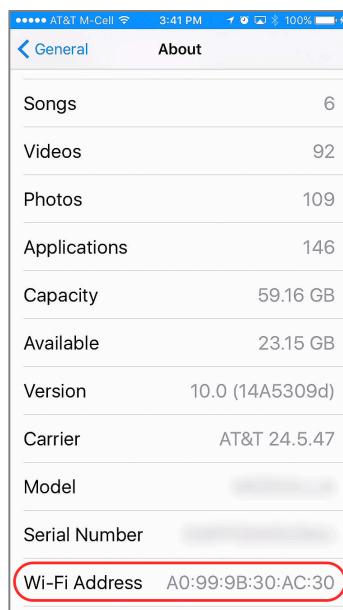
Make a list of the devices to be permitted access to your Wi-Fi network. Include an identifying description and the MAC address of the device.

1. The MAC address of a macOS/OS X computer may be found in the *System Preferences > Network > Advanced... button > Hardware tab*.

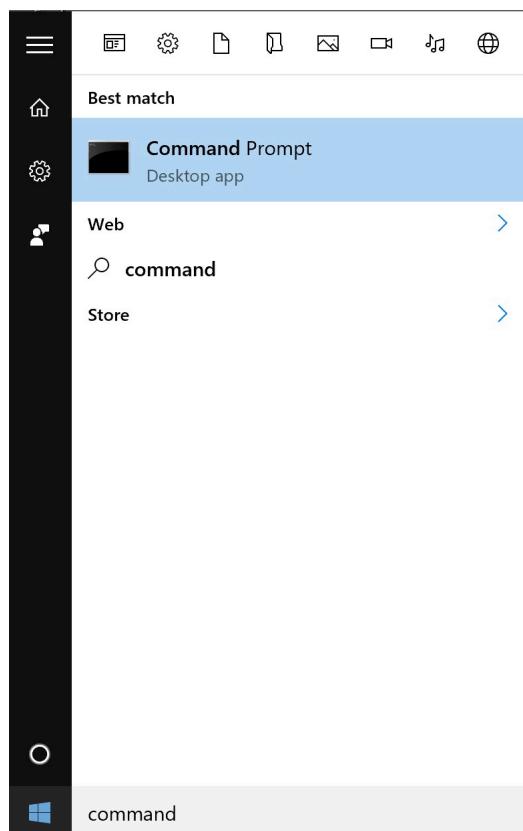


13 Local Network

2. The MAC address of an iPhone may be found in the *Settings > General > About > Wi-Fi Address* field

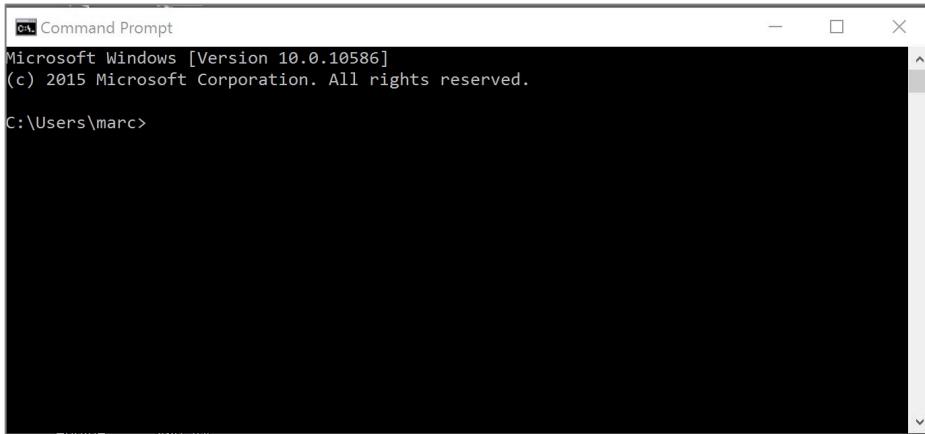


3. The MAC address of a Windows device can be found with the ipconfig command in the command prompt.
 - a) In Windows 10, click in the *Search the Web and Windows* field in the bottom left corner, and then enter *command prompt*. Double-click on *Command Prompt* in the *Best match* pop-up.



13 Local Network

- b) The Command Prompt window appears.



- c) Enter ipconfig -all. A listing of all network addresses for the device appears. The MAC address will show as the *Physical Address*.

```
C:\Users\marc>ipconfig -all

Windows IP Configuration

Host Name . . . . . : DESKTOP-GMC058I
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled . . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : localdomain

Ethernet adapter Ethernet0:

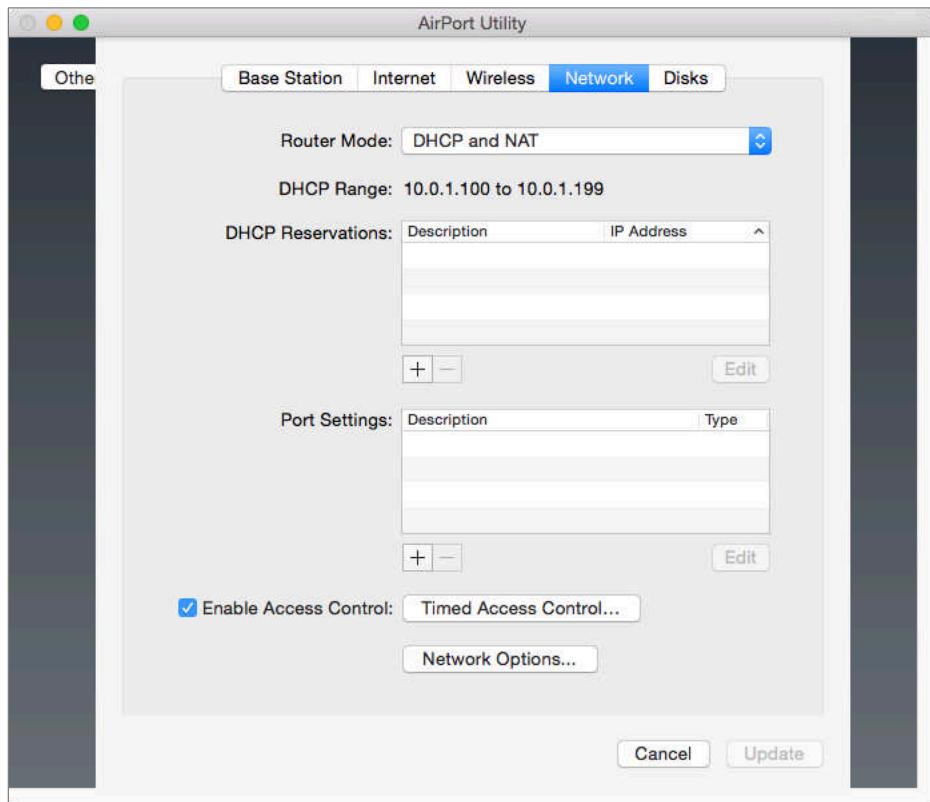
Connection-specific DNS Suffix . . . . . : localdomain
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-EF-94-53
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::a14c:8df4:5ee6:d49e%6(PREFERRED)
```

The "Physical Address" line for the "Ethernet adapter Ethernet0:" is circled in red.

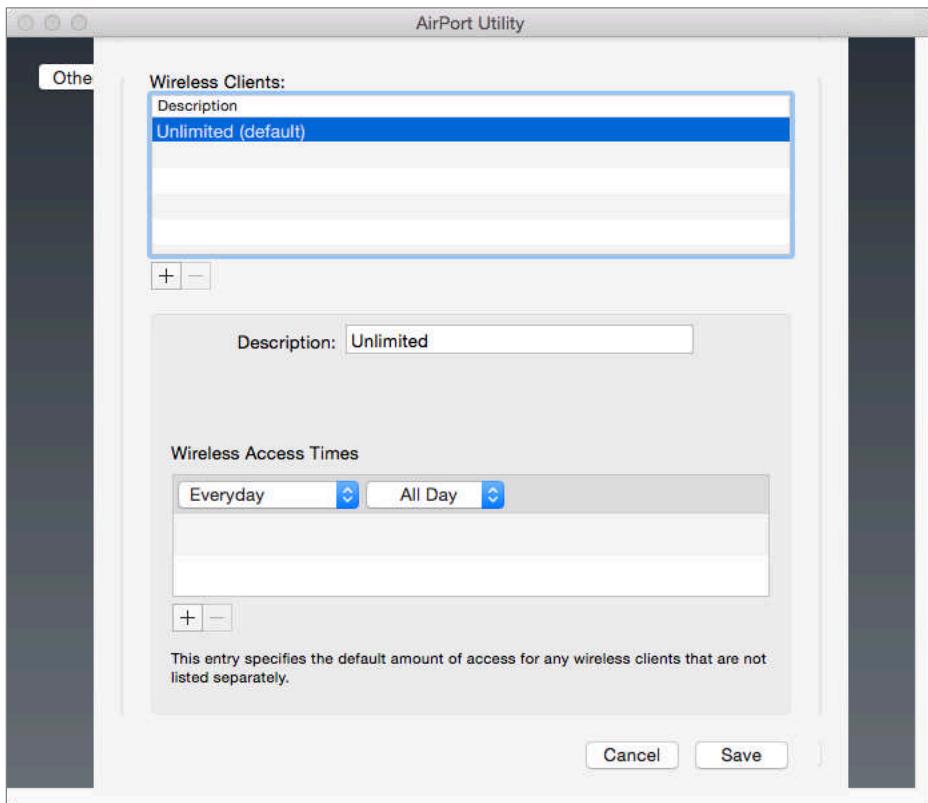
- d) Close the Command Prompt.

Configure Your Airport to allow only these devices

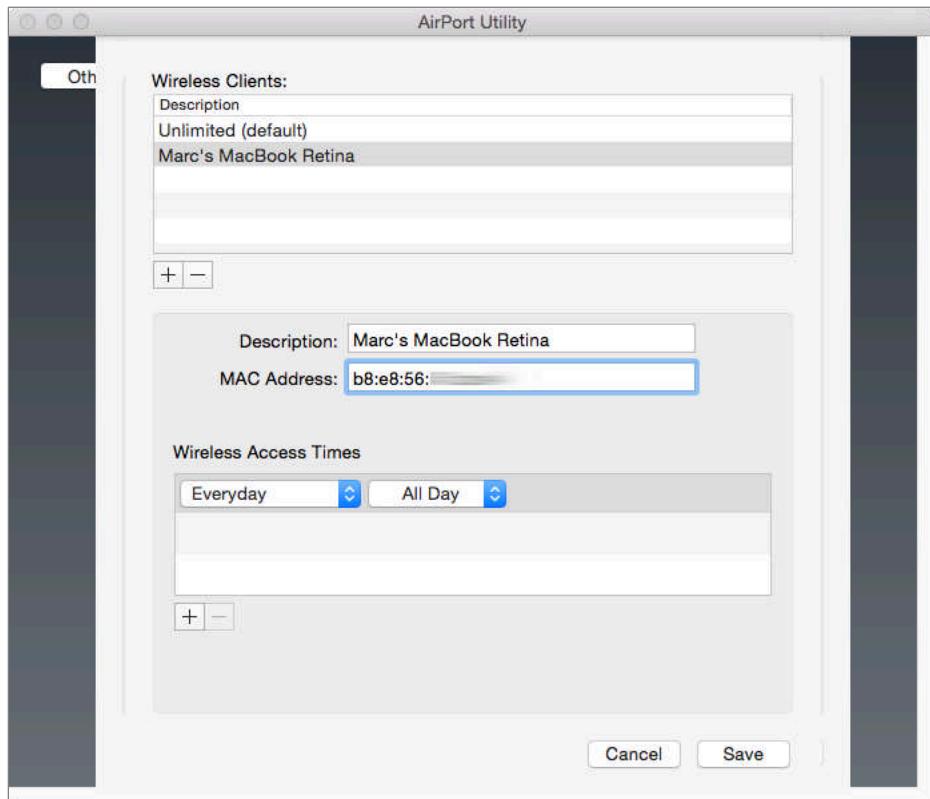
4. Launch Airport Utility. Located in the */Applications/Utilities* folder.
5. Select your *Airport base station*, select the *Edit* button, and if necessary, authenticate for access.
6. Select the Network tab, enable the Enable Access Control check box, and then select the Timed Access Control... button.



7. The *Timed Access Control* window appears.



8. At the bottom left of the *Wireless Clients* field, select the + button. Configure as below:



- *Description*: Enter a human-recognizable description of the device to be allowed access.
 - *MAC Address*: Enter the MAC address of the device.
9. Repeat step 6 for every wireless device to have access to your network.
 10. Select the Save button.
 11. Any device not listed will be immediately dropped from your network.
 12. Quit Airport Utility.

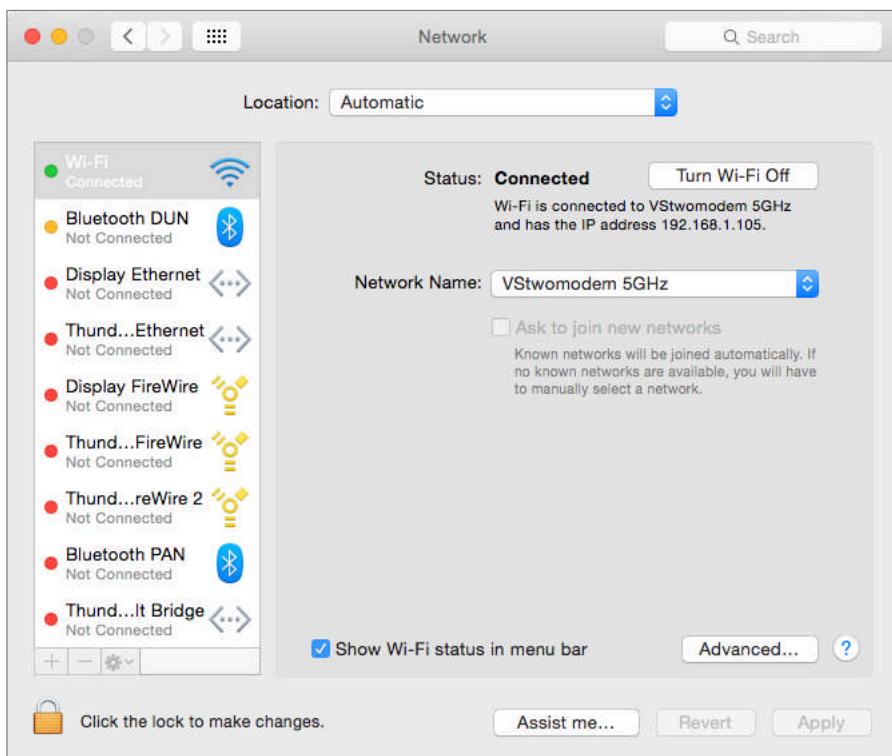
Congratulations! You have secured your wireless network so that only authorized devices are granted access.

13.5.2 Assignment: Restrict Access by MAC Address to a Non-Apple Router

In this assignment we will configure a non-Apple wireless router to allow only desired devices to connect. Although every wireless router or Wi-Fi base station is configured differently, they tend to use a similar template. In this example we will be using an Asus RT-AC3200.

Find and record the IP address of your wireless router.

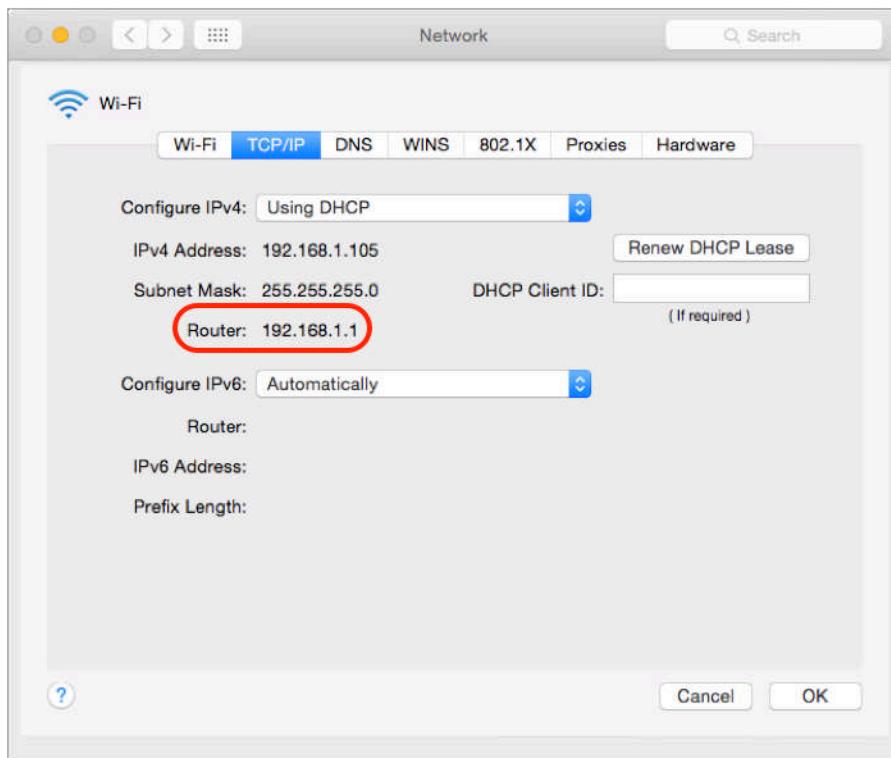
1. Open Apple menu > *System Preferences* > *Network*.



2. If necessary, unlock the preference.
3. Select the *Advanced* button.

13 Local Network

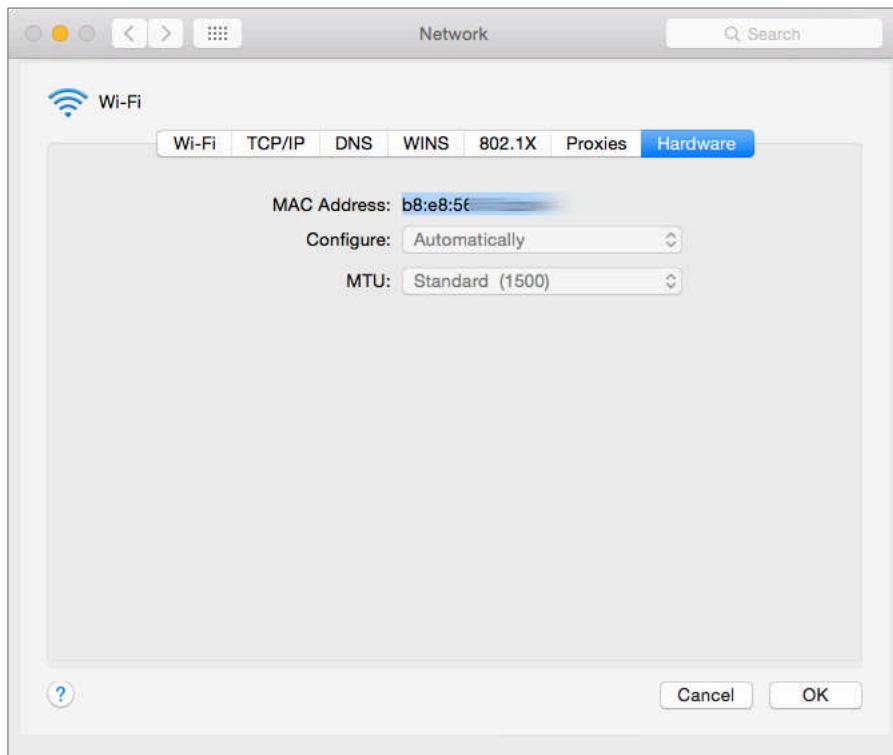
4. Select the *TCP/IP* tab. The wireless router/Wi-Fi base station IP address will be found at the *Router:* field.



5. Quit System Preferences.

Make a list of the devices to be permitted access to your Wi-Fi network. Include an identifying description and the MAC address of the device.

6. The MAC address of a Macintosh may be found in the *System Preferences > Network > Advanced... button > Hardware tab*.

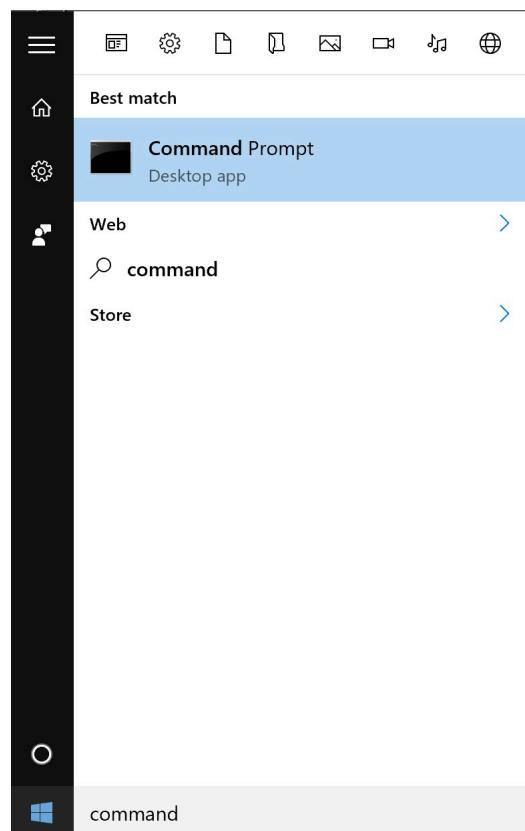


13 Local Network

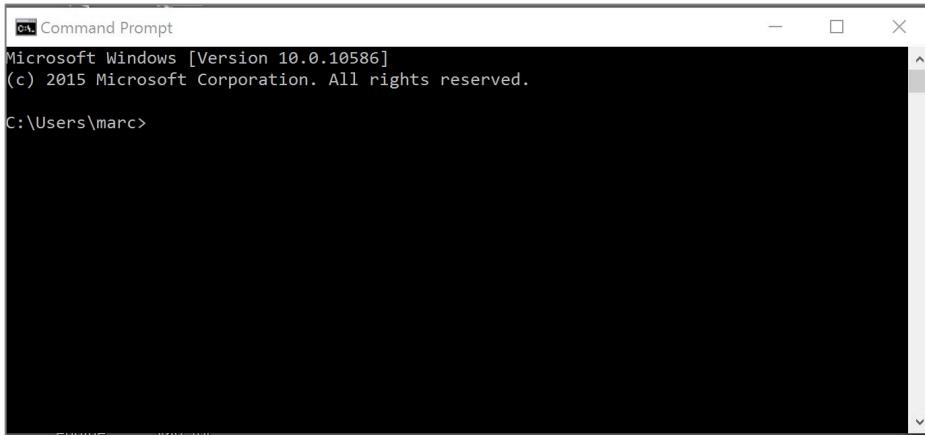
7. The MAC address of an iPhone may be found in the *Settings > General > About > Wi-Fi Address* field.



8. The MAC address of a Windows 10 device can be found with the ipconfig command in the command prompt.
 - a) In Windows 10, click in the *Search the Web and Windows* field in the bottom left corner, and then enter *command prompt*. Double-click on *Command Prompt* in the *Best match* pop-up.



- b) The *Command Prompt* window appears.



- c) Enter *ipconfig -all*. A listing of all network addresses for the device appears. The MAC address will show as the *Physical Address*.

A screenshot of a Windows Command Prompt window titled "Command Prompt". The window shows the output of the ipconfig -all command. It includes information about Autoconfiguration, Tunnel adapter Local Area Connection*, and various connection-specific details like Description, Physical Address, and Default Gateway. The Physical Address listed is 00-00-00-00-00-E0. The command prompt line shows "C:\Users\marc>^Z".

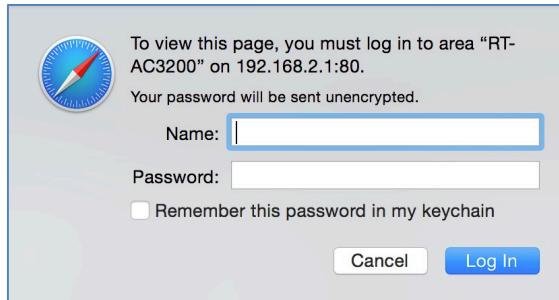
- d) Close the Command Prompt.

Create a list in your router of allowed devices:

9. Launch a web browser.
10. Enter the IP address of the wireless router.
11. In the *URL* or *Address* field, enter the IP address of the wireless router.

13 Local Network

12. At the *Authentication* window, enter the user name and password of the router administrator. This is not the administrator of your computer.

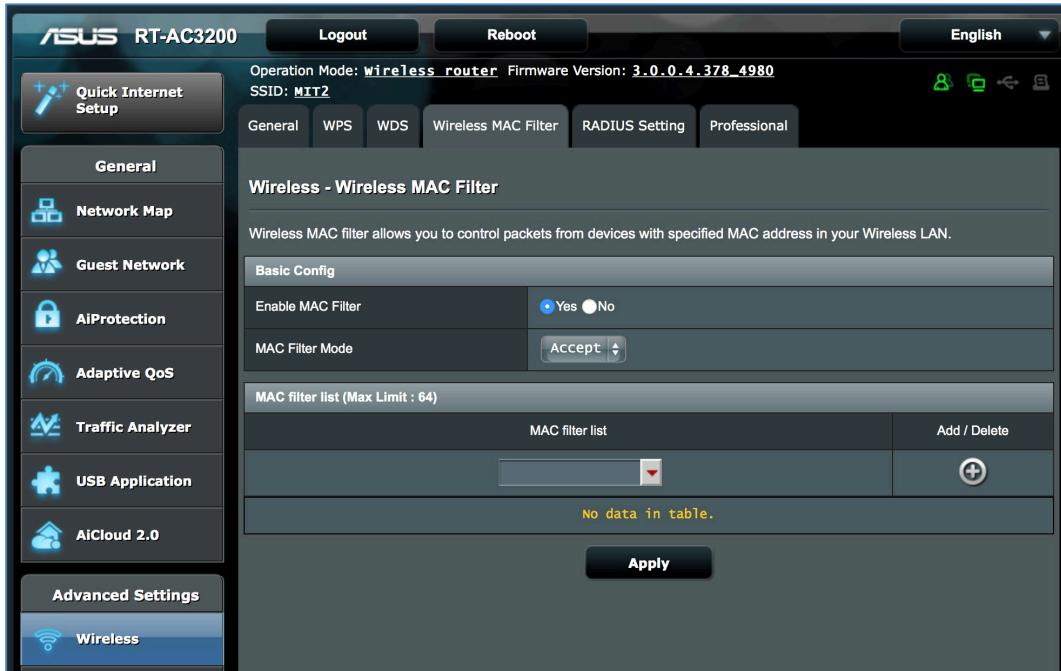


13. The wireless router control panel will appear.

- Please keep in mind that all routers—even from the same company—have slightly different interfaces.

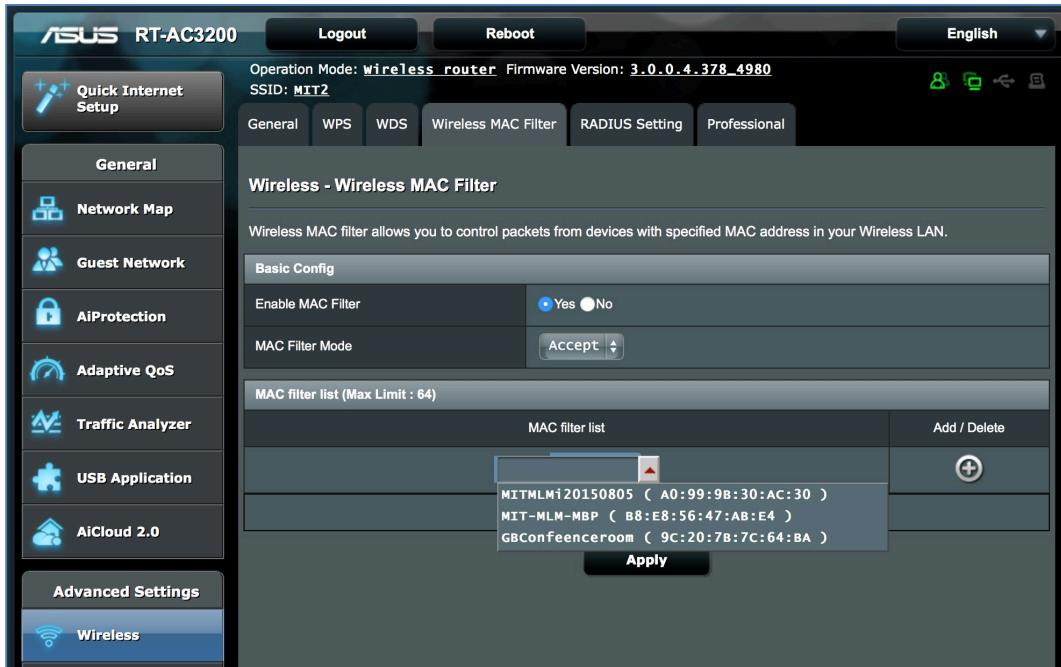


14. From the sidebar select *Wireless*, select the *Wireless MAC Filter* tab, enable the *Yes* radio button for *Enable MAC Filter*, and then set the *MAC Filter Mode* pop-up menu to *Accept*.



15. Clicking the disclosure triangle beneath the *MAC filter list* displays all of the devices currently connected to the router via Wi-Fi. Selecting any of these

adds its MAC address to the *MAC filter list*. You may also manually enter a MAC address to this field.



16. With a desired MAC address entered in to the *MAC filter list* field, click the *Add/Delete* button to add the device to the list.
17. Repeat the previous 2 steps for each device to be allowed onto the Wi-Fi network.
18. Click the *Apply* button to save changes.
19. Close the browser window to exit out of your wireless router.

Congratulations! You have secured your wireless network so that only authorized devices are granted access.

13.6 Router Penetration

The connection point between your Internet provider cable, DSL, fiber, radio, etc. and your Local Area Network (LAN) is a *Router*. A router is a device designed to connect two different types of networks.

Every router has at least some basic security controls built in, including the ability to filter out what it thinks are attempts to hack into your network, and the ability to forward specific types of data packets to a specific computer within your LAN, or to point specific types of data packets to a specific computer on the Internet.

Malware often attempts to alter these configurations so that either the malware or the criminals behind the malware have an easier time harvesting your data. Because of this, it is wise to routinely inspect the condition of your router. How often is “routine?” Within larger and security-conscious organizations, it is common to have a network administrator dedicated to maintaining watch over the status of network equipment. For a small business or household, once every month wouldn’t be too often.

Common areas of router penetration include:

- **Port forwarding**¹⁰: Port forwarding is useful if you have a service such as a web server running that you wish to be accessible from the internet. However, if ports are being forwarded without purpose, the firewall is being bypassed and your internal computers may be visible from the internet.
- **DMZ**¹¹: Related to Port Forwarding is the DMZ, or De-Militarized Zone. DMZ is typically used to route *all* external traffic for a specific IP address, regardless of service request, to a specific computer. Unless there is a unique need, it should remain disabled.
- **RAM-Resident Malware**: Many router malware make their home in the RAM of the router. In this way they can take control of your data traffic without showing in the interface.

¹⁰ https://en.wikipedia.org/wiki/Port_forwarding

¹¹ [https://en.wikipedia.org/wiki/DMZ_\(computing\)](https://en.wikipedia.org/wiki/DMZ_(computing))

- **Firmware¹²:** It is vital to keep the router firmware up to date. Just as with any software, router firmware will always have vulnerabilities. Over time, criminals (including some government organizations) discover how to use these vulnerabilities to their benefit. Keeping the firmware updated helps to stay a step ahead of this problem.

13.6.1 Assignment: Verify Apple Airport Port Security Configuration

In this assignment you will verify the integrity of your Apple Airport (Extreme or Express) base station.

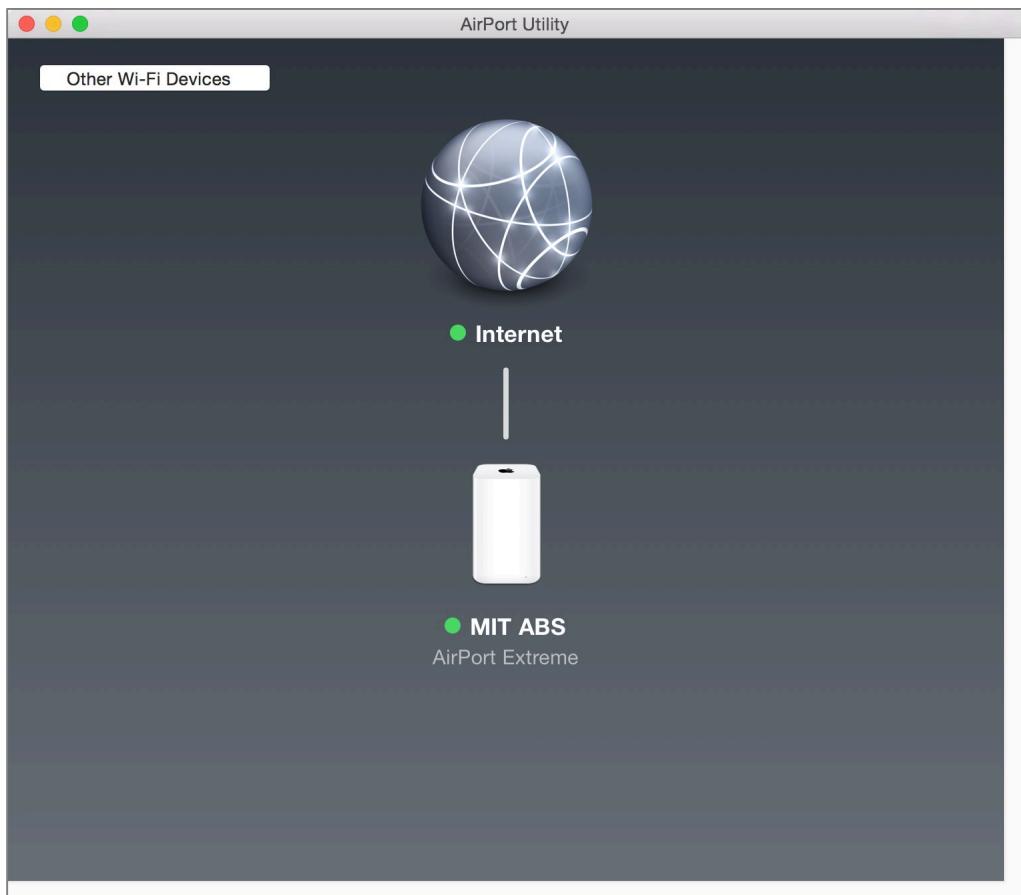
Some malware will make its home in the router RAM. Also, over time router RAM may accumulate corruption. The fix for both issues is the same—power cycling.

1. After verifying that all users have disconnected from the Internet and have closed any connections to other devices on the network, pull the power cord from the back of the Apple Airport.
2. Wait a minute.
3. Plug the power cord back into the Apple Airport. It may take up to two minutes for it to be fully operational.

¹² <https://en.wikipedia.org/wiki/Firmware>

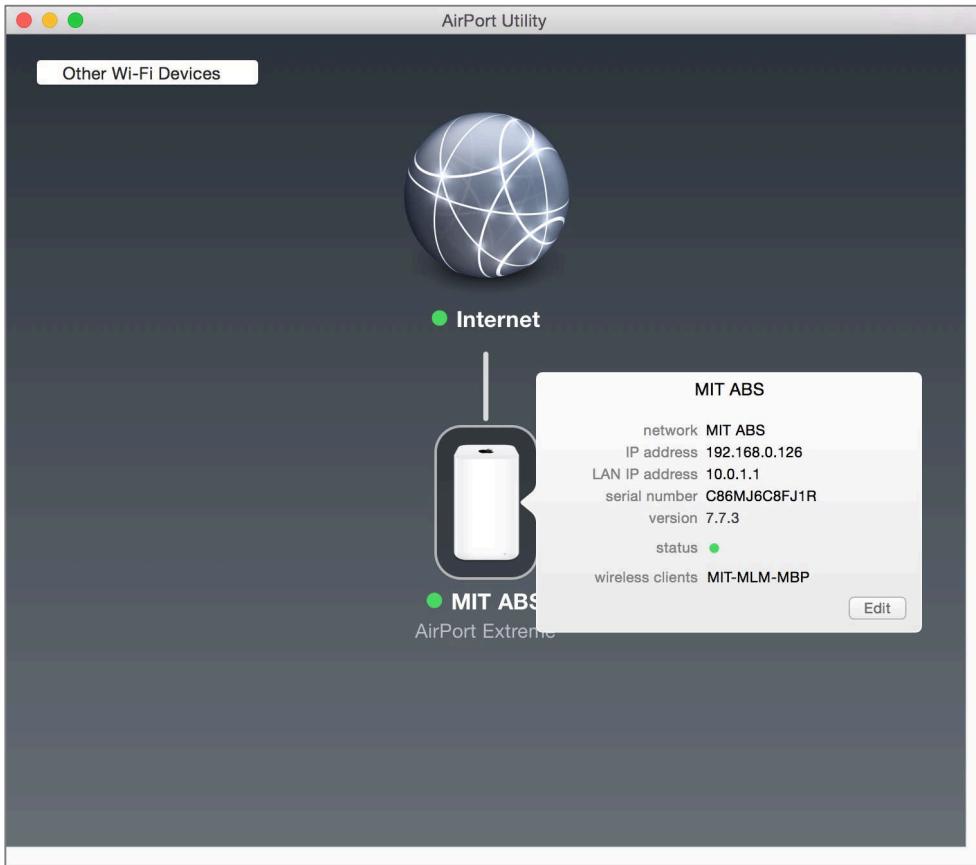
13 Local Network

4. Open *Airport Utility*, located in */Applications/Utilities*. The main window opens. Click on the target base station (in this example, the *MIT ABS*.)



Verify there are no reported problems or firmware updates available.

5. In the pop-up window, to the right of *Status*, verify that there are no reported problems and that no update notification is present. If either condition exists, select the associated button to either resolve the issue or update firmware.

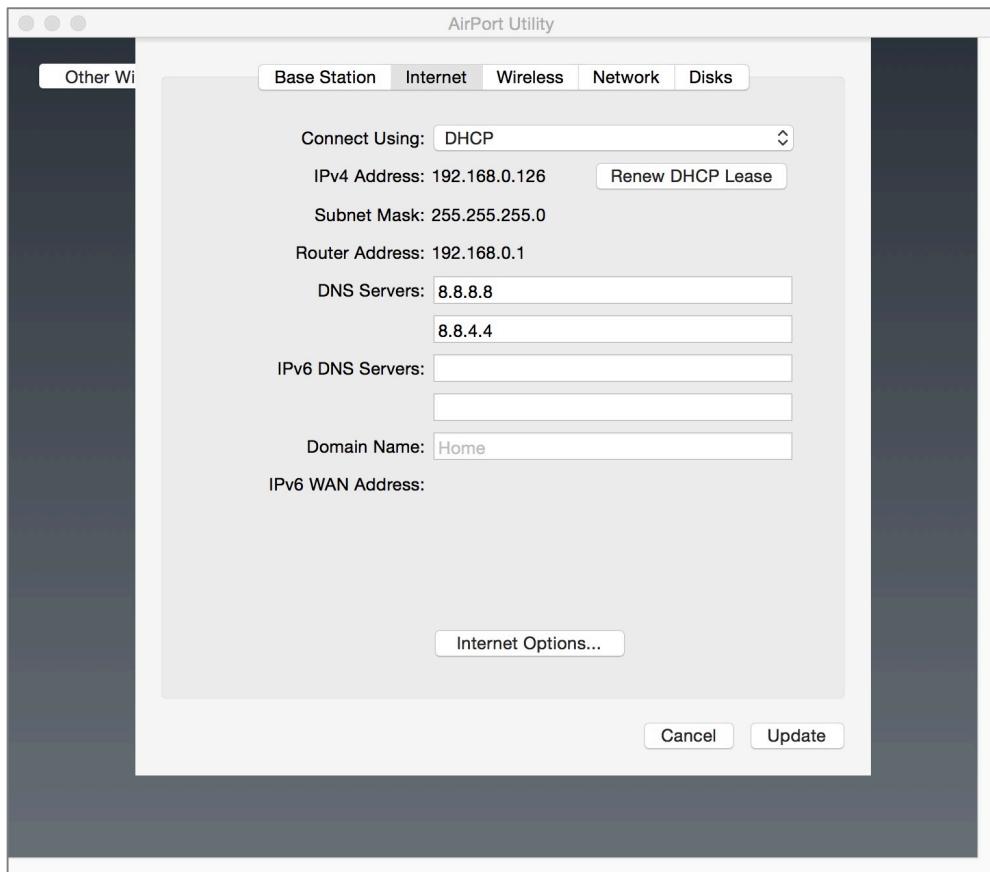


6. If there are no issues, select the *Edit* button.

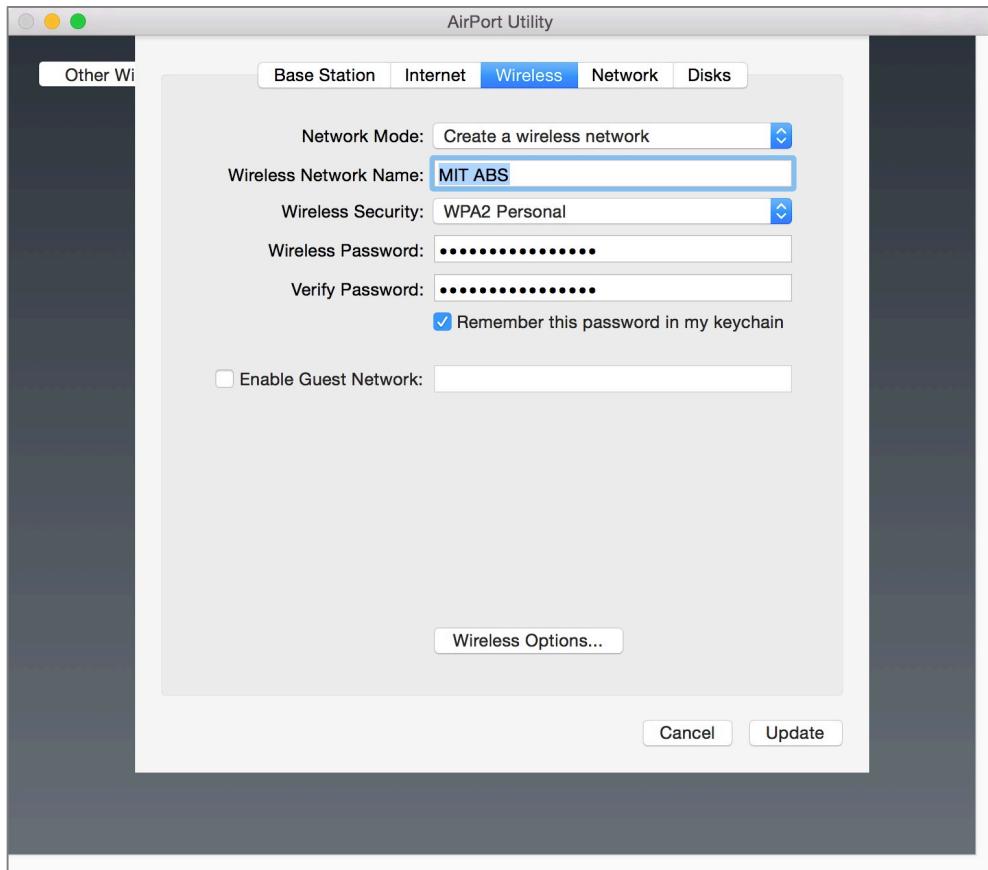
Verify your DNS Servers are configured properly.

7. Select the *Internet* tab. Look in the *DNS Servers* fields and verify these are set to the IP address of the servers you wish to use. If you are uncertain, these may be set to:
 - DNS Servers under the control of your Internet provider. You may contact them for the proper IP addresses.

- DNS Servers under the control of your organization. You may contact your IT department for the proper IP addresses.
- The IP address of your modem (not recommended, as you don't have certainty that the modem has not been compromised.)
- Any of the thousands of free and commercial DNS providers. In this example, we are using Google DNS.



10. Verify the *Wireless Security* field is set to *WPA2 Personal*, or if you know you have a RADIUS¹³ server within your environment, *WPA2 Enterprise*.



11. If changes have been made, select the *Update* button.

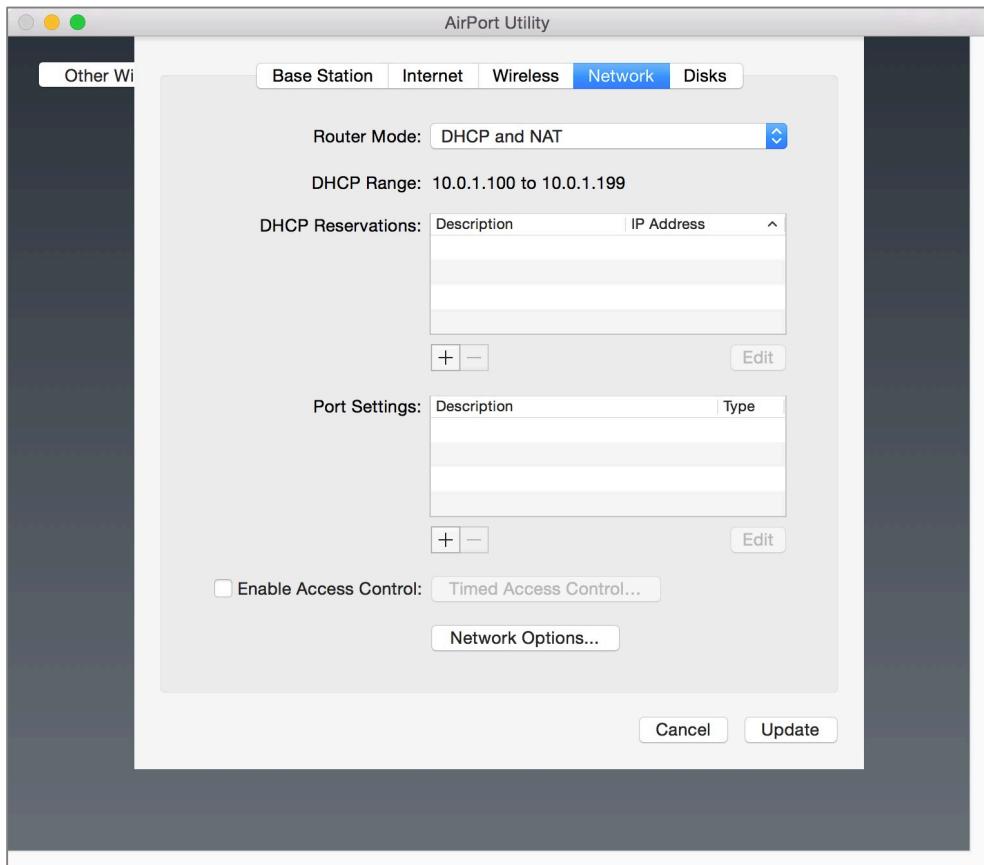
Verify port forwarding.

12. Select the *Network* tab. If there are any settings in the *Port Settings* area, verify there is a demonstrable business need for them, and that they are pointing to the proper devices. If not, remove them.

¹³ <https://en.wikipedia.org/wiki/RADIUS>

13 Local Network

13. If any changes have been made, select the *Update* button.



14. Quit Airport Utility.

You are in great shape. Be sure to repeat this check at least monthly.

13.6.2 Assignment: Verify Non-Apple Airport Router Security Configuration

In the example below I'm using an ASUS RT-AC3200. Although all routers have a somewhat different interface, most share the same functions.

Remove any RAM-resident malware

Some malware will make its home in the router RAM. Also, over time router RAM may accumulate corruption. The fix for both issues is the same—power cycling.

1. After verifying that all users have disconnected from the Internet and have closed any connections to other devices on the network, power off the router. If yours does not have an on/off switch, pull the power cord from the back of the router.
2. Remove the router batteries (if any).
3. Wait a minute.
4. Insert the router batteries (if any).
5. Power on the router. It may take up to 3 minutes for it to be fully operational.
6. Open a browser and enter the IP address of your router.
7. At the prompt, enter the administrator user name and password.

Verify router firmware is up to date.

8. Select *Administration* from the sidebar, and then select the *Firmware Upgrade* tab.
9. Scroll down to the *Firmware Version* field. The currently installed version number is listed.

13 Local Network

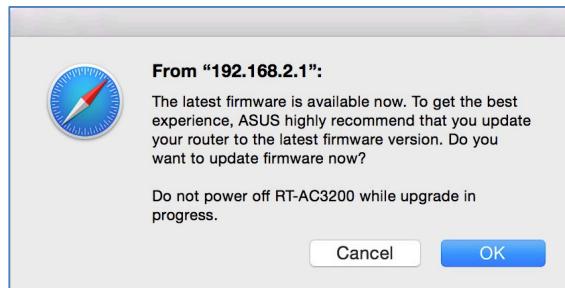
10. To the right of this field is the *Check* button. Select it.

The screenshot shows the ASUS RT-AC3200 router's web configuration interface. The top navigation bar includes 'Logout' and 'Reboot' buttons, and a language selection dropdown set to 'English'. The main header displays 'Operation Mode: Wireless router' and 'Firmware Version: 3.0.0.4.378_4980'. Below this, the SSID 'MIT2' is shown. A toolbar at the top has tabs for 'Operation Mode', 'System', 'Firmware Upgrade' (which is selected), and 'Restore/Save/Upload Setting'. On the left, a sidebar lists various features: General (Quick Internet Setup, Network Map, Guest Network, AiProtection, Adaptive QoS, Traffic Analyzer, USB Application, AiCloud 2.0); Advanced Settings (Wireless, LAN, WAN, IPv6, VPN, Firewall); and Administration (selected). The central content area is titled 'Administration - Firmware Upgrade'. It contains a note with four points about firmware upgrades. Below the note is a table with two rows:

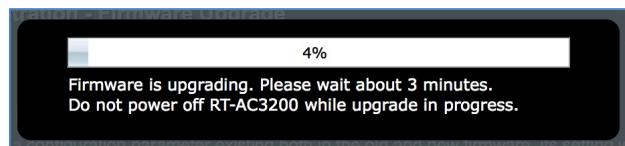
Product ID	RT-AC3200
Signature Version	1.064

Under 'Firmware Version', the current value is '3.0.0.4.378_4980-g8c12667'. To its right is a 'Check' button. Below this is a 'New Firmware File' input field with a 'Choose File' button and a message 'no file selected'. At the bottom right of the form is an 'Upload' button.

11. A dialog box will display, stating either the firmware is up to date, or a new version is available.



12. In this example, there is a more recent version, so we will select the *OK* button to download and install the update. If there is no new version available, exit the browser.
13. Note: During the download/install, the router will be offline, breaking Internet access for all on the network.
14. The firmware is downloaded.



15. When the download/install completes, you may exit the browser.

Verify no unnecessary Port Forwarding.

16. In the sidebar select WAN, select the *Virtual Server/Port Forwarding* tab, scroll down to the *Basic Config* area. View if *Enable Port Forwarding* is set to Yes. If it is, verify there is a demonstrable business need for this feature to be on. More information will be found in the next step.

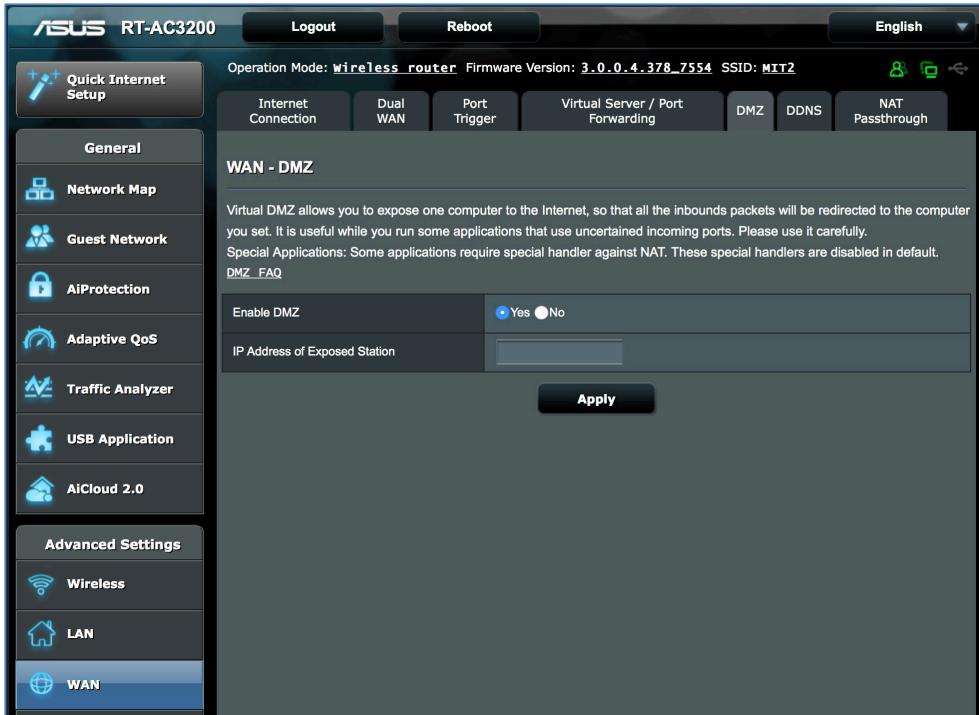
The screenshot shows the ASUS RT-AC3200 router's web interface. The sidebar on the left has icons for Quick Internet Setup, General (Network Map, Guest Network, AiProtection, Adaptive QoS, Traffic Analyzer, USB Application, AiCloud 2.0), Advanced Settings (Wireless, LAN, WAN, IPv6, VPN, Firewall), and WAN (selected). The main content area at the top shows operation mode as 'wireless router' and SSID as 'MIT2'. Below this, tabs include Internet Connection, Dual WAN, Port Trigger, Virtual Server / Port Forwarding (selected), DMZ, DDNS, and NAT Passthrough. A sub-section titled 'WAN - Virtual Server / Port Forwarding' explains the purpose of port forwarding. It includes a note about specifying a port range for clients on the same network, followed by two bullet points: one about a conflict with the web server and another about a conflict with the native FTP server. Below this is a 'Basic Config' section with an 'Enable Port Forwarding' checkbox set to 'Yes'. The 'Port Forwarding List' section shows a table with columns: Service Name, Port Range, Local IP, Local Port, Protocol, and Add / Delete. The table is currently empty, displaying 'No data in table.' At the bottom is an 'Apply' button.

17. Scroll further down to the *Port Forwarding List* area. If Port Forwarding is turned on, this area will list which network services are being routed to which devices. Verify there is a demonstrable business need for this configuration. If not, then turn *Enable Port Forwarding* to No.
18. Select the *Apply* button.

Verify DMZ configuration.

Similar to Port Forwarding is *DMZ*. When *DMZ* is enabled, all inbound packets are routed to that device. This allows a single device on your network to be accessible from the Internet. This presents a very high level of vulnerability for that device. Unless there is a demonstrated business need for this function, and adequate steps have been taken to prevent unwanted penetration, turn *DMZ* off.

- From the router control panel sidebar, select *WAN*, and then select the *DMZ* tab.



- Scroll down to the *Enable DMZ* area. If it is set to *Yes*, verify there is a demonstrable business need for this function. The next step will provide additional information.
- Below *Enable DMZ* is *IP Address of Exposed Station*. If *DMZ* is enabled, verify there is a true need for it based on this device. If not, set *Enable DMZ* to *No*.
- If changes were made, select the *Apply* button.

23. Exit the browser.

Congratulations, your router is in great shape. Remember to perform this same checkup at least monthly.

13.7 Review Questions

1. macOS client to macOS client communications are encrypted. (True or False)
2. macOS client to macOS server communications can be encrypted. (True or False)
3. The WEP Wi-Fi encryption protocol should be used whenever possible. (True or False)
4. The WPA Wi-Fi encryption protocol should be used whenever possible. (True or False)
5. The WPA2 Wi-Fi encryption protocol should be used whenever possible. (True or False)
6. Of the two encryption algorithms—TKIP and AES—which should be used?
7. The network hardware that decodes and modulates the signal from your Internet provider to your cable or telephone jack is called a _____.
_____.
8. The network hardware that allows hundreds or thousands of devices to interact between the local network and Internet is called a _____.
_____.
9. The network hardware or software that inspects data traffic between the Internet and local network devices is called a _____.
_____.
10. The network hardware that allows multiple devices to connect and interact with each other and the router is called a _____.
_____.
11. The network hardware that allows tens or hundreds of wireless devices to connect to a network is called a _____.
_____.
12. The network connection speed between a macOS computer and Wi-Fi Access Point can be found by _____.
_____.
13. A _____ address includes a unique manufacturer code and a unique device code.
_____.

14 Web Browsing

Distrust and caution are the parents of security.

–Benjamin Franklin¹

¹ https://en.wikipedia.org/wiki/Benjamin_Franklin

14.1 HTTPS

Due to an extraordinary marketing campaign, everyone knows the catchphrase: *What happens in Vegas, stays in Vegas.* With few exceptions, web surfers think the same thing about their visits.

Most websites use HTTP² (Hypertext Transport Protocol) to relay information and requests between user and website and back again. HTTP sends all data in clear text—anyone snooping on your network connection anywhere between your computer and the web server can easily see everything that you are doing.

Typically, the only exceptions you will come across are financial and medical sites, as they are mandated by law to use HTTPS³ (Hypertext Transport Protocol Secure). HTTPS uses the SSL⁴ (Secure Socket Layer) encryption protocol to ensure that all traffic between the user and server is military-grade encrypted.

- Note: With the recent changes in Google Search Engine Optimization⁵ (SEO) guidelines that give a higher priority to HTTPS sites, it will soon become common for sites to use encryption.

Although it is unlikely that you would ever be in the position to enter your password or bank account into an unsecure web page, you are almost guaranteed to enter your identity information, such as full name, address, phone number, and social security number. It is effortless for an identity thief to copy this information.

Anytime that you visit a web page that is secured using https, it will be reflected in the URL or address field of your web browser.

In the following example, I visit Wikipedia.org by entering <http://www.wikipedia.org> in my browser address field:



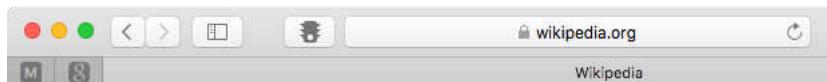
² https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol

³ <https://en.wikipedia.org/wiki/HTTPS>

⁴ https://en.wikipedia.org/wiki/Transport_Layer_Security

⁵ https://en.wikipedia.org/wiki/Search_engine_optimization

In the next example, I visit Wikipedia again, but this time I enter <https://www.wikipedia.org> in the address field:



Note how the address field reflects that I am now connected securely by displaying https and the *Lock* icon. Each browser will indicate security slightly differently—some displaying just the https, some just the lock.

- Note: As of this writing, Wikipedia has implemented automatic forwarding from HTTP to HTTPS, so if you enter <http://wikipedia.org>, you are automatically forwarded to <https://wikipedia.org>.

Now that I am connected securely to Wikipedia, snoops will not be able to see my actions. However, they still can see that I am connected to Wikipedia. If you would like to shield yourself completely, continue reading to our chapter on using a Virtual Private Network (VPN.)

Having to remember to connect via HTTPS for each web page is an impossible task. First, you have other, more important items to store in your synapses. Second, many websites do not have an HTTPS option, resulting in many error pages and wasted time during the day.

There are two options to resolve this:

- Automate the attempt to connect to sites via HTTPS
- Encrypt your entire online session using VPN

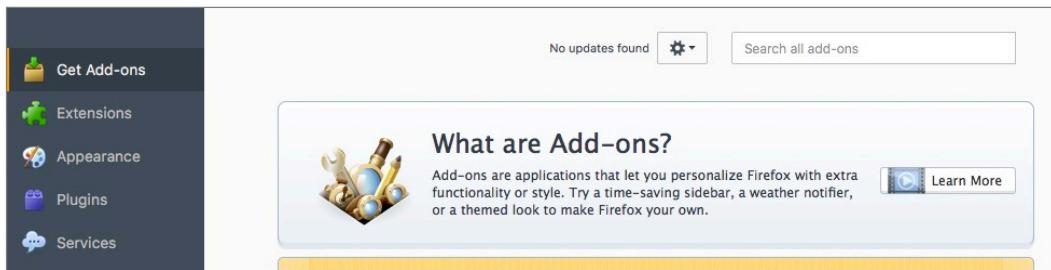
Using VPN is covered in a later chapter. Automating the attempt to connect via HTTPS is both easy and free. All it requires is a freeware plug-in, *HTTPS Everywhere*.

HTTPS Everywhere is available for Firefox, Opera, and Chrome. Unfortunately, this currently leaves Safari users without the option. If you are happy to use either of these two browsers instead of Safari, there is no reason not to install HTTPS Everywhere!

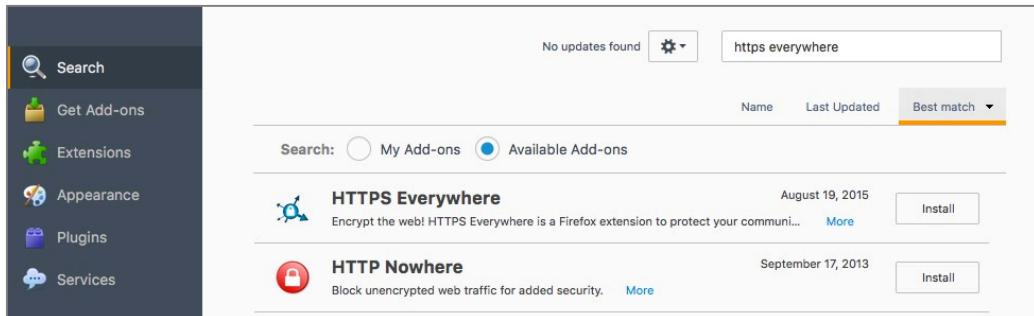
14.1.1 Assignment: Install HTTPS Everywhere

HTTPS Everywhere is available for Firefox, Opera, and Chrome. In this assignment, you will install HTTPS Everywhere into Firefox.

1. If the Firefox browser is not currently installed, open Safari, and the go to <http://firefox.com> to download Firefox.
2. Open Firefox.
3. Select the *Tools* menu > *Add-ons*.
4. Select *Get Add-ons* from the sidebar.



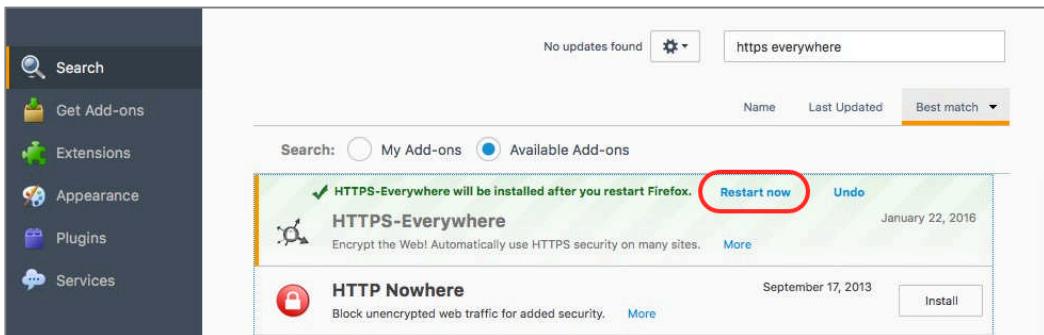
5. In the *Search* field, enter *https everywhere*, and then press the *Return* key. Matching items will appear below.



6. Select the *Install* button to the right of *HTTPS Everywhere*. HTTPS Everywhere will download.

14 Web Browsing

- When the download completes, select the *Restart Now* link.

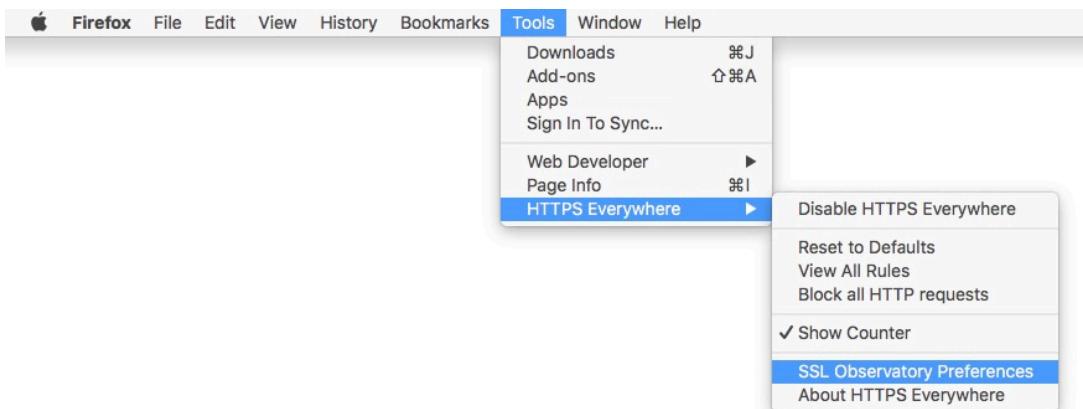


- Firefox will restart.
- The *SSL Observatory* window will open. Select *Yes*.

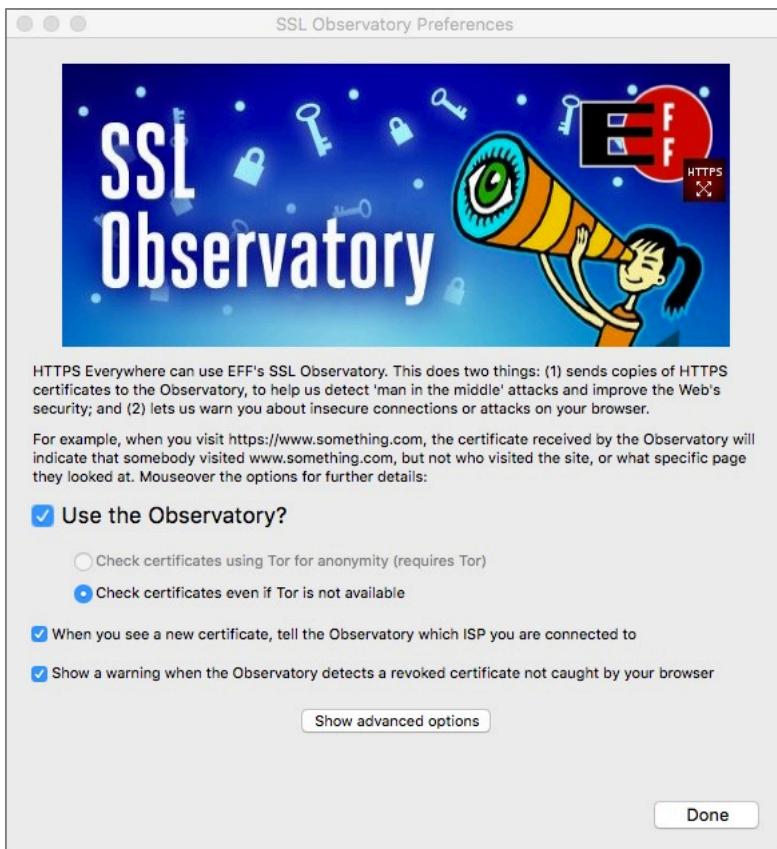


14 Web Browsing

10. Select the *Tools* menu > *HTTPS Everywhere* > *SSL Observatory Preferences*.



11. The *SSL Observatory Preferences* window opens. Select the *Show advanced options*. Configure as below, and then select the *Done* button:



From now on, if a website has an HTTPS option (not all do), then you will be routed automatically to that page instead of the default unsecure page. If the site does not have an HTTPS option, the default unsecure page will load.

14.2 Choose a Browser

There many web browsers available on the market, with each placing a different emphasis on various features. The three most popular browsers for macOS are Safari, Mozilla Firefox, and Google Chrome. Safari is included with macOS, while Chrome and Firefox are available as free downloads. Why might you want to replace Safari with another browser? Chrome integrates tightly with Google's own services, offering features such as direct voice translation and an ultra-minimalistic interface. Firefox touts itself as the most privacy-respecting browsers, and while that is a subjective claim, Firefox does not transmit your data to Google or any other 3rd party company every time you search using the address bar box. While Google considers this “non-identifying information”, IP addresses are identifying at the Internet Service Provider level. This functionality can be changed however, and with some tweaking, it is possible to make Chrome more privacy focused.

Browser	Platform	Price	Notable Features	Privacy
Chrome	Android, iOS, Linux, macOS, Windows	Free	Speed Google Services Integration	Good
Edge	Windows 10	Free (included with Windows 10)	Active X Windows Integration	Fair
Firefox	Android, iOS, Linux, macOS, Windows	Free (Open Source)	Add-ons Privacy	Good
Internet Explorer	Windows	Free (Included with Windows)	Active X Windows Integration	Poor
Safari	macOS, iOS, Windows	Free (included with macOS/OS X and iOS)	History can be shared between all of your macOS and iOS devices	Good

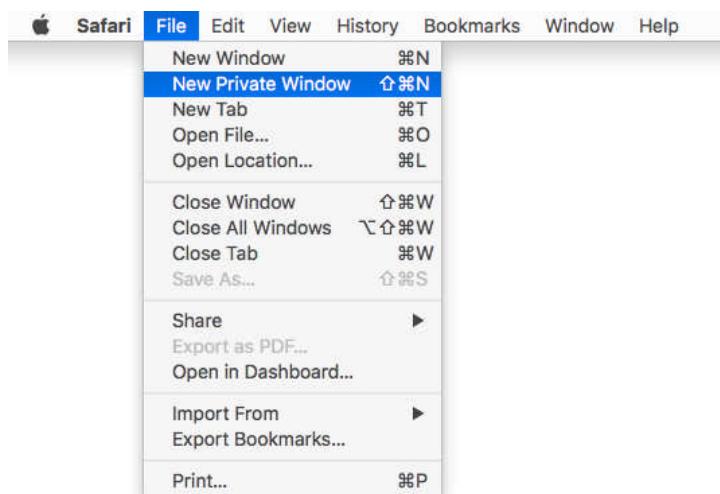
14.3 Private Browsing

Private Mode (Safari), *Private Browsing* (Firefox), and *Incognito Mode* (Chrome), are features that prevent any normally cached data from being written to storage while using a browser. This data includes browsing history, passwords, user names, list of downloads, cookies, and cached files. This is an essential tool if you work on a computer where your account is shared (what's with that?..), or if there is the possibility that someone else will examine your browsing habits. This does not prevent your company IT department or Internet Provider from seeing or recording your browsing habits.

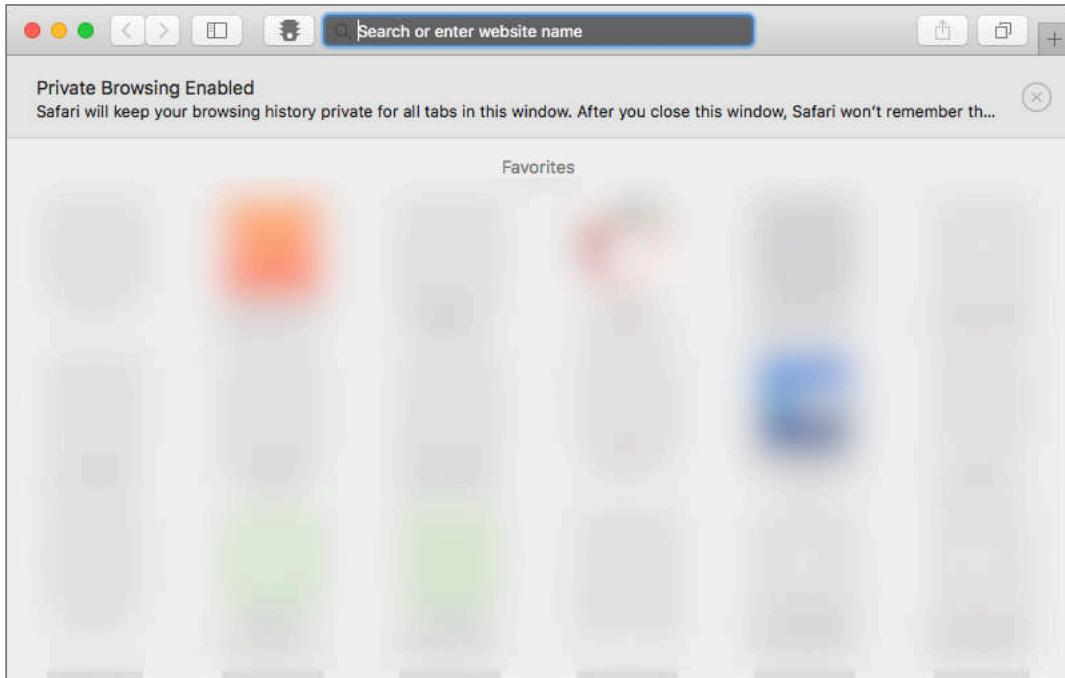
14.3.1 Assignment: Safari Private Browsing

Before we secure your website travels from roaming eyes out on the Internet, we should first be secure from the roaming eyes on the home front. If you have secured your computer to this point, including: Strong password, nobody else has access to your account, your *System Preferences > Security & Privacy* are set to *Require password after sleep or screen saver begins*, it is unlikely that you also need to implement *Safari Private Browsing*. But just in case...

1. From the *Safari File* menu, select *New Private Window*.



2. A new Safari window will appear. You can see that you are in *Private Browsing* by the *Search* field being dark.



Sites that are visited from within this window will leave no trace in the *History*, and cookies are not shared with any other browsing windows.

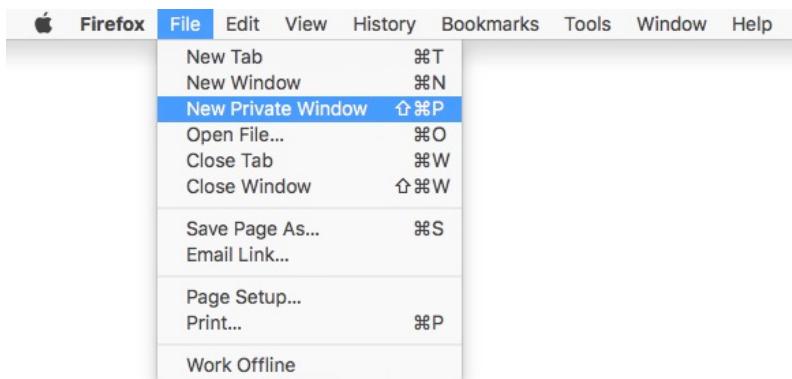
14.3.2 Assignment: Firefox Private Browsing

If you prefer Firefox to Safari, then let us enable its private browsing.

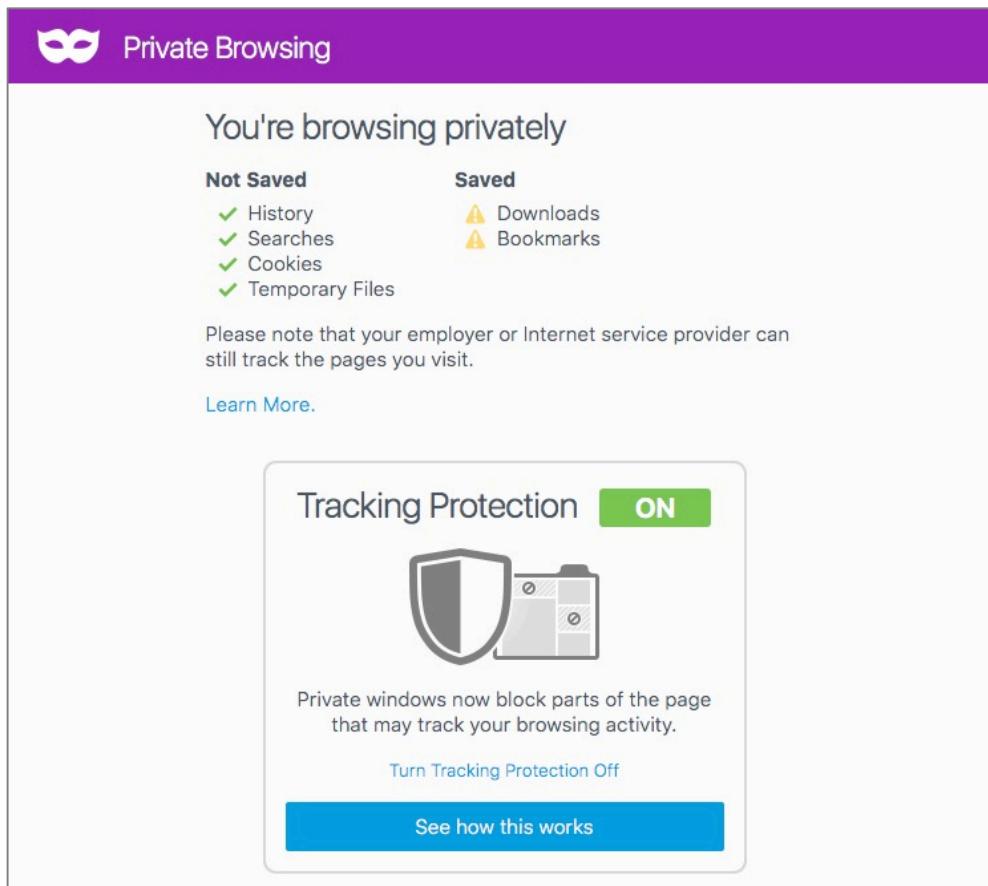
1. Launch Firefox.

14 Web Browsing

2. Select the Firefox *File* menu > *New Private Window*.



3. A new *Private Window* opens, informing that you are now, well, browsing privately.
 - Note: A Firefox *Private Window* will display a mask icon in the left side of a private tab, and in the top right corner of a private window.



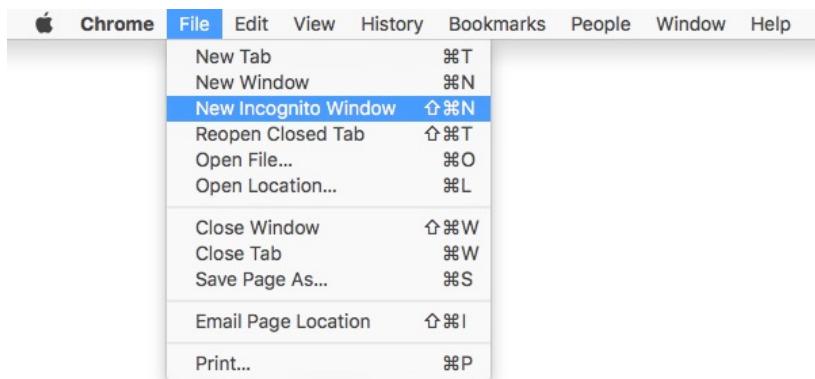
14.3.3 Assignment: Google Chrome Incognito Mode

If your preference leans toward Google Chrome, you can enable its *Incognito Mode*.

1. Launch Google Chrome.

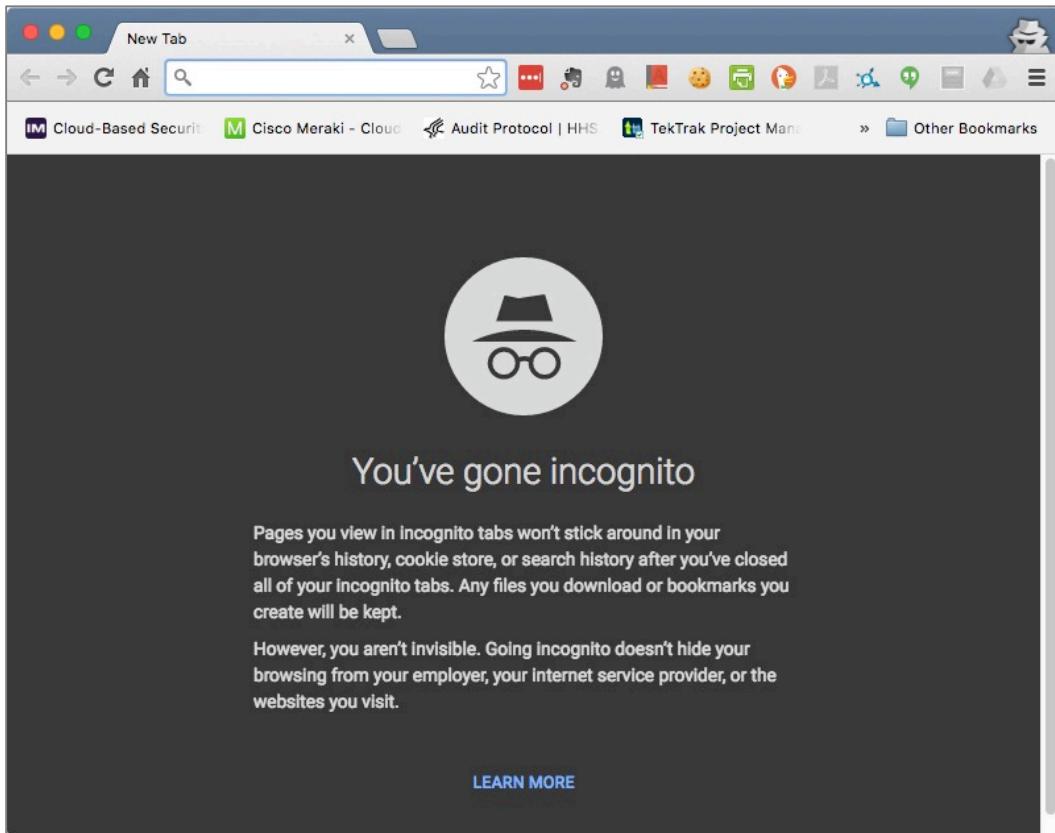
14 Web Browsing

2. Select the *File* menu > *New Incognito Window*.



3. A new *Incognito Window* opens, informing that you have now, gone incognito.

- Note: A Chrome *Incognito Window* will display the incognito icon in the top right corner, and the title bar will turn dark.



14.4 Secure Web Searches

With most web browsers, when performing a search, the search criteria and sites visited are collected and stored by the search engine. The Cookies assigned from one website can communicate with other sites and webpages you open. Also, most search engines record your searches and build a profile of your search history so that your search results will be unique and tailored to your interests.

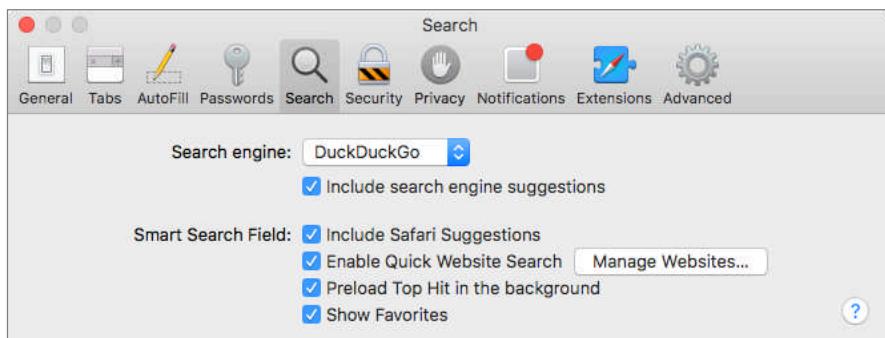
Not so with the *DuckDuckGo* search engine. DuckDuckGo's policy is that it keeps no information on user searches, nor does it track search queries via IP addresses. Subsequently, all search results are identical for everyone.

Starting with OS X 10.10, Safari offers the option to make DuckDuckGo your default search engine. This is a big step towards providing a better level of privacy on the Web.

14.4.1 Assignment: Make DuckDuckGo Your Safari Default Search Engine

In this assignment, you will change the default Safari search engine from Google to the secure search engine DuckDuckGo.

1. Open Safari.
2. Open the *Safari* menu > *Preferences*.
3. Select the *Search* icon from the Toolbar.
4. From the *Search Engine* pop-up menu, select *DuckDuckGo*.



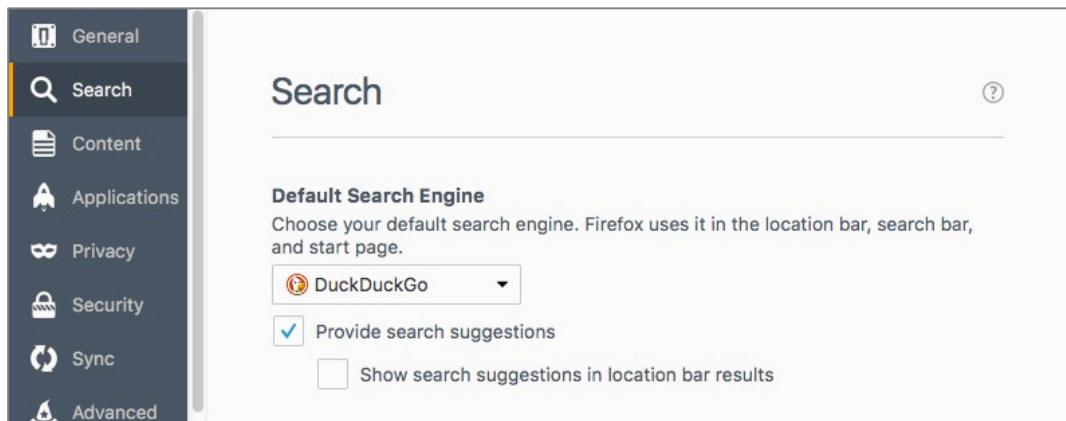
5. Close the Preferences window.

From now on, your default search engine for Safari will be *DuckDuckGo*, hiding your search activities.

14.4.2 Assignment: Make DuckDuckGo Your Firefox Default Search Engine

In this assignment, you will change the default Firefox search engine to the secure DuckDuckGo.

1. Open Firefox.
2. Select the *Firefox* menu > *Preferences*.
3. Select *Search* from the sidebar, and then select *DuckDuckGo* from the *Default Search Engine* pop-up menu.



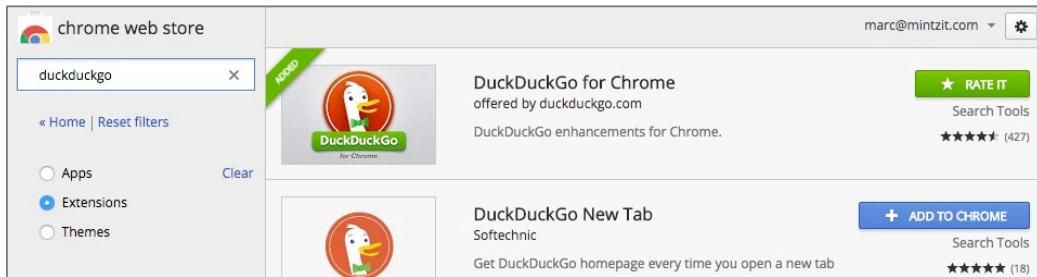
4. Close the Preferences window.

From now on, your default search engine for Firefox will be *DuckDuckGo*, hiding your search activities.

14.4.3 Assignment: Make DuckDuckGo Your Chrome Default Search Engine

In this assignment, you will change the default Chrome search engine to DuckDuckGo.

1. Open Chrome.
2. Select the *Chrome* menu > *Preferences*, and then select *Extensions* from the sidebar. Scroll to the bottom of the *Extensions* window, and then select *Get more extensions*.
3. From the sidebar, in the *Search* field, enter *DuckDuckGo*, select the *Extensions* radio button, and then press the *Return* key. *DuckDuckGo for Chrome* listing will appear.



4. To the right, select the *ADD TO CHROME* button.
5. Close the Preferences window.

From now on, your default search engine for Chrome will be *DuckDuckGo*, hiding your search activities.

14.5 Clear History

You just realized that: 1) Your mother is coming over, 2) you have been naughty on the web all day, 3) you did not turn on Private Browsing, and 4) your mom will feel insulted if you insist that an account for her must to be created instead of accepting her protest: *Oh, baby, I only need to check my AOL email. Just let me get on your account for a minute.*

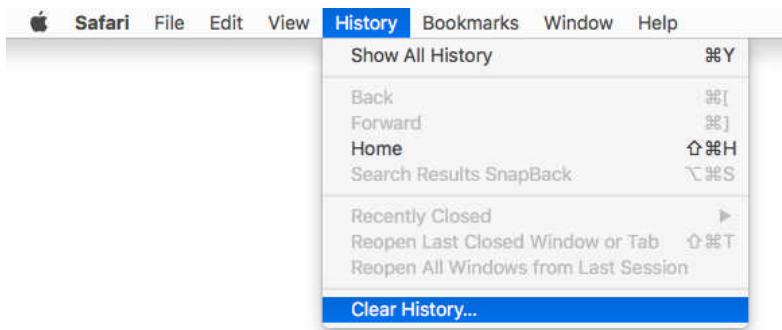
Is it time to panic?

Not yet! You can erase your entire (steamy) browsing history in one click.

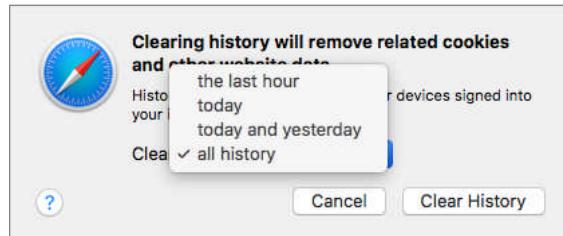
14.5.1 Assignment: Clear the Safari History

In this assignment you will clear your entire browsing history in Safari. Be forewarned, there is no recovery from this action. If you wish to keep your history, pass on this assignment.

1. Open Safari, and then select the *History* menu > *Clear History...*



2. A dialog box opens asking for what time frame you wish to clear your history. Make your selection, and then select the *Clear History* button.

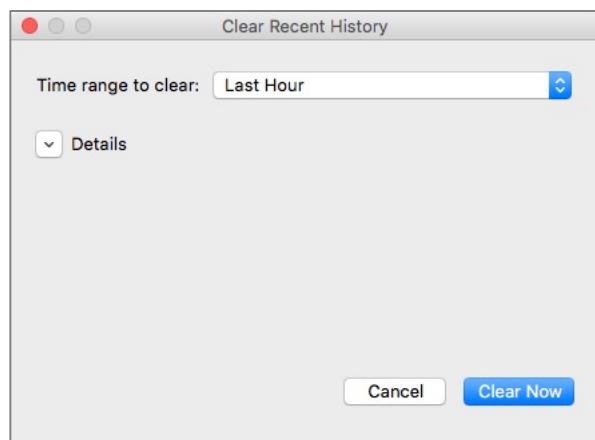


The Safari history is now cleared as you defined.

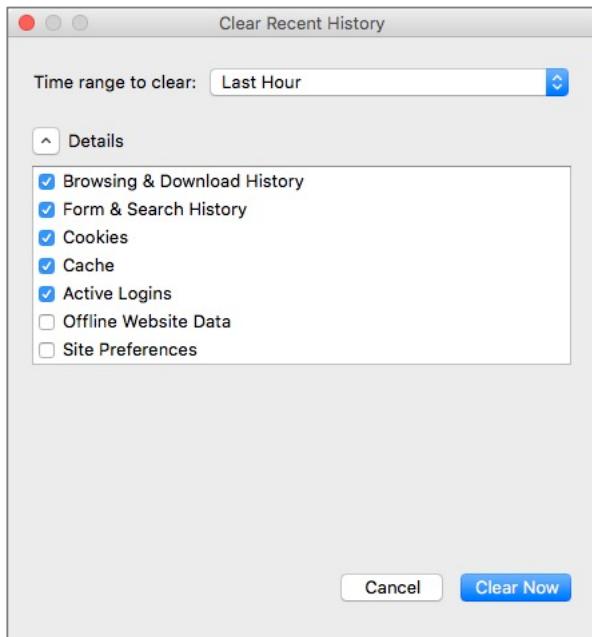
14.5.2 Assignment: Clear the Firefox Browsing History

In this assignment, you will clear your Firefox browsing history. Be forewarned, there is no recovery from this action. If you wish to keep your history, pass on this assignment.

1. Open Firefox.
2. Select the *History* menu > *Clear Recent History...* The *Clear All History* window opens.



3. Select the *Details* disclosure button to expand your options.



4. Select the *Time range to clear*, which history items are to be cleared, and then click the *Clear Now*.
5. Close the *Clear Recent History* window.

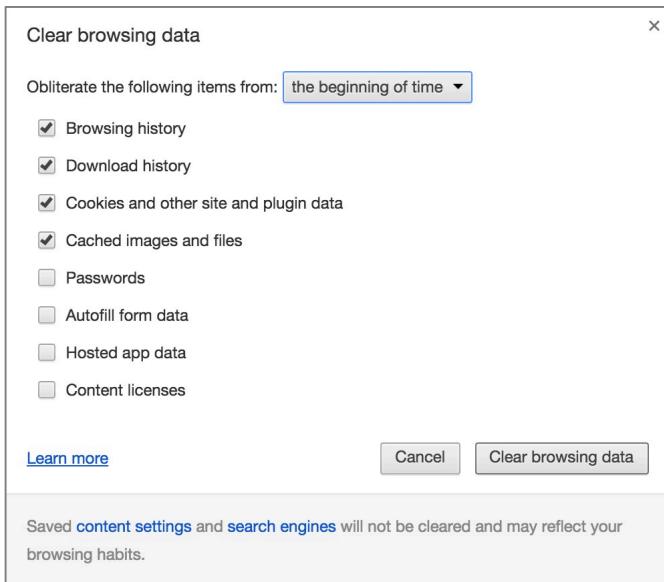
The Firefox history is now history.

14.5.3 Assignment: Clear the Chrome History

In this assignment you will clear your browsing history in Chrome. Be forewarned, there is no recovery from this action. If you wish to keep your history, pass on this assignment.

1. Open Chrome.

2. Select the *Chrome* menu > *Clear Browsing Data...* The *Clear Browsing Data* window opens.



3. Select which items are to be cleared, and then click the *Clear Browsing data* button.

Done!

14.6 Browser Plug-Ins

One of the great advances in personal computer software development was the concept of plug-ins or extensions⁶. These small strings of code add functionality to the host application. In the case of web browsers, this may be anything from the ability to encrypt web-based email, to viewing proprietary video formats.

The bad news about plug-ins is that they run with the full power of the host application. This means that a malicious plug-in may have the power to secretly redirect your web browser to fake websites (such as a phony copy of your bank), or harvest all of your passwords, monitor your purchases, etc.

There are many malicious plug-ins. It is vital to only install those plug-ins that you actually need to install, to know which plug-ins are installed, and to rid yourself of unnecessary plug-ins.

14.6.1 Assignment: Install Trafficlight Plug-In for Safari

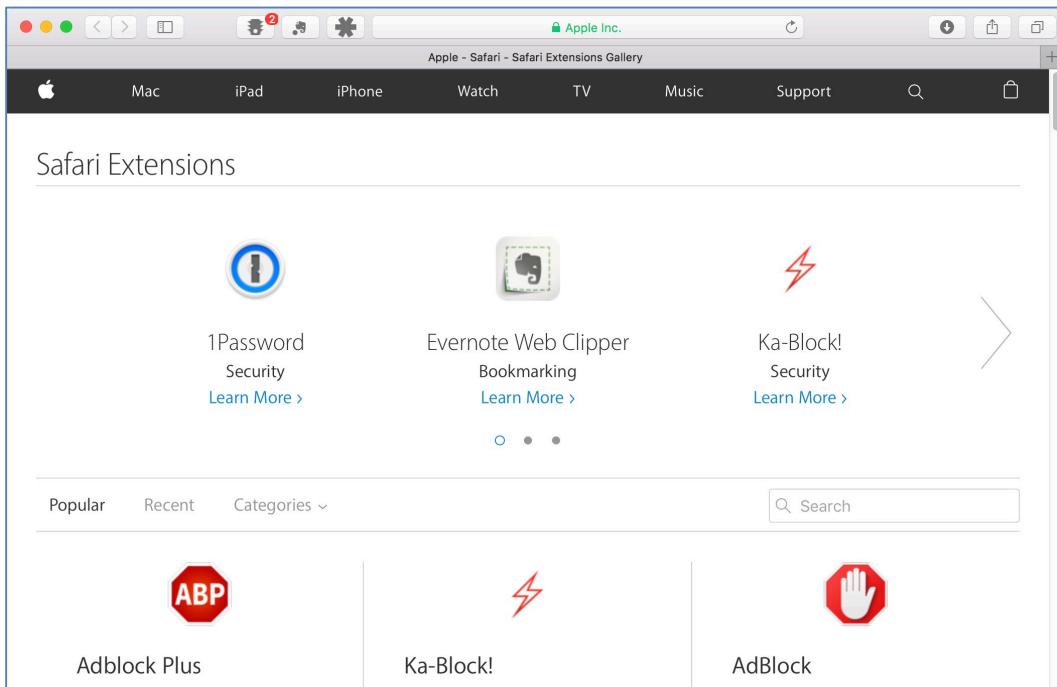
In this assignment, you will search for extensions for Safari, and install the *Trafficlight* anti-malicious website extension.

1. Open Safari.

⁶ [https://en.wikipedia.org/wiki/Plug-in_\(computing\)](https://en.wikipedia.org/wiki/Plug-in_(computing))

14 Web Browsing

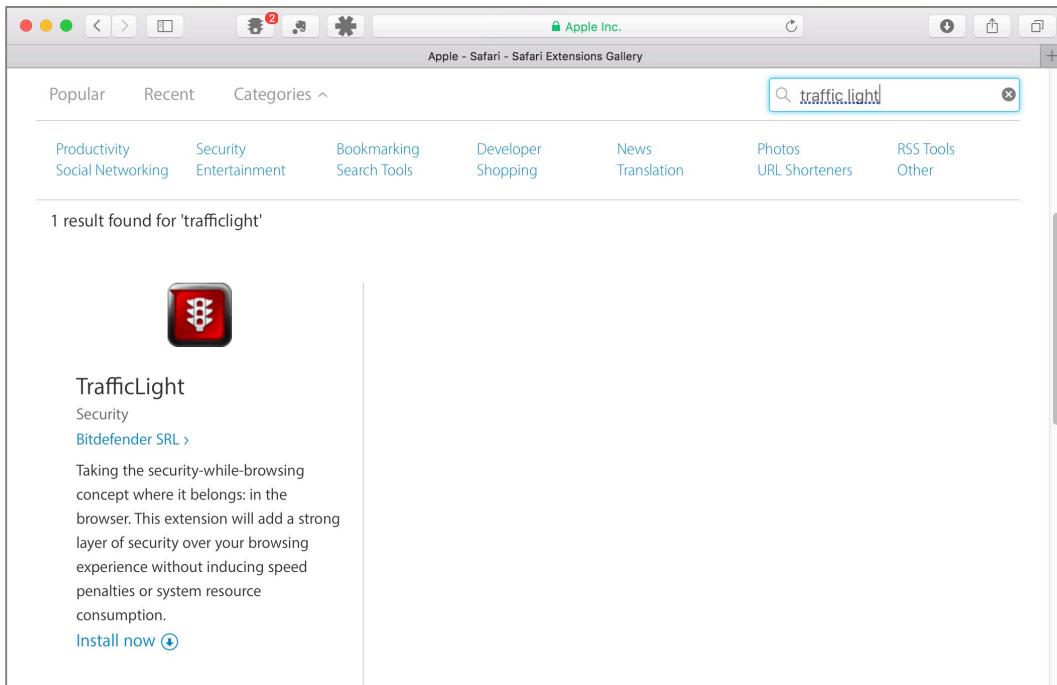
2. Select the *Safari* menu > *Safari Extensions...* The *Safari Extensions* page opens.



3. Select the *Popular*, *Recent*, or *Categories* links to explore the available *Safari Extensions*.
4. Explore and review some of the available extensions.
5. In the *Search* field, enter *Trafficlight*, and then tap the *Return* key. The *Trafficlight from Bitdefender* page opens. Trafficlight is a browser extension that adds protection from malicious websites. If you happen upon a

14 Web Browsing

compromised or malicious site, it will alert you and provide a button to back out of the site before your system is penetrated.



The screenshot shows the Safari Extensions Gallery interface. At the top, there's a navigation bar with icons for back, forward, and search, followed by the text "Apple - Safari - Safari Extensions Gallery". Below the search bar, there are categories: Popular, Recent, Categories (with a dropdown arrow), and a search input field containing "traffic.light". Underneath these are more categories: Productivity, Security, Bookmarking, Developer, News, Photos, RSS Tools, Social Networking, Entertainment, Search Tools, Shopping, Translation, URL Shorteners, and Other. A message below the categories says "1 result found for 'trafficlight'". The main content area displays a single extension card for "TrafficLight". It features a red traffic light icon, the name "TrafficLight", the category "Security", a link to "Bitdefender SRL >", and a descriptive text: "Taking the security-while-browsing concept where it belongs: in the browser. This extension will add a strong layer of security over your browsing experience without inducing speed penalties or system resource consumption." At the bottom of this card is a blue "Install now" button with a circular arrow icon. To the right of the card is a vertical scroll bar.

6. Select the *Install now* link located under the description of Trafficlight.
7. When installation completes, you will see a traffic light icon in your Safari tool bar.



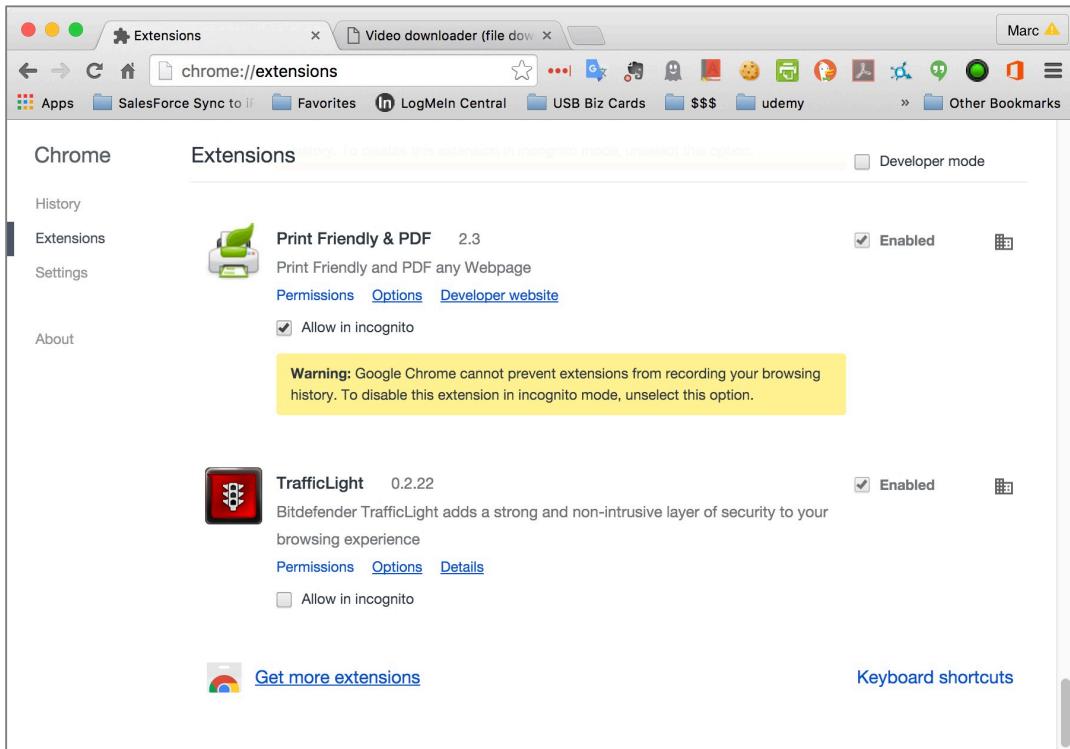
14.6.2 Assignment: Install Trafficlight Plug-In for Google Chrome

In this assignment, you will search for extensions for Chrome, and install the *Trafficlight* anti-malicious website extension.

1. Open Google Chrome.

14 Web Browsing

2. Select the *Menu* icon (3 lines at the right edge of the tool bar) > *Settings*.
3. Select *Extensions* from the left sidebar. The *Chrome Extensions* page opens.
4. Scroll to the bottom of the page, and then select *More Extensions*.



5. Explore the available extensions.

14 Web Browsing

- In the *Search* field, enter *Trafficlight*, and then tap the *Return* key. The results page appears.

The screenshot shows the Chrome Web Store interface. In the search bar at the top left, the text "trafficlight" is entered. Below the search bar, there are two main sections: "Apps" and "Extensions". Under "Apps", there is one result: "WOT" by bluecrx.com, which is described as "WOT: Web of Trust, Website Reputation Ratings". There is a blue "ADD TO CHROME" button next to it. Under "Extensions", there is one result: "TrafficLight" by trafficlight.bitdefender.com, which is described as "Bitdefender TrafficLight adds a strong and non-intrusive layer of security to your browsing experience". This extension has a green "ADDED" badge and a green "FREE" badge. There is a green "RATE IT" button next to it. Both extensions have a rating of four stars.

- In the *Trafficlight by Bitdefender* area, select the *Add To Chrome* button. If prompted to confirm, confirm the addition.
- Once installed, you will see the Trafficlight icon in the Chrome tool bar—a green dot.



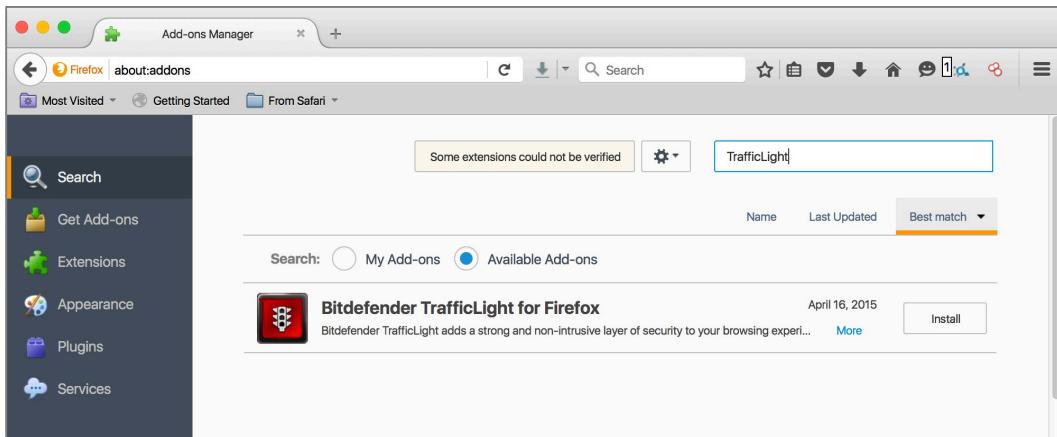
14.6.3 Assignment: Install Plug-Ins for Firefox

In this assignment, you will search for plug-ins for Firefox, and install the *Trafficlight* anti-malicious website extension.

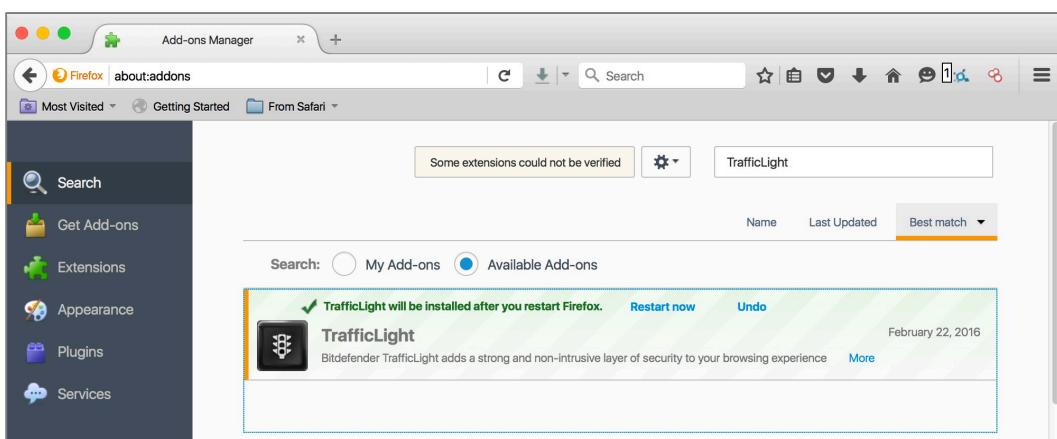
- Open Firefox.
- Select the *Menu* menu (3 lines at the right edge of the tool bar) > *Add-ons*.
- Select *Get Add-ons* from the left sidebar.
- Explore the available add-ons.

14 Web Browsing

5. In the *Search all add-ons* field, enter *Trafficlight*, and then tap the *Return* key. The results page appears.



6. In the Bitdefender TrafficLight for Firefox area, select the Install button.
7. At the confirmation window, confirm OK.
8. Once installed, select the Restart now link.



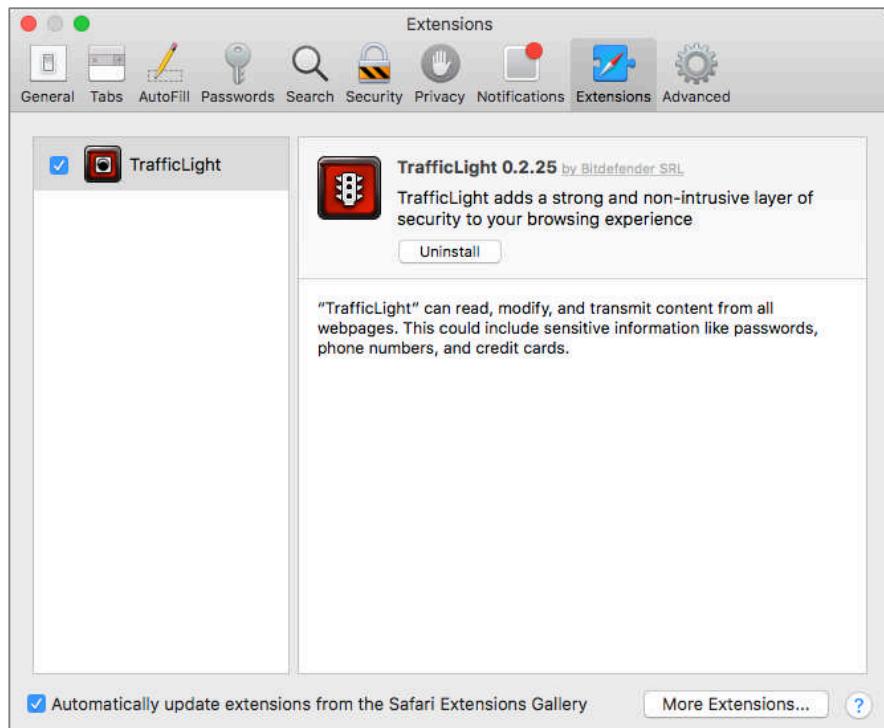
9. Once installed, you will see the Trafficlight icon in the Chrome tool bar—a green dot.



14.6.4 Assignment: Find and Remove Extensions From Safari

In this assignment, you will see the installed Safari Extensions, determine if they are what you need to be installed, and remove those that are not needed.

1. Open Safari.
2. Select the *Safari* menu > *Preferences*.
3. From the Preferences tool bar, select *Extensions*.



4. All currently installed Extensions will display in the sidebar.
5. If you see any Extensions that you do not remember installing, perform an Internet search to discover what they do, and if they present a vulnerability.
6. If you determine you don't want any Extensions installed, select the target Extension in the sidebar, and then select the *Uninstall* button under the target extension.

14.6.5 Assignment: Find and Remove Extensions From Google Chrome

In this assignment, you will see the installed Chrome Extensions, determine if they are what you need to be installed, and remove those that are not needed.

1. Open Chrome.
2. Select the *Menu* menu (3 lines at the right edge of the tool bar) > *Settings*.
3. Select *Extensions* from the left sidebar. The *Chrome Extensions* page opens.

The screenshot shows the 'Extensions' page in Google Chrome. The sidebar on the left has options for 'History', 'Extensions' (which is selected and highlighted in blue), 'Settings', and 'About'. The main area displays three extensions:

- Adobe Acrobat** (15.1.0.1): Converts current web pages to Adobe PDF files. It is enabled. A warning message states: "Warning: Google Chrome cannot prevent extensions from recording your browsing history. To disable this extension in incognito mode, unselect this option." There are 'Permissions', 'Options', and 'Details' links.
- Application Launcher for Drive (by Google)** (3.2): Opens Drive files directly from the browser. It is enabled. A warning message states: "Warning: Google Chrome cannot prevent extensions from recording your browsing history. To disable this extension in incognito mode, unselect this option." There are 'Permissions', 'Details', and 'Allow in incognito' checkboxes.
- Chrome Remote Desktop** (49.0.2623.40): Allows access to other computers over the Internet. It is enabled. A warning message states: "Warning: Google Chrome cannot prevent extensions from recording your browsing history. To disable this extension in incognito mode, unselect this option." There are 'Permissions', 'Details', and 'Allow in incognito' checkboxes.

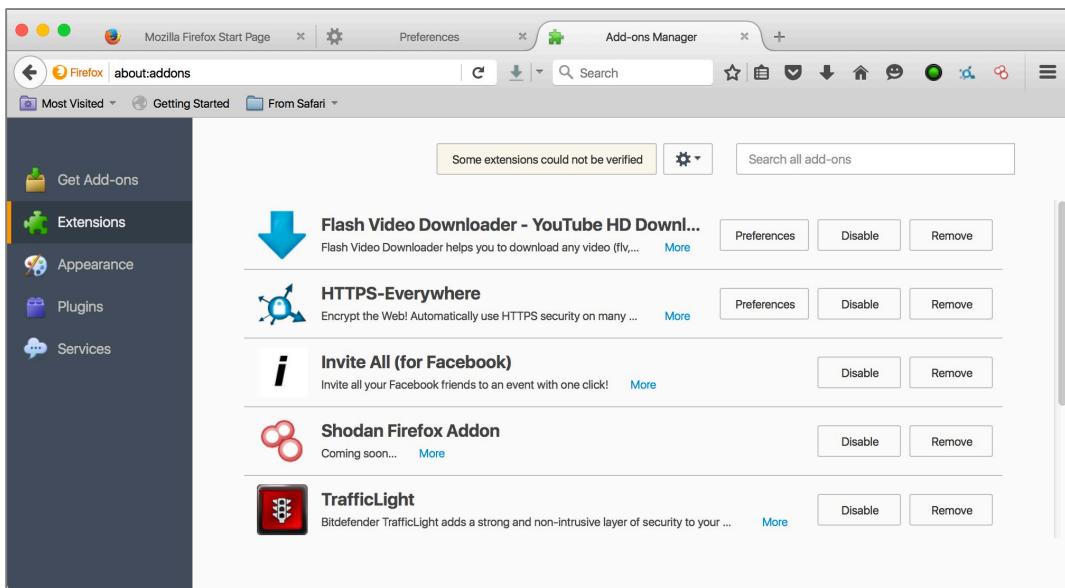
4. If you see any Extensions that you do not remember installing, perform an Internet search to discover what they do, and if they present a vulnerability.

5. If you determine you don't want any Extensions installed, click the *Trash* icon to the far right.

14.6.6 Assignment: Find and Remove Add-Ons From Firefox

In this assignment, you will see the installed Firefox Extensions, determine if they are what you need to be installed, and remove those that are not needed.

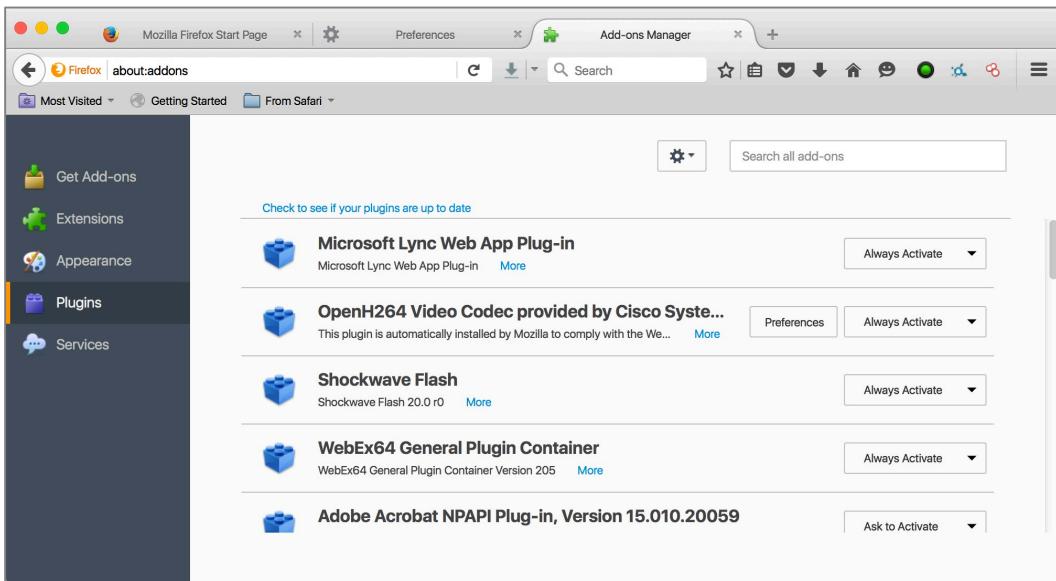
1. Open Firefox.
2. Select the *Menu* menu (3 lines at the right edge of the tool bar) > *Add-ons*.
3. Select *Extensions* from the left sidebar.



6. If you see any Extensions that you do not remember installing, perform an Internet search to discover what they do, and if they present a vulnerability.
7. If you determine you don't want any Extensions installed, click the *Remove* button to the far right.

14 Web Browsing

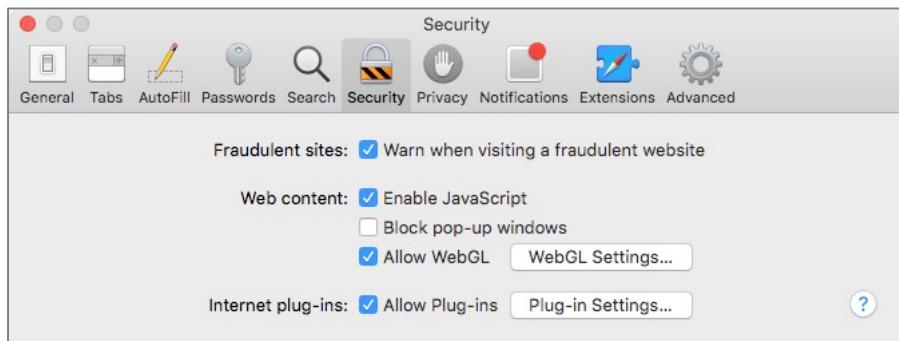
8. Select *Plugins* from the left sidebar.



9. Perform an Internet search on any plugins that are unfamiliar to you. If you determine you don't want one active, select *Never Activate* from the pop-up menu to the far right.

14.6.7 Assignment: Secure the Safari Browser

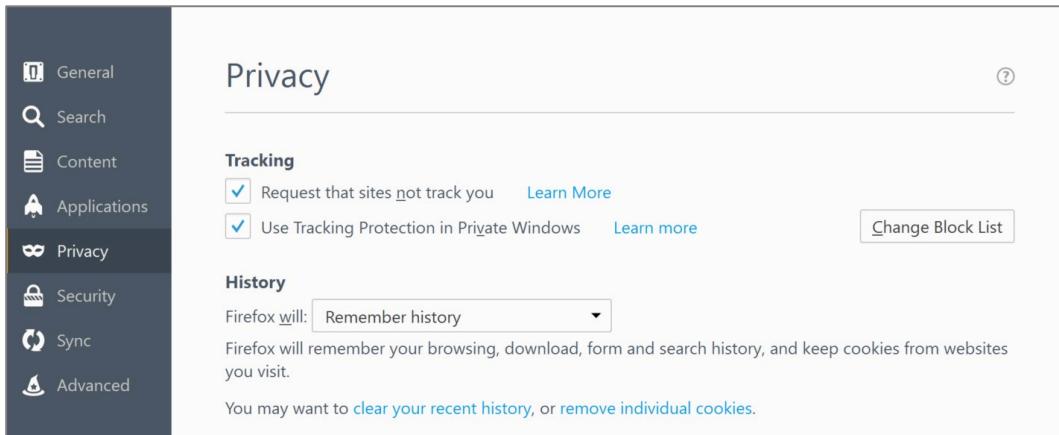
1. Open Safari, click the *Safari* menu > *Preferences*.
2. Click the *Security* button.
3. Enable *Warn when visiting a fraudulent website*.



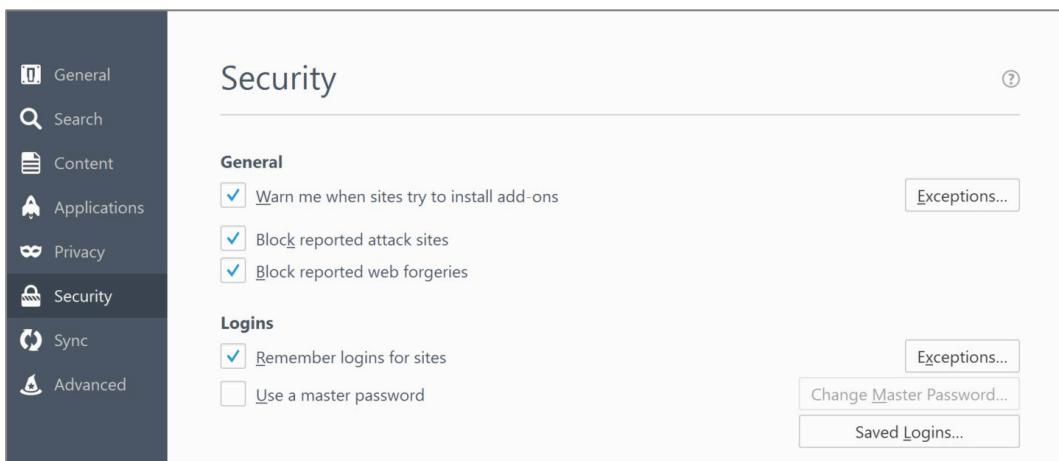
4. Close *Preferences*.

14.6.8 Assignment: Secure the Firefox Browser

1. Open Firefox, click the *Firefox menu* (three horizontal lines), and then select the *Preferences* button.
5. In the Preferences window, click on *Privacy* in the left-hand pane. In the *Tracking* area, enable *Request that sites not track you*, and *Use Tracking Protection in Private Windows*.



6. Click on *Security*. Check to enable *Warn me when sites try to install add-ons*, *Block reported attack sites*, and *Block reported web forgeries*.

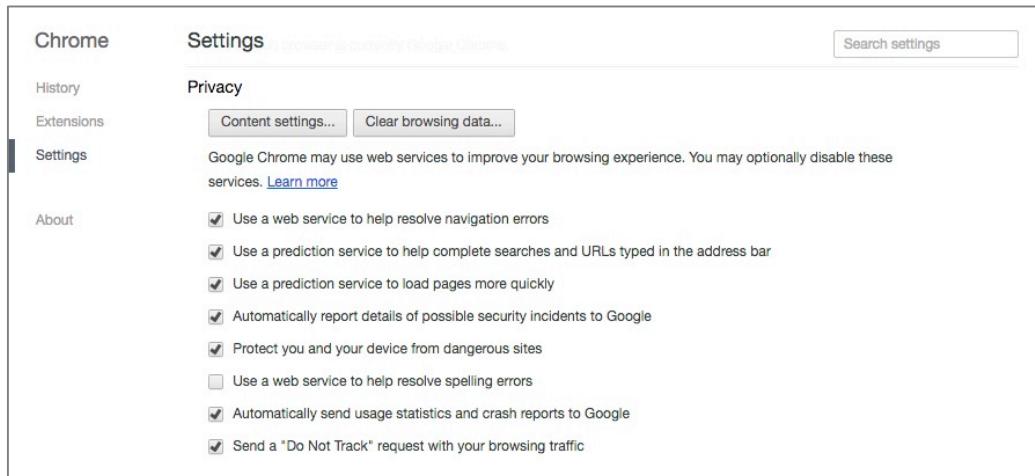


Congratulations. Your Firefox Browser is now secure from phishing attacks, third-party advertisers and known malware sites.

14.6.9 Assignment: Secure the Chrome Browser

Just the same as with Firefox, there are settings within Chrome that will keep you properly secured against the bad guys.

1. Open *Chrome*, select the menu item (3 dots), and then click *Settings*.
2. Scroll down to click on *Advanced Settings*.
3. Scroll down to *Privacy*. Enable *Protect you and your device from dangerous sites*, and *Do Not Track*.

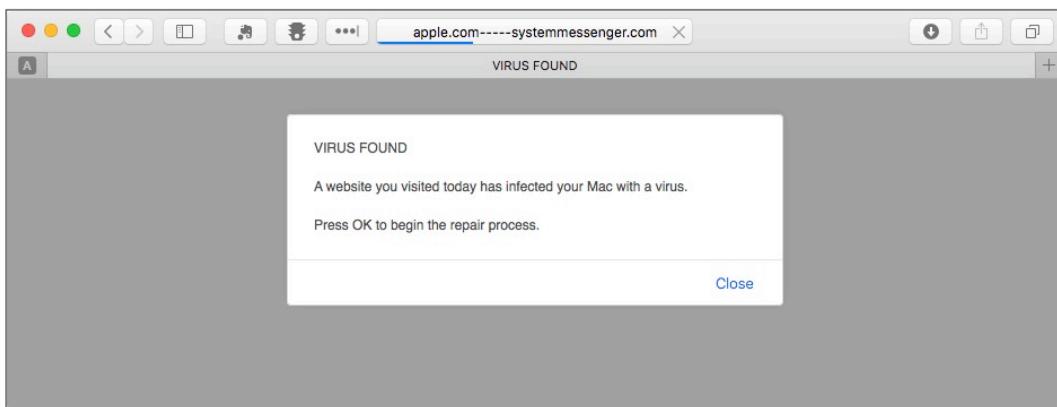


Congratulations. Your Chrome Browser is now secure from phishing attacks, third-party advertisers and known malware sites.

14.7 Fraudulent Websites

As of this writing, there are over 1,000,000,000 active websites⁷. Within that, there may be millions of fraudulent websites. Of the diverse types of fraud found on the Internet⁸, among the most common are websites that misrepresent who they are. This may be in the form of appearing like Bank of America, but with a URL of perhaps <http://bankofamerica.cm>, instead of the true <http://bankofamerica.com>. In this case, the criminal is hoping for someone to make the typo. Once at their site, you would enter your account and password as typical. The difference is that this time, the criminal now has your credentials—and all of your money within minutes.

As a side note, in this specific example as of the time of this writing, this URL actually *is* a scam site. But not for the scheme mentioned. When I went to <http://bankofamerica.cm>, I was routed to the following:



If we look at the full URL, it is: <http://apple.com-----systemmessenger.com/dgkg/?city=Albuquerque®ion>New%20Mexico&count ry=US&ip=71.222.135.33&isp=Qwest%20Communications%20Company%20Llc &os=OS%20X&osv=OS%20X%2010.11%20El%20Capitan&browser=Safari&brow serversion=Safari%209&voluumdata=BASE64dmlkLi4wMDAwMDAwNi01Yzg0 LTRjNjYtODAwMC0wMDAwMDAwMDBfX3ZwaWQuLmRl...>

⁷ <http://www.internetlivestats.com/total-number-of-websites/>

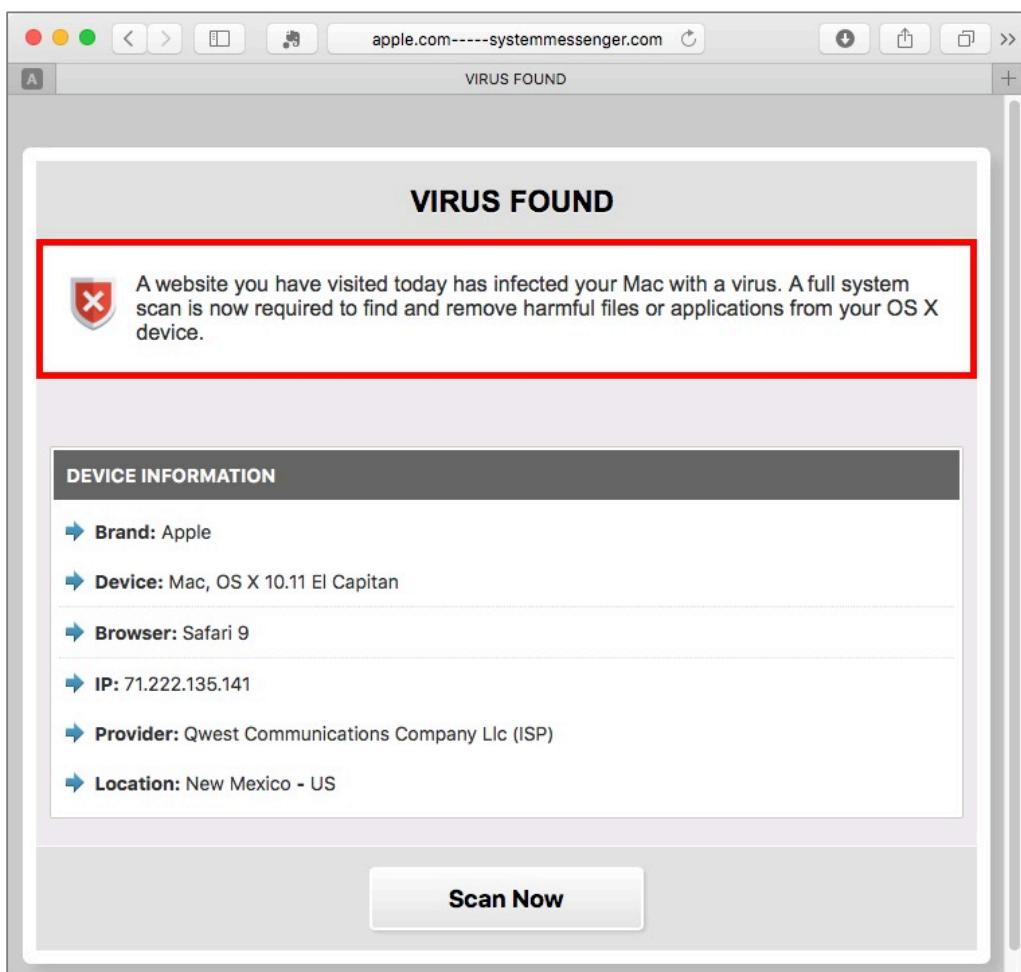
⁸ https://en.wikipedia.org/wiki/Internet_fraud

From this URL we can see that the criminal site attempts to appear as though it is Apple reporting that I have a virus.

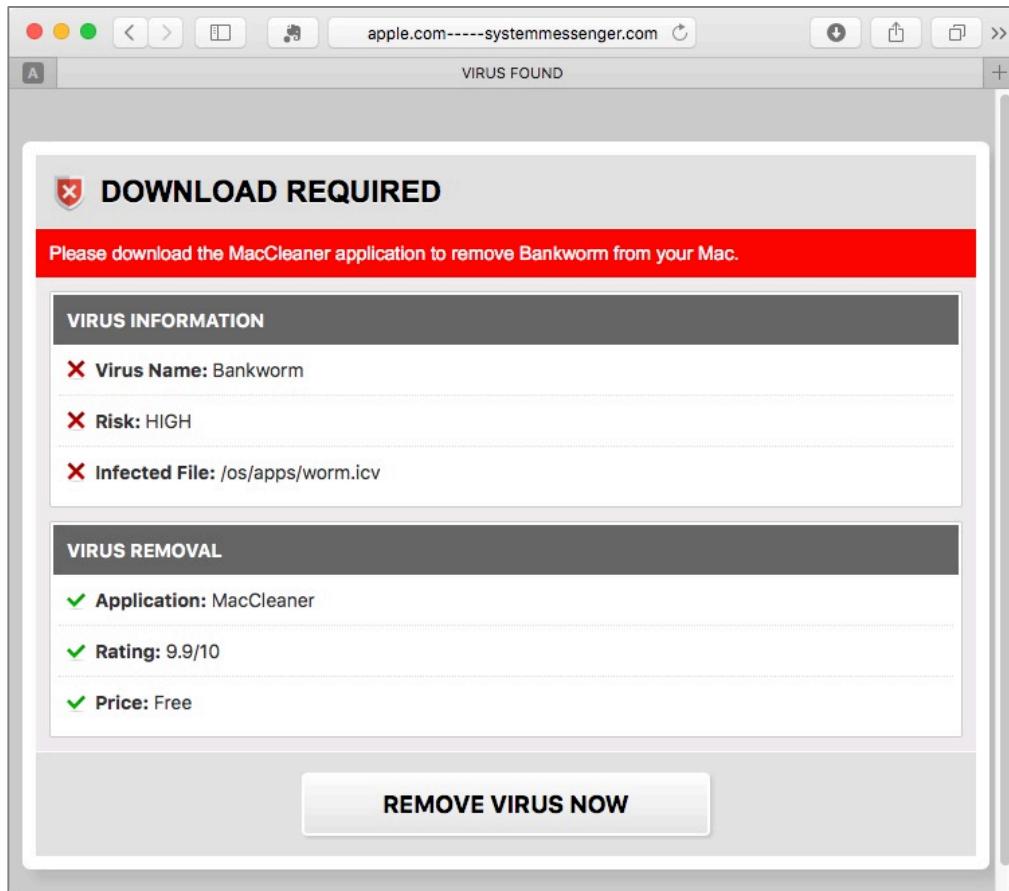
They have also discerned my city, state, IP address, Internet provider (Qwest Communications), that I am using OS X 10.11 El Capitan, with Safari version 9.

If I were the typical user, I'd probably think there was a virus present and press the *OK* button as recommended. You may have also noticed the criminal was bright enough to do all of this, but not bright enough to put an *OK* button in the script!

So, I press the *Close* button. I'm presented with a new window:

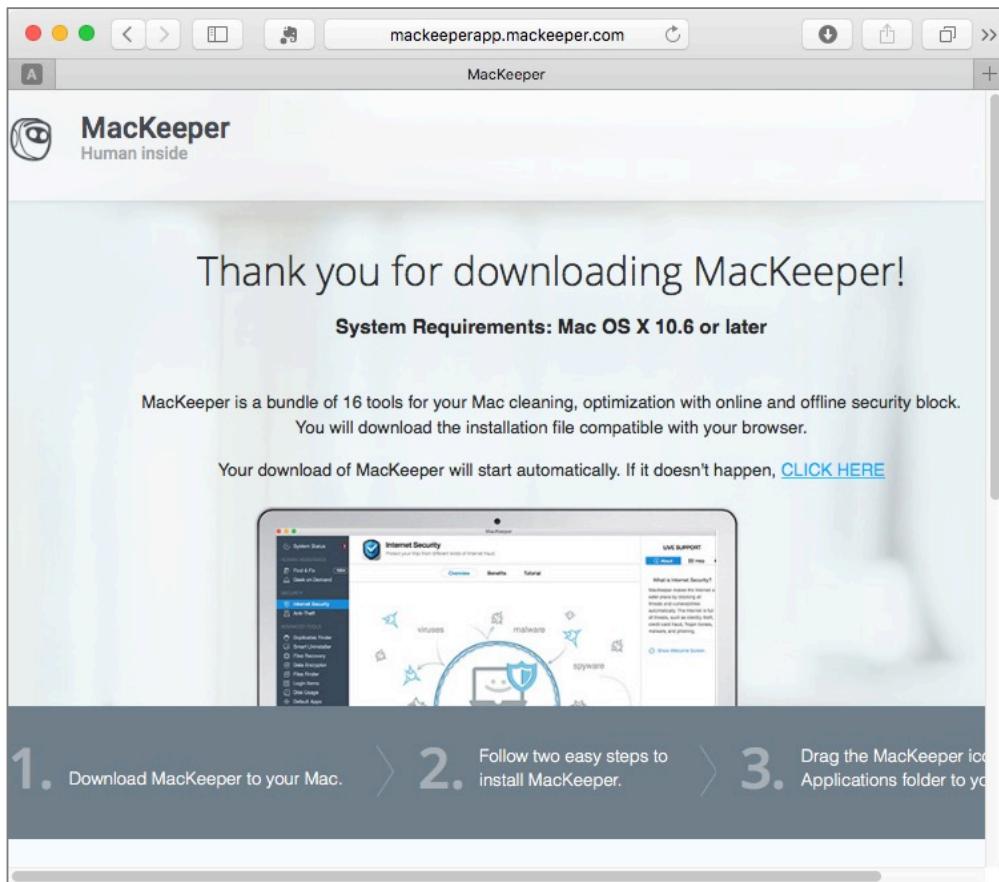


Hey, who needs an *OK* button when the *Close* button will do the intended scam! So let's see what happens when clicking the *Scan Now* button:



Appears they think I am infected with the *Bankworm* virus (which may or may not be a real malware name), and the infected file is located in */os/apps/worm.icv*. The only real problem I see is that there is no such file, and no such directory.

But they are offering a free solution to my non-existent problem. Let's see where that takes us by clicking the *Remove Virus Now* button:



MacKeeper?! Really! This product lost a class action lawsuit for deceptively advertising its functionality⁹.

If you have followed along so far, just trash the MacKeeper download.

So, how to protect yourself against fraudulent sites? We will go through the few steps that can be taken, but the most important tool is your awareness.

⁹ <https://topclassactions.com/lawsuit-settlements/closed-settlements/94767-mackeeper-class-action-settlement/>

14.7.1 Assignment: Warn When Visiting a Fraudulent Website in Safari

In this assignment, you will enable Safari to use its Fraudulent Website Tracking.

1. Open Safari.
2. Select the *Safari* menu > *Preferences* > *Security* tab.



3. Enable the *Fraudulent sites: Warn when visiting a fraudulent website* checkbox.
4. Close Safari Preferences.

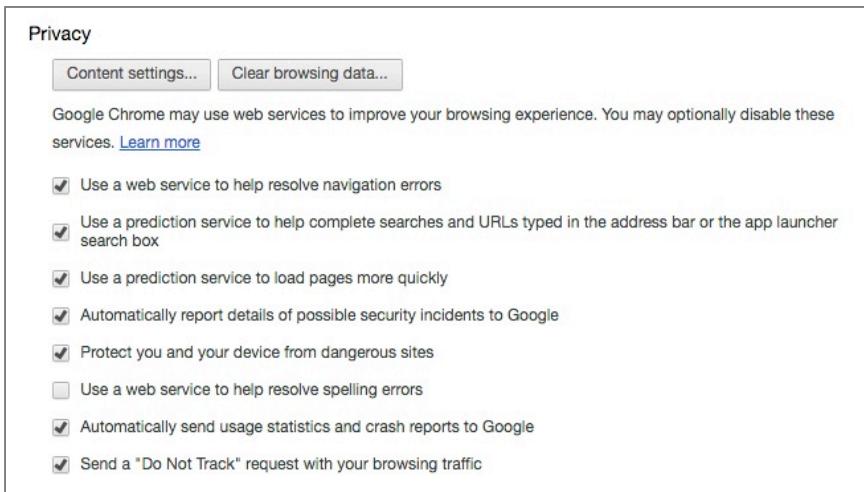
From now on, Safari will pass the website you are visiting to Google for analysis. If the site is on Google's warning list, you will see an alert advising to back away.

14.7.2 Assignment: Warn When Visiting a Fraudulent Website in Chrome

In this assignment, you will enable Chrome to use Google Fraudulent Website Tracking.

1. Open Chrome.
2. Select *Chrome* menu > *Preferences* > *Show Advanced Settings...* link.

3. In the *Privacy* section, enable the *Protect you and your device from dangerous sites* checkbox.



4. Close Chrome Preferences.

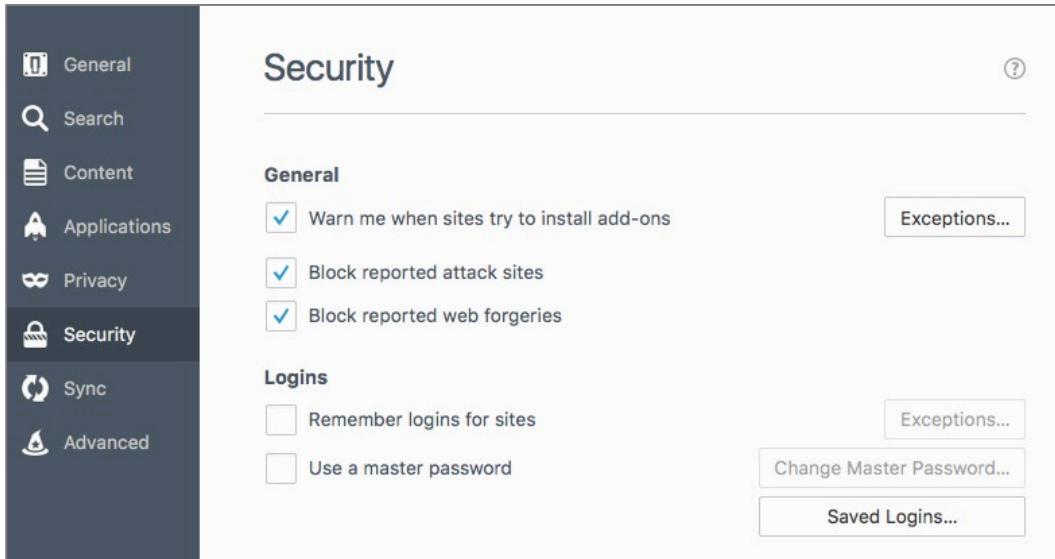
From now on, Chrome will pass the website you are visiting to Google for analysis. If the site is on Google's warning list, you will see an alert advising to back away.

14.7.3 Assignment: Warn When Visiting a Fraudulent Website in Firefox

In this assignment, you will enable Firefox to use Mozilla Fraudulent Website Tracking.

1. Open Firefox.
2. Select *Firefox* menu > *Preferences* > *Security*.

3. In the *General* area, enable the *Warn me when sites try to install add-ons*, *Block reported attack sites*, and *Block reported web forgeries* checkboxes.



4. Close Firefox Preferences.

From now on, Firefox will pass the website you are visiting to Mozilla for analysis. If the site is on the warning list or attempts to install an add-on, you will see an alert.

14.8 Do Not Track

Most websites track which pages you visit, how long you stay on each page, and other metrics to better understand their visitors. That in itself is a little creepy. Imagine going to the library, and having a librarian looking over your shoulder as you scan the card catalogue, and records each of the books and pages you glanced at.

Now let's take the analogy further. You leave the library and go across town to have lunch, and then shop for shoes. You look around and the same librarian is still watching and recording not only everything you have eaten, but everything you looked at on the menu.

Later you go for a date, and the librarian is sitting right behind you in the theater, noting who you are with, what scenes you reacted to, and more.

Web browsing isn't much different—except the snoop is normally invisible in the form of *cookies*.

Any website can initiate cookies on your browser. These keep a record of the pages you visit on the site. But they have evolved to report all of the other places you visit and things that you do. This is why you can visit Amazon, look up my books, quit the web browser, launch it, go to okcupid, and see an ad for my books!

No, I'm not doing it, Amazon is. They know that you were interested in my book, and will prod you with images of it for a few days, assuming that you eventually succumb and buy.

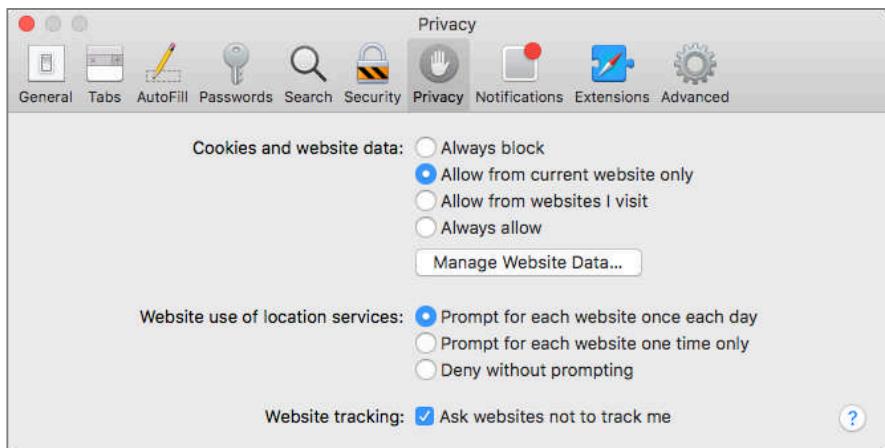
There is the option to disable cookies, but most of your websites will demand they be enabled in order to visit the site.

Although there is no 100% solution to this intrusion, you can configure your browser to ask websites to not track your activities. And if you believe that works, I've got a bridge to sell you.

14.8.1 Assignment: Enable Do Not Track In Safari

In this assignment, you will configure Safari to limit cookies and to request websites to not track you.

1. Open Safari.
2. Open *Safari* menu > *Preferences* > *Privacy* tab.



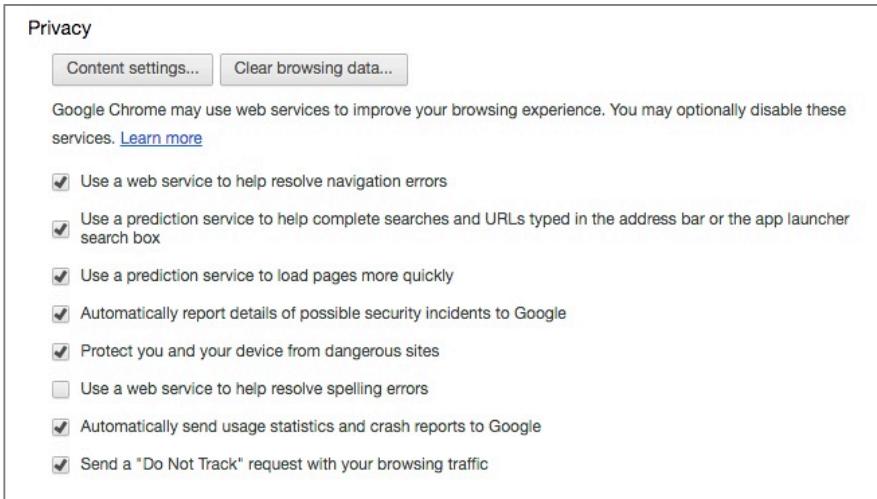
3. Enable *Cookies and website data: Allow from current website only*.
4. *Website use of location services* set to your taste.
5. Enable *Website tracking: Ask websites not to track me*.
6. Close Safari Preferences.

14.8.2 Assignment: Enable Chrome Do Not Track

In this assignment, you will configure Chrome to limit cookies and to request websites do not track you.

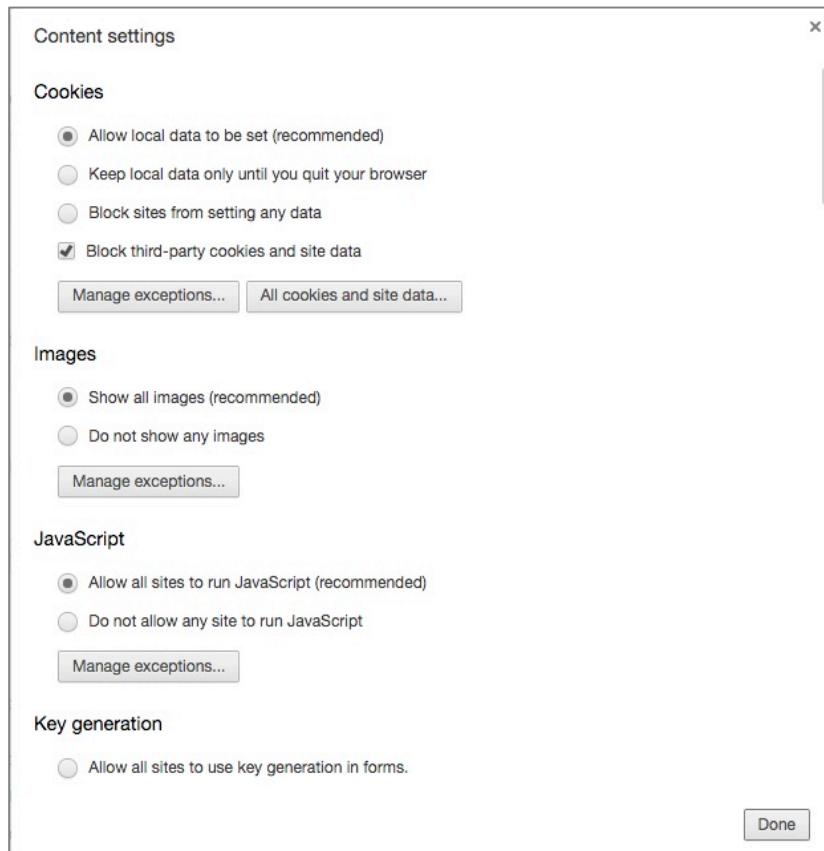
1. Open Chrome.
2. Select *Chrome* menu > *Preferences* > *Show advanced settings...* link at the bottom of the page.

3. In the *Privacy* area, enable *Send a "Do Not Track" request with your browsing traffic.*

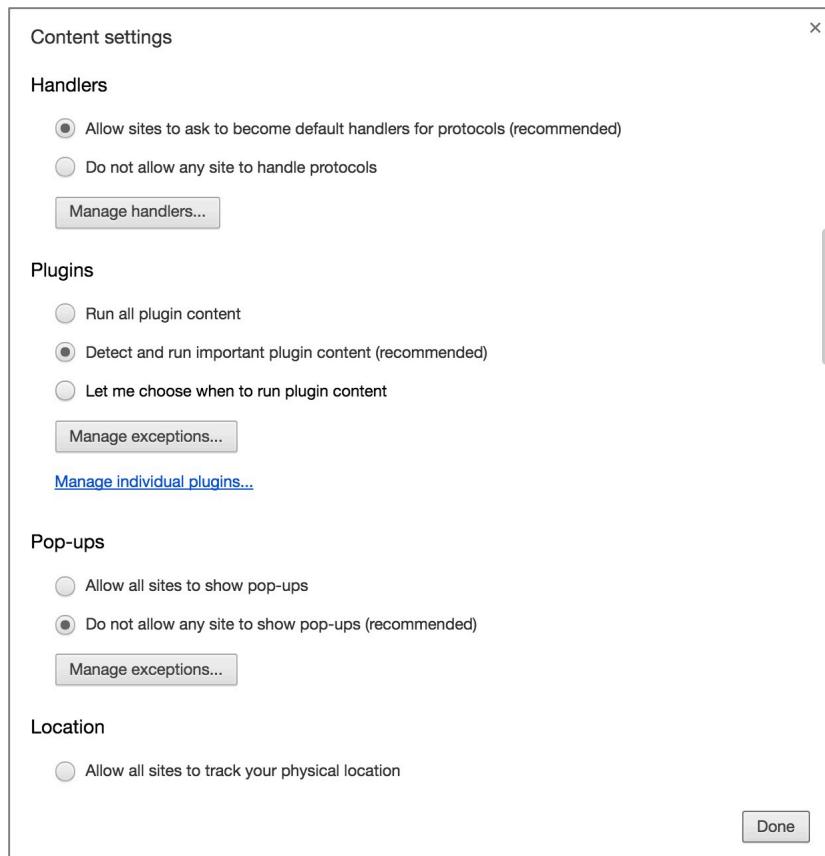


4. While you are here, configure the rest of the *Privacy* area as shown above.
5. In the *Privacy* area, select the *Content settings...* button.

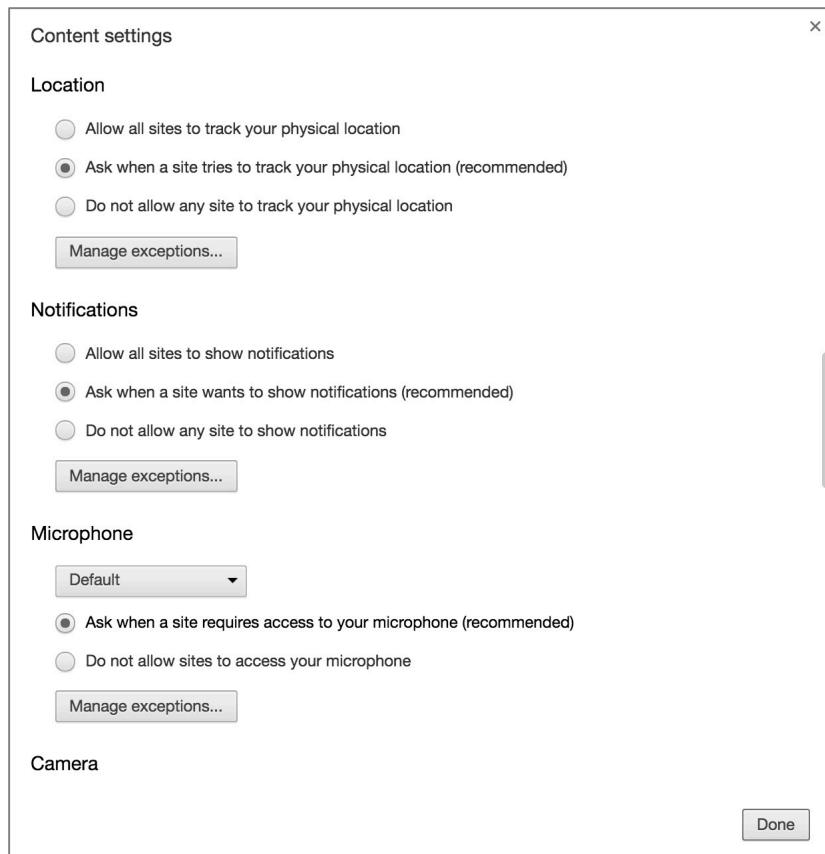
6. In the *Cookies* area, Configure to your taste. Shown below are my settings.



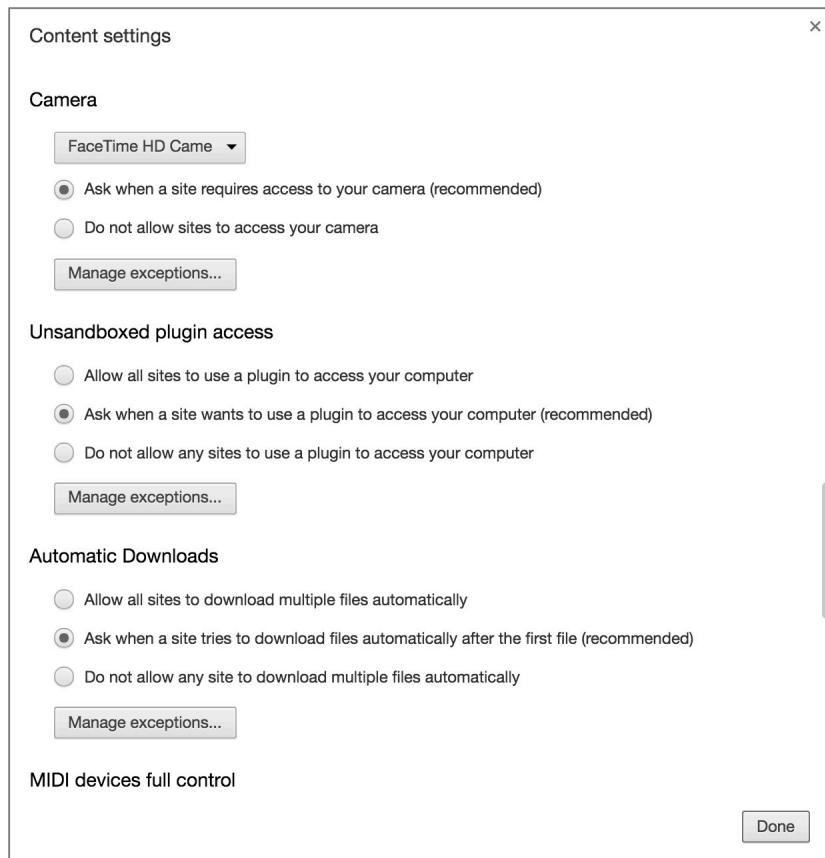
14 Web Browsing

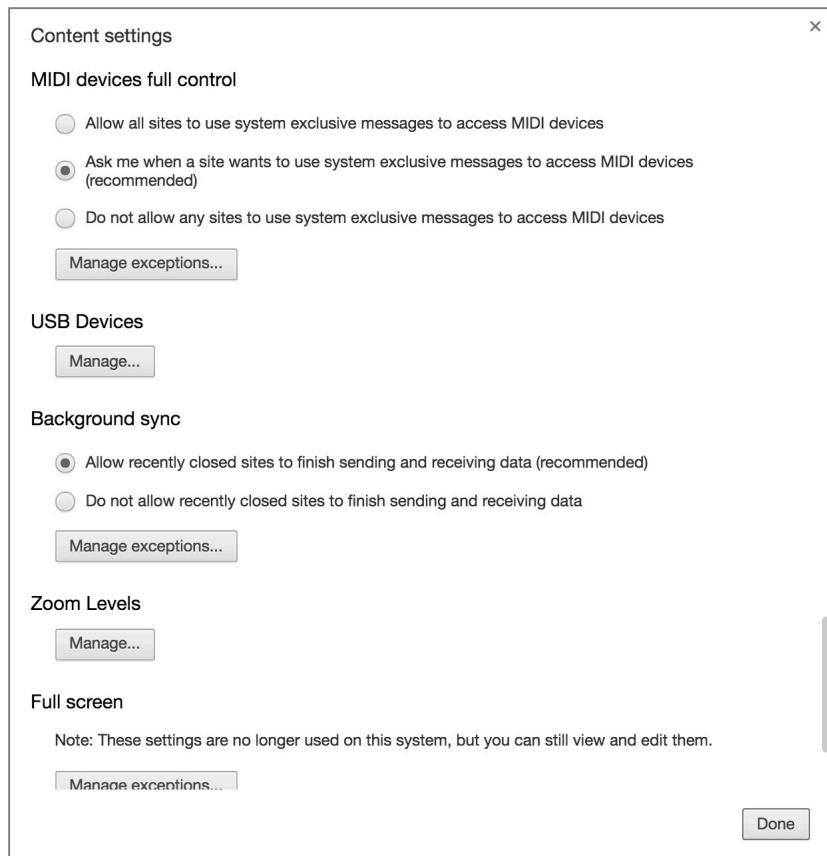


14 Web Browsing



14 Web Browsing





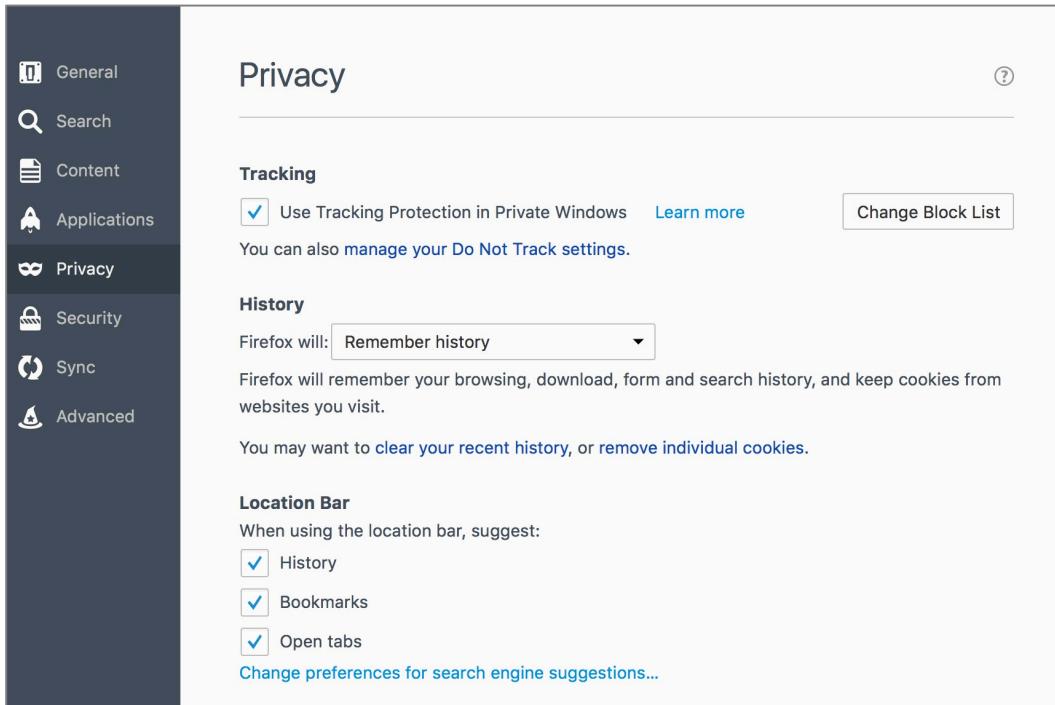
7. Select the *Done* button.
8. Close Chrome Preferences.

14.8.3 Assignment: Enable Firefox Do Not Track

In this assignment, you will configure Firefox to limit cookies and to request websites do not track you.

1. Open Firefox.

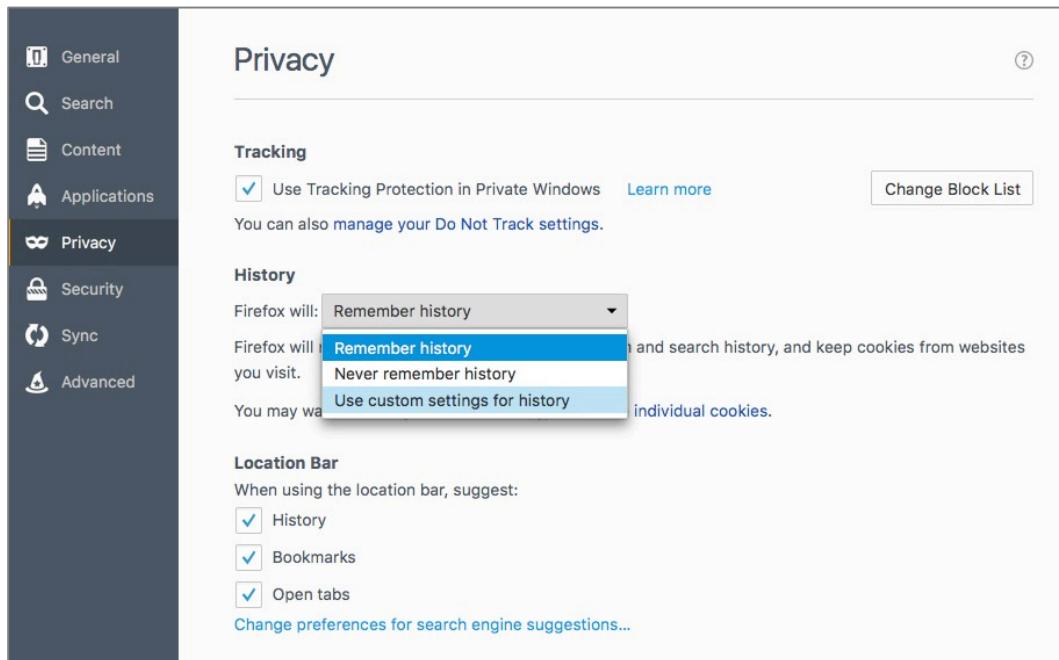
2. Select *Firefox menu > Preferences > Privacy*.



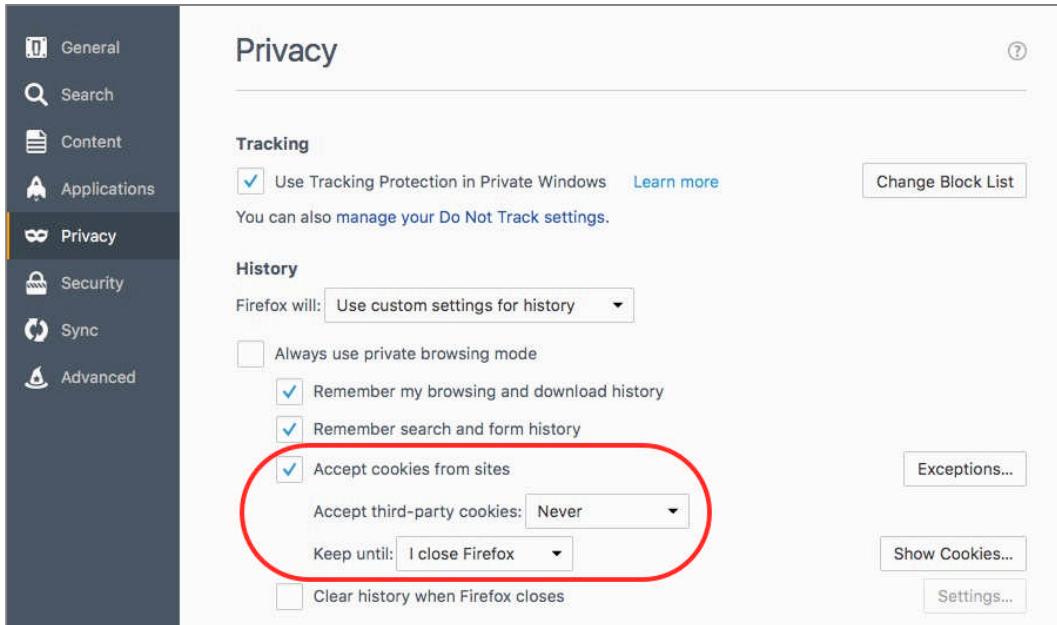
3. Enable the *Use Tracking Protection in Private Windows* checkbox.
4. Select *Manage your Do Not Track settings*.
5. Enable the *Use Do Not Track* checkbox, and then select the *OK* button.



6. In the *History* area, select *Firefox will: Use custom settings for history*.



7. In the *History* area, configure cookies to your taste. Shown below are my settings:



8. Close Firefox Preferences.

14.9 Adobe Flash and Java

Both Adobe Flash and Oracle Java are used by many websites to create a more animated or interactive web experience. The functions of both may soon be absorbed by HTML 5. Until that day comes, many of us will require both products in order to have fully-functioning website behaviors.

However, the power these products offer is a double-edged sword. They can also be used to take control of your computer. And very often are. There is a vicious cat and mouse game played by hackers who have discovered how to bend Flash and Java to their wills, and Adobe and Oracle patching these vulnerabilities.

The end result for users is they have a choice to make:

- Do not install Flash or Java, which renders some sites unusable.
- Install Flash and Java, and be vigilant with updates.
- Install Flash and Java, but don't be vigilant with updates. This renders their system highly vulnerable.

I suspect if you are one who ops for the last option, you aren't taking this course.

Either of the other two options are legitimate strategies. Both Adobe and Oracle have tried to make updates automatic, but we have found this process to be less than perfect. Many times we have found systems with out of date versions, even with their preference settings on *Automatic Updates*.

Associated with the vulnerabilities caused by out of date Flash and Java, are malicious or compromised web pages that prompt the visitor to update Flash, Java, or some audio/video codec. In most cases, if you follow the links provided on the site all that gets downloaded is malware.

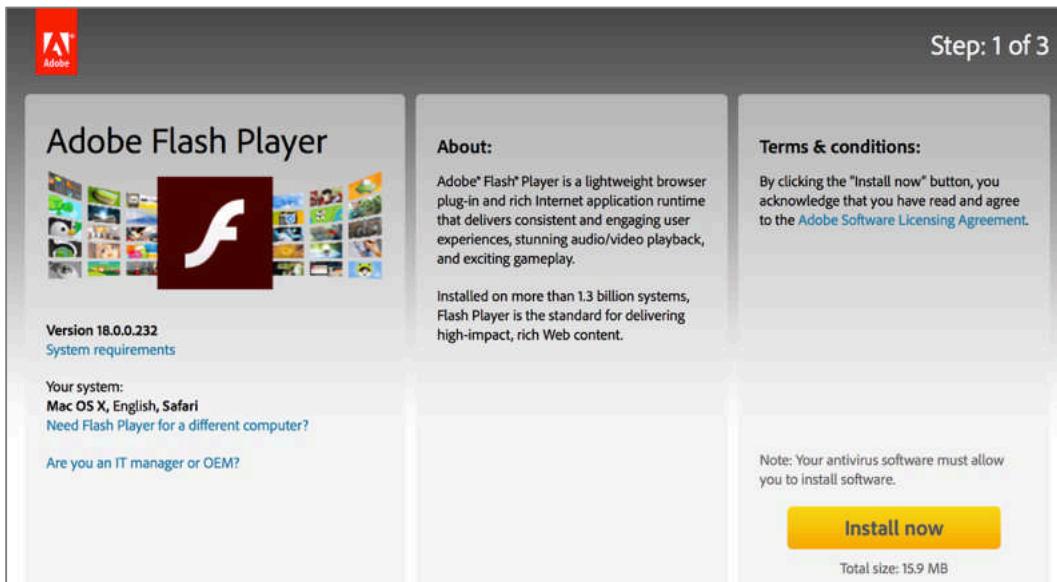
If a site prompts you do install software, visit the website of the recommended software and download from there, not from the requesting site.

14.9.1 Assignment: Configure Adobe Flash Automatic Updates

In this assignment you will install Flash and configure it for automatic updates.

Install Adobe Flash.

1. Open *Apple* menu > *System Preferences*. If you see the Flash icon, it is already installed. If so, skip to the next section *Configure Flash for Auto-Updates*.
2. Open a browser, and then surf to <http://www.adobe.com/>.
3. Click the menu icon (3 lines) > *Adobe Flash Player*.
4. Click the *Install Now* button.



5. The Flash installer will download and open.
6. Double-click the installer, and then follow the on-screen instructions to complete installation.

Configure Flash for Auto-Updates.

7. Open *System Preferences* > *Flash Player*.
8. Select the *Updates* tab, select the *Allow Adobe to install updates (recommended)* radio button, and then click the *Check Now* button. This (at

least in theory), verifies your system has the latest version of Flash, and authorizes Flash to automatically update.



Manually check for Flash updates.

9. Open *System Preferences > Flash Player*.
10. Select the *Updates* tab.
11. Click the *Check Now* button. If an update shows as available, follow the on-screen instructions to download and install.

14.9.2 Assignment: Configure Oracle Java for Automatic Updates

In this assignment, you will install Java and configure it to automatically update.

Install Oracle Java.

1. Open *Apple menu > System Preferences*. If you see the Java icon, it is already installed. If so, skip to the next section *Configure Java for Auto-Updates*.

2. Open your browser to surf to <http://www.java.com/>.

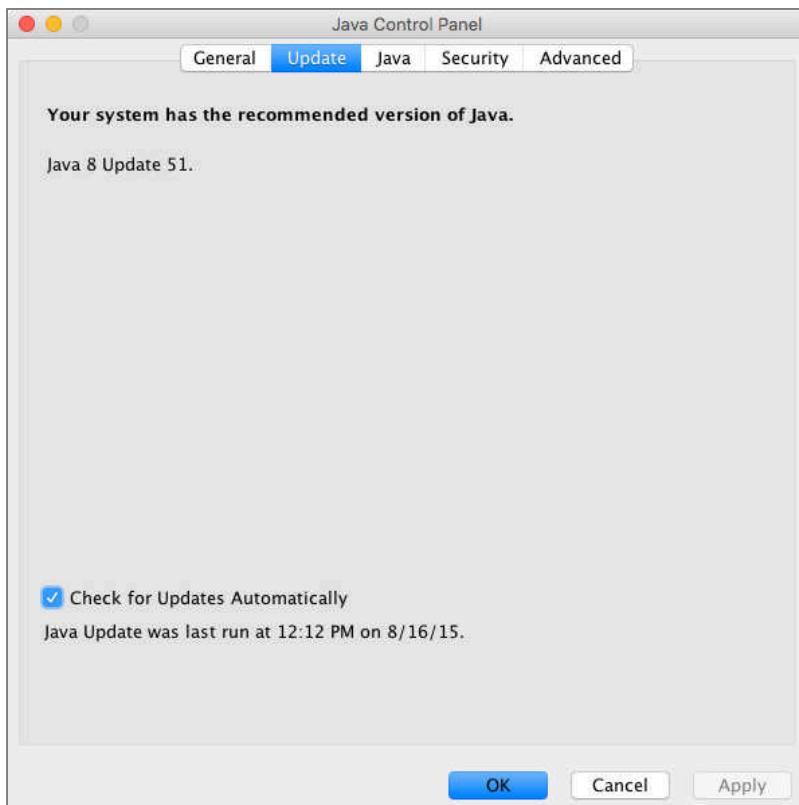


3. Click the *Free Java Download* button.
4. Click the *Agree and Start Free Download* button.
5. Once the Java installer has downloaded, launch it, and then follow the on-screen instructions to complete installation.

Configure Java for Auto-Updates.

6. Select *System Preferences > Java*.

7. Select the *Update* tab, and then enable the *Check for Updates Automatically* checkbox.

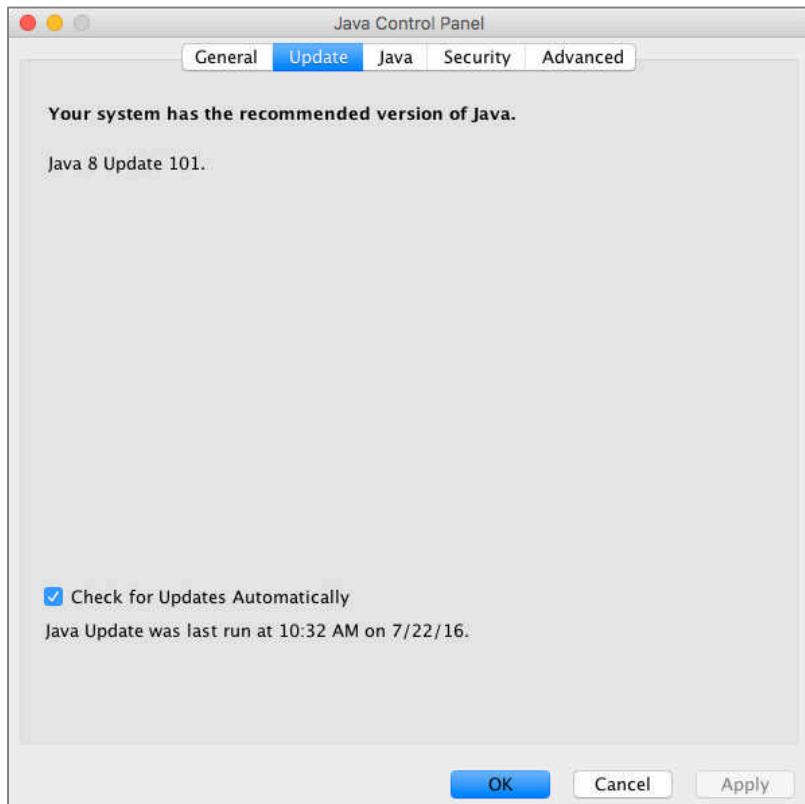


At this point, both your Flash and Java are up to date, and configured to automatically update. However, there is a decent chance that they will not do so. It is wise to perform a manual update check at least monthly.

Manually check for Java updates.

8. Open *System Preferences > Java*.

9. Select the *Update* tab.



10. If updates are available, select the *Update Now* button, and then follow the on-screen instructions to download and install.

14.10 Web Scams

Over the past couple of years, a new type of scam has become popular. Instead of directly compromising the user computer, web sites are either compromised, or are deliberately designed to be malicious.

When a user visits such a site, they may receive a pop-up window stating something to the effect of: *Your computer has been found to be infected with XX viruses. Please call Apple at XXX-XXX-XXXX to have this infection removed.*

Upon calling the provided toll-free phone number (which, of course, is not really Apple, but that of the scammer), with your permission, they will install remote control software. After looking around your computer, they will assure they can remove the malware for only \$\$\$.

There are two problems here. First, they have installed remote control software that allows the criminal access any time they wish. This gives them access to your usernames, passwords, banking, and other information. The second is that they now have your credit card information.

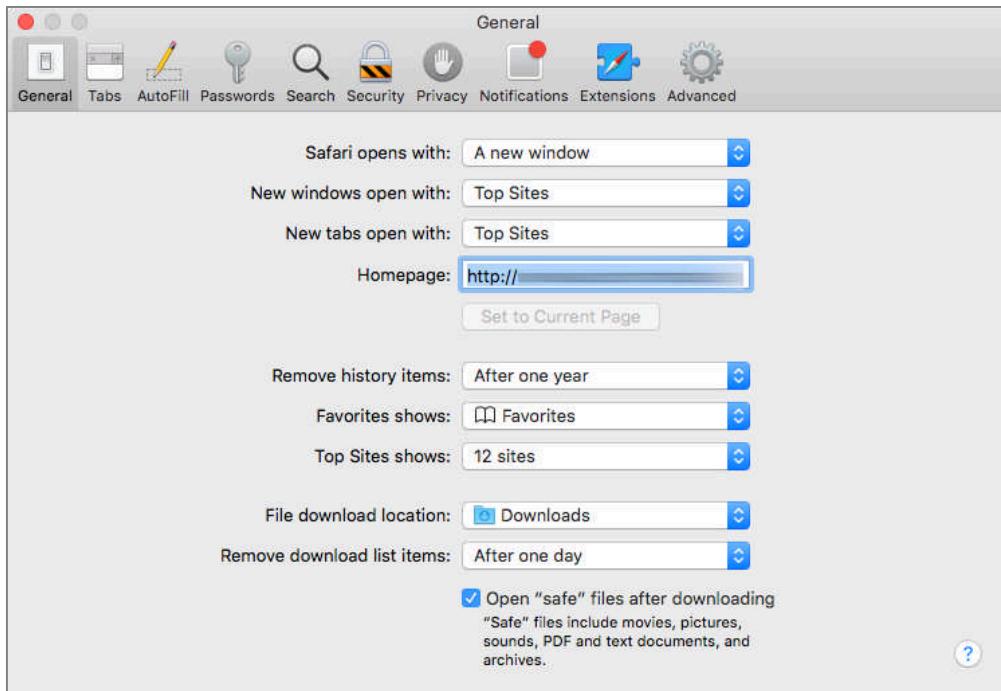
What to do if this happens to you?

1. Don't call!

In most cases, the malicious website has modified your web browser preferences to make the malicious page your home page.

14 Web Browsing

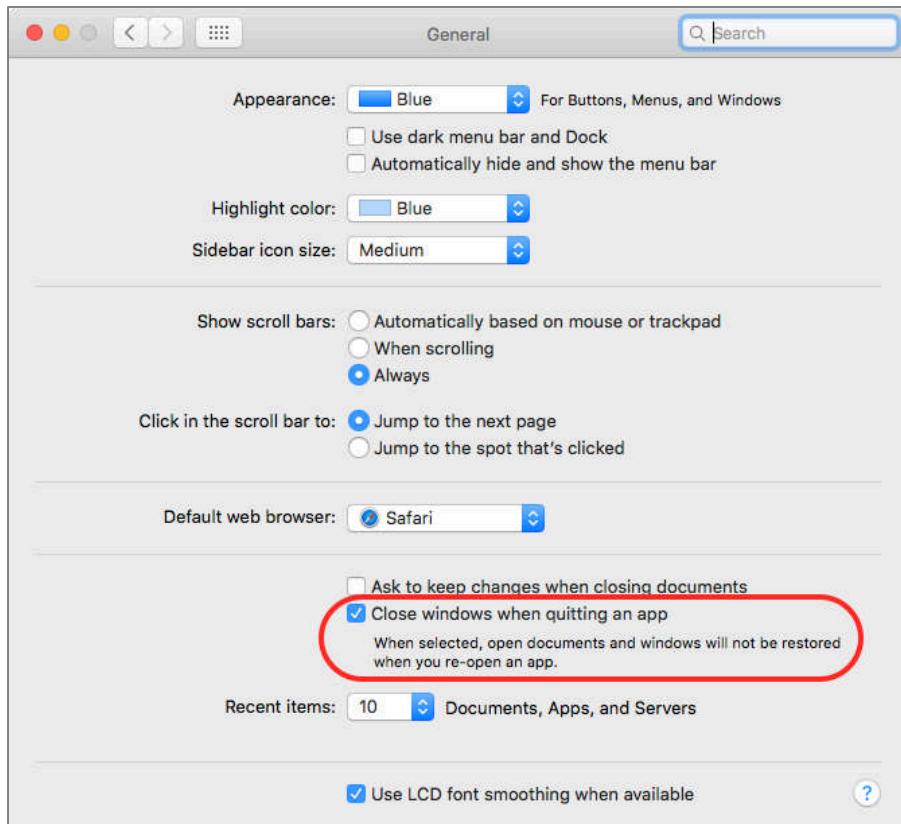
2. Open your browser *preferences* (in this example, Safari) > *General*. If the *Homepage* field is not what you have set, delete the entry.



3. Malicious attacks on a browser often will block access to the browser preferences. If you are not able to access your browser preferences to delete

14 Web Browsing

the homepage setting, open *System Preferences > General*, and then enable *Close windows when quitting an app*.



4. Quit Safari.
5. Open Safari to test. You should no longer have the malicious page open.

Done!

14.11 Tor

Tor¹⁰ is a technology developed by the US Department of the Navy that enables anonymous web browsing. It has long since been released to the open source community for the public to use in the form of the *Tor Browser*. Many people within the security community are strong supporters of Tor, including Edward Snowden. Entire books have been written on just Tor. I'm not so sadistic as to subject you to that. What we are going to do is cut to the core of Tor, and learn the basics of how to surf the web anonymously.

The advantages of Tor include:

- Strong anonymity for all activity on the Internet.
- Can be used with Tails¹¹ which is a bootable, self-contained, flash drive that can run on most Windows, Linux, and Apple computers that leaves no trace behind.
- The bootable Tails flash drive can be immediately disconnected from the host computer, causing the computer to erase memory of all trace of your session, and reboot.

The disadvantages of Tor include:

- It was developed by the US Department of the Navy. It is possible there are back doors only the government knows about.
- The US government has been forthright about having its own Tor relays in place, which enable it to monitor online activity. Not a big deal if you only wish to be anonymous to criminals. It is a big deal if you wish to be anonymous while performing black-market deals for my Aunt Rose's raisin Noodle Koogle recipe.

These features make Tor ideal for those in oppressed countries, journalists working undercover, and anyone who may need to use someone else's computer and leave no trace behind.

¹⁰ [http://en.wikipedia.org/wiki/Tor_\(anonymity_network\)](http://en.wikipedia.org/wiki/Tor_(anonymity_network))

¹¹ <https://tails.boum.org>

Tor works by encrypting your packets as they leave your computer, routing the packets to a Tor relay computer hosted by thousands of volunteers on their own systems, many of which are co-located at ISPs. The relay knows where the packet came from, and the next relay the packet is handed to, but that is all. The user computer automatically configures encrypted connections through the relays. Packets will pass through several relays before being delivered to the intended destination. Tor will use the same relays for around 10 minutes, and then different relays will be randomly selected to create the next path for 10 minutes.

Alas, there is no free lunch. The encryption process and the relay process combine to create *latency*, which mean a delay in processing. Most users will experience around a four-fold performance degradation. So, if accessing a web page without Tor normally takes 3 seconds, it may take 12 seconds with Tor.

Even though Tor does as good a job as anything to keep you anonymous on the Internet, you must take precautions to protect your identity. These steps include:

- Don't enable JavaScript when using Tor. This has been used to track users within the Tor network.
- Don't reveal your name or other personal information in web forms.
- Don't customize the Tails boot flash drive. This will create a unique digital fingerprint that can be used to identify you.
- Connect to sites that use HTTPS so your communications are encrypted point to point.

For many security-conscious users, Tor becomes their only tool for defense. However, Tor by itself is at best a partial solution. It can protect your anonymity while surfing the web. At the very least, this still leaves email and messaging to be secured. A bigger issue is what to do when you need to use a computer and leave no trace behind on that system. This is where *Tails* comes into play.

Tails is a Linux Debian fork designed with two primary purposes in mind:

- Provide a highly secure operating system in a format that can be booted from either DVD or thumb drive on almost any PC or Apple computer, and
- Include the tools and applications necessary to provide a secure, anonymous Internet experience

What this means is that you can create a thumb drive that has an operating system capable of booting almost any computer, whereby you can then run Tor for secure anonymous Internet activity, send and receive email that is securely encrypted with GPG/PGP, and message with others in complete privacy. Then, when you remove the Tails thumb drive, there is absolutely no record of your activity on either the computer *or* the thumb drive!

For those of you chomping at the bit to just use Tor, we will start there. When your curiosity has been satisfied, please take the next step to learn Tails¹².

14.11.1 Assignment: Install Tor for Anonymous Internet Browsing

Tor is a stripped down, simplified web browser, designed to provide an encrypted, anonymous browsing experience. In this assignment, we will download and install Tor.

1. As a first step, we need to know our public IP address. This information will be used a few steps away to verify Tor has hidden our address. Open a web browser to <https://whatismyip.com>. Write down *Your IP*.



¹² <https://tails.boum.org>

14 Web Browsing

2. Open a web browser and then go to <https://www.torproject.org>. Select the *Download Tor* button.

The screenshot shows the official Tor Project website. At the top, there's a navigation bar with links for Home, About Tor, Documentation, Press, Blog, and Contact. Below the navigation is a purple header bar with the text "Recent Blog Posts". Underneath the header, there's a green section titled "Anonymity Online" which says "Protect your privacy. Defend yourself against network surveillance and traffic analysis." To the right of this text is a box containing four bullet points about Tor's features: it prevents location/browsing habits from being tracked, it's for web browsers and messaging clients, it's free and open source, and it's available for multiple platforms. At the bottom left of the main content area is a large purple button labeled "Download Tor".

3. Select the *Download Tor Browser* button. The Tor installer will begin to download.

This screenshot shows the "Download" section of the Tor Project website, specifically for Mac users. The top navigation bar is identical to the main site. Below it, a yellow warning box says "Want Tor to really work? You need to change some of your habits, as some things won't work exactly as you are used to. Please read the [full list of warnings](#) for details." The main content area is titled "Tor Browser for Mac" and mentions "Version 6.0.2 - OS X (10.6+)" and a link to "Read the release announcements!". It also says "Everything you need to safely browse the Internet." and has a "Learn more" link. On the right side, there's a large yellow "DONATE" button and a link to "Other donation options...". At the bottom, there's a purple "DOWNLOAD" button with a cloud icon, and text saying "Not Using Mac? Download for [Windows](#) or [Linux](#)". There are also links for "(sig) What's This?" and "English".

4. While the download is in progress, scroll down the page to read all of the other steps that one must take to ensure your privacy is maintained. These include:
 - **Use the Tor Browser.** If you are concerned about protecting your privacy and security, do not use other browsers.

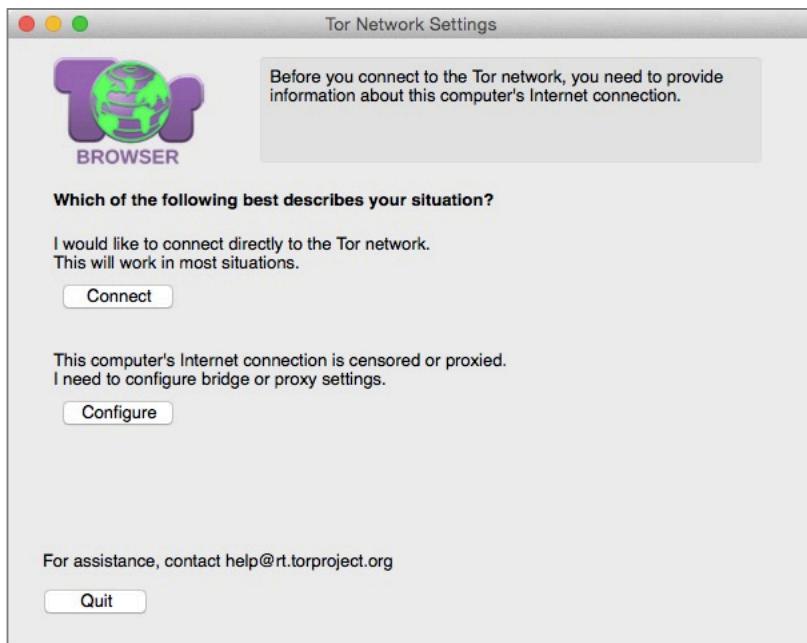
- **Don't torrent over Tor.** If you wish to file-share via torrent, don't use Tor. It is painfully slow, it slows down others using the Tor network, and in many cases, torrent software bypasses all of the security and anonymity precautions built into Tor.
- **Don't enable or install browser plugins in Tor.** Tor is designed to protect your security and anonymity. Many innocuous-looking plugins break that security.
- **Use HTTPS versions of websites.** Tor has *HTTPS Everywhere* built in (more on HTTPS Everywhere later in this book.) It will force a secure connection if a website has an option for https. This will enable a point-to-point encryption between your computer and the web server.
- **Don't open documents downloaded through Tor while online.** Many documents—particularly .doc, .xls, .ppt, and .pdf—contain links or resources that will force a download when the document is opened. If they are opened while Tor is open, they will reveal your true IP address and you will lose your anonymity and security. If you are concerned about these issues, we strongly recommend that you instead:
 - **Open the documents on a computer fully disconnected from the Internet.** This prevents any malicious files from “phoning home” or infecting your computer.
 - **Install a Virtual Machine (VM) such as Parallels, Fusion, or VirtualBox, configured with no network connection, and open documents within the VM.** This is an alternate way to prevent malicious files from phoning home or infecting your computer.
 - **Or use Tor while within Tails.** This is an alternative way to prevent malicious files from phoning home or infecting your computer.
- **Use bridges and/or find company.** Tor cannot prevent someone from looking at your Internet traffic to discover you are using Tor. If this is a concern for you, reduce the risk by configuring Tor to use a *Tor Bridge relay* instead of a direct connection to the Tor network. Another option is to have many other users running Tor on the same network. In this way, your use of Tor is hidden.

5. Locate the Tor installer, and then double-click to open. It will mount and open a disk image onto the Desktop.
6. Drag the *TorBrowser.app* into your *Applications* folder.



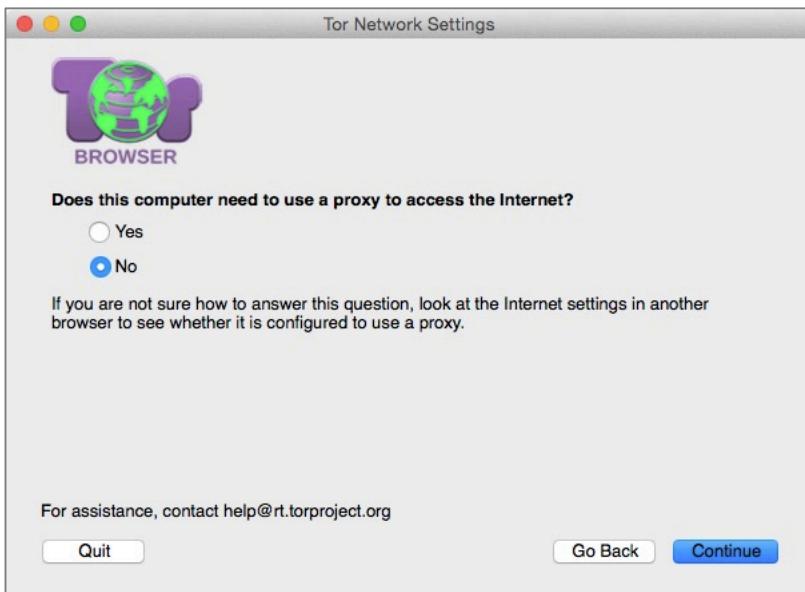
7. Locate the *Tor Browser* in your Applications folder, and then double-click to open it. The *Tor Network Settings* window appears. Select how you would like to connect to the Tor Network
 - *I would like to connect directly to the Tor network.* This will work in most situations. This option provides a faster Internet experience with no additional configuration. The possible downside is that a network administrator or your ISP is able to see that you are using the Tor Network.
 - *This computer's Internet connection is censored or proxied. I need to configure bridge or proxy settings.* This option provides a more secure and anonymous Internet experience as a network administrator or ISP is

unable to see you using the Tor Network. The downside is a slower Internet experience, and some additional configuration.

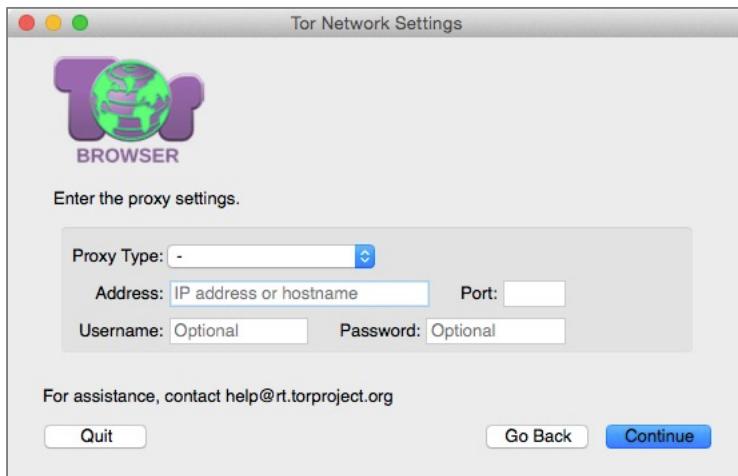


8. If you selected *This computer's Internet connection is censored or proxied. I need to configure bridge or proxy settings*, go to the next step. If you selected *I would like to connect directly to the Tor network*, skip to step 12.

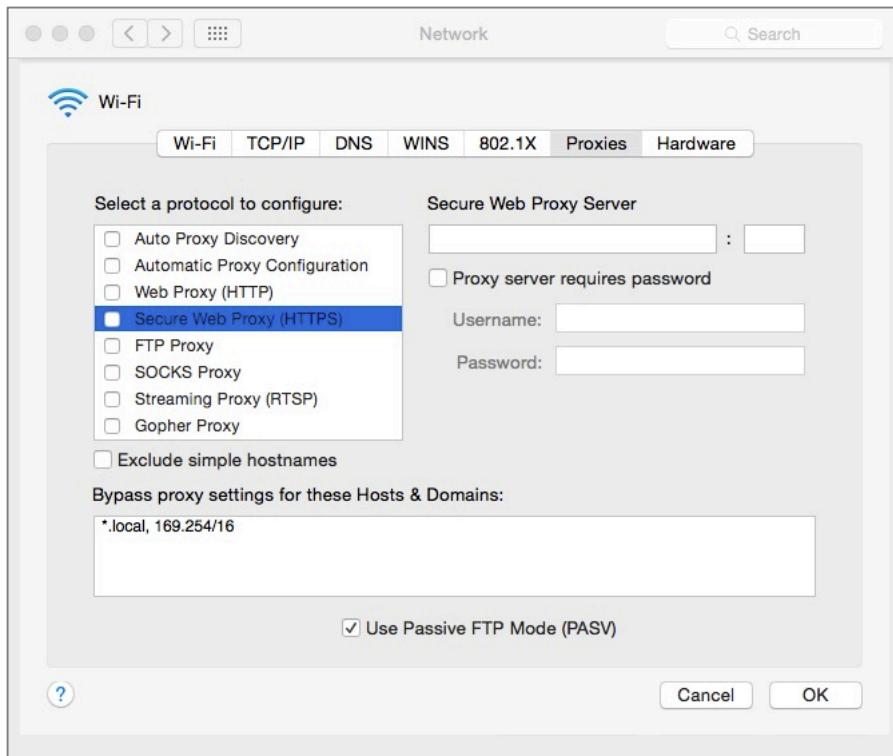
9. If you elected to use a *Tor bridge relay*, the following window appears. If your network requires a proxy to access the Internet, go to the next step and select *Continue*. Otherwise, select *No*, select the *Continue* button, and skip to step 12.



10. If you selected *Yes* to *Does this computer need to use a proxy to access the Internet* you will now see the Enter the Proxy settings window.



11. These will be the same settings your computer requires normally, and if used, will be found in *System Preferences > Network > Advanced > Proxies* tab. Copy your settings from this pane into the Tor window, and then select the *Continue* button. If your ISP blocks or otherwise censor's connections to the Tor network, go to the next step to create a Tor bridge relay. If they do not, skip to step 14 to start using Tor.



12. At the *Does your Internet Service Provider (ISP) block or otherwise censor connections to the Tor Network* window, for the overwhelming majority of users the answer is *No*, and then select the *Connect* button, and then skip to

14 Web Browsing

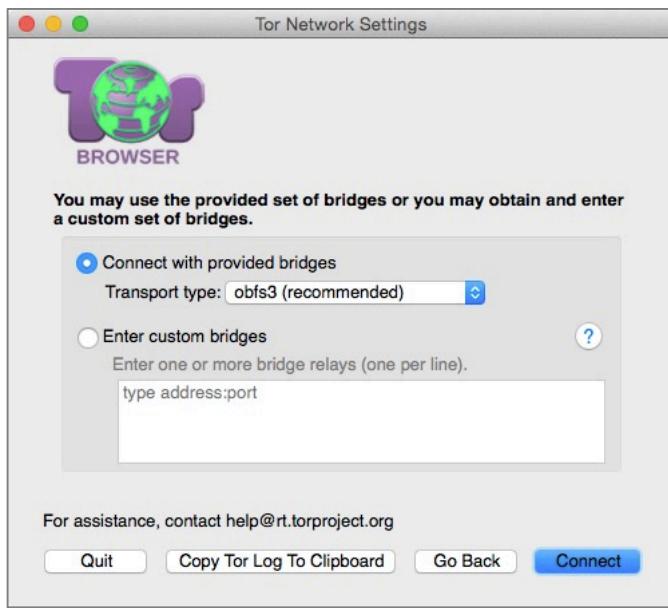
step 14. If your answer is Yes, select the Yes option, select the *Continue* button, and go to the next step.



13. If you selected Yes to the *Does your ISP block or otherwise censor connections to the Tor Network* window, you now see the You may use the provided set of bridges or you may obtain and enter a customer set of bridges window. Select

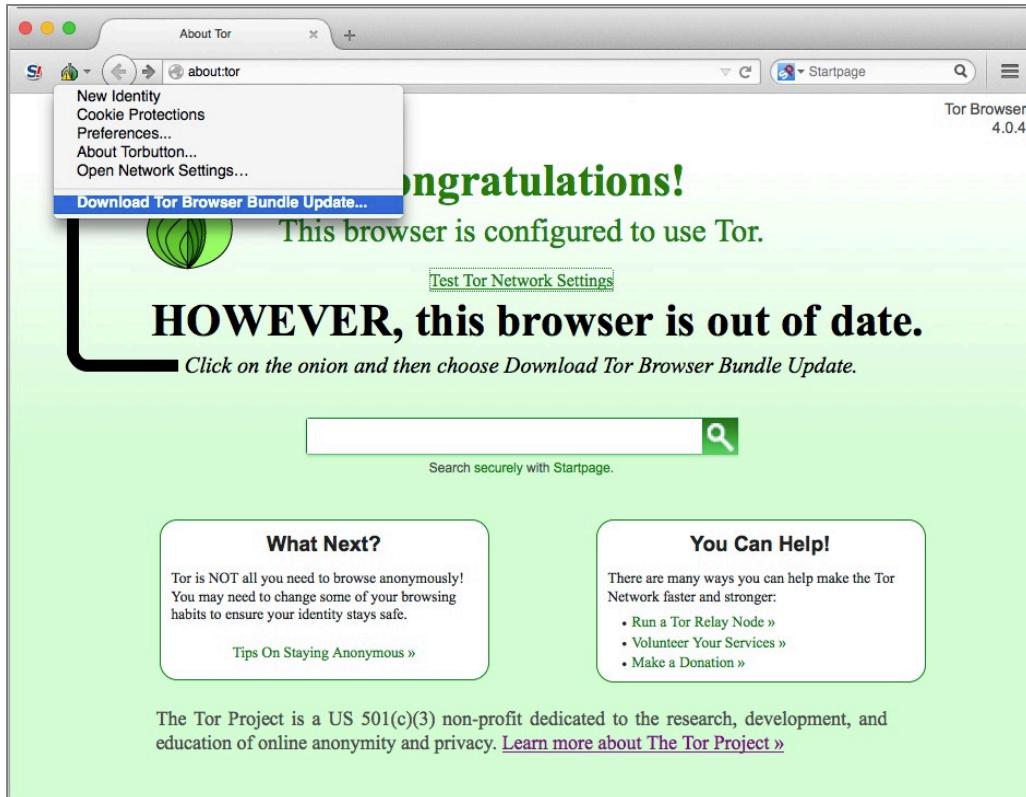
14 Web Browsing

Connect with provided bridges, Transport type *obfs3* (recommended), and then select the *Connect* button.



14. The Tor Browser updates often. If your copy is out of date, you will be welcomed by a message asking you to update. Follow the instructions, clicking on the onion icon > *Download Tor Browser Bundle Update...*to update. Once

the download is complete, Quit Tor Browser, and then replace it with the new version. Otherwise, if you are up to date, skip to the next step.



15. It is vital to test your connection to verify your IP address is hidden. While in Tor, go to <https://check.torproject.org>. You can also return to <https://whatismyip.com> as well.



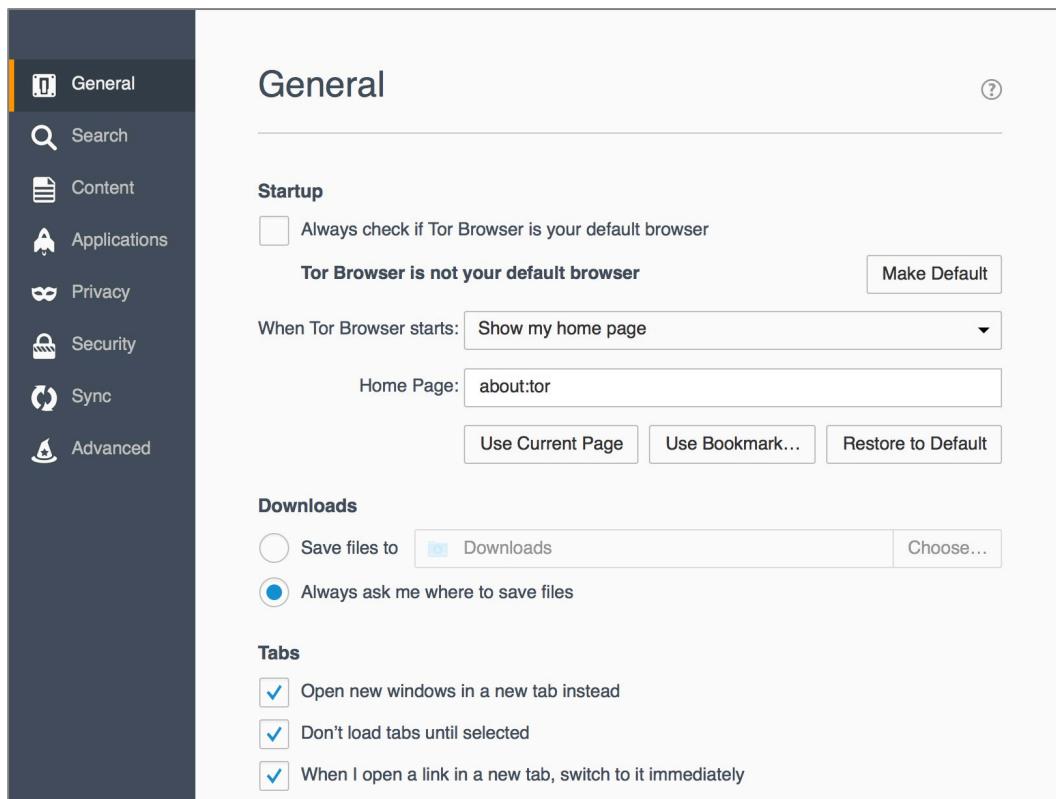
The screenshot shows the WhatIsMyIP.com website. At the top left is the logo "WhatIsMyIP" with the URL "whatismyip.com" below it. To the right are social media sharing buttons for Facebook, Twitter, and Google+. A "Site Navigation" dropdown menu is visible. Below the header is a blue navigation bar with buttons for "SPEED TEST", "IP LOOKUP", "CHANGE MY IP", and "HIDE MY IP". The main content area displays the following information: "Proxy: No Proxy Detected", "City: Akersberga", "State/Region:Stockholms Lan", "Country: SE - 🇸🇪", and "ISP: Teknikbyran I Sverige Ab". At the bottom of this section, the IP address "Your IP: 78.108.63.44" is shown in a red-outlined box. Below this box is a button labeled "MY IP INFORMATION".

Wahoo! You are now on Tor, completely anonymous and encrypted on the Internet. Next step is to configure Tor.

14.11.2 Assignment: Configure Tor Preferences

One of the first things one should do when launching an application for the first time is to configure its preferences. No different for Tor. In this assignment we will configure Tor preferences.

1. Open TorBrowser, and then select the *Tor Browser* menu > *Preferences* > *General* tab. This pane may be configured to taste.



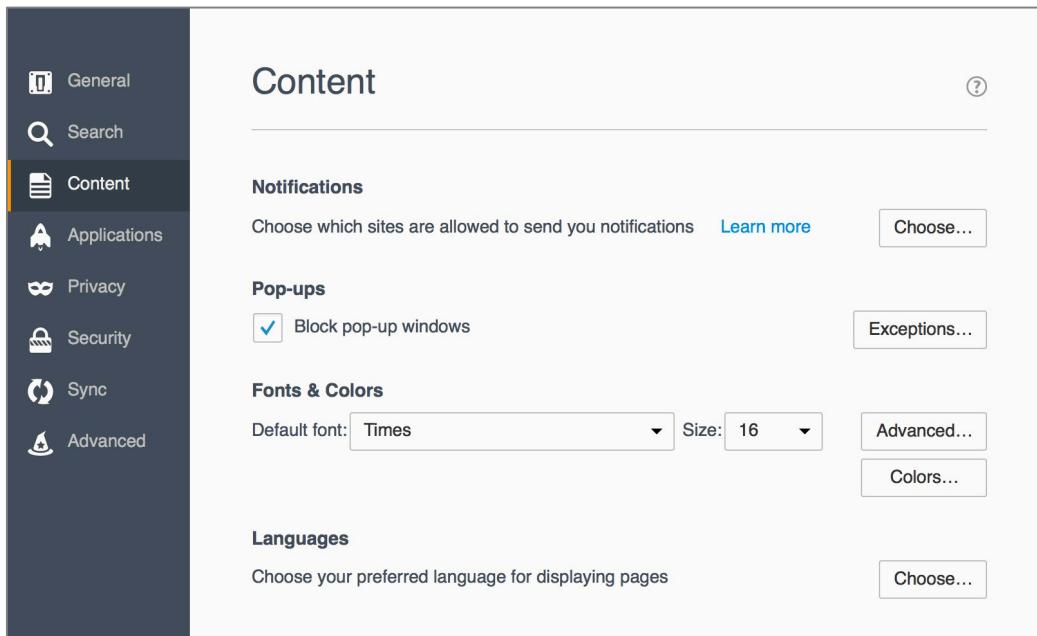
2. Select the *Search* tab.

The screenshot shows the Tor Browser's configuration interface. On the left is a sidebar with icons and labels for General, Search (which is highlighted with an orange border), Content, Applications, Privacy, Security, Sync, and Advanced. The main area is titled "Search". It contains a section for the "Default Search Engine" where "DuckDuckGo" is selected. There are checkboxes for "Provide search suggestions", "Show search suggestions in location bar results" (disabled), and a note explaining why suggestions won't appear. Below this is a "One-click search engines" section with a table listing several engines: Disconnect, YouTube, Google, Yahoo, DuckDuckGo, Startpage, Twitter, and Wikipedia (en). Each engine has a checked checkbox next to its name. At the bottom are buttons for "Restore Default Search Engines", "Remove", and "Add more search engines...".

Search Engine	Keyword
Disconnect	
YouTube	
Google	
Yahoo	
DuckDuckGo	
Startpage	
Twitter	
Wikipedia (en)	

- For *Default Search Engine*, select *DuckDuckGo*.
- Other settings may be configured to your taste.

3. Select the *Content* tab. Configure to your taste.



4. Select the *Applications* tab. Configure to your taste.

The screenshot shows the 'Applications' tab selected in a configuration interface. On the left is a sidebar with icons and labels: General, Search, Content, Applications (selected), Privacy, Security, Sync, and Advanced. The main area is titled 'Applications' and contains a search bar. Below it is a table with two columns: 'Content Type' and 'Action'. The table lists various file types and their associated actions:

Content Type	Action
irc	Always ask
ircs	Always ask
mailto	Always ask
Podcast	Preview in Tor Browser
Portable Document Format (PDF)	Preview in Tor Browser
Video Podcast	Preview in Tor Browser
Web Feed	Preview in Tor Browser
webcal	Always ask

5. Select the *Privacy* tab.

The screenshot shows the 'Privacy' tab selected in the left sidebar of the Tor Browser's preferences. The main content area is titled 'Privacy' and contains sections for 'Tracking', 'History', and 'Location Bar'. In the 'Tracking' section, two checkboxes are checked: 'Request that sites not track you' and 'Use Tracking Protection in Private Windows'. A 'Change Block List' button is also present. The 'History' section shows a dropdown menu set to 'Never remember history'. It includes a note about using the same settings as private browsing and a link to clear all current history. The 'Location Bar' section suggests items for the location bar and has a link to change search engine suggestions.

General
Search
Content
Applications
Privacy
Security
Sync
Advanced

Privacy

Tracking

Request that sites not track you [Learn More](#)

Use Tracking Protection in Private Windows [Learn more](#) [Change Block List](#)

History

Tor Browser will:

Tor Browser will use the same settings as private browsing, and will not remember any history as you browse the Web.

You may also want to [clear all current history](#).

Location Bar

When using the location bar, suggest:

History

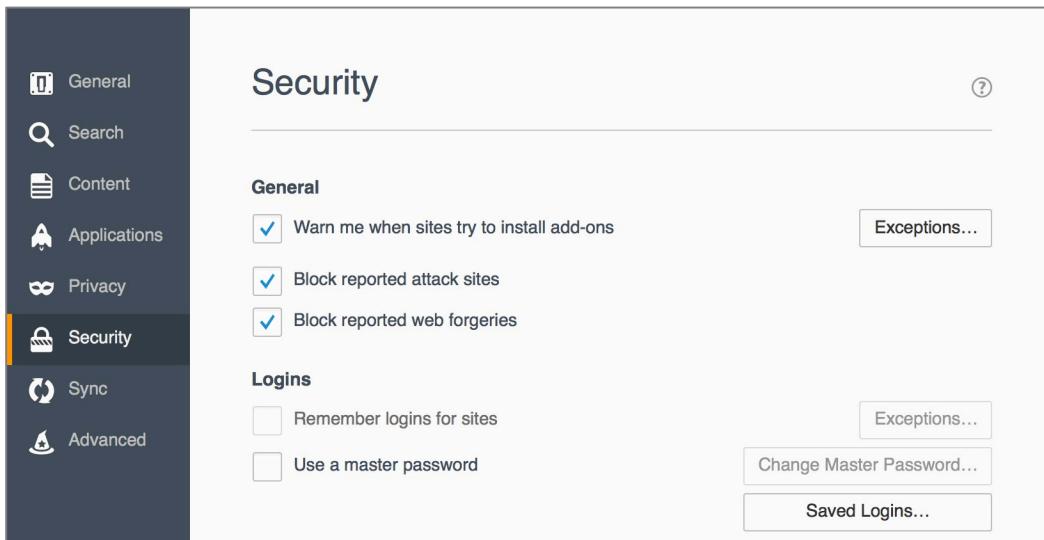
Bookmarks

Open tabs

[Change preferences for search engine suggestions...](#)

- Enable *Tracking > Request that sites not track you*
- Enable *Tracking > Use Tracking Protection in Private Windows*
- Enable *History > Tor Browser will: > Never remember history*
- *Location Bar* may be configured to your taste.

6. Select the *Security* tab.



- Enable *General > Warn me when sites try to install add-ons*.
- Enable *General > Block reported attack sites*.
- Enable *General > Block reported web forgeries*.
- Configure other settings to your taste.

7. Select the *Sync* tab.

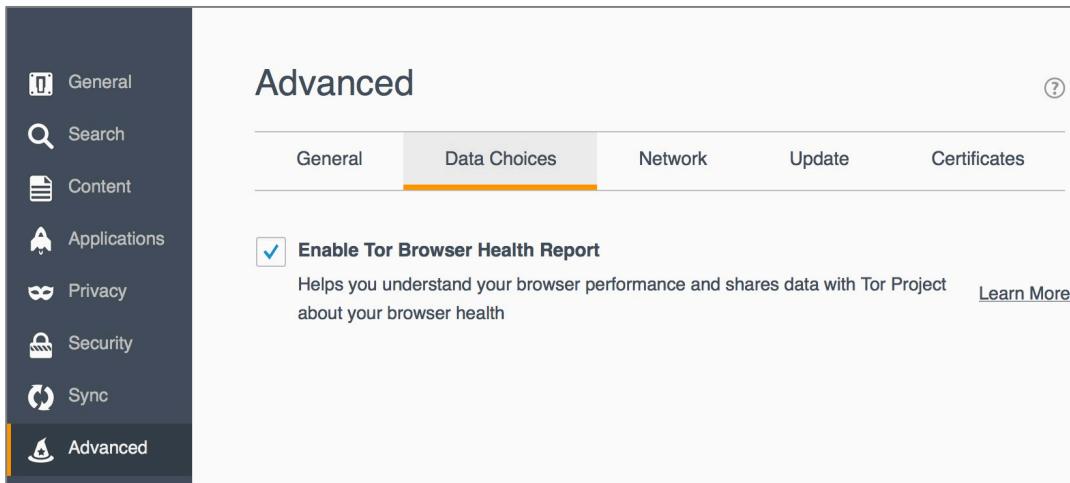
14 Web Browsing

The screenshot shows the 'Sync' settings page in the Firefox preferences. On the left, a sidebar lists options: General, Search, Content, Applications, Privacy, Security, Sync (which is selected and highlighted in orange), and Advanced. The main content area is titled 'Sync' and features a sub-section 'Take your Web with you'. It explains that users can synchronize bookmarks, history, tabs, passwords, add-ons, and preferences across devices. A 'Connect with a Firefox Account' section includes a Firefox logo, a 'Create Account' button, and a 'Sign In' button. To the right, there's a diagram showing a cloud connected to a laptop, smartphone, and tablet, with arrows indicating bidirectional sync. Below the diagram, text encourages users to sync with their mobile device by downloading the Firefox app for Android or iOS.

- Configure to your taste.
8. Select the *Advanced* tab, and then select the *General* tab.

The screenshot shows the 'Advanced' settings page in the Firefox preferences. The sidebar on the left remains the same, showing General, Search, Content, Applications, Privacy, Security, Sync, and Advanced. The main content area is titled 'Advanced' and has a tab bar with 'General', 'Data Choices', 'Network', 'Update', and 'Certificates'. The 'General' tab is selected and highlighted in orange. Under the 'General' tab, there are two sections: 'Accessibility' and 'Browsing'. The 'Accessibility' section contains three checkboxes: 'Always use the cursor keys to navigate within pages', 'Search for text when I start typing', and 'Warn me when websites try to redirect or reload the page'. All three are currently unchecked. The 'Browsing' section contains four checkboxes: 'Use autoscrolling', 'Use smooth scrolling', 'Use hardware acceleration when available', and 'Check my spelling as I type'. The first three are checked (indicated by a blue checkmark), while the last one is unchecked.

- Configure to your taste.
9. Select the *Data Choices* tab, and then enable *Enable Tor Browser Health Report*.

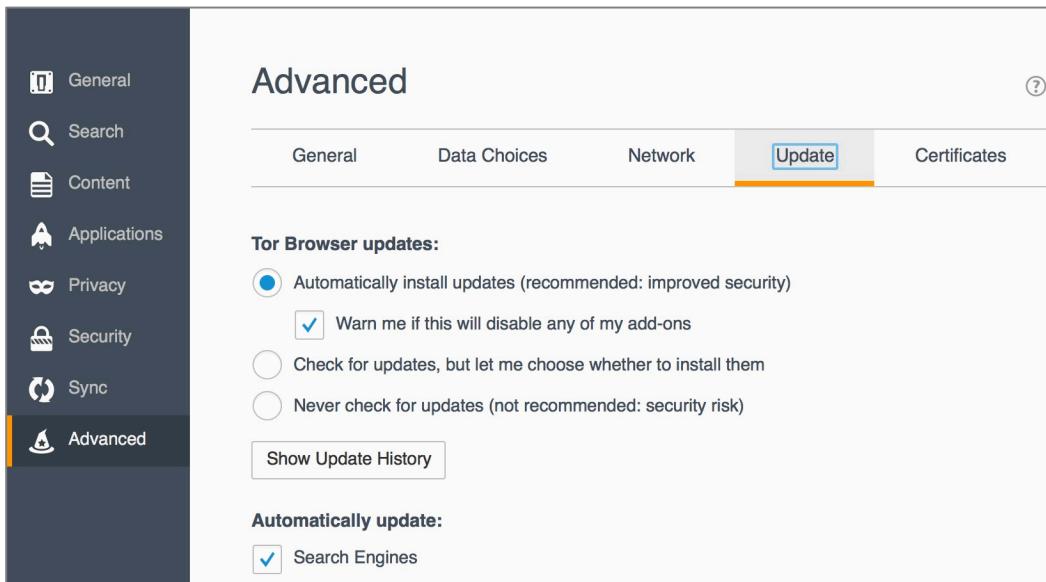


10. Select the *Network* tab.

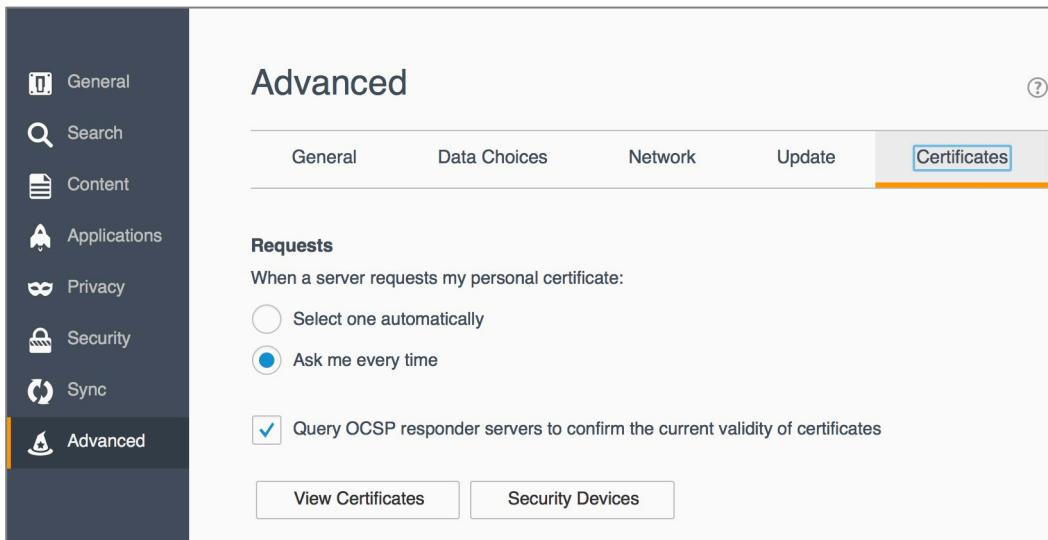
The screenshot shows the 'Advanced' settings page in the Tor Browser. The left sidebar has icons for General, Search, Content, Applications, Privacy, Security, Sync, and Advanced, with 'Advanced' currently selected. The main area has a tab bar with General, Data Choices, Network (which is highlighted in orange), Update, and Certificates. The 'Network' tab contains sections for 'Connection' (Configure how Tor Browser connects to the Internet) with a 'Settings...' button, 'Cached Web Content' (Your web content cache is currently using 0 bytes of disk space) with a 'Clear Now' button, 'Override automatic cache management' (checkbox), and 'Limit cache to' (input field set to 350 MB). The 'Offline Web Content and User Data' section shows 'Your application cache is currently using 0 bytes of disk space' with a 'Clear Now' button, a checked checkbox for 'Tell me when a website asks to store data for offline use', and a 'Exceptions...' button. A large empty box below is labeled 'The following websites are allowed to store data for offline use:' with a 'Remove...' button.

- Enable *Tell me when a website asks to store data for offline use.*
- Configure other settings to your taste.

11. Select the *Update* tab.



- Enable *Automatically install updates (recommended: improved security)*.
- Enable *Warn me if this will disable any of my add-ons*.
- Enable *Automatically update: Search Engines*.
- Configure other settings to taste.

12. Select the *Certificates* tab.

- Enable *Requests > Ask me every time.*
- Enable *Query OCSP responder servers to confirm the current validity of certificates.*

13. Close the preferences tab in Tor.

Great work! You are now ready to use Tor to securely and anonymously browse the Internet.

But remember, Tor is just one small part of *real* anonymity and security on the Internet. Many in the Internet Security field (including Edward Snowden) believe that to do this right, you will want a bootable Tails thumb drive. Learn all about it in our upcoming *Practical Paranoia: Tails Security Essentials* book. In the meantime, visit the Tails¹³ home page.

¹³ <https://tails.boum.org>

14.12 Onion Sites and the Deep Web

Tor not only allows you to have anonymous access to your regular web sites, it is also the only gateway to the *Deep web*¹⁴. The deep web is also known as the *Invisible Web*. It consists of web content deliberately not indexed with standard search engines, and only accessible by Tor. These sites are also called *Onion sites*, as they end with *.onion*.

Although the deep web is primarily thought of as a collection of sites to sell illegal products and services, there are also good and responsible uses for it. For example, in repressive countries such sites provide an avenue for freedom workers to work, for reporters to securely exchange information with sources (Ed Snowden did this), and there are sites to provide resources for whistleblowers.

As the deep web is not indexed by Google, Bing, or any other standard search engine, how do you go about discovering its resources? The list is in constant flux, but as of this writing, here are some good starting points:

- [TorLinks¹⁵](#)
- [Torch¹⁶](#)
- [Wikipedia¹⁷](#)

¹⁴ [https://en.wikipedia.org/wiki/Deep_web_\(search\)](https://en.wikipedia.org/wiki/Deep_web_(search))

¹⁵ <http://torlinkbgs6aabns.onion>

¹⁶ <http://xmh57jrzrnw6insl.onion/>

¹⁷ https://en.wikipedia.org/wiki/List_of_Tor_hidden_services

14.13 Review Questions

1. HTTPS uses the _____ encryption protocol.
2. To ensure your browser goes to https even if entering http, install the _____ plug-in.
3. To ensure your browser doesn't store browsing history, passwords, user names, list of downloads, cookies, or cached files, enable _____ mode.
4. By default, any two people will have the same results for a given Google search. (True or False)
5. By default, any two people will have the same results for a given DuckDuckGo search. (True or False)
6. TOR is based on the _____ browser.
7. It is OK to install browser plug-ins to TOR. (True or False)

15 Email

Human beings the world over need freedom and security that they may be able to realize their full potential.

—Aung San Suu Kyi¹, Burmese opposition leader and chairperson of the National League for Democracy in Burma

¹ https://en.wikipedia.org/wiki/Aung_San_Suu_Kyi

15.1 The Killer App

It can be rightfully argued that email is the killer app that brought the Internet out of the geek world of university and military usage and into our homes (that is, if you can ignore the overwhelming impact of Internet pornography.) Most email users live in some foggy surreal world with the belief they have a God or constitutionally given right to privacy in their email communications.

No such right exists. Google, Yahoo!, Microsoft, Comcast, or whoever hosts your email service all are very likely to turn over all records of your email whenever a government agency asks for that data. In most cases, your email is sent and received in clear text so that anyone along the dozens of routers and servers between you and the other person can clearly read your messages. Add to this knowledge the recent revelations about PRISM², where the government doesn't have to ask your provider for records, the government simply *has* your records.

If you find this as distasteful as I do, then let's put an end to it!

² [https://en.wikipedia.org/wiki/PRISM_\(surveillance_program\)](https://en.wikipedia.org/wiki/PRISM_(surveillance_program))

15.2 Phishing

The act of phishing is epidemic on the Internet. Phishing³ is the attempt to acquire your sensitive information by appearing as a trustworthy source. This is most often attempted via email.

The way the process often works is that you receive an email from what appears to be a trustworthy source, such as your bank. The email provides some motivator to contact the source, along with what appears to be a legitimate link to the source website.

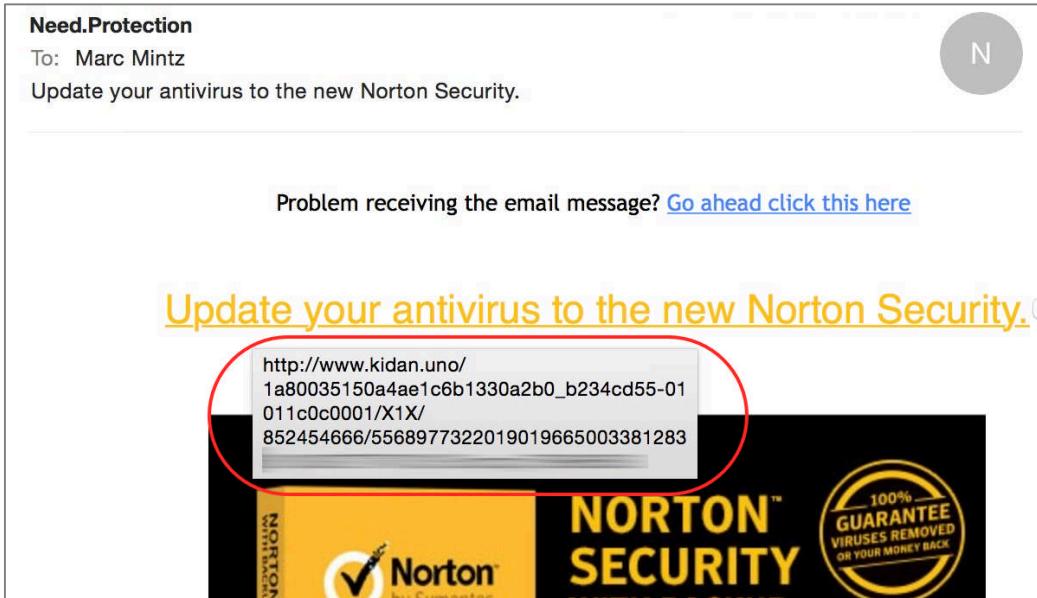
When you click the link, you are taken to what appears to be the trustworthy source (perhaps the website of your bank), where you are prompted to enter your username and password.

At that point they have you. The site is a fraud, and you have just given the criminals your credentials to access your bank account. In a few moments your account may be emptied.

The key to preventing a successful phishing attack is to be aware of the *real* URL behind the link provided in the email.

³ <https://en.wikipedia.org/wiki/Phishing>

The link that appears in an email may have nothing at all to do with where the link takes you. To see the *real* link, hover (don't click) your cursor over the link. After 3 seconds, the *real* link will pop-up.



Some of these scams are getting a bit more sophisticated in their choice of URL links, and attempt to make them appear more legitimate. For example, the email may say it is from *Bank of America*, and the link say *bankofamerica.com*, but the actual URL will be *bankofamerica.tv*, or *bankofamerica.xyz.com*.

If you have any doubts at all, it is best to contact your bank, stock broker, insurance agent, etc. directly by their known email or phone number.

15.3 Email Encryption Protocols

There are three common protocols that provide encryption of email between the sending or receiving computer and the SMTP (outgoing), IMAP (incoming), and POP (incoming) servers:

- **TLS⁴** (Transport Layer Security)
- **SSL⁵** (Secure Socket Layer), the TLS predecessor
- **HTTPS⁶** (Hypertext Transport Layer Secure)

Understand that these protocols only encrypt the message as it travels between your computer and your email server and back. Unless you are communicating with only yourself (sadly, as most programmers are prone), this does little good unless you know that the other end of the communication also is using encrypted email. If they aren't, then once your encrypted mail passes from your computer to your email server, it becomes clear text from your email server, through dozens of Internet routers, to the recipient email server, and finally onto the recipient's computer.

⁴ http://en.wikipedia.org/wiki/Secure_Sockets_Layer

⁵ http://en.wikipedia.org/wiki/Secure_Sockets_Layer

⁶ <http://en.wikipedia.org/wiki/Https>

15.4 TLS and SSL With Mail App

In order to use TLS or SSL, the following criteria must be met:

- Your email provider offers a TLS or SSL option. Many do not. If your provider does not offer this, *run*, don't walk, to another provider. If you are not sure which to select, I'm a fan of Google mail.
- You are using an email application as opposed to using a web browser to access your email.
- Your email application supports TLS or SSL.
- Your email provider has configured your email service to use TLS or SSL.
- You have configured your email application to use TLS or SSL
- Lastly, although not a requirement for TLS or SSL, a requirement to stall off breaking your password is that your email provider allows for strong passwords, and you have assigned a strong password to your email (many providers still are limited to a maximum of 8 character passwords.)

15.4.1 Assignment: Configure Email to Use TLS or SSL

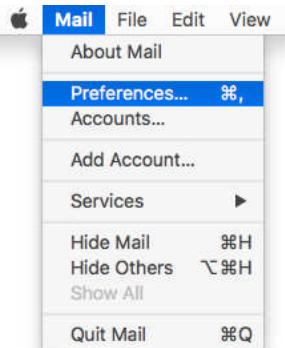
If you use a web browser for email, you may skip this assignment and move on to the next where we configure your browser-based email to use https.

First we need to verify if your email currently uses TLS or SSL:

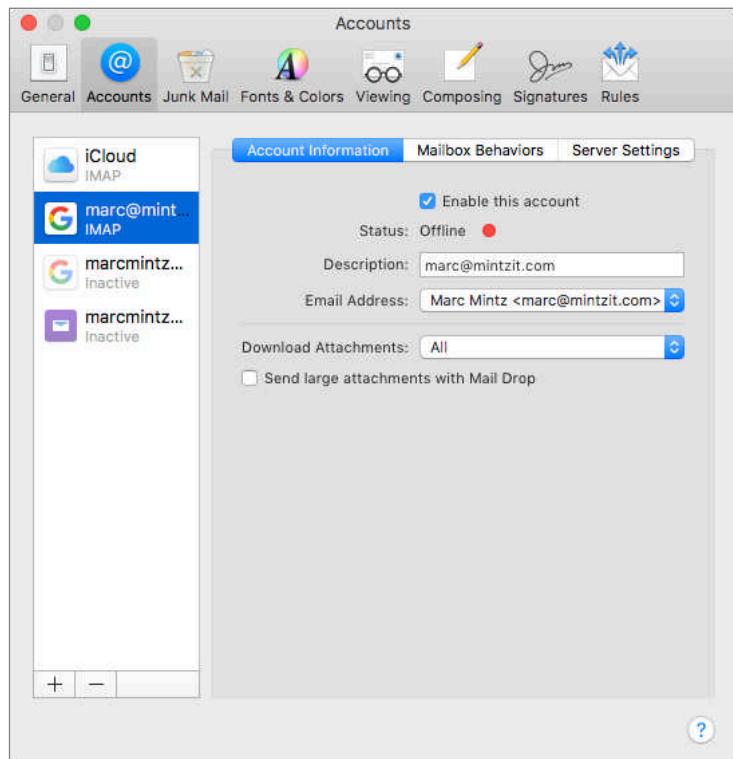
1. Open Mail.app, located in */Applications* and in your *Dock*.

15 Vulnerability: Email

2. Select the *Mail* menu > *Preferences*.



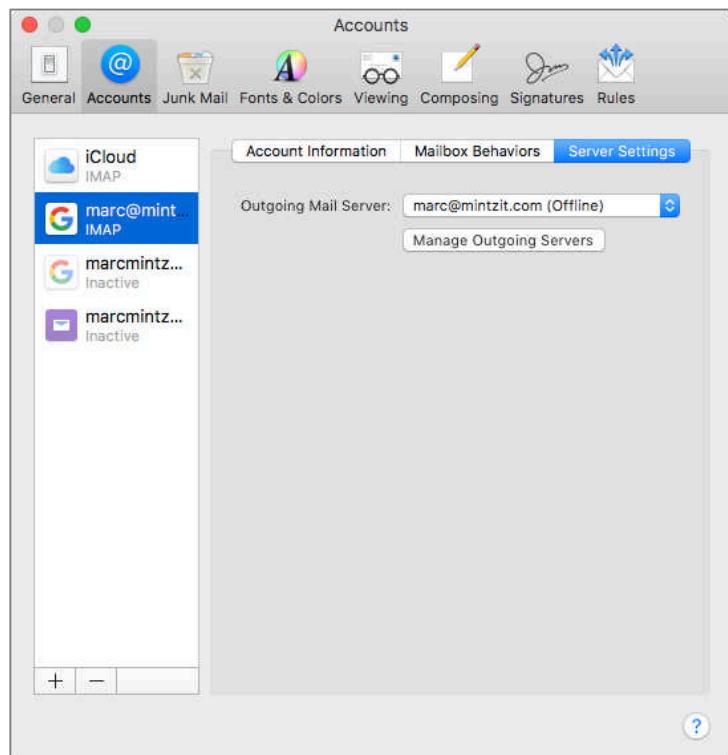
3. From the *Mail Preferences*, select the *Accounts* tab.



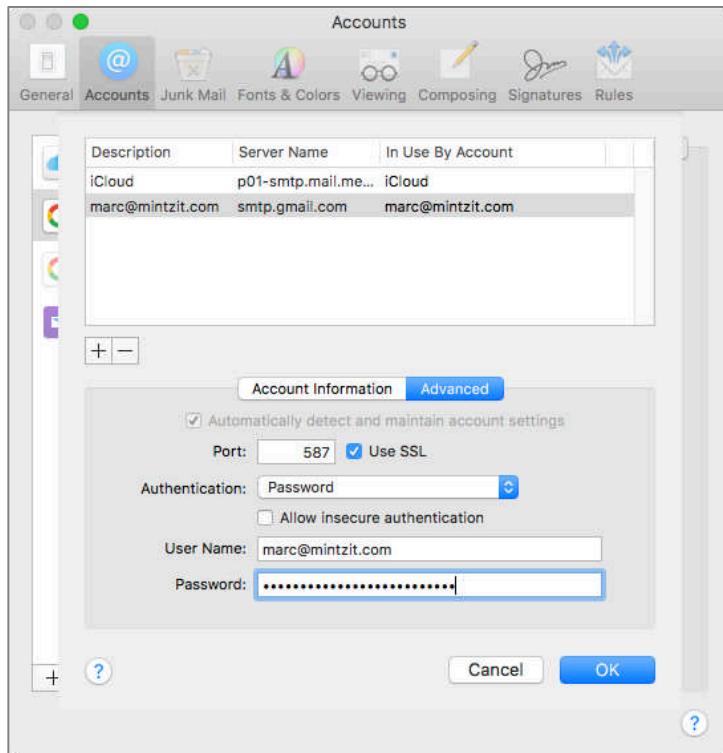
4. From the side bar, select your email account.
5. Select the *Server Settings* tab.

15 Vulnerability: Email

6. Select the *Manage Outgoing Servers* button.



7. From the *Manage Outgoing Servers* window, select the target email account, and then select the *Advanced* tab in the middle of the window.



8. Verify that the *Port: Use SSL* checkbox is enabled.
- Although macOS only provides a checkbox for SSL, this will enable TLS as well.
 - If SSL is not enabled, contact your email provider and ask if they do work with TLS or SSL. If they don't, change providers NOW.
9. If they do support TLS or SSL, find out if there are any special settings that need to be changed in this window, and then make the changes.
10. Keep the provider on the line for the next steps.
11. Select the *OK* button, returning you to the *Accounts* window.
12. Close the *Mail Preferences* window.

15 Vulnerability: Email

You now are sending and receiving encrypted email between your computer and your email server. Keep in mind you have no control over any encryption of your email between your server and the sender/recipient at the other end.

15.5 HTTPS With Web Mail

We discussed HTTPS in the previous chapter. It is an encryption protocol used with web pages. It also can be used to secure email that is accessed via a web browser. When using HTTPS your user name and password are fully encrypted, as are the contents of all email that you create or open.

When using a web browser to access email, it is vital that your email site use the HTTPS encryption protocol to help ensure data and personal security.

15.5.1 Assignment: Configure Web Mail to Use HTTPS

If you use a web browser to access your email, it is critical that your web connection use HTTPS. In this assignment we will verify that your browser-based email uses HTTPS:

1. Launch your web browser.
2. Go to your log in page for your email. In the example here we will be using Google Mail (Gmail).
3. As in the screen shot below, make sure that the URL field shows either the lock to the left of the URL, or *https://* and not *http://*. This indicates you are communicating over a secure, encrypted pathway.



4. If instead your browser shows the URL to be *http://*, try revisiting your email log in page, but this time manually enter *https://*.
5. If you get to the log in page, all is good. Just bookmark the *https://* URL and use it instead of the previous non-secure URL.
6. If you cannot get to your log in page, change your email provider NOW!

15.6 End-To-End Secure Email With ProtonMail

Using TLS/SSL or HTTPS for email is a good start. Unfortunately, unless you are certain that the other end of the communication chain also is using *the same email system as yourself*, this is much like locking your front door when leaving for vacation, while leaving the back door open. The reason is that even if the other user has TLS/SSL or HTTPS, this only ensures security between their computer and their server. When the two of you exchange email, there is no guarantee that the email is not in plain text once it hits either server, or when being transmitted from sender to recipient servers.

If you are serious about email security, then you need to use an end-to-end secure email solution.

There are two ways to approach this:

- Use an email encryption utility. This works well as long as the other end of the communication also is using the same encryption utility. Our next section will cover this strategy using *GNU Privacy Guard* and *S/MIME*.
- Use a cloud-based option. This method makes it every bit as simple to send and receive email as the user is accustomed to. The downside is that instead of using an email client, a website is used to send and receive mail. An example of this is *Sendinc.com*⁷.

An interesting hybrid option is found in *ProtonMail*. ProtonMail includes PGP public key/private key encryption, so that neither you nor the other party need deal with the potential headaches of installing and configuring PGP encryption.

ProtonMail has several advantages for the typical user, including:

- Free with optional monthly/yearly plans.
- Based in Switzerland so all user data is protected by Swiss privacy laws.
- Allows the user to determine the destruction date and includes unlimited retention.

⁷ <https://sendinc.com/>

- Allows for encrypted and password protected emailing to non-ProtonMail users.
- Allows for rich text email.

When sending from ProtonMail to a non-ProtonMail user, your recipient receives an email stating that a secure message is waiting. The recipient clicks the link, taking the recipient to an authentication page. Upon entering the password the recipient then sees the message. The recipient can directly and securely reply to the message, then you receive their reply in your inbox.

When sending from ProtonMail to ProtonMail, the interface is very similar to other email providers.

Although not quite as convenient as using your own email software, when security, convenience, and cost are taken into consideration against the impacts of data theft, or the potential drama of confidential communications being intercepted, we find ProtonMail to be an easy choice.

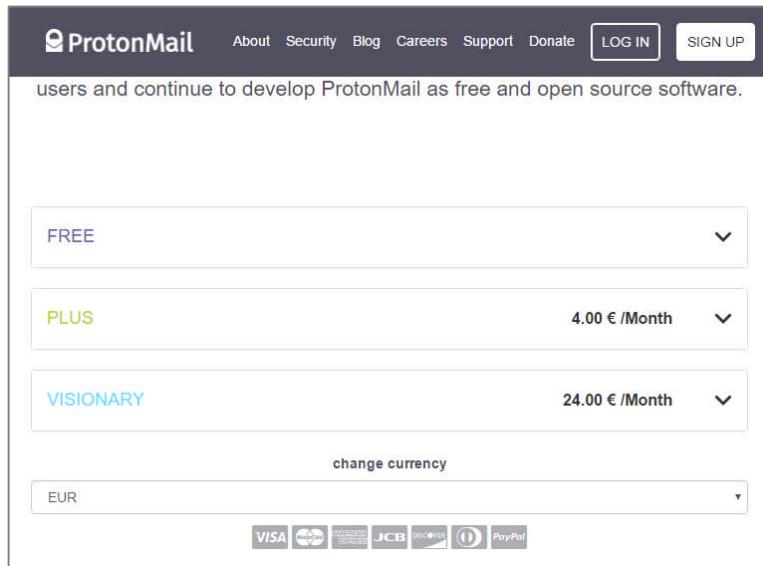
15.6.1 Assignment: Create a ProtonMail Account

In this assignment, you will create a ProtonMail account.

1. Using your web browser, visit <https://protonmail.com>. Select either the *Sign Up* or *Get Your Encrypted Email Account* button.

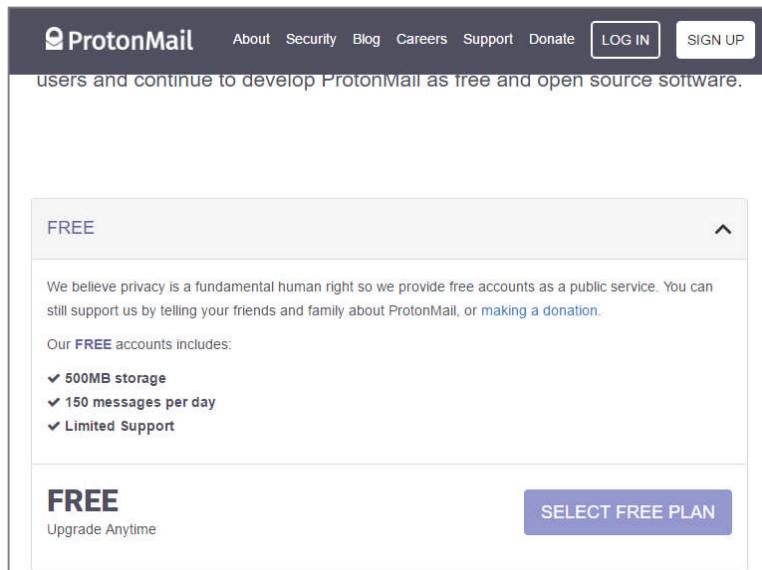


2. Scroll down to click the drop down arrow next to the plan you wish to use (PLUS is selected by default). In this tutorial we will be making a free account. If you wish to use a monthly plan, make sure to double check the currency used on the bottom of the page.



15 Vulnerability: Email

3. Click the *Select Free Plan* button.

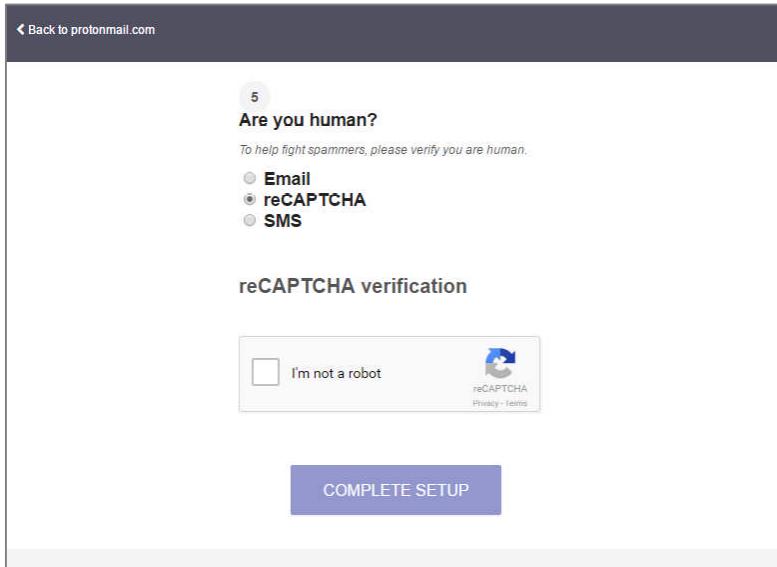


4. Enter the *Username* and *Password* you wish to use. We recommend using easy to remember 15 character passphrases.

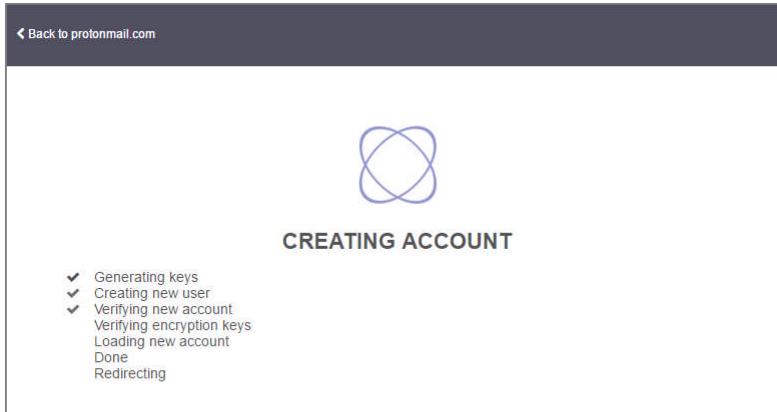
The screenshot shows the ProtonMail account creation process. Step 1, 'Username and domain', asks for a new email address. The input field contains 'MintzIT' followed by '@' and 'protonmail.com'. A green banner below the field indicates the username is available. Step 2, 'Login password', asks for a login password and its confirmation. Step 3, 'Mailbox password', asks for a mailbox password. Each step includes a note explaining its purpose: the login password is used to decrypt the inbox, and the mailbox password is used to encrypt and decrypt messages. All fields include a small question mark icon for help.

15 Vulnerability: Email

5. Provide a method of verification.

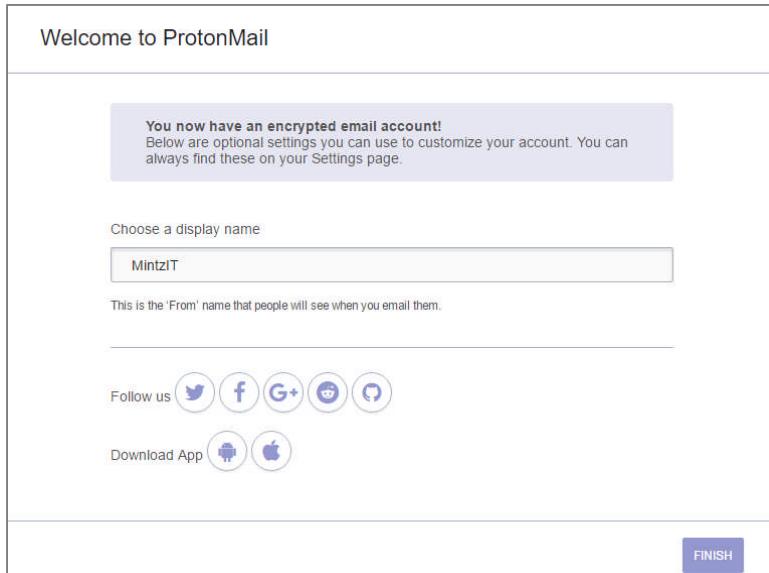


6. ProtonMail begins to create your account.

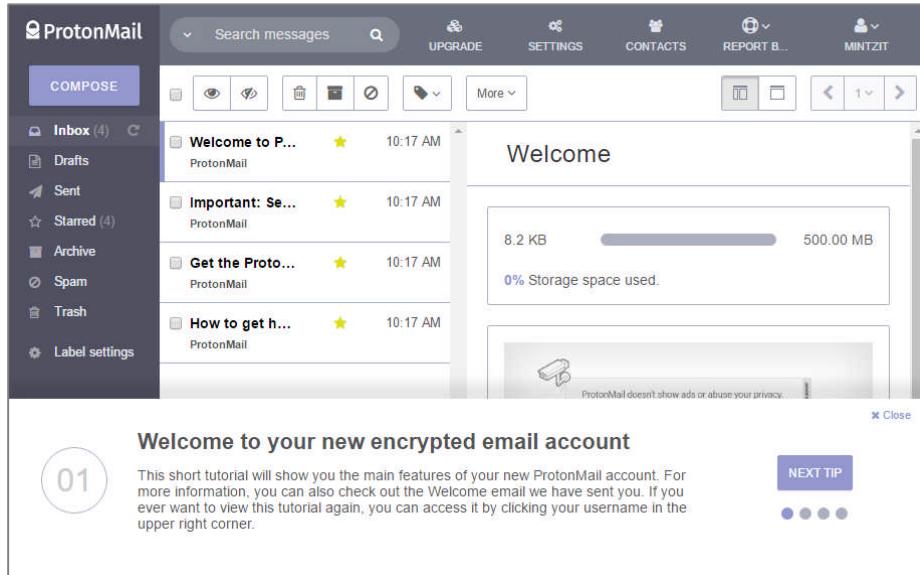


15 Vulnerability: Email

- At this stage enter the name that will be seen by other users. You also have the option of downloading iOS or Android Apps. Next click on the *Finish* button.



8. You have now finished the setup process. You will see a short tutorial on the bottom of your screen, it is recommended to read through it to understand some more of the features available to you.



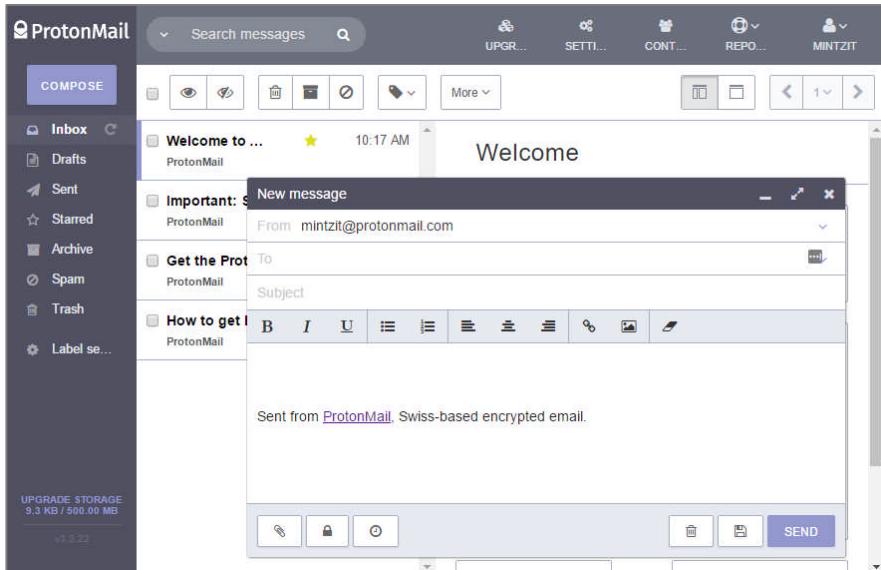
15.6.2 Assignment: Create and Send an Encrypted ProtonMail Email

In this assignment, you will send your first fully encrypted email through ProtonMail.

- **Prerequisite:** Completion of the previous assignment, or an existing ProtonMail account.
1. If you have just completed the previous assignment, select the *Compose* button in the top left. If not, use your web browser to visit *ProtonMail* at <https://ProtonMail.com>, select the *Login* link, and then log in.

15 Vulnerability: Email

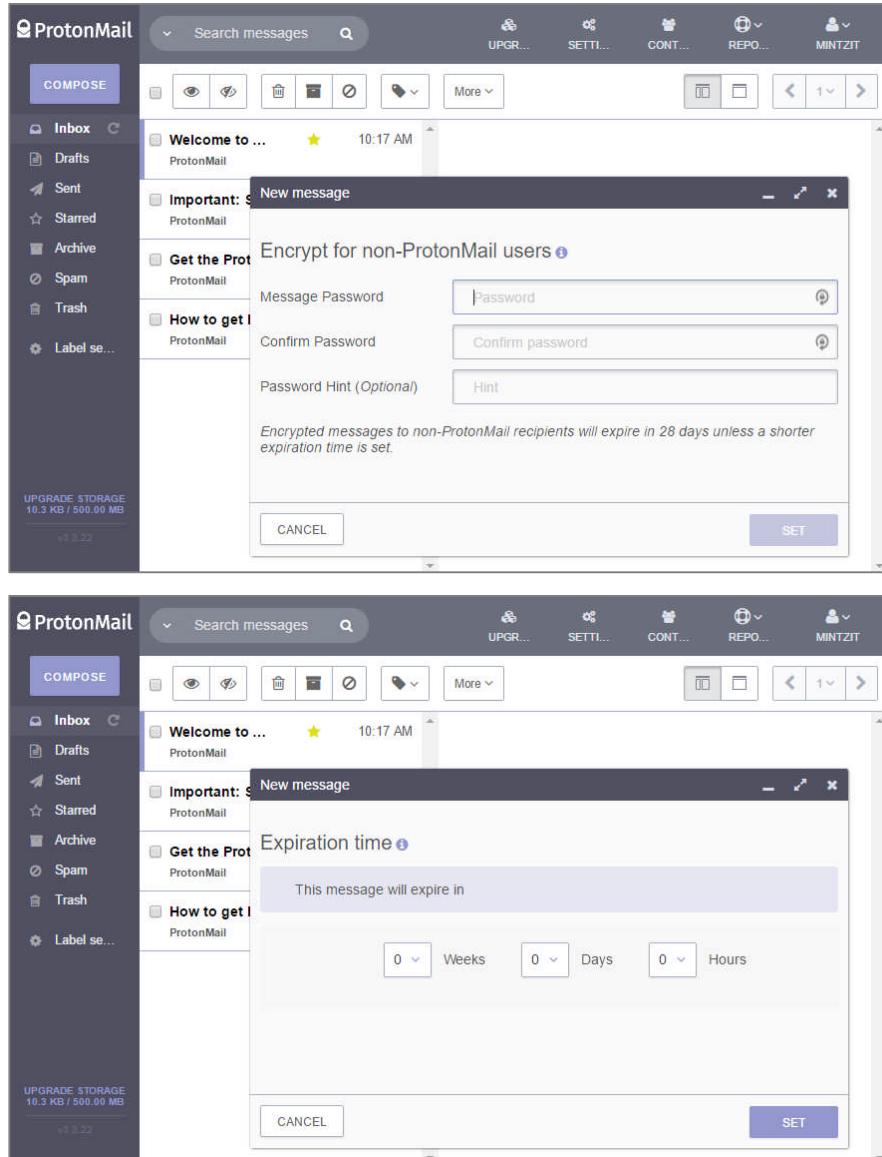
2. The *New Message* window should now be showing, enter the recipient email address, subject and a brief message.



3. Scroll to the bottom of the page, and then configure to your taste. The *Lock* icon allows you to set a password requirement to open the email from a non-

15 Vulnerability: Email

ProtonMail account. The *Clock* icon allows you to set an expiration time for the email.



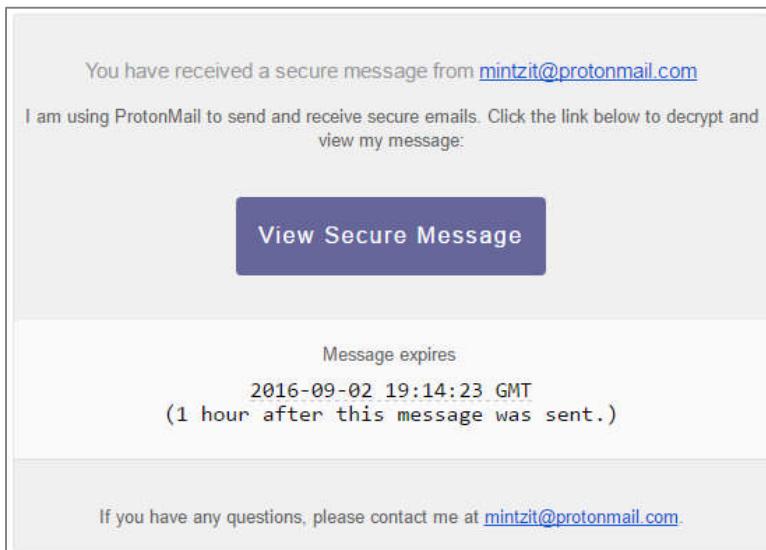
- Once you have finished configuring your email, click the *Send* button. It will take a moment to encrypt and then send.

Notification of your email has been sent to the recipient.

15.6.3 Assignment: Receive and Respond to a ProtonMail Secure Email

In this assignment you reply to a ProtonMail secure email.

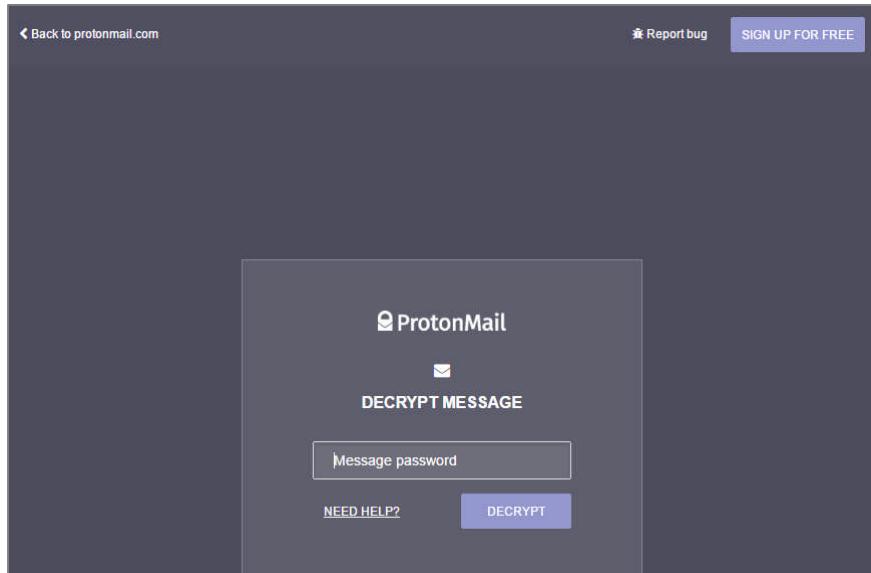
- **Prerequisites:** The previous two assignments must first be completed.
1. After you have sent an email from your ProtonMail account (previous assignment), the recipient receives the following email. To view the message, the recipient selects the *View Secure Message* button within the email.



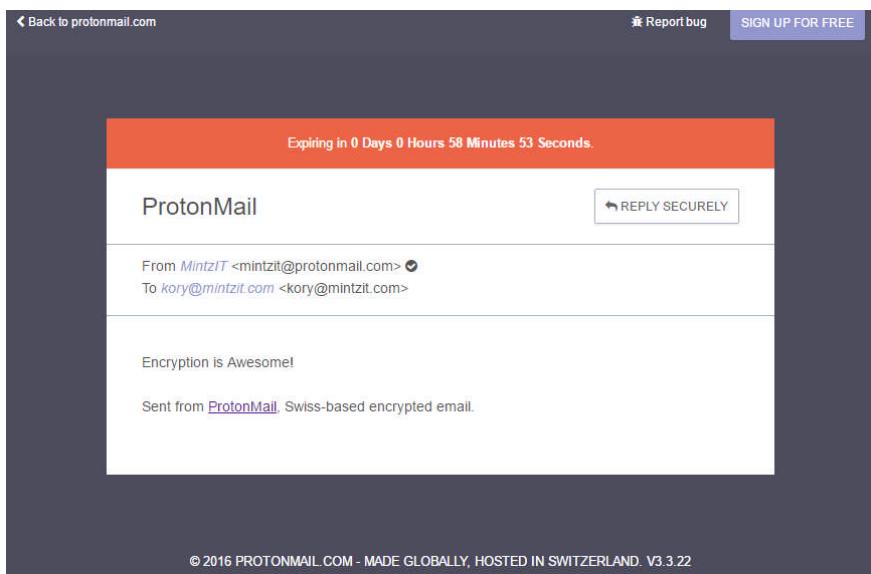
2. If the recipient already has a ProtonMail account, go to step 5. If the recipient does not have a ProtonMail account, they have the option of signing up for

15 Vulnerability: Email

ProtonMail in the top right of the webpage. If they do not wish to sign up they may instead enter the required password to access their email on this page.

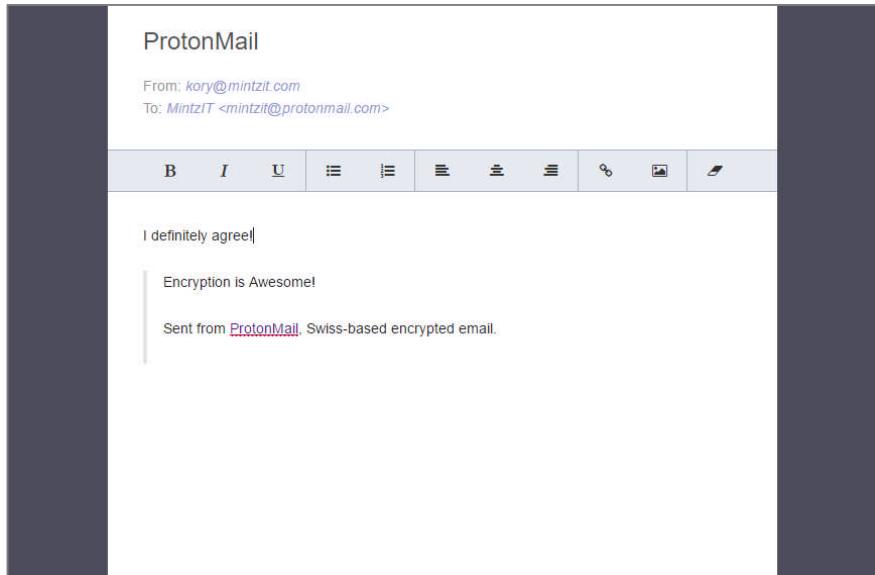


3. After entering the required password, the email is displayed in the recipient's browser. The recipient is also able to reply via this webpage by selecting *Reply Securely*.



15 Vulnerability: Email

4. The recipient then types in their reply and clicks on the *Send* button in the bottom right.

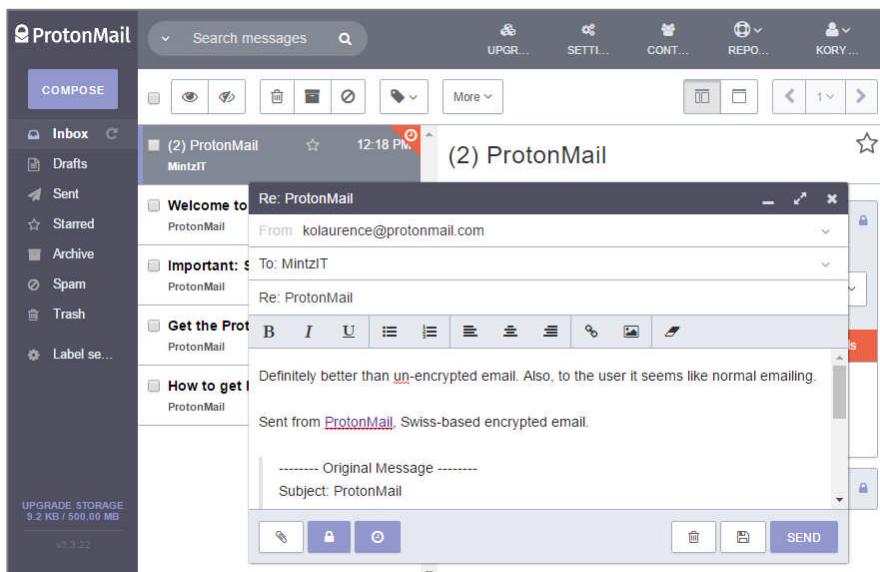
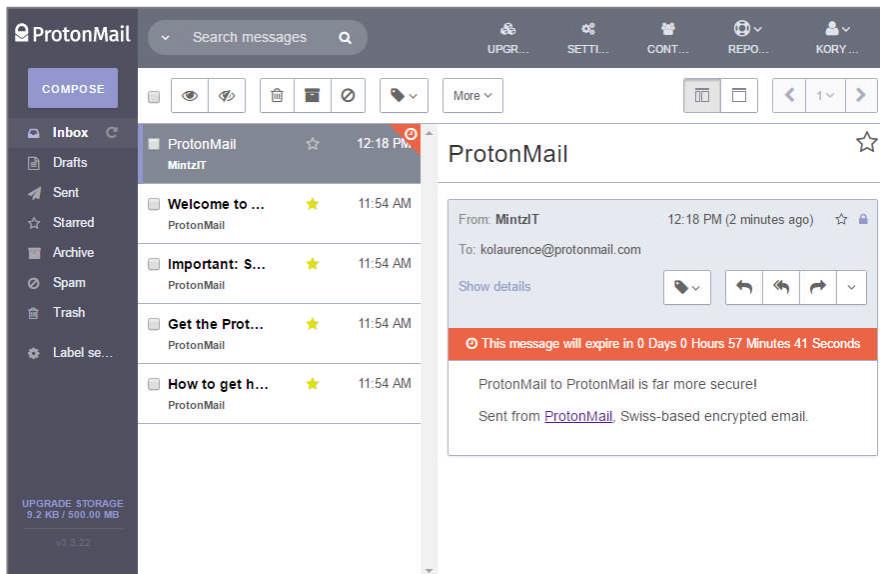


5. The original sender will receive a reply.

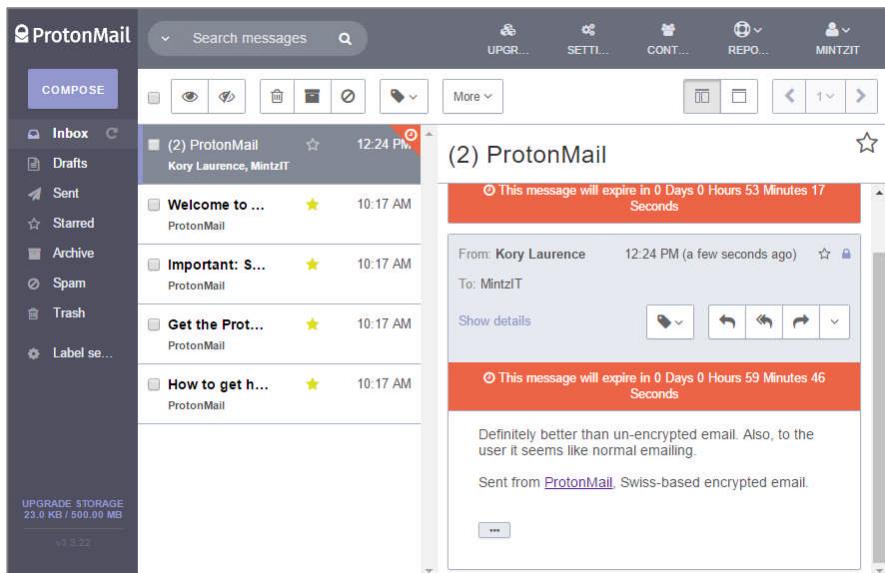
A screenshot of the ProtonMail inbox. On the left, a sidebar shows navigation links like COMPOSE, Inbox, Drafts, Sent, Starred, Archive, Spam, Trash, and Label se... A banner at the bottom left says "UPGRADE STORAGE 18.8 KB / 500.00 MB". The main area shows two messages from "ProtonMail". The top message is from "MintzIT" with the subject "(2) ProtonMail" and the body "I definitely agree! Encryption is Awesome! Sent from ProtonMail. Swiss-based encrypted email.". The bottom message is from "kory@mintzit.com" with the subject "(2) ProtonMail" and the body "This message will expire in 0 Days 0 Hours 57 Minutes 22 Seconds". It includes the same message content as the reply above. The ProtonMail logo is visible in the top right corner of the inbox area.

15 Vulnerability: Email

6. For either the original sender or the recipient, if they are using ProtonMail, it will show in their inbox like normal email. The email is decrypted and is fully viewable. Note that at no point is the message transmitted across the internet without encryption.



15 Vulnerability: Email



15.7 End-To-End Secure Email With GNU Privacy Guard

The gold standard for email security is to fully encrypt the message at the sender's computer in a format that only the intended recipient can decrypt. This tool also must be capable of alerting the recipient if the message has been tampered with in any way (i.e., a man-in-the-middle attack.) The leader in this arena is PGP (Pretty Good Privacy), now owned and maintained by Symantec. Fortunately, there is an open source utility that provides all of the core functionality and security of PGP, for free.

Setting up GPG⁸ (GNU Privacy Guard)—available for macOS/OS X, Windows, and Linux—takes a few more steps than our previous strategies in this section, and those with whom you wish to exchange secure email will need to also install GPG. But once both sender and recipient have their GPG in place, it is effortless to share fully encrypted messages.

Both PGP and GPG use the same strategy to securely encrypt email communications, and can exchange email with each other. Each user creates a *public key* and a *private key*. The Public Key typically is stored at a GPG server in the cloud, which can be found with a search for your name. The Private Key remains only on the user's computer. When sending an email to another person, your email application will automatically use the recipient's Public Key to encrypt the message. When the recipient receives the email, only the recipient's Private Key is able to decrypt and open the message.

If there are shortcomings to PGP and GPG, one is that as of this writing, there are only two iOS apps and one Android app, none of which are well received. Also, GPG is designed to work within an email client application, not a web browser. Although there are plug-ins for FireFox to allow for GPG, you are best to stick with the built-in Mail.app. Another issue is that before one can exchange encrypted email with someone else, both need to manually retrieve each other's public key. This typically is just a two-click process, but still...

⁸ <https://gnupg.org/>

Cryptography can quickly become Ph.D.-level material. I will cover everything you are likely to need to fully enable encryption and digital signing using GPG. Should you wish to delve deeper, visit the GPGTools Support site⁹.

15.7.1 Assignment: Install GPG and Generate a Public Key

To encrypt your email, you will need to have GPG installed, and have your recipient's Public Key installed in your GPG keychain. In order for your intended recipient to decrypt and read your email, the recipient needs to have GPG installed (or Gpg4win¹⁰ if using Windows, or GPA¹¹ if using Linux.) The recipient will also need to have your Public Key stored in their computer.

In this first assignment, you will install GPG on your computer, and upload your Public Key to the *GPG Public Key Server*, making it available to anyone wishing to send encrypted email to you.

- Note: As of this writing, GPGTools has just been certified as Mac OS X 10.11 El Capitan compatible. It will be some time before it is certified for macOS 10.12. However, it is anticipated the steps will be the same as below.

⁹ <http://support.gpgtools.org/kb>

¹⁰ <https://www.gpg4win.org>

¹¹ https://www.gnupg.org/related_software/gpa/index.en.html

1. Use your browser to visit *GPGTools* <https://gpgtools.org>, and then select the *Download GPG Suite* button.

The screenshot shows the GPG Suite 2016.08 release page. At the top left is the GPG Tools logo with a padlock icon. The top right features navigation links: GPG Suite, Donate, News, Open Source, Support, netidee, and a Twitter icon. The main title "GPG Suite 2016.08" is prominently displayed in the center. To its right is the date "August 16th, 2016". Below the title, a bold heading says "This is an important bugfix release." A paragraph explains that a subtle change to the auto check mechanism in the last release broke the automatic check for updates. It advises users to install this release or update from GPGPreferences by pressing the "Check Now" button. Another paragraph notes that GPGMail is not yet ready for macOS 10.12 Sierra and suggests holding off from installing it. At the bottom, there are two buttons: "Release Notes" (gray background) and "Download GPG Suite" (red border). Below these buttons, text indicates support for OS X 10.9 and newer, and provides a GPG Signature and Source link, along with a SHA1 hash: "SHA1 6adb52ce063b3952542037fa37394a0279acce3d".

2. The software will begin to download to your computer.

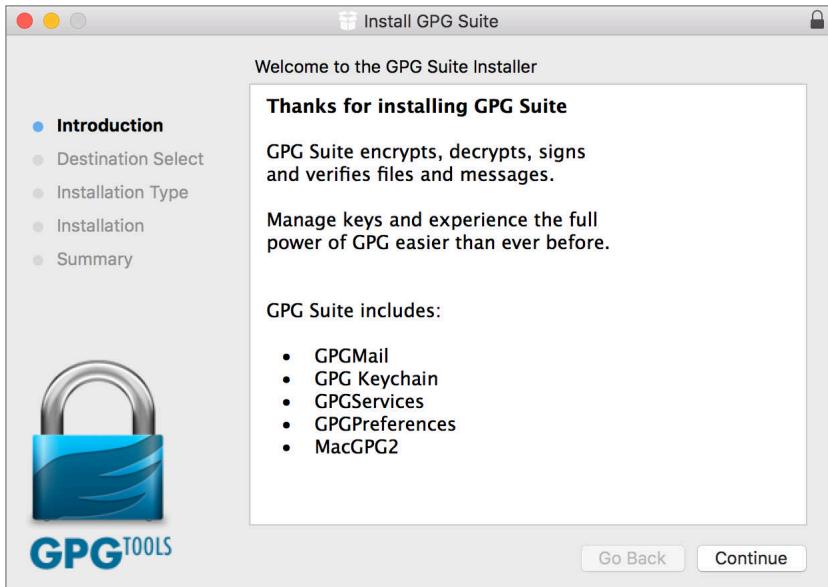
3. Go to your Downloads folder, locate and then double-click on the *GPG Suite.dmg* file. This will mount the GPG disk image to your desktop, and then open the disk image to reveal the GPG Suite window.



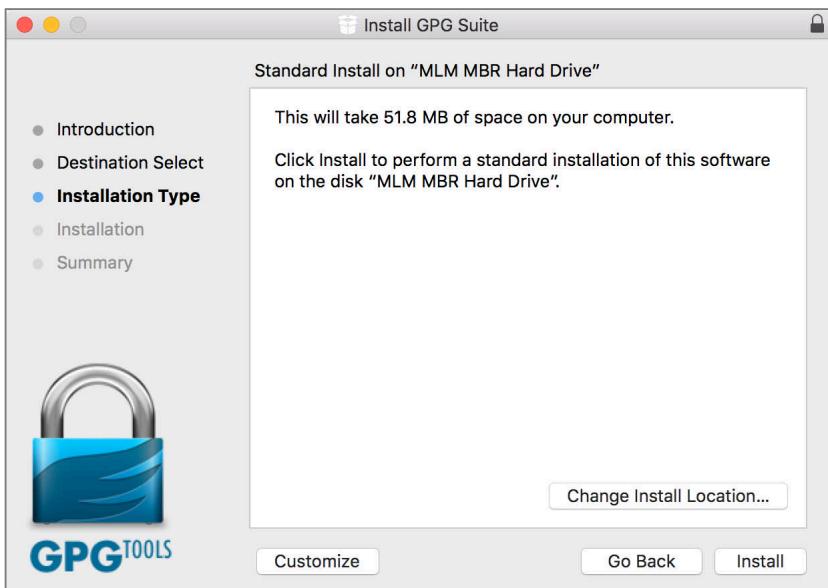
4. Double-click the *Install.pkg* icon inside of the GPG Suite window to launch the *Install GPG Suite installer*.

15 Vulnerability: Email

5. Select the *Continue* button.

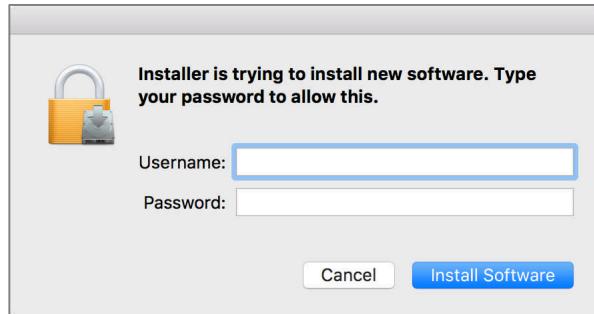


6. At the *Standard Install on “<Name of hard drive>”* window. Select the *Install* button.

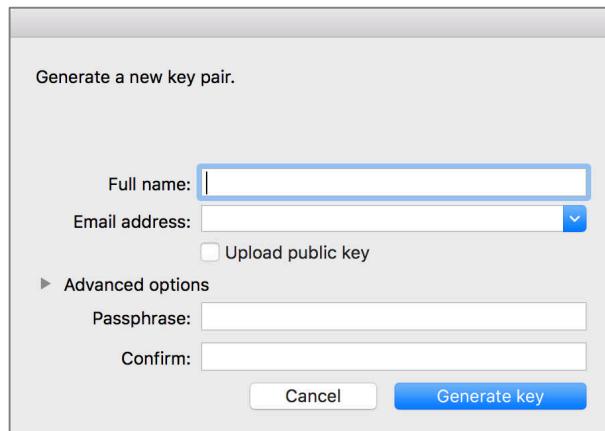


15 Vulnerability: Email

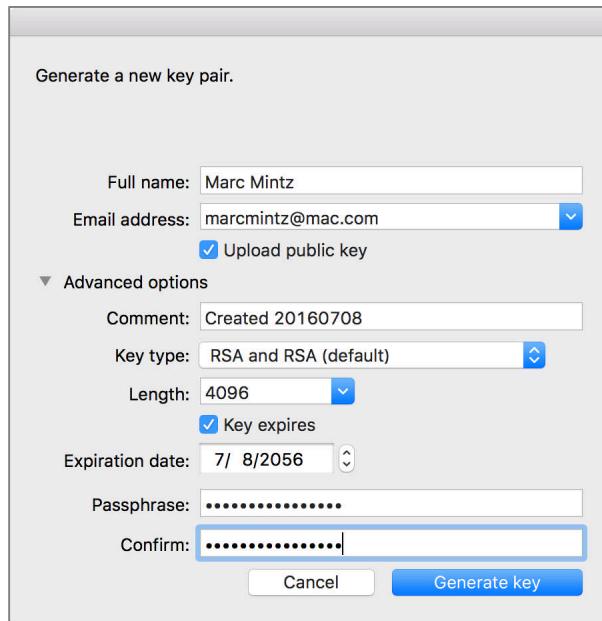
7. The authentication window will appear. Enter an administrator name and password, and then select the *Install Software* button.



8. *The installation was completed successfully* window appears.
9. The *GPG Keychain.app*, located in /Applications opens.



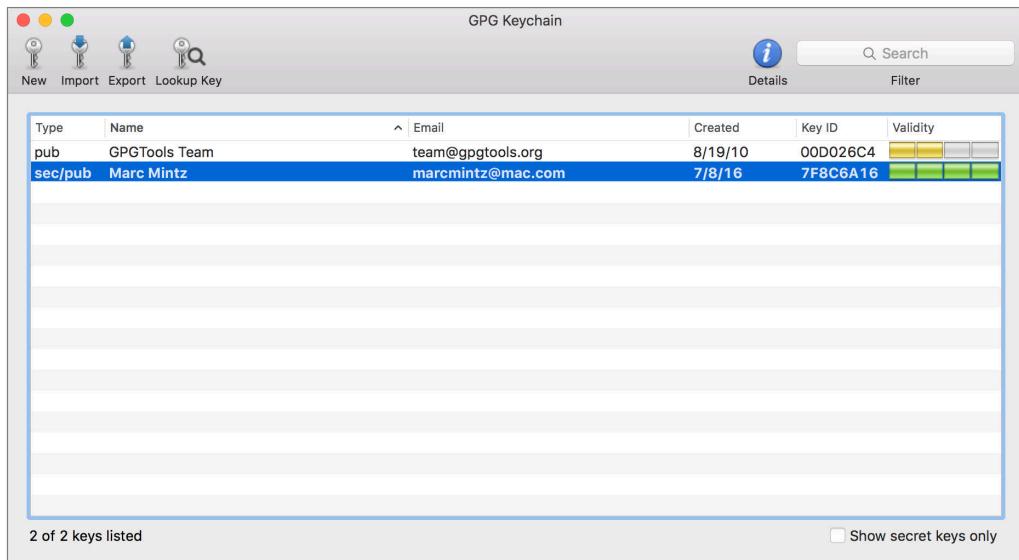
10. Select the *Advanced Options* link to expand the window, and then complete all fields.



- *Full Name:* Enter your full name as used in your email.
- *Email Address:* Enter the email address for which GPG encryption is being configured.
- *Upload Public Key after generation:* Enable. Once you generate a key, this cannot be removed from the key server. Be certain that the name you are using is the one you want others to be able to find you by via a server search.
- *Key type:* Select *RSA and RSA (default)*.
- *Length:* Select 4096. The larger the encryption bit depth, the more secure.
- *Key Expires:* I typically leave this disabled, allowing any of my encrypted email to be accessed (given the proper credentials) forever. However, if you prefer to set your key to self-expire, making any sent emails created with it unreadable after a certain date, then by all means enable this option.

- *Expiration Date:* If you have set your key to expire, this option will allow you to set the expiration date.
- *Passphrase:* This is a password to protect access to this record. As with all passwords, make it strong.

11. Select the *Generate key* button.
12. The new key will start to generate. During this time, the random key generator uses activity on your computer to help create a random key. You should move your cursor, or type some characters in another application during this time.
13. When your Public Key generation completes, the *GPG Keychain* window will display your new key.



Congratulations! You have successfully installed GPG to help encrypt your email.

15.7.2 Assignment: Add Other Email Addresses to a Public Key

- Prerequisite: GPGTools must be installed.

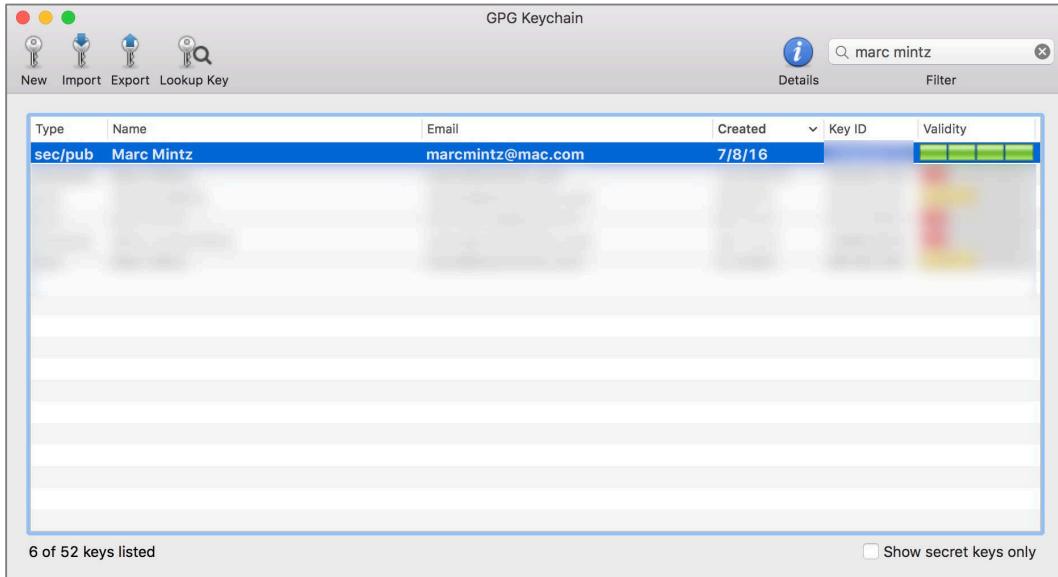
Many people have more than one email address. If you wish, you may create keys for each of your other addresses simply by repeating each of the steps in the

15 Vulnerability: Email

previous assignment. However, you may find that both tedious and somewhat redundant.

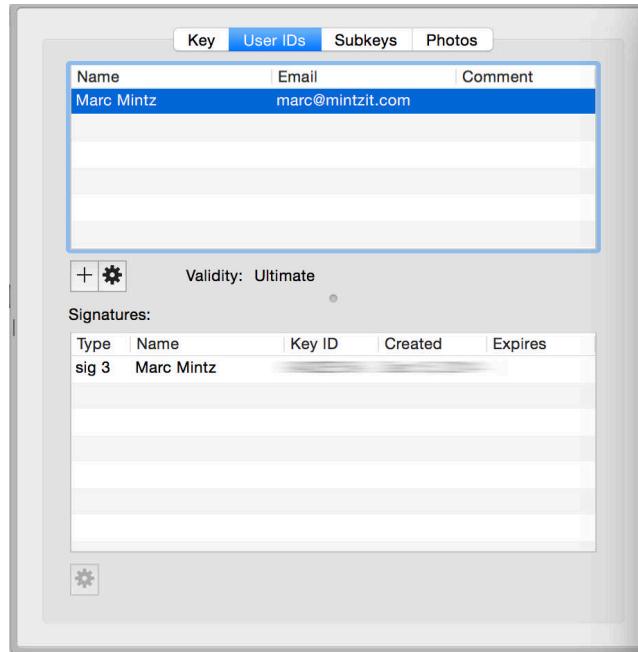
An alternative is to bind all of your email addresses together under one key. In this assignment we will do just that.

1. Open *GPG Keychain*, located in your */Applications* folder, and then double-click on your entry from the previous assignment.

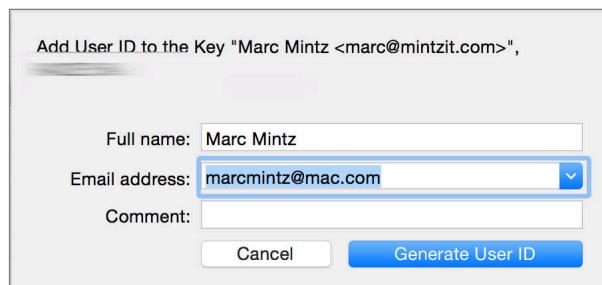


15 Vulnerability: Email

2. The *Key Inspector* window will open. Select the *User IDs* tab, select the account *Name*, and then select the + button.



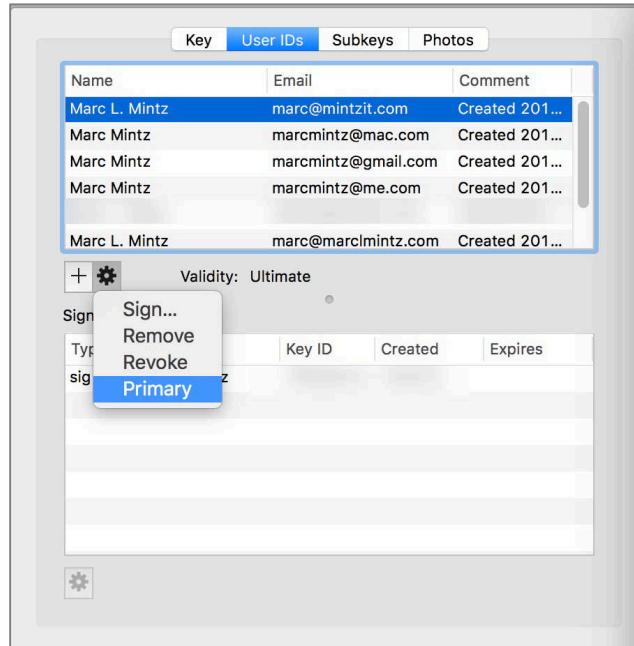
3. In the window that opens, enter your *Full name*, along with the new *Email address* you want to be bound to your original email/key combination, and then select the *Generate user ID* button.



4. Repeat steps 2 and 3 for each of your email addresses.

15 Vulnerability: Email

- When all of your email addresses have been added, select the one address you use most often, click the *gear* icon, and then select the *Primary* button to set this as your primary account.



15 Vulnerability: Email

- Though not required, let's add a photo to better identify you. Select the *Photos* tab.



15 Vulnerability: Email

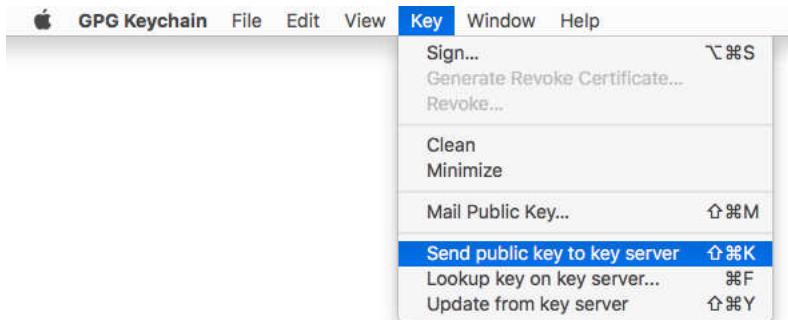
7. Select the + button, navigate your drive, and then select the desired ID picture. You are returned to the Photos window with the picture displayed.



8. You may have multiple ID pictures. After adding them, scroll through the Photos window to the one you want as your primary, and then select the Primary button.

9. Lastly, upload your changes to the Public Key Server. Select the *Key* menu > *Send Public Key to Server*.

- Note: You may also mail your public key to someone else from the *Key* menu > *Mail Public Key...*



Congratulations! You have successfully added all of your email accounts to GPG, allowing encrypted communications with any account.

15.7.3 Assignment: Install a Friend's Public Key

In order for you to send encrypted mail to someone else, it is necessary to have their *GPG Public Key*. In this exercise, you will find a friend's Public Key and add it to your GPG Keychain.

- Prerequisite: GPGTools must be installed.

Option A: The No Sweat Strategy

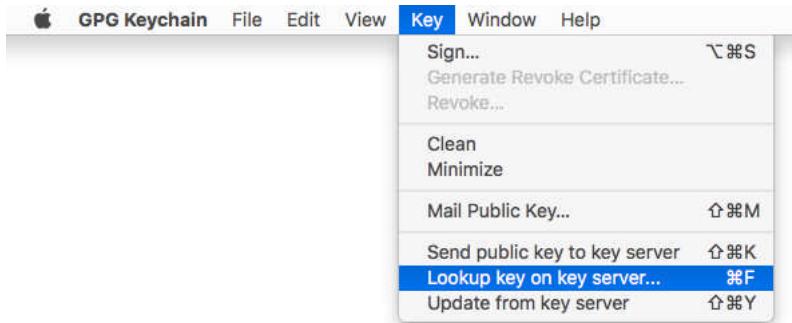
The easiest way to add a friend's Public Key is to have them send you an email from their GPG-enabled account (signed, but not encrypted.) Once you have their email, you also have their Public Key. But you may be listening a long time to crickets before they send you an email.

Option B: DIY

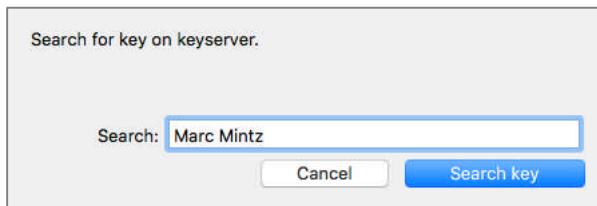
1. Open the *GPG Keychain Access.app* located in your */Applications/* folder.

15 Vulnerability: Email

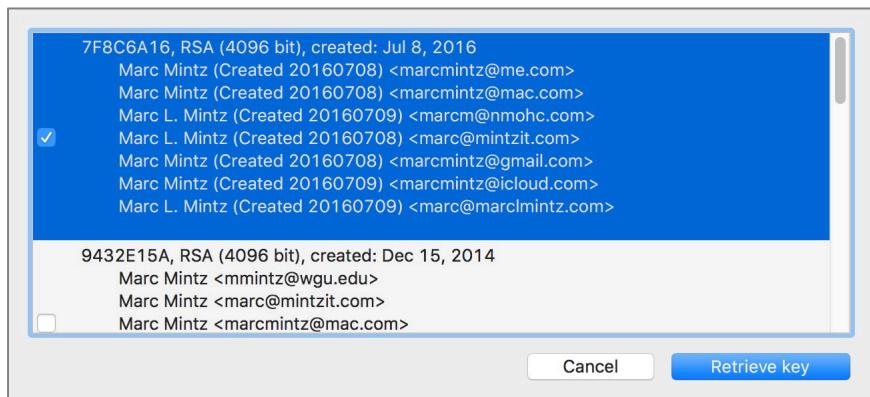
2. Select Key menu > *Lookup key on key server*.



3. The *Search for key on keyserver* window opens.



4. Enter the full name of the person you wish to either send encrypted mail to, or receive from, and then select the *Search key* button. A list of possible matches appears. If you don't yet know anyone with a GPG key, feel free to use *Marc L. Mintz*. Shown below are the search results for a *Marc L. Mintz*.



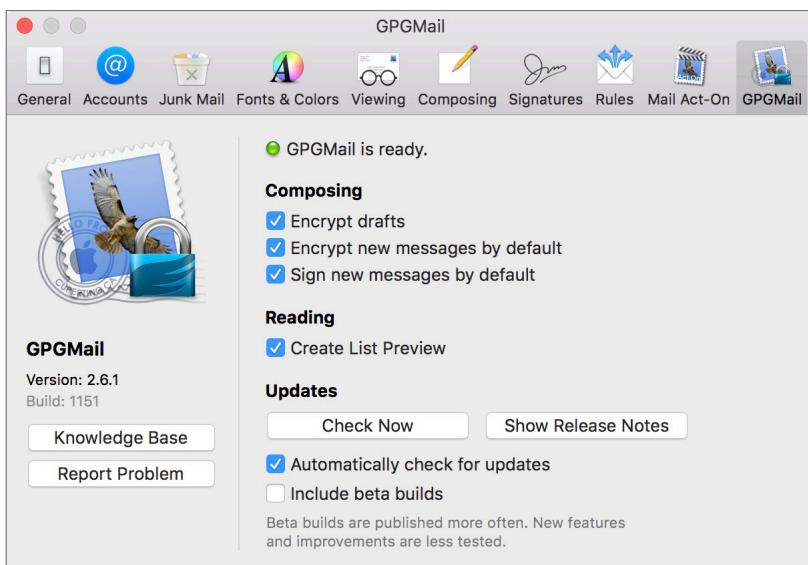
5. Once the *Search Key* has been selected, any public GPG keys that are stored will display. Select the target public key (if you aren't sure which is correct, select all of them), and then select the *Retrieve key* button.
6. The Public Key is now added to your GPG Keychain.

You are now ready to send encrypted email to your friends!

15.7.4 Assignment: Configure GPGMail Preferences

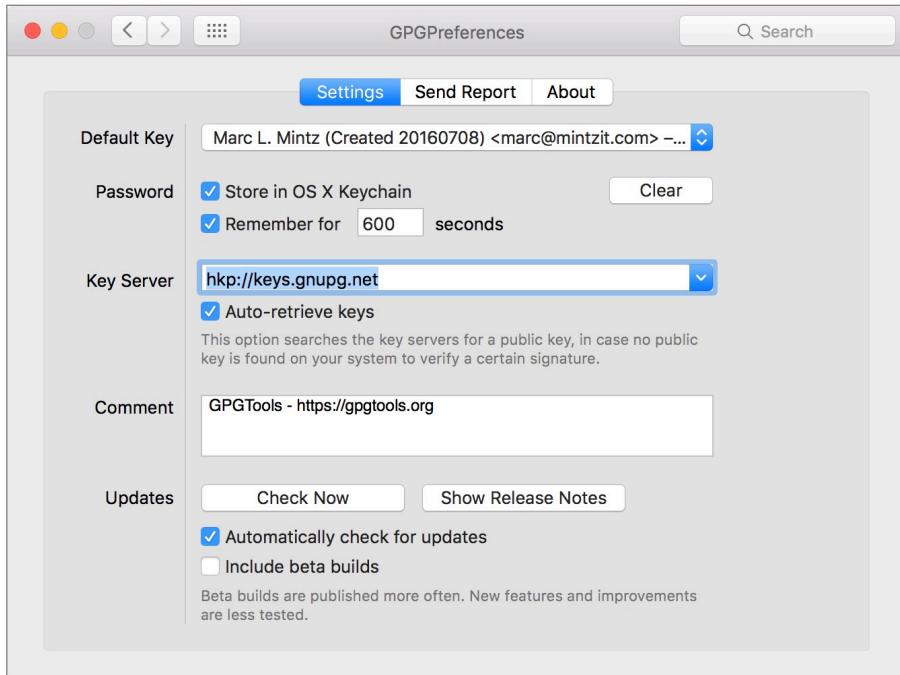
With GPG installed, the next step is to configure the *GPGMail Preferences* within your macOS/OS X Mail.app.

1. Open the *Mail.app*, open the *Mail* menu > *Preferences* > *GPG Mail*, and then enable the following functions. Hover the cursor over an option for more information.



2. Close the *Preferences* window.
3. *Quit Mail.app*.

4. Open the *Apple* menu > *System Preferences* > *GPGPreferences*, select the *Settings* tab, and then configure as follows.



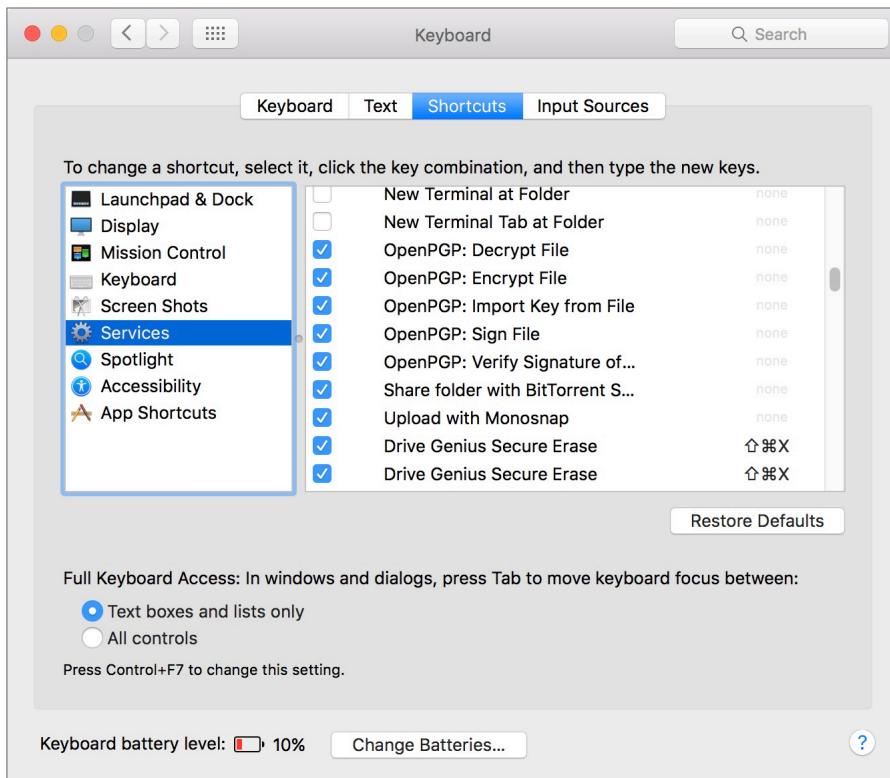
- *Default Key:* From the pop-up menu select your primary email account.
 - Enable *Password: Store in OS X Keychain*.
 - Enable *Password: Remember for 600 seconds*.
 - *Key server:* Unless your organization prefers using another server, stick with the default of *hkp://keys.gnupg.net*.
 - Enable *Updates: Automatically check for updates*.
5. *Quit System Preferences.*

Your GPG is now fully installed, configured, and ready for use!

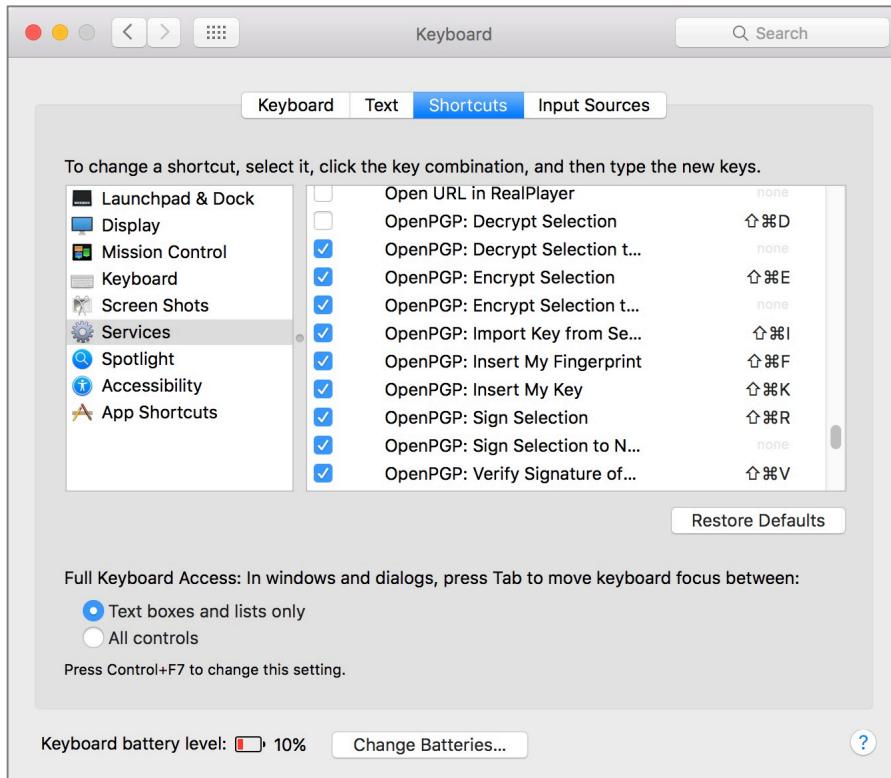
15.7.5 Assignment: Encrypt and Sign Files with GPGServices

GPGServices allows encryption, decryption, and signing of any type of file for cross-platform use. After installing GPG (see previous exercises), verify all GPGServices have been activated:

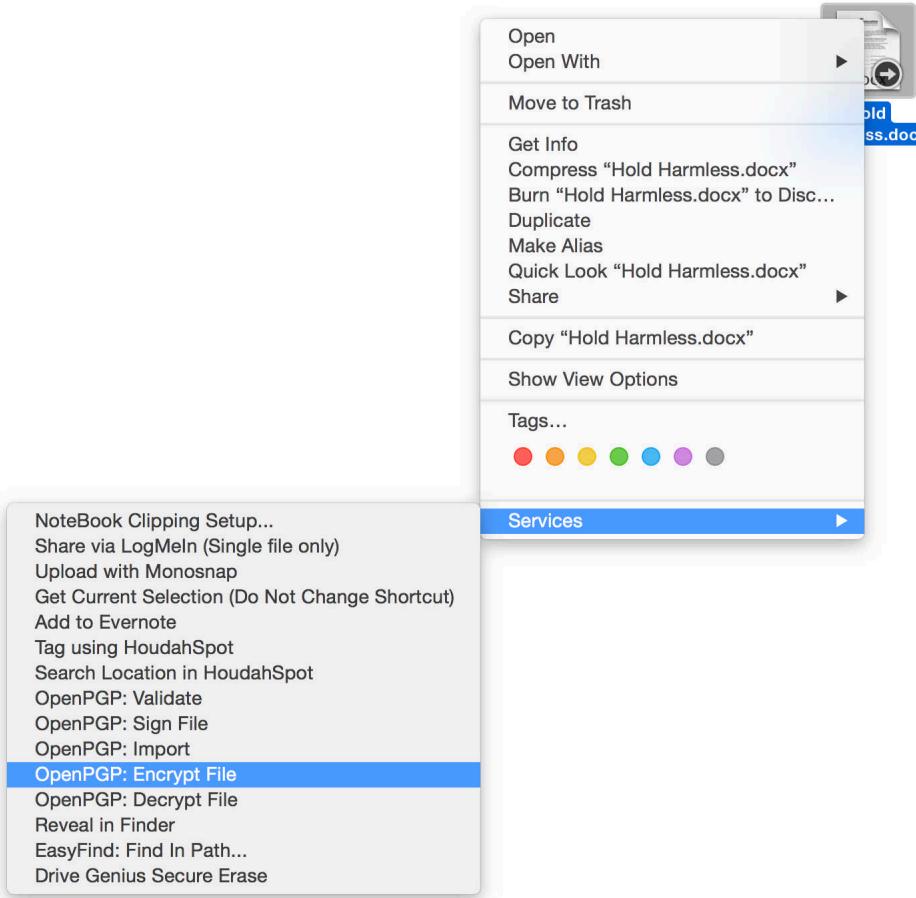
1. Open *System Preferences > Keyboard > Shortcuts tab > Services* in sidebar.
2. From under the *Files and Folders* group, verify that all *OpenPGP* modules are enabled.



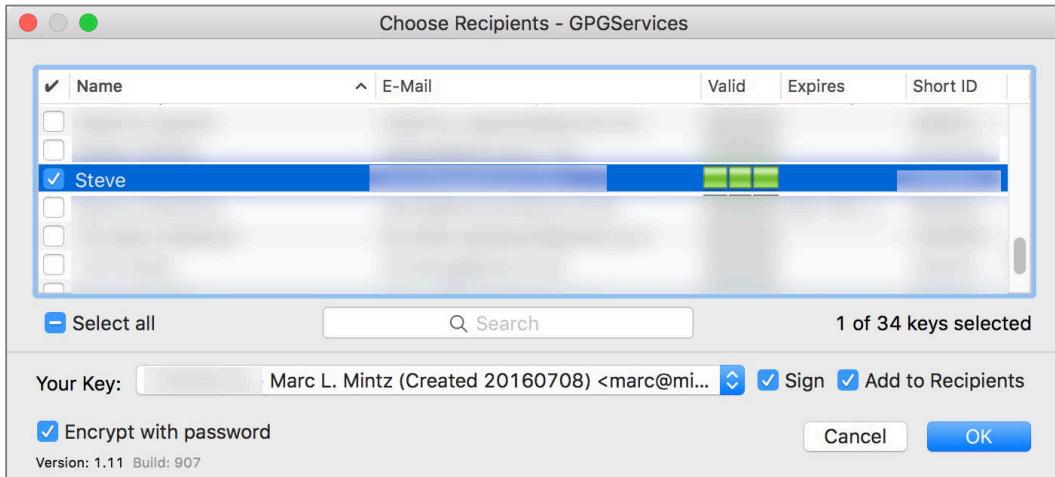
3. While still in the *System Preferences > Keyboard > Shortcuts tab > Services*, scroll down to the *Text* group, and then verify that all *OpenPGP* modules are enabled.



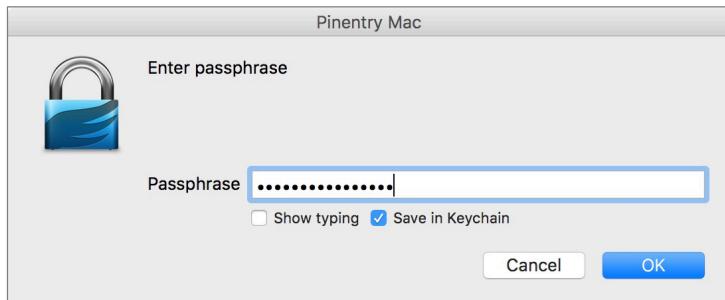
4. To sign or encrypt a file or folder, right-click on it. From the pop-up menu, select *Services > OpenPGP: Encrypt File*.



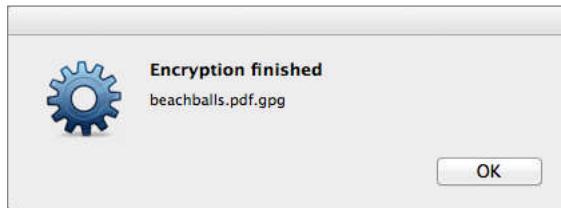
5. The *Choose Recipients – GPGServices* window appears. Configure as:



- Enable the checkbox for those you wish to allow to access this encrypted file or folder.
 - Select which *Secret Key* will be used (which of your emails).
 - Enable the *Sign* checkbox so the recipient can validate the file/folder came from you.
 - You can further enhance security by enabling *Encrypt with password*.
6. Select the OK button.
7. At the *Pinentry Mac* window, enter the desired password in the *Passphrase* field, and then select the OK button.



8. You will be prompted a second time to enter the passphrase, do so, and then select the *OK* button.
9. In a few seconds the *Encryption Finished* window appears. Select the *OK* button.



10. Your encrypted file will be found next to the original, with a *.gpg* file extension.

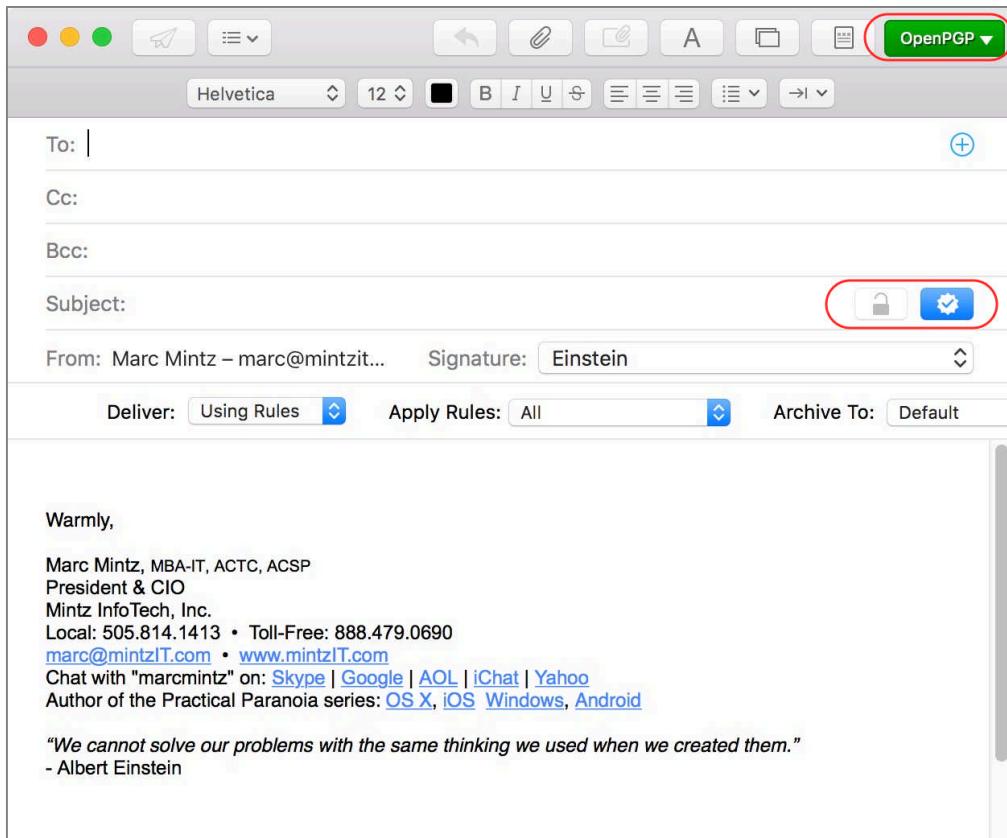
This encrypted file can now be attached to an email and securely sent to any recipient who also has GPG or PGP installed.

15.7.6 Assignment: Send a GPG-Encrypted and Signed Email

Once you have created your key and have the Public Key of the intended recipient from the previous assignments, you are ready to send your first encrypted and signed email.

1. Open your macOS *Mail.app*.

2. Create a new outgoing mail document. Notice that you have two new icons to the left of the *Subject* line.



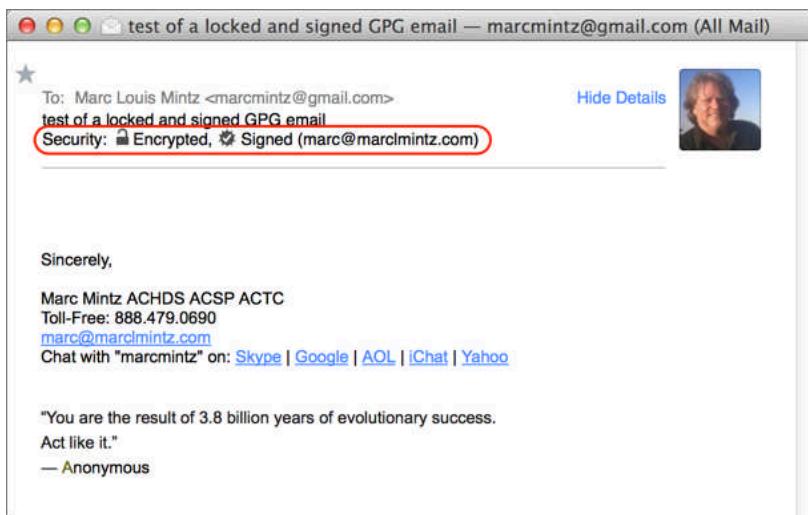
- *Lock* icon: Enables encryption for your document.
 - *Signed* (checkmark) icon: Enables signed emails. A signed email will notify the recipient if the message has been altered in any way between the sender and recipient.
3. In the *To:* field, enter the email address of someone with GPG enabled on their computer (feel free to use my address of marc@mintzit.com for your test). Once you have entered an email address that is registered with GPG (as you have done in the previous assignment), the *Lock* icon will turn black, allowing selection/enabling.
 4. Click the *Lock* icon to encrypt the message.

5. Select the *Send* button, and your email is on its way to the recipient, fully secure because only the designated recipient will be able to read the email.

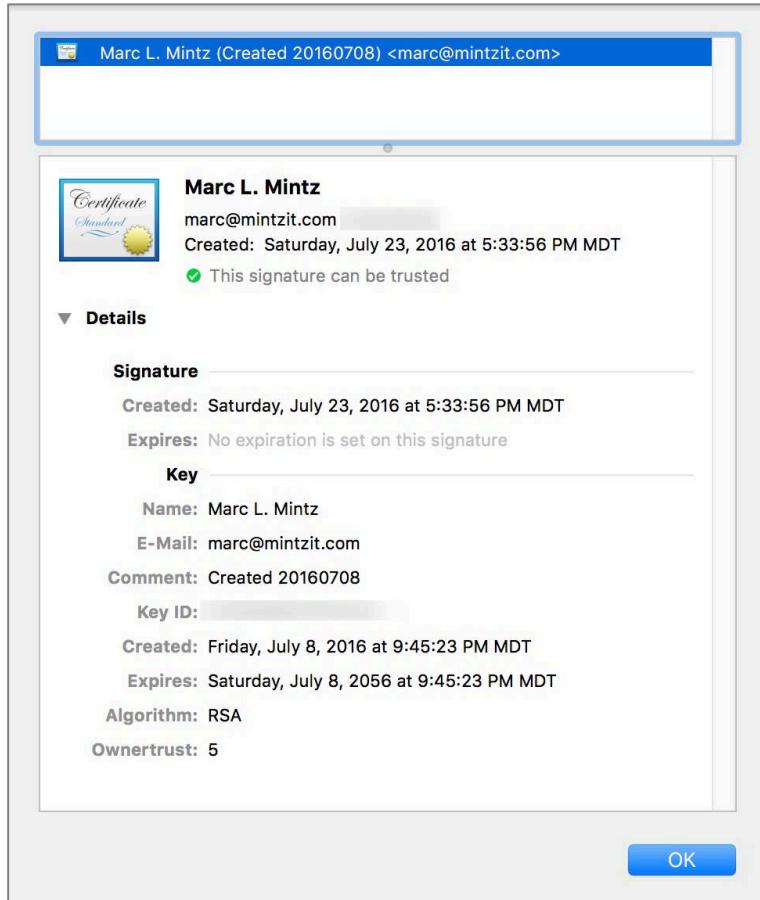
Wahoo! You have sent your first securely encrypted email.

15.7.7 Assignment: Receive a GPG-Encrypted and Signed Email

1. When the email arrives at the recipient, it automatically is decrypted (assuming the recipient also has followed the steps detailed in the *Get Your Friend's Public Key* assignment). The message will have an indicator if it is encrypted or signed.

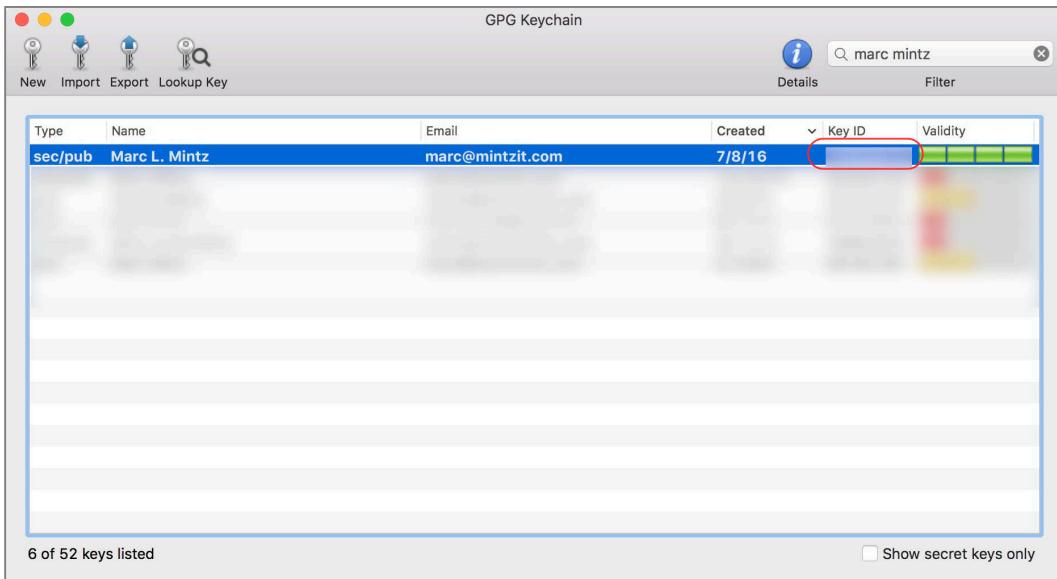


- Should the recipient have any doubts as to the authenticity of the email, click on the *Signed* icon. The certificate will display. Note the Short ID to the right of the sender's email address.



15 Vulnerability: Email

3. This Short ID can be verified. The recipient can open *GPG Keychain Access* to view the sender's Short ID.



15.8 End-To-End Secure Email With S/MIME

S/MIME¹² (Secure/Multipurpose Internet Mail Extensions) uses the same fundamental strategy of employing both Public and Private Keys to secure email as do PGP and GPG. Each person has a Private Key to decrypt a received email, and a Public Key that others may use to encrypt email to send out. An advantage of S/MIME over GPG is that S/MIME is built right into both the macOS/OS X and the iOS Mail.app. No need to install another application.

Unlike GPG, you will need to acquire an *email certificate* from a *Certificate Authority (CA)*. There are many Certificate Authorities available. Your Internet Provider or Web Host may be able to do this for you. Free certificates for personal use, which are valid for one year, are available. However, using these can become tedious, as you will need to repeat all the steps below every year. Purchasing a commercial certificate will set you back \$10 to \$100 per year, but you will only have to go through the process once.

Because your keys are stored with a CA, if that CA resides in a country that complies with USA National Security Letters, then it is possible for the US Government agencies to gain access to your private key, giving them full access to your email. Should you have concerns over the government having access to your communications, you should use either PGP/GPG, or S/MIME with a CA located in a country that does not comply with National Security Letters.

S/MIME offers three certificate classes:

- **Class 1:** This level of certificate is acquired without any background check or verification that the person requesting it has anything to do with the email address it will be assigned to. In fact, it is even possible to roll your own certificate! That said, it will verify that the email address in the *From* field is actually the address that sent the email, and do the job of encrypting email so that only the intended recipient can decrypt and read it.

¹² <http://en.wikipedia.org/wiki/S/MIME>

- **Class 2:** This level takes it a step further, validating that not only is the email address in the *From* field the one that actually sent the email, but that the name in the *From* field is tied to that email address.
- **Class 3:** This is the highest-level validation, with a background check performed to verify not only the name of the individual or company, but physical address as well. **This is the only class suitable for healthcare (HIPAA), financial, legal, and business use.**

15.8.1 Assignment: Acquire a Free Class 1 S/MIME Certificate

In this assignment you will sign-up for a free 1-year free S/MIME certificate for personal use from a leading Certificate Authority, Comodo. This can be converted into a long-term commercial certificate.

1. Open your web browser and surf to Comodo at <https://comodo.com>.
2. From the navigation bar, select the *Personal* tab > *Free Personal Email Certificate*.

The screenshot shows the Comodo website homepage. At the top, there's a navigation bar with links for North America, Search our website, About Us, Resources, Newsroom, Career, and Login. Below the navigation bar, there are tabs for PERSONAL, SSL CERTIFICATES, ENTERPRISE, PARTNERS, SUPPORT, and CONTACT US. The PERSONAL tab is currently selected. On the left, there's a section for 'Security Software for Windows' featuring two large icons for Comodo Internet Security (one yellow, one red). To the right of these icons is a list of security products: Free Internet Security, Comodo Antivirus, Comodo Antivirus Advanced, Comodo Firewall, and TrustConnect WiFi Security. On the far right, there's a section titled 'Email And Security Messaging' with a sub-section for 'Free Personal Email Certificate'. This sub-section has a red rectangular box around it, highlighting the text 'Free Personal Email Certificate' next to an icon of an envelope with an '@' symbol. Below this, there's an icon for 'Cloud Based Spam Filtering' and another for '5GB Free Cloud Storage'.

15 Vulnerability: Email

3. This takes you to the *Email Security & Messaging* page. Select the *Free Email Certificate > Free Download* button.

The screenshot shows the Comodo website's "Email Security & Messaging" section. At the top, there's a navigation bar with links for North America, Search our website, About Us, Resources, Newsroom, Career, and Login. Below the navigation is a horizontal menu with links for PERSONAL, SSL CERTIFICATES, ENTERPRISE, PARTNERS, SUPPORT, and CONTACT US. The main content area features a large heading "Email Security & Messaging" with the subtext "Prevent Spam, Phishing and Ensure Private Communications". Below this, there are two main download sections. The first section, "Free Email Certificate", includes a yellow icon with a lock and '@' symbol, the text "Free Email Certificate", and a description: "Email certificates allow you to encrypt and digitally sign messages before sending." It has a prominent orange "FREE DOWNLOAD" button with a right-pointing arrow. The second section, "Comodo Antispam Gateway", includes a blue icon with a shield and 'C' symbol, the text "Comodo Antispam Gateway", and a description: "Strengthen your pre-perimeter defenses using our cloud-based email filtering solution removing spam, malicious attachments & phishing emails." It also has an orange "FREE DOWNLOAD" button with a right-pointing arrow. At the bottom left of the main content area, there's a link "Learn More".

4. The *Application for Secure Email Certificate* page opens. Complete the form, specifying *2048 (High Grade)* for your *Key Size*, and then select the *Next* button.

Application for Secure Email Certificate

Your Details

First Name
Last Name
Email Address
Country United States

Private Key Options

Key Size (bits): 2048 (High Grade)

Note: Backup your private key! We do not get a copy of your private key at any time so, after completing this application procedure, we strongly advise you create a backup. Your certificate is useless without it. [More info](#)

Revocation Password
If you believe the security of your certificate has been compromised, it may be revoked. A revocation password is required to ensure that only you may revoke your certificate:

Revocation Password
Comodo Newsletter Opt in?

Subscriber Agreement
Please read this Subscriber Agreement before applying for, accepting, or using a digital certificate. If you do not agree to the terms of this Subscriber Agreement, do not apply for, accept, or use the digital certificate.

Email Certificate Subscriber Agreement

THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE AGREEMENT CAREFULLY BEFORE ACCEPTING THE TERMS AND CONDITIONS.

IMPORTANT - PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING A COMODO EMAIL CERTIFICATE. BY USING, APPLYING FOR, OR ACCEPTING A COMODO EMAIL CERTIFICATE OR BY ACCEPTING THIS AGREEMENT BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT, THAT YOU UNDERSTAND IT, THAT YOU ACCEPT THE TERMS AS PRESENTED, AND AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS SUBSCRIBER AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE A COMODO EMAIL CERTIFICATE AND CLICK "DECLINE" BELOW.

1. Application of Terms

I ACCEPT the terms of this Subscriber Agreement.

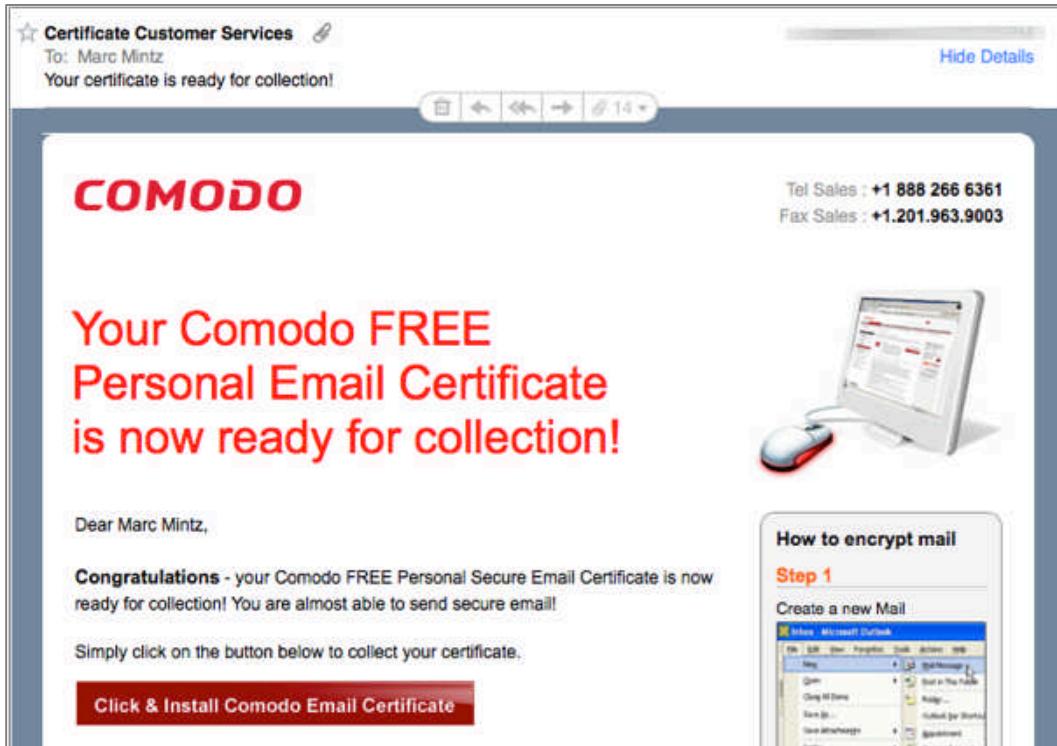
Next >

5. If all was completed correctly, you will see the *Application is Successful* page!

The screenshot shows a web page from COMODO titled "Application for Secure Email Certificate". The main message is "Application is successful!" followed by instructions: "Details on how to collect your free Secure Email Certificate will be sent to marcmintz@gmail.com." and "Congratulations on choosing Secure Email Certificates to keep your email confidential." To the right, there's a sidebar titled "Secure Email Certificates" with two steps: "Step 1: Provide details for your certificate" and "Step 2: Collect and install your certificate". At the bottom left is the copyright notice "© Copyright 2016. All rights reserved." and at the bottom right is the date "Saturday August 6, 2016".

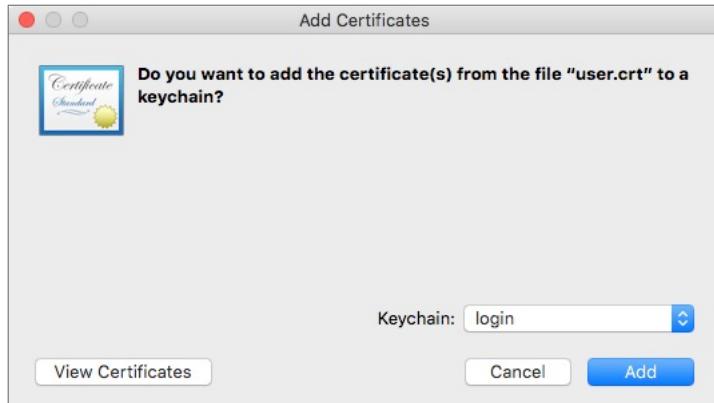
6. The certificate will be sent to the email address you specified.

7. Open your Mail.app to find the email, and then select the *Click & Install Comodo Email Certificate* button.



8. Although the button says *Click & Install Comodo Email Certificate*, all it really does is download the certificate. You will need to manually install the certificate.
9. Once downloaded, the certificate will be found in your *Downloads* folder, named something like *user.crt*. Navigate in the Finder to your *Downloads* folder to find this certificate file.
10. Double-click the *CollectCCC.p7s* certificate. An *Add Certificates* window will open asking if you want to add the certificate to your Keychain. From the

Keychain pop-up menu, select *Login*, and then select the *Add* button. This will add the certificate to your own default Keychain database,

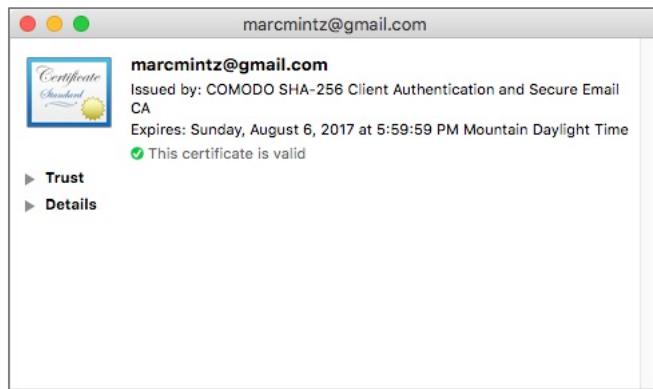


Validate Certificate Installation

- To quickly find the new certificate, in the Keychain Access utility, in the Search field, enter the email address for the new certificate, and then tap the *Return* or *Enter* key.

Name	Kind	Date Modified
marcmintz@gmail.com	certificate	--
com.apple.account.Google.accounts	application password	Aug 1, 2016, 10:18:14 AM
com.apple.account.Google.oauth-token	application password	Aug 1, 2016, 10:18:14 AM
com.apple.account.Google.oauth-expiry-date	application password	Aug 1, 2016, 10:18:14 AM
com.apple.account.Google.oauth-token-nosync	application password	Apr 22, 2016, 2:10:17 PM
com.apple.facebook.accounts	application password	Mar 5, 2016, 9:37:52 AM
com.apple.facebook.oauth-token	application password	Mar 5, 2016, 9:37:52 AM
com.apple.facebook.oauth-expiry-date	application password	Mar 5, 2016, 9:37:51 AM
com.apple.facebook.oauth-token-nosync	application password	Mar 5, 2016, 9:37:51 AM
m.facebook.com (marcmintz@gmail.com)	Web form password	Dec 29, 2015, 7:58:27 PM
@ www.facebook.com (marcmintz@gmail.com)	Web form password	Dec 29, 2015, 7:54:05 PM
@ www.facebook.com	Internet password	Sep 1, 2015, 2:14:01 PM
com.apple.account.Google.oauth-refresh-token	application password	Aug 23, 2015, 2:19:33 PM

- Double-click on the new certificate. This will open the certificate info window.



13. Quit the Keychain Access application.
14. Repeat steps 1-10 for each of your email addresses for which you need secure communications.

Wahoo! The hard part is over. You now are the proud owner (at least for a year) of email certificates for each of your email accounts. Next step is to migrate the certificate to your iOS device.

15.8.2 Assignment: Acquire a Class 3 S/MIME Certificate for Business Use

Getting a Class 3 certificate is significantly more involved than that of a Class 1. This is due to the need for identity verification, but also to the need for an infrastructure to help with managing potentially thousands of email addresses within an organization.

To set up a Class 3 certificate account with Comodo:

1. Using your web browser, visit *Comodo.com*

15 Vulnerability: Email

- From the Navigation bar, select *Enterprise > Secure Email Certificate*.

The screenshot shows the Comodo website's Enterprise section. The top navigation bar includes links for North America, Search our website, About Us, Resources, Newsroom, Career, and Login. Below the navigation is a horizontal menu with tabs: PERSONAL, SSL CERTIFICATES, ENTERPRISE (which is highlighted), PARTNERS, SUPPORT, and CONTACT US. The main content area displays several service cards:

- Enterprise Certificate Manager**: Manage PKI and Certificates. Get Organized With Your Own Certificate Manager!
- Comodo Device Manager**
- SecureBox**
- Web Application Firewall**
- Two Factor Authentication**: Security solutions that prevent cyber-attacks and maintain your company's reputation.
- PCI Compliance**: HackerGuardian helps you automate PCI compliance reporting. Fast and easy.
- Endpoint Protection**
- Endpoint Security Manager**
- TrustConnect WiFi Security**
- Comodo Cleaning Essentials**
- Comodo Rescue Disk**
- Comodo Antispam Gateway**
- Secure Email Certificate**

- In the *Secure Email Certificates* page, select the *Buy Now* button.

The screenshot shows the Comodo website's Secure Email Digital Certificate page. The top navigation bar and horizontal menu are identical to the previous screenshot. The main content features a large banner for the Secure Email Digital Certificate, which includes the following text and visual elements:

- Secure Email Digital Certificate**
- Keep your email communications private with Comodo SecureEmail Certificates.
- BUY NOW >** (An orange button with white text)
- Starting at \$12.00/year** (Text with a blue arrow pointing towards the button)
- A small image of an email client window showing a message being composed, with the text "Easily encrypt messages" above it.
- A detailed view of an email message in an inbox, showing the recipient's name and a snippet of the message content.

15 Vulnerability: Email

4. In the *Purchase Corporate Secure Email Digital Certificate* page, enter your desired *Term* and *Quantity*. And then select the *Next* button.

The screenshot shows the Comodo Enterprise SSL website. At the top, there's a banner for 'Fully validated, Enterprise SSL Certificates'. Below it, a navigation bar includes 'Products', 'Resellers', 'Comparisons', 'Corporate', 'Support', and 'Contacts'. A woman smiling at a laptop is shown in a large image. The main content area has a grey header 'Products' and a sub-header 'Purchase Corporate Secure Email Digital Certificate'. To the left, there's contact information and a video link. The central part features a table for pricing, and below it, a section for selecting 'Term' and 'Quantity'.

Per Certificate	1 Year	2 Year	3 Year
1 - 25	\$12.00	\$21.50	\$29.00
26 - 100	\$11.20	\$20.40	\$27.00
101 - 250	\$10.50	\$18.90	\$25.20
250 +	CALL	CALL	CALL

Below the table, there are radio buttons for 'Term' (selected), 'Quantity', and 'Total Price', with dropdown menus for each.

5. In the *Open an Enterprise S/MIME Enterprise PKI Manager (E-PKI) Account* window. Enter a domain name for your certificates, and then select the *Next* button.

The screenshot shows a web-based interface for opening an Enterprise S/MIME account. At the top, there's a red header bar with the Comodo logo and 'Enterprise SSL' text. To the right of the header are links for 'Can We Help?' (with two phone numbers), 'Certification Authorities' (WestTrust), 'Certification Authorities' (WestTrust), and an 'enterpriseolutions@comodo.com' email link. Below the header, a sidebar on the right lists steps for 'Signup': '1: Your E-PKI Details', '2: Your Corp Details', '3: Payment', and '4: Management'. The main content area has a title 'Enterprise PKI Manager (E-PKI)' with a user icon. It displays a message 'Open an Enterprise S/MIME Enterprise PKI Manager (E-PKI) Account'. Below this, a note says 'Welcome to the Enterprise S/MIME E-PKI signup pages. Please complete the following steps to apply to open an Enterprise S/MIME E-PKI Account.' A form field 'Email Domain Name (optional)' with placeholder 'e.g. @acme.com' and a text input box containing 'mintzit.com'. Below the form is a section titled 'Initial Prepayment Amount (USD)' with a note about prepayment amounts determining banding and discounts. A table shows the selection of 'E-PKI S/MIME 1 - 25 Certs' with a deposit amount of '\$12.00' and a 'View' button. At the bottom of the main content area is a 'Next >' button.

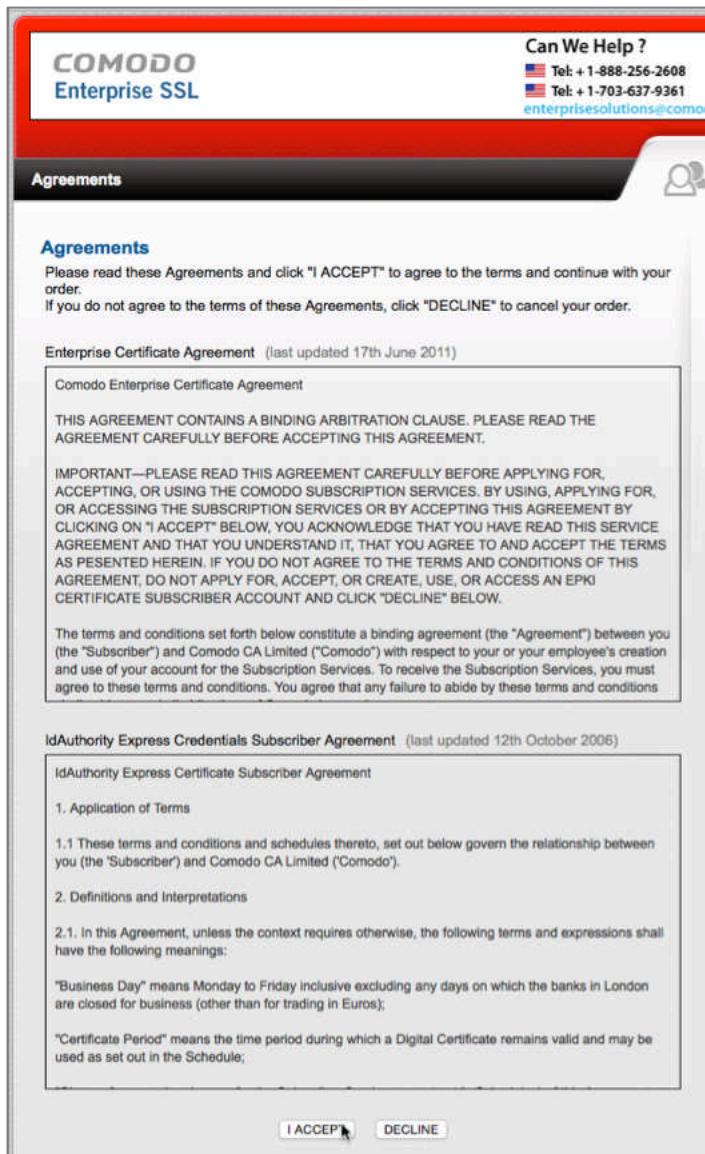
6. In the *Step 2: Your Corporate Details* page, enter all requested information, and then select the *Next* button.

The screenshot shows a web-based form titled "Step 2: Your Corporate Details". The form is divided into several sections:

- Company Details - These must be your Registered Address:** This section contains fields for Company Name, Dept, PO Box, Address 1, Address 2, Address 3, City / Town, State / Province / County, Zip / Postcode, Country (with a dropdown menu showing "United States"), Company Number, and DUNS Number.
- VAT Details:** A note states: "Please note that advertised prices are exclusive of Value Added Tax (VAT). VAT is only payable by EU companies." There is a field to "Enter VAT number, if applicable".
- Your Contact Details:** A note says: "If the following Admin Contact Details are incorrect, please amend with the correct details." It includes fields for Title, First Name, Last Name, Email Address, and Telephone Number. Below these are four radio buttons:
 - > Click if you would like to provide additional Admin Contact details
 - > Click if your Billing Contact is different to your Admin Contact
 - > Click if you would also like to provide an Organisational Contact
 - > Click if your Trading Address is different to the Address provided in the Company Details
- Choose your Admin Contact's Management Details:** This section includes fields for Username (min 6 characters), Password (min 8 characters with a "Rules" link), and Confirm Password (re-enter).

At the bottom are two buttons: "Cancel & Start Again" and "Next >".

7. At the *Agreement* page, select the *I ACCEPT* button.



8. In the *Secure Payment Page*, enter your credit card information, and then select the *Make Payment* button.

The screenshot shows a secure payment form titled "Secure Payment". At the top right, there's a "Can We Help?" section with contact information: Tel: +1-888-256-2608, Tel: +1-703-637-9361, and an email address enterprisesolutions@comodo.com. Below this is a user icon.

The main form area has two sections:

- Card Details:** Fields include "Card Number" (red border), "Card Code (3 or 4 digits)" (red border), "Expiry Date" (dropdown menus), and "Cardholder's Name" (Marc Mintz).
- Cardholder Address and Contact Details:** Fields include "Company Name" (Mintz InfoTech Inc.), "Address 1" (7000 Phoenix Ave NE), "City / Town" (Albuquerque), "State / Province / County" (NM), "Zip / Postcode" (87110), "Country" (United States dropdown), "Phone" (888.479.0690), and "Email" (marc@mintzit.com).

At the bottom are "Cancel & Start Again" and "Make Payment" buttons.

15 Vulnerability: Email

9. You will receive an email from Comodo informing you of receipt of your order, and stating that you will soon be receiving another email requesting documents to validate your identity.

Comodo Security Services
To: Marc Louis Mintz
ORDER ————— - CONFIRMATION

COMODO
Enterprise SSL

Can We Help ?
Tel: + 1-888-256-2608
Tel: + 1-703-637-9361
enterprisesolutions@comodo.com

Certification Authorities

Certification Authorities


Your order has been received!

Dear Marc Mintz,

Thank you for placing your order. Your Order Number is ————— Please quote this Order Number in all correspondence.

Please treat this confirmation as your official invoice number: —————

An E-PKI Account Manager will review your application and contact you shortly.

PLEASE NOTE: This order can only be completed once we have been able to fully validate your application details. Normally this process takes a few minutes but it may take up to two working days. Our validation staff will attempt to validate your organization information using third party information sources. If we require information from you to complete this process you will receive a request via email. If you have questions regarding the validation process please email docs-enquiries@comodogroup.com

10. Soon you will receive an email requesting the validation documents. Submit the requested documents and information.

COMODO Validation Team  

To: Marc Louis Mintz
Information Required Order _____

Thank you for your recent order.

We have begun validating your information so that we can issue your order. The following is the account information you submitted:

Company: Mintz InfoTech, Inc.
Domain Name: mintzit.com
Address 1: 7000 Phoenix Ave NE
Address 2: 310
Address 3:
City: Albuquerque
State: NM
Postal Code: 87110
Country: United States of America

Although we have begun processing your order, we have been unable to complete validation for the following reasons:

In order to verify the existence of your organization we must be able to find it listed either in an official government database or a third party database such as Dunn & Bradstreet (www.dnb.com)

If the address on your account does not match the database record we may use one of the following documents for verification of the address. Please provide us with one of the following documents so we may complete your validation:

A. Articles of Incorporation (with address)
B. Government Issued Business License (with address)
C. Copy of a recent company bank statement (you may blacken out the Account Number)
D. Copy of a recent company phone bill
E. Copy of a recent major utility bill of the company (i.e. power bill, water bill, etc.) or current lease agreement for the company

*Note: Recent=dated within the last 6 months

Please fax any validation documentation to 1-866-831-5837(U.S. and Canada) or +1 801-303-9291 (Worldwide). When faxing documents, please include the attached coversheet. You may also respond by going to <https://support.comodo.com>, registering, and opening a ticket and attaching the documents. Please be sure to include your name, order number, domain name, e-mail address, and phone number in either your fax or support ticket.

If you need assistance, or wish to speak to a Customer Service Representative, please contact us toll-free at anytime at 1-888-266-6361 (U.S.) and +1-206-203-6361 (Worldwide).

Regards,
COMODO Validation Team

11. You will receive an email informing you that your account has been created, with a link to their *Getting Started Guide*. Although the steps outlined in this book will take you through the process, it is not a bad idea to download and read the Guide as well. Download the *Getting Started Guide*.

12. Register for Comodo technical support by clicking the link provided in the email, and then follow the on-screen instructions. This will save you significant time and headache in the event that you ever need technical support from Comodo.

15.8.3 Assignment: Purchase a Class 3 S/MIME Certificate for Business Use

Once you have set up your Class 3 business account with Comodo, you are able to order S/MIME certificates for you and your staff at any time. In this exercise, you will purchase your first certificate.

1. From your web browser, go to the Comodo home page at <https://comodo.com>.
2. Select the *Login* link, and then login. This opens the *SSL CA Providers Comodo Account Management* page.

3. In the *Comodo Certificate Authority* area, enter your *Username* and *Password* used to start your account with Comodo, and then select the *Log on* button.

4. The *Account Options: Management* window opens. Select the *E-PKI Manager* link.

5. This will take you to the *E-PKI Manager: Account Options: Management* page. With Comodo, you pay for certificates not directly, but by pulling from

monies on deposit with Comodo. If there are inadequate funds on deposit, you will need to deposit money now. To do so, select the *Deposit additional funds* link.

The screenshot shows the Comodo E-PKI Manager interface. At the top, there's a red header bar with the Comodo logo and "Enterprise SSL". On the right side of the header, there's a "Can We Help?" section with two telephone numbers and an email address: Tel: +1-888-256-2608, Tel: +1-703-637-9361, and enterprisesolutions@comodo.com. Below the header, the main title "E-PKI Manager: Account Options: Management" is displayed. A user icon is visible on the right. The main content area has a dark grey header bar with the title. The main body text says: "Welcome to E-PKI Manager. Use the E-PKI Manager to securely manage your account and your digital certificates." Below this, there are two sections: "Account Actions:" and "Using your E-PKI Manager:". Under "Account Actions:", there are two items: "Deposit additional funds" (with a bank deposit icon) and "Buy Prices" (with a price tag icon). Under "Using your E-PKI Manager:", there is one item: "E-PKI Manager pages" (with a computer monitor icon).

6. In the *Deposit Funds: Account Options: Management* page, enter at least the amount needed to purchase your S/MIME certificates. Rates per certificate as of this writing are.

Per Certificate	1 Year	2 Year	3 Year
1 - 25	\$12.00	\$21.50	\$29.00
26 - 100	\$11.20	\$20.40	\$27.00
101 - 250	\$10.50	\$18.90	\$25.20
250 +	CALL	CALL	CALL

15 Vulnerability: Email

The screenshot shows a web application interface for Comodo Enterprise SSL. At the top, there's a red header bar with the Comodo logo and "Enterprise SSL". On the right side of the header are links for "Can We Help?", "Certification Authorities", "Certification Authorities", and "Logout". Below the header, a black navigation bar displays "Deposit Funds: Account Options: Management". To the right of this bar, a welcome message says "Welcome: Marc Mintz Mintz InfoTech, Inc." with a user icon. The main content area contains a message "Your Current Credit is: \$0.00" in a grey box. Below it, a form asks "How much would you like to deposit (US Dollar)?", with a text input field and "Cancel" and "Next >" buttons.

7. In the *Secure Payment* page enter your credit card information, and then select the *Make Payment* button.

The screenshot shows a secure payment interface. At the top left is the Comodo Enterprise SSL logo. On the right, there's contact information: "Can We Help?", Tel: +1-888-256-2608, Tel: +1-703-637-9361, and an email address enterprisesolutions@com. Below this is a "Secure Payment" header. The main content area is titled "Secure Payment Page". It displays two sets of form fields:

Card Details

Card Number:	[Redacted]
Card Code (3 or 4 digits):	[Redacted]
Expiry Date:	[Redacted] / [Redacted]
Cardholder's Name:	Marc Mintz

Cardholder Address and Contact Details

Company Name:	Mintz InfoTech, Inc.
Address 1:	7000 Phoenix Ave NE
City / Town:	Albuquerque
State / Province / County:	NM
Zip / Postcode:	87110
Country	United States
Phone:	888.479.0690
Email:	marc@mintzit.com

At the bottom are two buttons: "Cancel & Start Again" and "Make Payment".

8. Return to the *Account Options: Management* page, and then select the *E-PKI Manager* link.

Can We Help ?

Logout

Certification Authority

Certification Authority

enterprisesolutions@comodo.com

Welcome:
Marc Mintz
Mintz InfoTech, Inc.

My Account Summary:

Last Login Time
21-NOV-2014 04:33:40 (UTC)

Status
Active

Verification Level
Class 3

My Account Areas:

E-PKI Manager Place orders through your E-PKI Manager

IdAuthority Add / Update details of your website(s) in the IdAuthority

9. In the *E-PKI Manager: Account Options: Management* page, select the *User Management* link.

Can We Help ?

Logout

E-PKI Manager pages

E-PKI Manager: Account Options: Management

Welcome to E-PKI Manager. Use the E-PKI Manager to securely manage your account and your digital certificates.

Account Actions:

Deposit additional funds

Buy Prices

Management Facilities:

User Management

Reporting Facilities:

Report on Your Orders

10. In the *User Management: Account Options: Management* page, select the *New User* button.

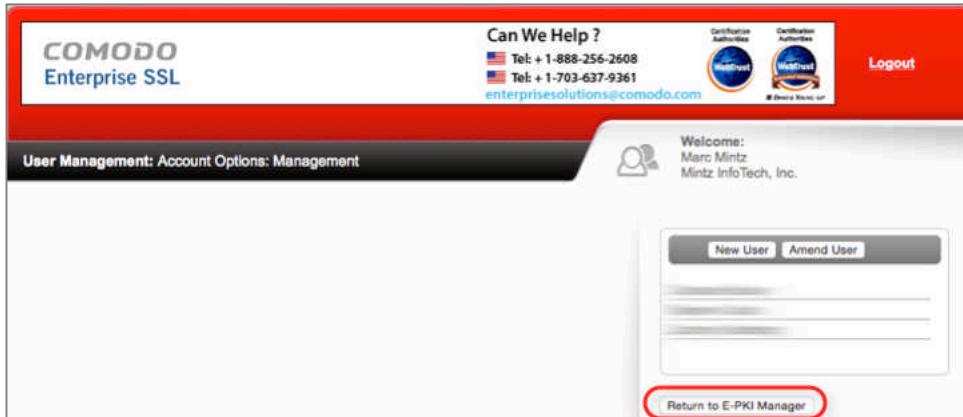
The screenshot shows a web-based user management interface for Comodo Enterprise SSL. At the top left is the Comodo logo and "Enterprise SSL" text. To the right is a "Can We Help?" section with two telephone numbers: "Tel: +1-888-256-2608" and "Tel: +1-703-637-9361". Below this are links for "Certificate Authority" and "Comodo Approved". On the far right are "Logout" and "SSL Site Seal" buttons. The main header reads "User Management: Account Options: Management". To the right of the header is a welcome message: "Welcome: Marc Mintz Mintz InfoTech, Inc.". Below the header is a form area with "New User" and "Amend User" buttons. The form fields are currently empty. At the bottom right of the form area is a "Return to E-PKI Manager" link.

11. In the *New User* window, enter all information for your new user, and then select the *Save Changes* button.

User Details	
Title	<input type="text"/>
First Name	<input type="text"/>
Surname	<input type="text"/>
Email Address	<input type="text"/>
Telephone No.	<input type="text"/>
Fax No.	<input type="text"/>
Is Active?	<input checked="" type="checkbox"/>
Login Name	<input type="text"/>
Password	<input type="password"/>
Password Confirmation	<input type="password"/>
Is Api User? Enabling this will disable the users Order Management Link.	<input type="checkbox"/>
User Address	
Department	<input type="text"/>
PO Box	<input type="text"/>
Street Address 1	7000 Phoenix Ave NE
Street Address 2	310
Street Address 3	<input type="text"/>
City	Albuquerque
State / Province / County	NM
Postal / Zip Code	87110
Country	<input type="text"/> United States <input type="button" value="▼"/>
<input type="button" value="Cancel"/> <input type="button" value="Save Changes"/>	

12. Repeat steps 7-10 to enable each user/email account to have an S/MIME certificate.

13. When all certificates have been requested, return to the *User Management: Account Options: Management* window, and then select the *Return to E-PKI Manager* button.



14. In the E-PKI Manager: Account Options: Management page, scroll to the bottom, and then select the *Corporate Secure Email Certificate Buy* button.

The screenshot shows the E-PKI Manager interface. At the top, it says "E-PKI Manager: Account Options: Management". Below that is a welcome message: "Welcome to E-PKI Manager. Use the E-PKI Manager to securely manage your account and your digital certificates." There are several sections:

- Account Actions:**
 - Deposit additional funds** (with a bank deposit icon)
 - Buy Prices** (with a price tag icon)
- Using your E-PKI Manager:**
 - E-PKI Manager pages** (with a computer monitor icon)
- Management Facilities:**
 - User Management** (with a user icon)
- Reporting Facilities:**
 - Report on Your Orders** (with a checkmark and report icon)
- Customer Order Options:**

Apply for a new product through your E-PKI Manager:

Product	
Corporate Secure Email Certificate	BUY
Personal Authentication Certificate	BUY

15 Vulnerability: Email

15. In the *Corporate Secure Email Certificate: E-PKI Manager: Management* page, complete the information for the user/email address you wish to assign an S/MIME certificate, and then select the *Submit* button.

The screenshot shows the 'Corporate Secure Email Certificate: E-PKI Manager: Management' page. At the top, there's a red header bar with the 'COMODO Enterprise SSL' logo, contact information ('Can We Help? Tel: +1-888-256-2608, Tel: +1-703-637-9361'), and links for 'Logout', 'Certification Authorities', and 'Certification Requests'. Below the header, a 'Welcome' message for 'Marc Mintz' from 'Mintz InfoTech, Inc.' is displayed. A sidebar on the right shows a placeholder for 'Your Current Credit is: [redacted]'. The main form area is titled 'User Details' and contains fields for 'Email Address' (example: 'username@mintzit.com'), 'First Name' (Marc), 'Last Name' (Mintz), and a checkbox for confirming employee status. There's also an advanced security section with dropdowns for 'Cryptographic Service Provider' (Microsoft Enhanced Cryptographic Provider v1.0) and checkboxes for 'Is Private Key "User-Protected"' (unchecked) and 'Is Private Key "Exportable"' (checked). A 'Certificate validity period' section includes a dropdown for selecting 'Validity Period' (1 year, 2 years, 3 years) and a note that the total cost is \$12.00. At the bottom, there are 'Cancel' and 'Submit' buttons.

Can We Help ?
Tel: +1-888-256-2608
Tel: +1-703-637-9361
enterprisesolutions@comodo.com

Welcome:
Marc Mintz
Mintz InfoTech, Inc.

Your Current Credit is: [redacted]

User Details

1. Email Address
Example: username@[redacted]
marc@[redacted] mintzit.com

You may only apply for Corporate Secure Email Certificates containing domain names for which your right of use has been validated.
If your required domain name does not appear in the above list, you may submit it for validation by clicking [here](#) to register an IdAuthority Website.

2. First Name
Marc

3. Last Name
Mintz

I confirm that the above individual is an employee / authorized representative of Mintz InfoTech, Inc. and is permitted to use the above email address for email communication.

Advanced Security Options
(Only applicable if the User will obtain their Certificate using Internet Explorer)

4. Cryptographic Service Provider
Microsoft Enhanced Cryptographic Provider v1.0

5. Is Private Key "User-Protected"?

6. Is Private Key "Exportable"?

Certificate validity period

7. Select the validity period for your Certificate:
1 year
2 years
3 years

Total Cost: \$12.00

Cancel Submit

16. At the *Order Confirmation: E-PKI Manager: Management* page, print your receipt, and then select the *Management Area...* button.

Product	Value
Corporate Secure Email Certificate for marc@mintzit.com	\$12.00
Total Value \$12.00	

Your Account has been debited by \$12.00.
A collection email will shortly be sent to marc@mintzit.com.
A confirmation email will shortly be sent to marc@mintzit.com.
Comodo Contact Details:
Support Telephone: +1.888.266.6361 / +1.703.581.6361
Support Website: <http://support.comodo.com>
Validation Docs Fax: US and Canada +1.866.831.5837 / Worldwide +1.801.303.9291

We now operate a registration-based system for support.
Please submit your ticket at the [support website](#).

Comodo Group, Inc. - US Office
1255 Broad Street
Clifton, NJ 07013-3398
United States

Comodo CA Limited - European Office
26 Office Village,
Exchange Quay, Trafford Road,
Salford, Manchester M5 3EQ,
United Kingdom

Comodo offers essential infrastructure to enable e-merchants, and other Internet-connected companies, software providers, and individual consumers to interact and conduct business via the Internet safely and securely. Our PKI solutions, including SSL Certificates, EV SSL Certificates, Code Signing Certificates as well as Secure E-Mail Certificates, increase consumer trust in transacting business online, secure information through strong SSL encryption, and satisfy many industry best practices or security compliance requirements. You may now go to the Management Area for further options. Or you may log into your account at any time to use the Management Area.

[Management Area...](#)

17. Repeat steps 13-15 for each user/email account to be assigned an S/MIME certificate.

15.8.4 Assignment: Download and Install a Business S/MIME Certificate

Once you have completed the steps above to provide a user/email account, that email address will receive notification of S/MIME certificate availability.

15 Vulnerability: Email

1. At the user's computer, check email for a message from Comodo, select and copy the *Your Certificate Password*, and then select the *Begin Corporate Secure Email Certificate Application* button.

Comodo Security Services

To: Marc Louis Mintz

Collecting your Corporate Secure Email Certificate

CS

Dear Marc Mintz,

Your Corporate Secure Email Certificate has now been issued and is ready to be collected.

Please click the button below to begin collection.

Begin Corporate Secure Email Certificate Collection

If the above button does not work, please navigate to <https://secure.comodo.com/products/CorporateSecureEmail>.
Your Certificate Password is:

This email message was sent on behalf of your System Administrator. Should you have any questions regarding your Corporate Secure Email Certificate application, please contact your System Administrator.

Kind Regards,

Comodo Security Services
noreply_support@comodo.com

2. In the *Corporate Secure Email Certificate Center*:

- Enter the **exact same email address** as used during the certificate creation.
- Paste in the *Certificate Password* that was included in the Comodo email sent to the email address.
- Enable the *I Accept* checkbox.
- Select the *Submit & Continue* button.

Corporate Secure Email Certificate Center

User Details:
Please enter the following details:

Email Address

Certificate
Password

Subscriber Agreement
Please read this Subscriber Agreement before applying for your certificate.
If you do not agree to the terms of this Subscriber Agreement, do not click the "I ACCEPT" tickbox.

Email Certificate Subscriber Agreement

THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE AGREEMENT CAREFULLY BEFORE ACCEPTING THE TERMS AND CONDITIONS.

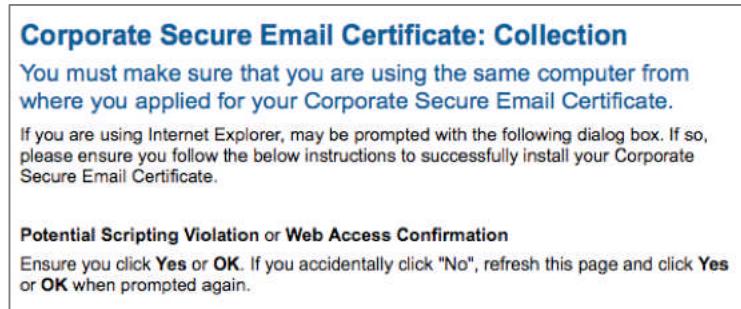
IMPORTANT - PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING A COMODO EMAIL CERTIFICATE. BY USING, APPLYING FOR, OR ACCEPTING A COMODO EMAIL CERTIFICATE OR BY ACCEPTING THIS AGREEMENT BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT, THAT YOU UNDERSTAND IT, THAT YOU ACCEPT THE TERMS AS PRESENTED, AND AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS SUBSCRIBER AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE A COMODO EMAIL CERTIFICATE AND CLICK "DECLINE" BELOW.

1. Application of Terms

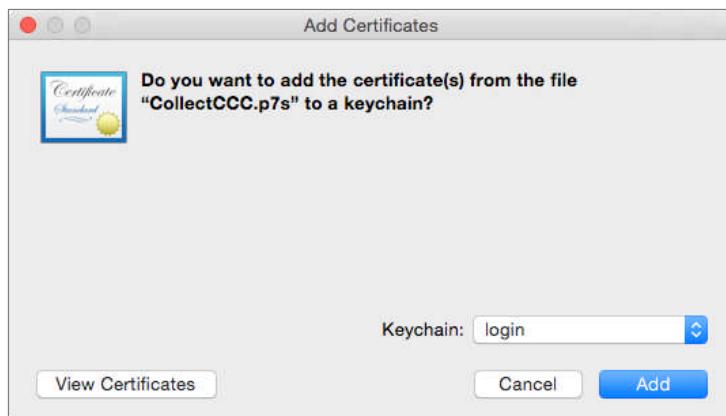
I ACCEPT the terms of this Subscriber Agreement.

Submit & Continue

3. The *Corporate Secure Email Certificate: Collection* page will open, your certificate will be generated and begin to download.



4. When the certificate has been generated, it will start downloading. When downloaded, you will find it in your *Downloads* folder named something like *CollectCCC.p7s*.
5. Open your *Downloads* folder and locate the *CollectCCC.p7s* file.
6. To install your S/MIME certificate into the *Keychain Access.app*, double-click on the *CollectCCC.p7s* file.
7. The *Add Certificates* window opens. Select *Keychain: login*, and then select the *Add* button.



8. *Quit Keychain Access.*
9. *Quit the Mail.app.*

10. Open the *Mail.app*. This forces the Mail application to search for new certificates.
11. If you use multiple computers, place a copy of your *CollectCCC.p7s* file on each of your computers, and repeat steps 6-10.

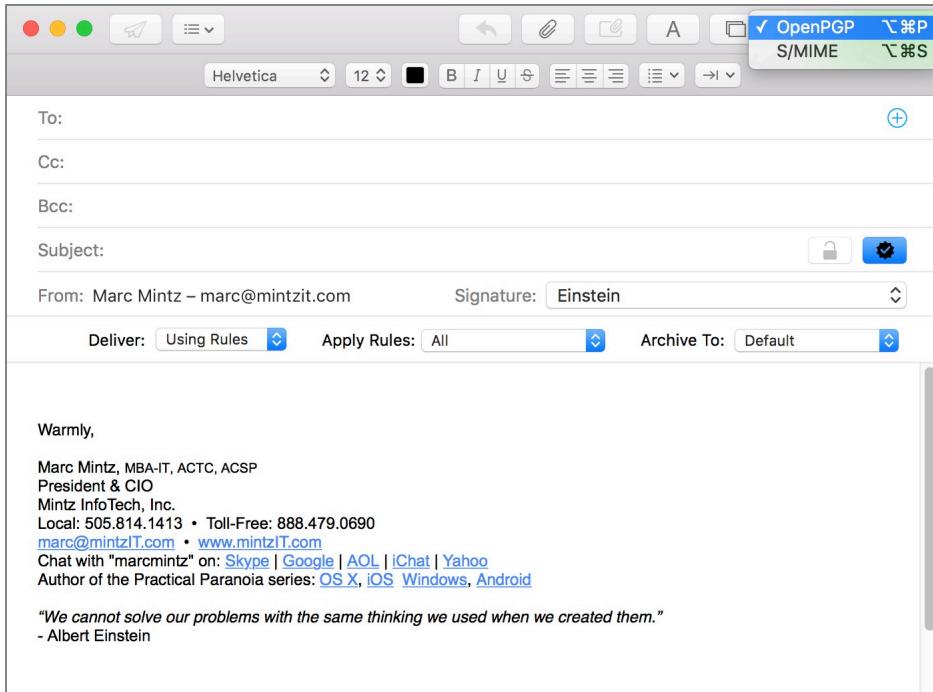
Your S/MIME certificate, which includes both your *Public Key* (used by others to encrypt email to you) and *Private Key* (used by you to decrypt email received by you) is now installed.

15.8.5 Assignment: Exchange Public Keys with Others

Before you are able to send or receive encrypted email with others, you need to exchange Public Keys with each other. This is as simple as sending a signed email to each other. To start, you will send a signed email to a friend. This will give this recipient your Public Key, as well as instructions for the recipient to set up S/MIME on their own system.

1. From a computer that now has your newly acquired email certificates, Open the *Mail.app*. This process forces *Mail.app* to look for new certificates.
2. Select the *File* menu > *New Message*.
3. From the *From:* pop-up menu, select the email account with the new certificates. (If you have only one email account, the *From* field typically does not appear.)
4. At the bottom right of the header area, note the two new icons—an encryption lock and signed check. If you have performed the earlier GPG assignments, these are the same and are shared between the two systems. The lock becomes available when you have the Public Key of the recipient, allowing for encryption. The check is available for anyone once you have your certificate. It will verify that the sender (you) are who you say you are.
5. If you have performed the earlier GPG assignments, the drop-down menu at the top right corner allows you to select either GPG or S/MIME as your

encryption protocol. If you have not performed the earlier GPG assignments, this menu is absent.



6. Address your email to an associate with whom you would like to be able to exchange encrypted email. Feel free to address the email to me at marc@mintzit.com.
7. If you have installed both PGP and S/MIME, ensure the *S/MIME* is the selected protocol, and that the *S/MIME signed check* is enabled (it should be by default.) This will ensure your Public Key is sent to your designated recipient.
8. In the Subject line, be clear about the intent of the email by noting something like: *S/MIME Public Key Attached*.
9. In the body area you may want to include instructions for how to acquire an email certificate—or better yet—point to this book at its website <http://thepracticalparanoid.com>.

10. When the recipient receives and opens the email, that recipient now has your Public Key and can determine that the email truly did come from you due to your signing the email with your certificate.

Marc Louis Mintz

To: Marc Louis Mintz

S/MIME Public Key Attached

Security:  Signed (Marc Mintz)



Hello;

With everyone from my ISP to the NSA reading our email, I'd like to have a bit more privacy.

Attached to this email is my S/MIME Public Key. By opening this email your computer has already copied and stored it securely, and is now ready to exchange encrypted and signed email with me.

To learn how to fully enable email encryption, get this awesome book by Marc Mintz, "Practical Paranoia." <http://thepracticalparanoid.com>.

Warmly,

Marc Mintz, MBA-IT, ACTC, ACSP
Chief Information Officer
Mintz InfoTech, Inc.
Local: 505.814.1413 • Toll-Free: 888.479.0690
marc@mintzIT.com • www.mintzIT.com
Chat with "marcmintz" on: [Skype](#) | [Google](#) | [AOL](#) | [ICQ](#) | [Yahoo](#)

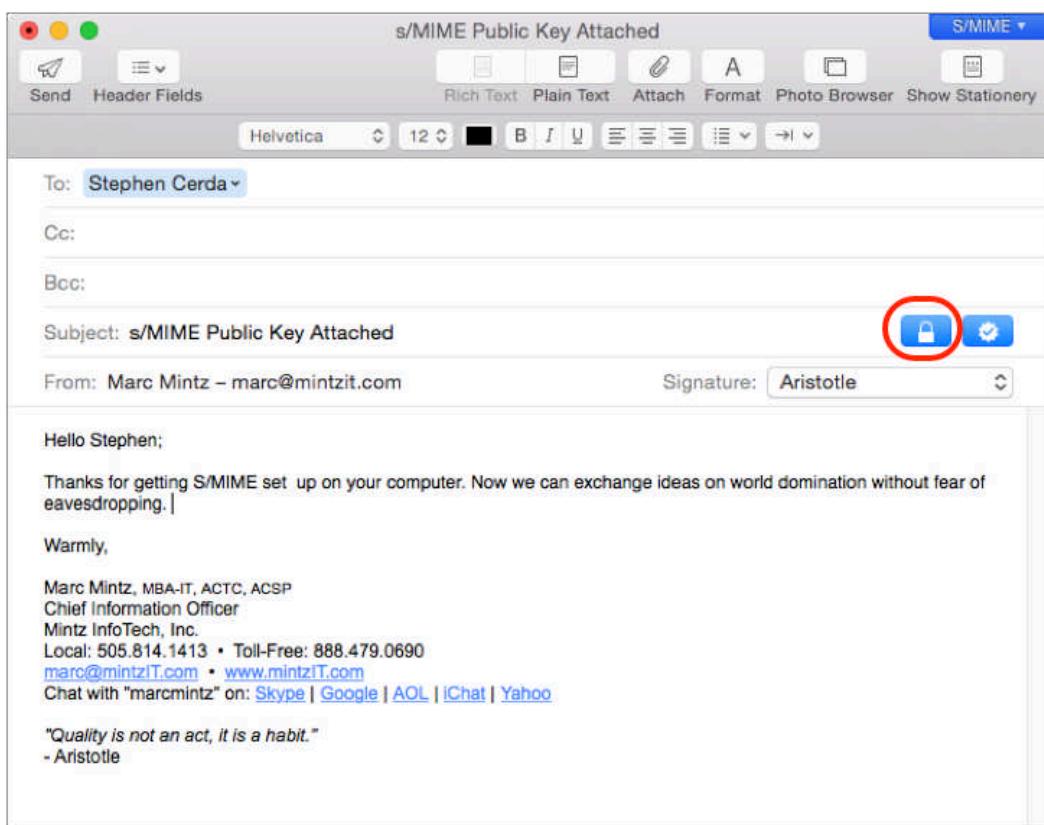
"Quality is not an act, it is a habit."
- Aristotle

11. The recipient then needs to repeat the steps in this and the previous assignments to acquire an email certificate, and then send a signed email to you. Once this is done, the two of you may exchange encrypted email.

15.8.6 Assignment: Send S/MIME Encrypted Email

To exchange encrypted email using S/MIME, the previous assignments must be completed by yourself and at least one other person with whom you wish to have secure communication. Once done, each has an email certificate, a private key, and a public key that is embedded in the other's computer.

1. Open your *Mail.app*.
2. Create a new message, addressed to someone with whom you share public keys.
3. If you have also installed GPG, set the *GPG-S/MIME* menu in the top right corner of the message to *S/MIME*.
4. Enable the *encrypted* lock icon in the bottom right area of the message header.



5. Send the message. When received by the recipient, the message is instantly and automatically decrypted, and the recipient gets a notice that the message is encrypted as well as signed.

Marc Louis Mintz

To: Marc Louis Mintz

Our first encrypted email

Security:  Encrypted



Warmly,

Marc Mintz, MBA-IT, ACTC, ACSP
Chief Information Officer
Mintz InfoTech, Inc.
Local: 505.814.1413 • Toll-Free: 888.479.0690
marc@mintzIT.com • www.mintzIT.com
Chat with "marcmintz" on: [Skype](#) | [Google](#) | [AOL](#) | [iChat](#) | [Yahoo](#)

"Quality is not an act, it is a habit."
- Aristotle

Congratulations! You are now able to send and receive securely encrypted email using the S/MIME protocol.

15.9 Closing Comments on Encryption and the NSA

Using PGP, GPG, S/MIME, or secure email hosts will give 100% protection against your communications being intercepted or eavesdropped by pranksters, criminals, master criminals, and virtually all government personnel (my apology for being redundant.) The bad news is that the NSA may have the ability to bypass virtually any security system should the NSA take a strong enough interest. The question then becomes: *Am I someone of such strong interest to the NSA that they will focus their full legal (and illegal) powers upon me?* If so, you may want to consider a change of career or lifestyle.

15.10 Review Questions

1. The attempt to acquire your sensitive information by appearing as a trustworthy source in electronic communication is called _____.
_____.
2. In the Mail.app, to reveal the actual URL in a link, just do this _____.
_____.
3. TLS stands for _____.
_____.
4. Which encryption protocol(s) may be used with an email client?
_____.
5. Which encryption protocol(s) may be used with a web browser accessing email?
_____.
6. TLS, SSL, and HTTPS encrypt email between _____ and _____.
_____ and _____.
_____.
7. S/MIME stands for _____.
_____.
8. In order to use S/MIME, the user must acquire an S/MIME certificate from a Certificate Authority. (True or False)
_____.
9. An S/MIME certificate that is acquired without any background check or verification that the person requesting it has anything to do with the email address is a Class _____.
Class _____.
_____.
10. An S/MIME certificate that validates that the email address in the from field is the address that actually sent the email, and that the person's name in the from field is tied to that email address is a Class _____.
Class _____.
_____.
11. An S/MIME certificate that is validated with a background check on the individual or company, as well as a physical address is a Class _____.
Class _____.
_____.
12. macOS Mail.app has separate settings for SSL and TLS. (True or False)
_____.
13. Email encrypted with either PGP or GPG can be decrypted with either. (True or False)
_____.

16 Apple ID and iCloud

Even in the common affairs of life, in love, friendship, and marriage, how little security we have when we trust our happiness in the hands of others!

—William Hazlitt¹, English writer and philosopher

¹ https://en.wikipedia.org/wiki/William_Hazlitt

16.1 Apple ID and iCloud

In 2012 a well-known journalist had his Apple ID hacked, allowing the hacker full access to the victim's Apple ID, and through that, his iCloud account, including calendar, contacts, and email. This was accomplished not by traditional black hat hacking, but with a bit of social engineering. All the hacker needed was to discover the victim's birthdate and email address associated with his Apple ID. With a quick email to Apple saying something like, *I've forgotten my Apple ID password and would like to reset it. Here is my birthdate and my email address*, the hacker was able to reset the Apple ID password. With this, he could access the victim's iCloud website as if he were the victim himself.

Over the past 6 months I have had 3 clients whose iTunes accounts have been compromised in a similar fashion, one to the tune of \$1,400 in music purchases.

As of March 21, 2013, Apple has implemented an optional Two-Step Verification (also referred to as a 2-Factor Authentication) process to harden your Apple ID security. Adding this security layer makes it extremely difficult for anyone to hijack your Apple ID and make fraudulent purchases. I consider this a mandatory step for all iCloud users.

Remember that every password can be broken. Your defense is to make it so difficult and time consuming to break that the hacker moves on to an easier target. The vast majority of security questions can be accurately guessed or broken through social engineering (*What is your birthday? In what city did your parents marry? What is the name of your first pet?* etc.) Both of these types of security are based on what you know. And if there is something that you know, someone else can know it as well. Unfortunately, even those you love and trust may occasionally use this information against you.

Apple has implemented Two-Step Verification for Apple ID so that whenever you sign in to your Apple ID on the web to manage your account, purchase something from iTunes, App Store, or iBooks Store from a new (unknown) device, or attempt to get Apple ID-related support from Apple, a code is sent to your previously verified i-device. You are prompted to provide this code before the purchase or support can be made.

In the event that your iOS device has been stolen or lost, you can log in to <https://appleid.apple.com> to remove that device from the verified list, so that no code will be sent to that device.

- Note: As of August 2016, NIST has begun not recommending Two-Step Verification that involves SMS/text messaging as the second factor². This is due to the ease of which this can be intercepted.

16.1.1 Assignment: Create an Apple ID

Although it is possible to have a different Apple ID for the iTunes Store, iCloud, App Store, etc., life soon becomes far more complex than necessary. Unless you have a solid case to do otherwise, I strongly recommend having a single Apple ID (email address and password) for all of your various Apple accounts.

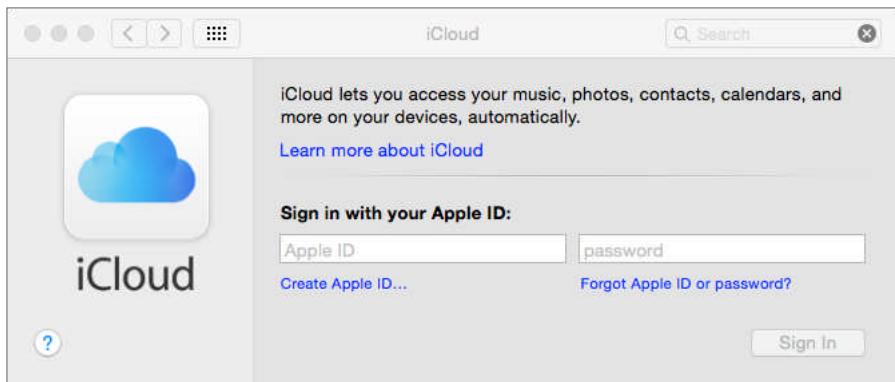
If you already have an Apple ID, skip this exercise. If you do not already have an Apple ID, no better time than the present to create one!

1. Open *Apple* menu > *System Preferences* > *iCloud*.



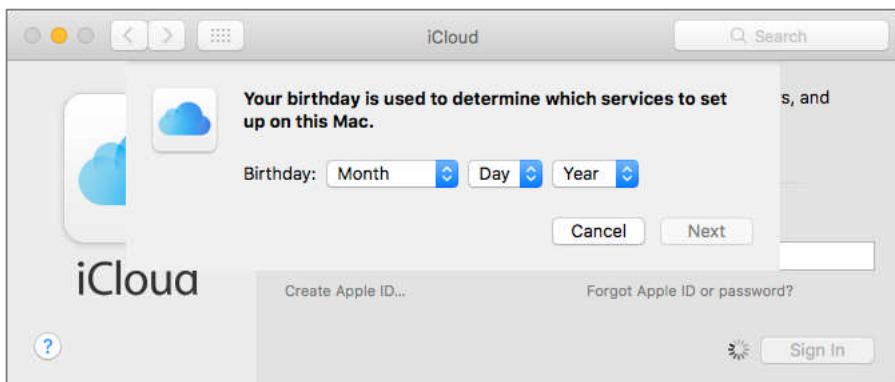
² <https://pages.nist.gov/800-63-3/sp800-63-3.html>

2. In the *iCloud* pane, select the *Create Apple ID...* link.



3. In the *Create an Apple ID* pane, enter accurate information, and then select the *Next* button.

- Note that it is almost always a bad idea to enter accurate information in security question areas. However, in this instance you *must* enter the real deal. Reason is that should you ever need to prove your identity to Apple via driver's license, birth certificate, etc., the records from your Apple ID had better match.



4. In the *Create an Apple ID* pane, complete the required fields, and then select the *Continue* button



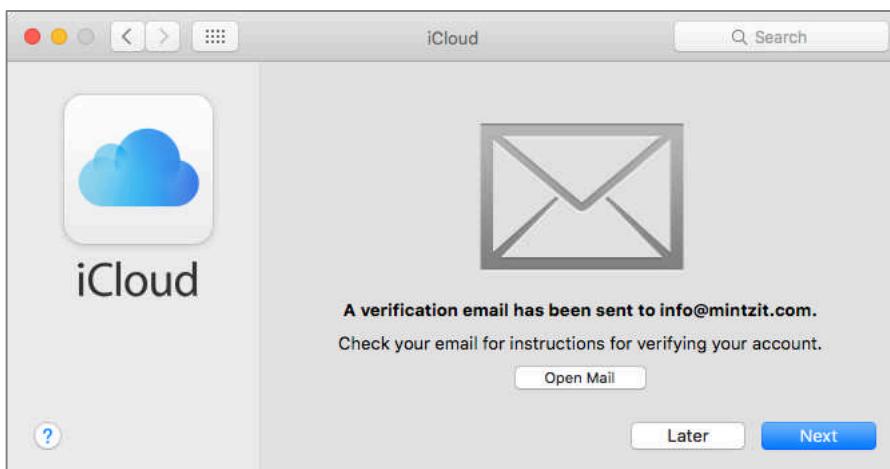
5. In the *Create an Apple ID: Security Questions* pane, set up your security challenge questions. As the truthful answers are easy to discover by someone looking to hack your account, it is strongly recommended providing false answers. Do make sure to record the questions and answers (I do so in my Contacts.app.).



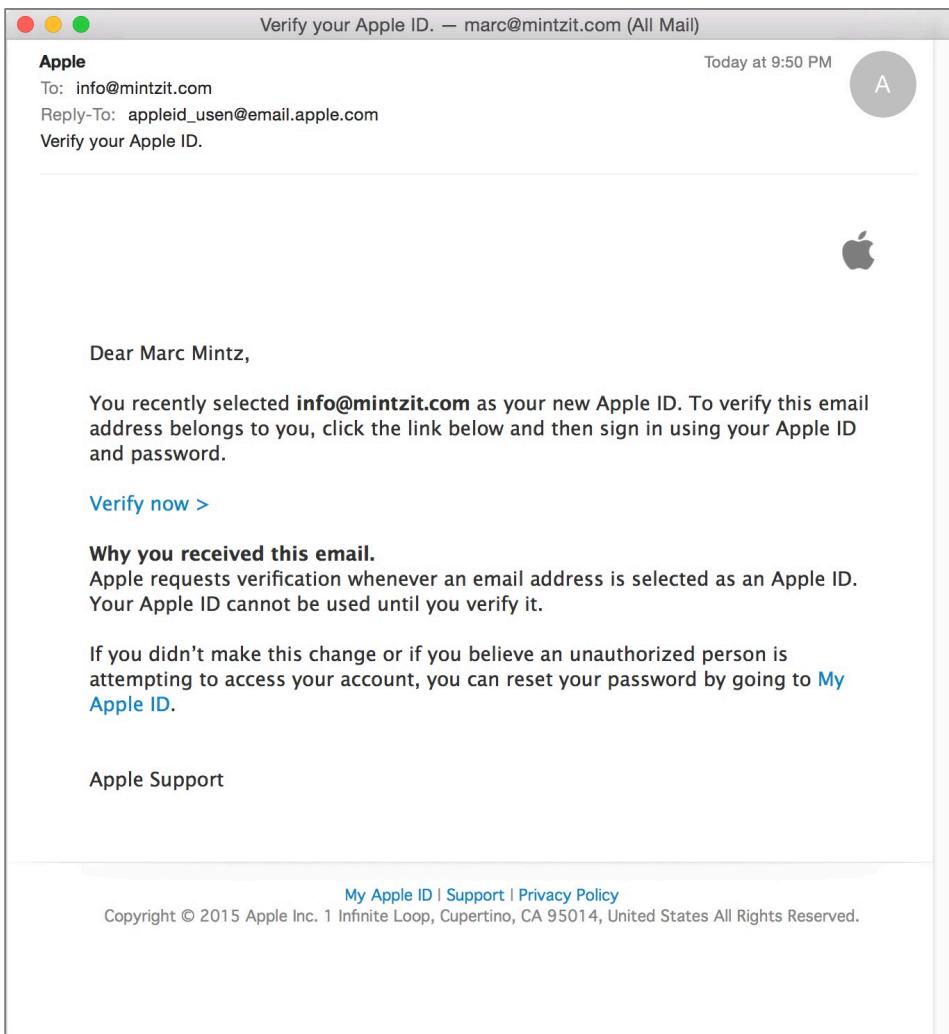
6. At the *Accept the iCloud Terms and Conditions to use iCloud* pane, gather round your team of attorneys, review the document, enable the checkbox, and then select the *Continue* button.



7. At the *iCloud Terms and Conditions* window, enable the *I have read and agree* checkbox, and then select the *Agree* button.
8. At the *A verification email has been sent to <your email address>*, select the *Next* button.

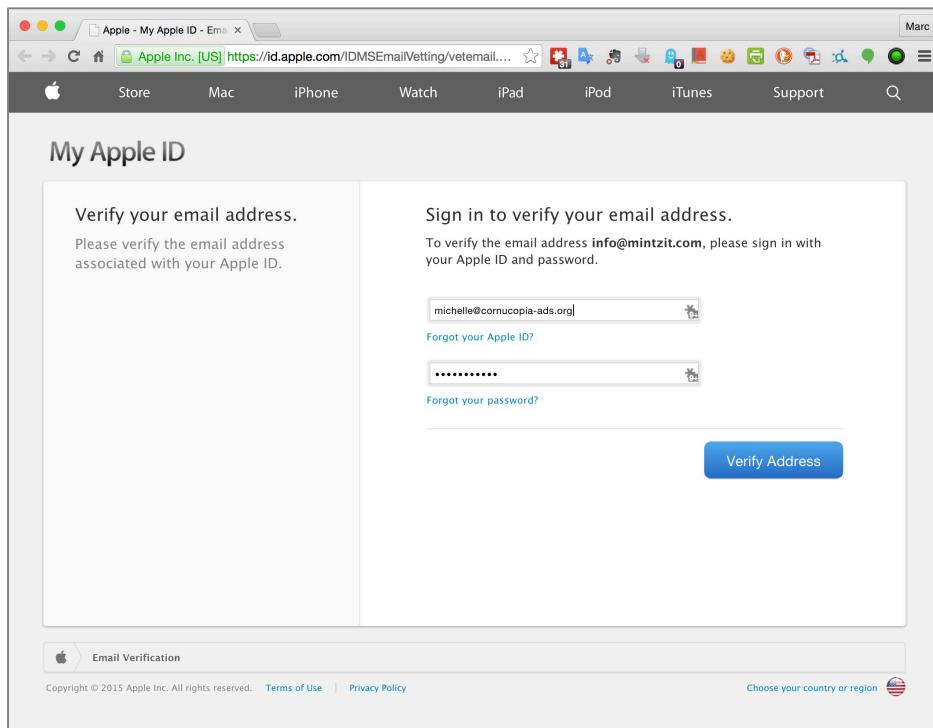


9. Check your mail app for the verification email, and then click the *Verify Now* link.



16 Apple ID and iCloud

10. A browser will open to the *My Apple ID* page. Enter the email address and password used above to create the account, and then click the *Verify Address* button.



11. The *My Apple ID – Email address verified* page will appear. You may close your browser and open *System Preferences > iCloud*.



- Enable *Use iCloud for Contacts, Calendars, Reminders, Notes, and Safari*, if you wish to synchronize these services with other macOS/OS X or iOS devices.
- Enable *Use Find My Mac*, so that in the event it is stolen, there is a chance of finding it.

12. In the *iCloud* pane, click the *Enter Password* button.

16 Apple ID and iCloud

13. In the *iCloud* pane, enable the desired features.



14. OS X 10.9 Mavericks introduced the ability to synchronize your Keychain with iCloud, sharing it with all of your devices. If you would like to do this, enable

16 Apple ID and iCloud

the *Keychain* checkbox, enter your *Apple ID password*, and then select the *OK* button.



15. At the *Create an iCloud Security Code*, enter a 6-character code to allow setting up iCloud on this device, and then click the *Next* button. This will be the same code used to synchronize Keychain on your other devices.



16. The same window will reappear as a verification stage. Reenter your 6-digit code, and then click the *Next* button.
17. At the *Enter a phone number that can receive SMS messages* dialog, enter a phone number that you will always have access to in order to verify your

identity. This is part of setting up 2-factor authentication. Then click the *Done* button.



18. Once brought back to the *iCloud* pane, verify that all of your desired features are enabled, and then *Quit* System Preferences.

Congratulations! You have successfully created a new Apple ID, and have secured your identity with Two-Step Verification.

16.1.2 Assignment: Implement Apple ID Two-Step Verification

Two-step verification, also called two-step authentication, helps to prevent someone else from pretending to be you to reset your Apple ID settings. Anytime significant settings are modified, you will receive an alert on your mobile phone. If you made the changes, ignore the alert. If you did not make the changes, the alert will provide a link to take security actions.

16 Apple ID and iCloud

1. Open a browser to <https://appleid.apple.com>. Enter your *Apple ID* and *Password*.



16 Apple ID and iCloud

2. Select the *TWO-STEP VERIFICATION > Get Started* button.

The screenshot shows the Apple ID account settings page for 'Marc Mintz'. At the top, there's a navigation bar with links for Mac, iPad, iPhone, Watch, TV, Music, Support, a search icon, and a sign-out button. Below the navigation bar, the user's name 'Marc Mintz' and email 'Your Apple ID is webmaster@mintzit.com' are displayed. Under the 'Account' section, there are fields for 'APPLE ID' (webmaster@mintzit.com), 'REACHABLE AT' (webmaster@mintzit.com), and a 'BIRTHDAY' placeholder. In the 'Security' section, there are fields for 'PASSWORD' (Change Password...), 'SECURITY QUESTIONS' (Change Questions...), 'RESCUE EMAIL' (Add a Rescue Email...), and a 'TWO-STEP VERIFICATION' section. The 'TWO-STEP VERIFICATION' section contains the text 'Add an extra layer of security to your account.' and a 'Get Started...' button, which is highlighted with a red oval.

3. In the *Answer your security questions* pane, enter the answers for the questions, and then click the *Continue* button. These were created in Assignment 17.1.1 above.

Answer your security questions

You must verify your identity before making certain changes to your account.

What is the last name of your favorite elementary school teacher?

What is your favorite children's book?

[Cancel](#) | [Continue](#)

4. In the *Getting Started with Two-Step Verification* pane, read the instructions, and then click the *Continue* button.

Getting Started with Two-Step Verification

With two-step verification, your identity will be verified using one of your devices before you can make changes to your account, sign in to iCloud, or make iTunes or App Store purchases from a new device.

The diagram illustrates the three steps of two-step verification:

- Step 1:** A box shows an email address (j.appleseed@icloud.com) and a masked password (*****).
- Step 2:** A hand holds a smartphone displaying a verification code (1234).
- Step 3:** A grid of four boxes contains the numbers 1, 2, 3, and 4, representing the code entered.

You enter your Apple ID and password as usual.

We send a verification code to one of your devices.

You enter the code to verify your identity and complete sign in.

You will also get a Recovery Key for safekeeping which you can use to access your account if you ever forget your password or lose your device.

[Learn more](#) | [Cancel](#) | [Continue](#)

5. In the *Add a trusted phone number* pane, enter your mobile phone number, and then click the *Continue* button.

- Note: It must be able to receive SMS text messages.

Add a trusted phone number

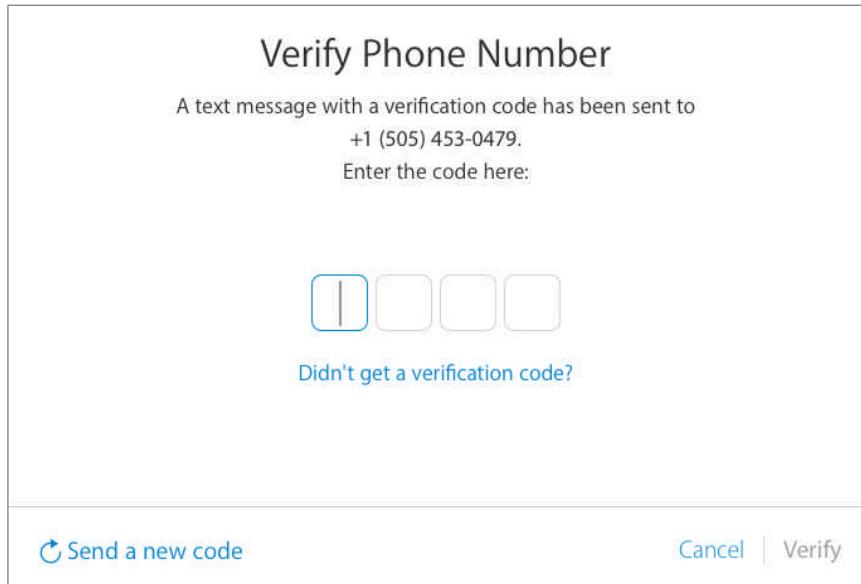
Enter the phone number you want to use to receive verification codes when signing in. This phone number must be able to receive SMS text messages.

Add phone number:

This can be your own number, or the number of someone you trust.

[Cancel](#) | [Continue](#)

6. In the *Verify Phone Number* pane, enter the SMS code that was just sent to your mobile phone, and then click the *Verify* button.



7. In the *Verify Trusted Devices* pane, if you have other mobile devices configured with this same Apple ID, they may be configured to receive

verification codes as well. If you wish, enable them, and then click the *Continue* button.

Verify Trusted Devices

You can also receive verification codes using any device that has Find My iPhone, iPad or iPod touch enabled. Verify each of the devices below.

No devices available

Don't see a device? [Refresh Devices](#) or [Set up Find My iPhone](#).

[Cancel](#) | [Continue](#)

8. The *Print Your Recovery Key* pane appears. This should be recorded in a secure location. This key may be used should you ever forget your Apple ID password or lose one of your mobile trusted devices.

Print Your Recovery Key

You will need your Recovery Key to access your account if you ever forget your password or lose your trusted devices.

Recovery Key:

 RK-

Print or write down your Recovery Key. Keep at least one copy in a safe place.
Do not save it on your computer.

[Where should I keep my Recovery Key?](#)

[Print Recovery Key](#) Cancel | Continue

9. Remember in the previous step when I said to record the recovery key? Well, you should have listened. You will need to re-enter it in the *Confirm Recovery Key* pane, and then click the *Continue* button.
- Note: If you didn't record it, no worries. You can click the *Go Back* button to see it again!

Confirm Recovery Key

Enter your recovery Key below to confirm you have a copy.

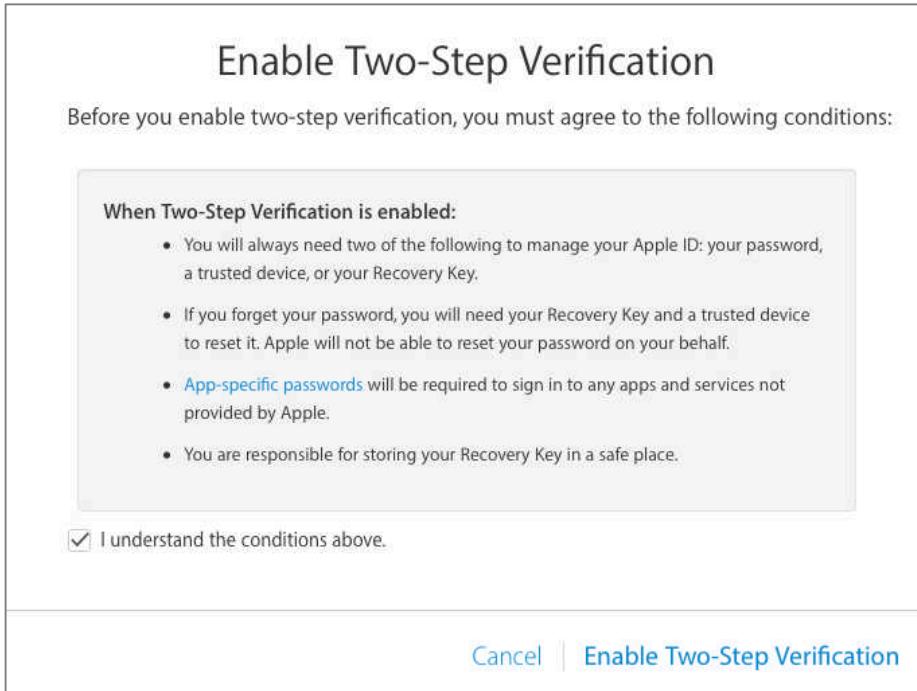
Recovery Key:

 RK -

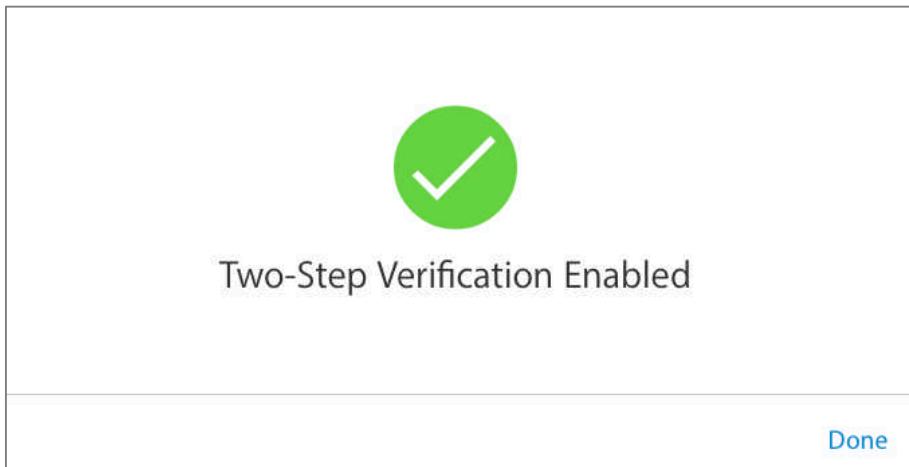
[Where should I keep my Recovery Key?](#)

[Go Back](#) | [Confirm](#)

10. At the *Enable Two-Step Verification* pane, read the instructions, enable the *I understand the conditions above* checkbox, and then click *Enable Two-Step Verification*.



11. At the *Two-Step Verification Enabled* pane, click *Done*.



12. Exit from this page.

You have now made it virtually impossible for anyone to impersonate you to Apple, thereby preventing anyone from gaining access to your Apple ID and iCloud information!

16.2 Review Questions

1. In the event that your iOS device is stolen or lost, you should log in to _____ to remove that device from the verified list, so that no 2-step verification code will be sent to it.
2. You must have a current email address in order to create an Apple ID. (True or False)
3. The services that can be synchronized using iCloud are: _____.
4. A mobile phone number that is capable of receiving texts is a requirement for iCloud 2-step verification. (True or False)

17 Documents

No matter how paranoid or conspiracy-minded you are, what the government is actually doing is worse than you imagine.

—William Blum¹, American author, and former State Department employee

¹ https://en.wikiquote.org/wiki/William_Blum

17.1 Document Security

If your documents never leave your computer, and you have encrypted your storage devices using FileVault 2, there is no need to go the extra step to encrypt your documents. But should you ever need to email your sensitive data to someone else, or pass a sensitive document via any storage device, encrypting the document goes a long way to a good night of sleep.

There are several options to document encryption, each with its own benefits and drawbacks. We will discuss each here.

17.2 Password Protect a Document Within Its Application

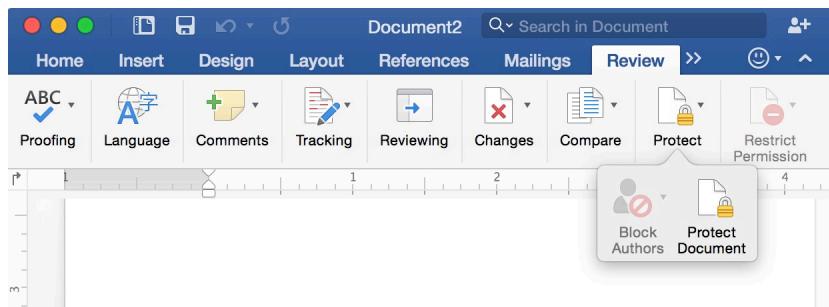
A few applications are designed with document security in mind, and offer their own encryption scheme. Microsoft Office, Adobe Acrobat Pro, and Apple Preview are common examples.

Microsoft Office products make it an easy process to password protect your documents. Office 2008 (for OS X) and earlier used an easily breakable encryption scheme, making it unsuitable for security. As of Office 2007 (Windows) and Office 2011 (macOS/OS X) and higher, AES 128-bit is used for Office document encryption. This is the same as used by government, and is considered secure.

17.2.1 Assignment: Encrypt an MS Word Document

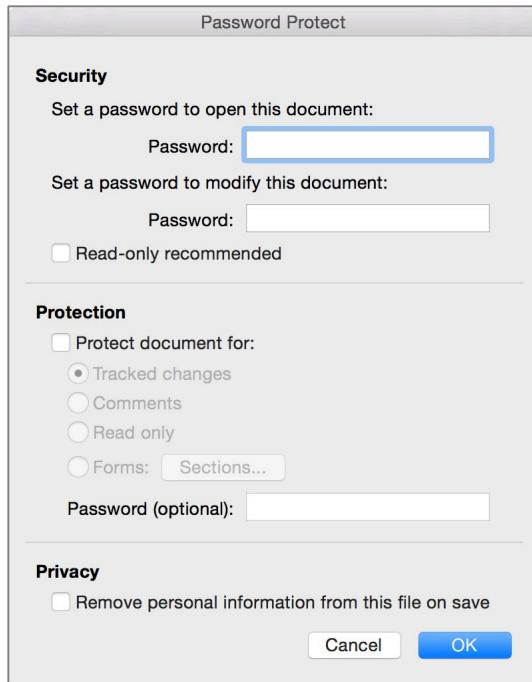
In this assignment you will encrypt a Microsoft Word file (although the process is nearly identical for an Excel file) from within the application.

1. Open the target document in Microsoft Word 2016.
2. Select *Review* tab > *Protect* > *Protect Document*.

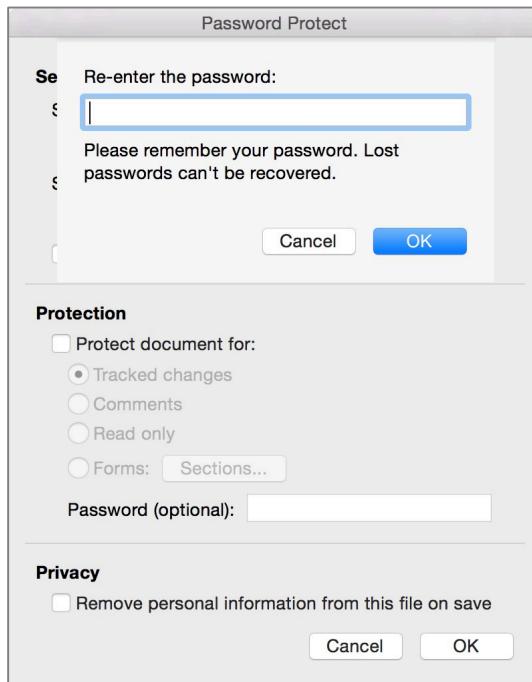


3. The *Password Protect* dialog opens. You may set a separate password to *Open*, and to *Modify* this document. Enter a password for the desired function.

- Note: Passwords for Microsoft Office products are limited to 15 characters.



4. Re-enter the password, and then click *OK*.



5. Click the *OK* button at the bottom right of the *Password Protect* dialog.
Your document is now protected.

17.3 Encrypt a PDF Document

As there are only a few applications that can encrypt their own documents, chances are you will be working with a file whose application cannot perform the encryption. macOS can “print” any document to pdf format, and in the process, add password-protected encryption to the pdf.

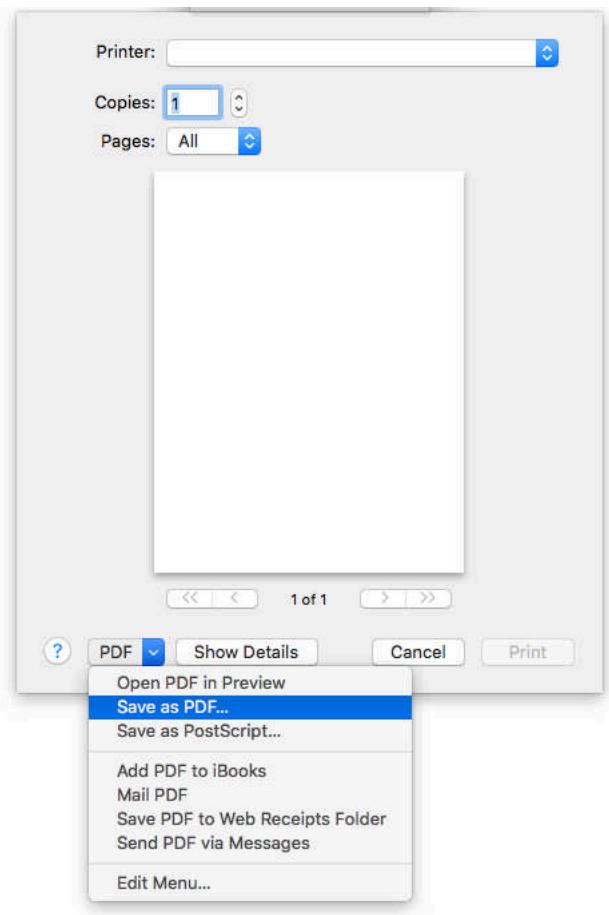
- Note: macOS print to pdf services saves the file in a pdf version 1.4/Acrobat 5 format. This format uses RC4 128-bit encryption, which is considered weak, and should not be used for HIPAA, SEC, legal, or other high-security needs
- Note: Adobe Acrobat 7 and higher use AES 128-bit encryption. Adobe Acrobat 9 and higher use AES-256-bit encryption. These are considered secure, as long as strong passwords are used.

17.3.1 Assignment: Convert a Document to PDF for Password Protection

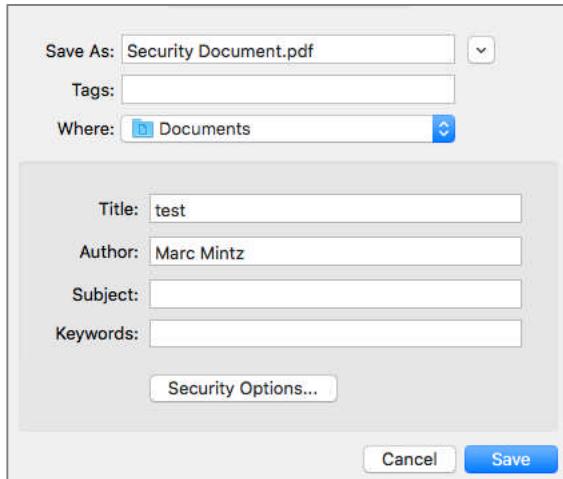
1. Open any printable document currently on your computer.
2. Select *File* menu > *Print*.

17 Documents

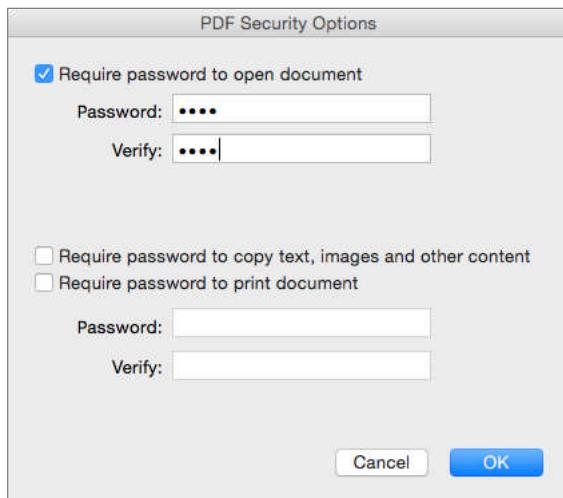
3. From the *Print* window, select the *PDF* button > *Save as PDF*.



4. In the window that opens, in the *Save As* field, name the pdf version of the document, and then select the *Security Options...* button.



5. In the *PDF Security Options* window, enable the *Require password to open document* check box, enter a desired password in the *Password* and *Verify* fields, and then select the *OK* button.



6. Quit the current document and application.

The pdf version of the document is now encrypted. If the original document is no longer needed, it may be trashed.

17.4 Encrypt a Folder for Only macOS/OS X Use

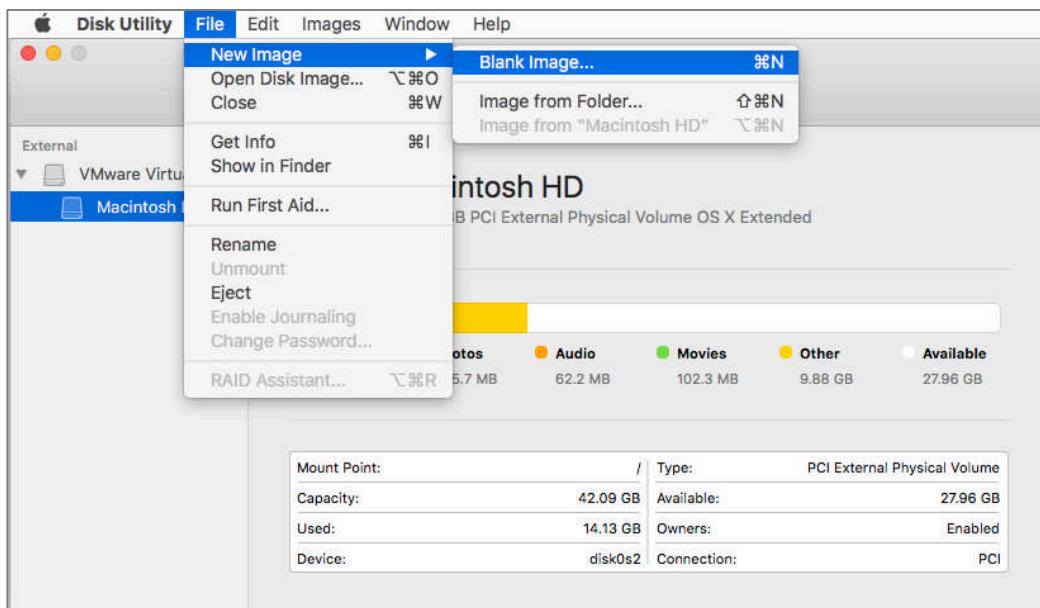
Perhaps you need to securely send an entire folder of files. An easy way to accomplish this is to use a utility to archive (compress to a single file) the files or folder, and have that same utility protect the archive with a password.

macOS has a built-in utility to do this for you—*Disk Utility*. The only downside is that the archives created with Disk Utility are only readable on another macOS/OS X computer—they are not cross-platform compatible. However, if your documents will be passed along only to others using macOS/OS X, it is an excellent tool.

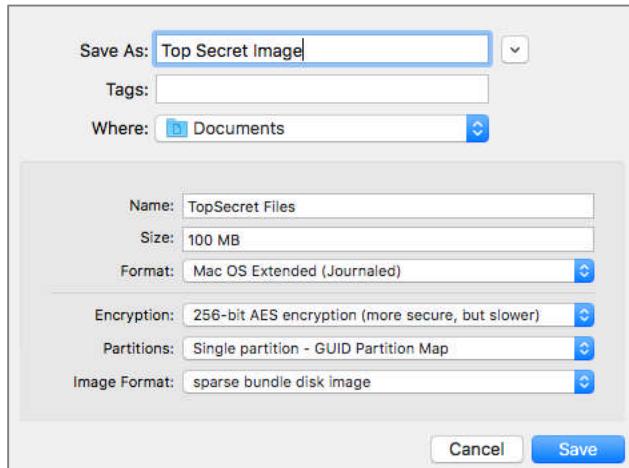
17.4.1 Assignment: Create an Encrypted Disk image

In this assignment you will create an encrypted disk image to may store some or all of your most sensitive data.

1. Open Disk Utility, located in */Applications/Utilities*.
2. Select *Disk Utility* *File* menu > *New Image* > *Blank Image...*



3. Configure the *New Image* screen as below.



- *Save As*: The desired name for the archive that will hold all of your files to be password protected.
- *Where*: Navigate to where you want the archive to be saved.
- *Name*: Enter the name of the mounted disk image. To avoid confusion, this is normally named the same as the *Save As* field. For demonstration purposes, we are naming them differently in this example.
- *Size*: This should be somewhat larger than the total size of files the archive will hold. It can be much larger, as the archive will compress out all unused space.
- *Format*: *Mac OS Extended (Journaled)*. This is the macOS standard format.
- *Encryption*: 256-bit takes more time to encrypt and decrypt than 128-bit, but is also more secure. When selecting this option, you will be prompted to provide a password. Enter your desired password, and then click *OK*.
- *Partitions*: Single Partition, GUID Partition Map. This is the macOS standard.
- *Image Format*: *Sparse Bundle Disk Image*. This is the format that will compress out all unused space.

4. Select the *Save* button.

5. The archive is saved, and the Disk Image (the opened format of the archive) is displayed in the Finder Window Sidebar, and depending on your *Finder Preferences* menu > *General > Hard Disks*, may display as mounted on the Desktop. You now have an encrypted, password protected archive, but it's currently empty. Time to fill it.
6. Locate the mounted disk image on the Desktop. In our example, it will be called *Top Secret Files*.
7. Drag the various files and folder that you have targeted for password protection into the mounted image.
8. Eject/unmount the mounted image. It will close, remove itself from the Desktop, leaving just the password protected archive in the location you specified in step 3 above (Desktop).

This archive may be securely passed to macOS/OS X users by any method. If they know the password, double-clicking the archive will mount the disk image to their Desktop, and they will have full read and write access to the documents inside.

17.5 Encrypt a Folder for Cross Platform Use with Zip

If you need to exchange a file or files with others and they do not use macOS/OS X, we can use the same strategy as we did with Disk Utility, but this time we need to password protect our archive in a format that is readable by any OS. Although there are over a dozen cross-platform compression formats, *zip* has become the most common standard.

macOS/OS X has the built-in ability to create zip archives, but it has left out the encryption option from the user interface. In order to encrypt our zip archives, we will need to get under the hood and use the command line. No need to go running for the hills. I promise this won't hurt at all.

Once you have created an encrypted archive of your file or files, the archive can be uploaded to a file server, shared by email, or passed along via drive, disc, or thumb drive. As long as the other party knows the (strong) password, your data is safe from spying eyes.

- Note: The encryption protocol used in zip is considered weak, and should not be used for HIPAA, SEC, legal, or other high-security needs.

17.5.1 Assignment: Encrypt a File or Folder using Zip

In this assignment you will encrypt a file using the built-in zip utility. The same process can be used to encrypt a folder full of items.

1. Open *Terminal* (located in */Applications/Utilities/*)
2. Enter the following command in Terminal:
`zip -ejr archive_name path_to_target_item`
 - *e* tells zip to encrypt the archive
 - *j* tells zip to junk the archive path, else it would archive the full folder hierarchy leading to the target file
 - *r* tells zip to be recursive, to encrypt all items inside the target folder
 - *archive_name* is the name to give the encrypted zip archive

- *path_to_target_item* is the full URL to the item to be zipped. You can make easy work of this by drag-and-drop the item into the Terminal window
3. Press the *Return* or *Enter* key.
 4. The zip archive will be found at the root level of your home folder.

17.5.2 Assignment: Open an Encrypted Zip Archive

In this assignment you will open the encrypted zip archive created in the previous assignment.

- Prerequisite: An encrypted zip archive must be present on your file system.
1. Double-click on the encrypted zip archive.
 2. At the prompt, enter the password used to encrypt it.
 3. The archive will open.

17.6 Cross-Platform Document Encryption

By many in the IT security fields, the ultimate in document encryption comes with *VeraCrypt*². VeraCrypt is free encryption software developed by *IDRIX*³, who specialize in security solutions. It is based on *TrueCrypt*⁴ that ceased development in 2014.

Although Linux, macOS/OS X, and Windows versions are available, no Android or iOS support is directly offered. Android users may create and decrypt, as well as read and write to TrueCrypt files using *EDS* (Encrypted Data Store), available from Google Play. iOS users may use *Disk Decipher*, available from the App Store, to create and decrypt, as well as read and write to TrueCrypt files.

VeraCrypt is actually a disk encryption utility, as opposed to file encryption. It creates an encrypted virtual disk, or as it is referred to by VeraCrypt, a container.

VeraCrypt presents a very high level of security, with a resultant greater complexity to the end-user. Given the speed of current systems and a strong password, data stored in a container may be considered immune from brute-force attacks.

As VeraCrypt creates a container, you are able to place anything within the container for secure storage. The container may reside only on the local drive, or be placed on a server for network access, or within a cloud storage solution (such as DropBox, Google Drive, etc.) to provide Internet access to files and folders, without the cloud provider (or hacker, malware, or government) being able to view the contents.

² <http://veracrypt.codeplex.com>

³ <https://www.idrix.fr>

⁴ <http://en.wikipedia.org/wiki/TrueCrypt>

17.6.1 Assignment: Install FUSE for OS X

VeraCrypt makes use of the *FUSE for OS X* utility, and it must be installed prior to installing VeraCrypt. FUSE for OS X enables your computer to create and work with non-native file systems, such as the *container* system created with VeraCrypt.

In this assignment you will install FUSE for OS X.

1. Open your browser and go to the *OSXFuse* github repository at <https://osxfuse.github.io>.
2. Click the *Downloads* button.



3. From the sidebar, select the version appropriate for your computer. The installer will begin downloading.
- Note: As of this writing, macOS users will need to download the osxfuse-3.x version. Mac OS X users may download the latest stable release.

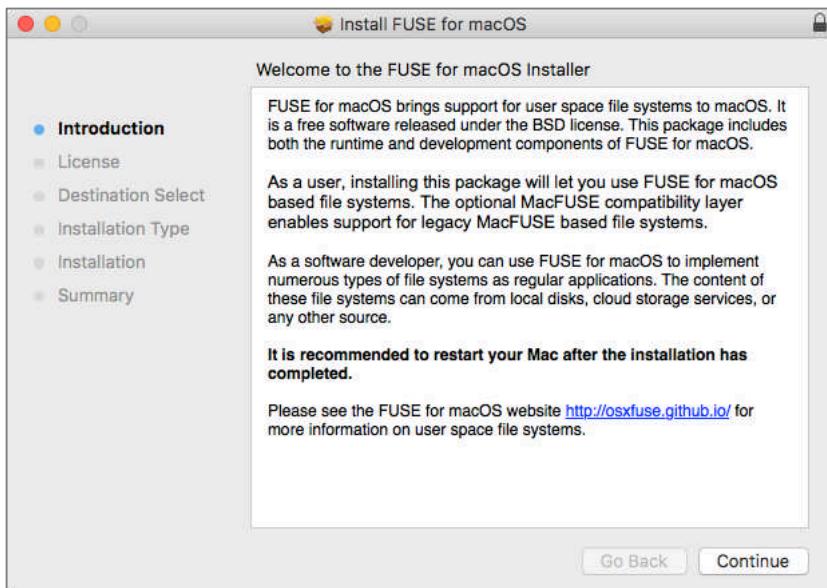
The screenshot shows a web browser window for sourceforge.net. The URL bar says "sourceforge.net". The main header includes the SourceForge logo, a search bar, and navigation links for "Browse", "Enterprise", "Blog", "Deals", and "Help". Below the header, there's a menu bar with "SOLUTION CENTERS", "Go Parallel", and links for "Resources", "Newsletters", "Cloud Storage Providers", "Business VoIP Providers", and "Internet Speed Test". The main content area shows the "FUSE for OS X" project page. It features a thumbnail of a book titled "FUSE", the title "FUSE for OS X", a subtitle "Extends OS X via third party file systems", and a note "Brought to you by: bfleischer". Below this, there are links for "Summary", "Files", "Reviews", and "Support". A callout box on the right side contains the text "Only CA has the agile and support make you re...". The "Files" section lists four versions of the software:

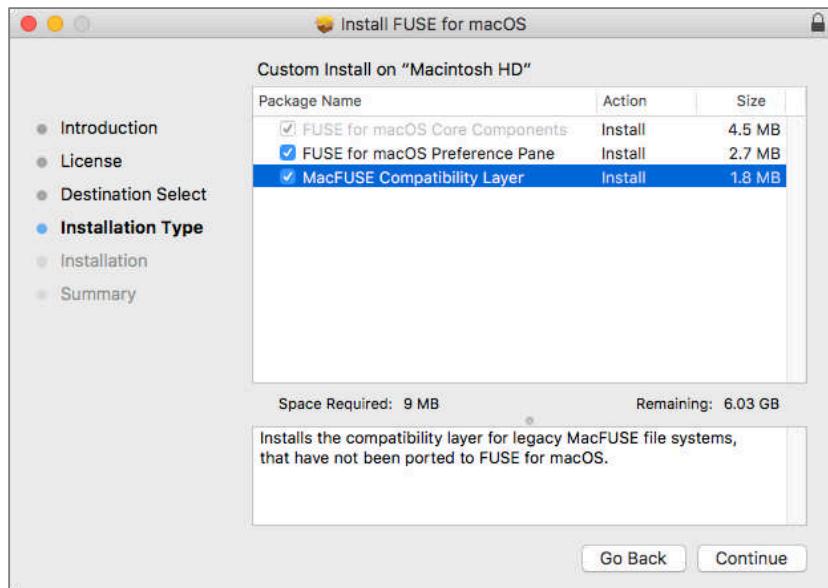
Name	Modified	Size	Downloads / Week
osxfuse-3.x	2016-01-18		242
osxfuse-2.8.3	2016-01-18		10,655
osxfuse-2.8.2	2015-10-25		225
osxfuse-2.8.1	2015-09-24		11

4. Locate the installer in your Downloads folder, and then double-click to open. It will mount and open a disk image. Double-click to launch the installer.



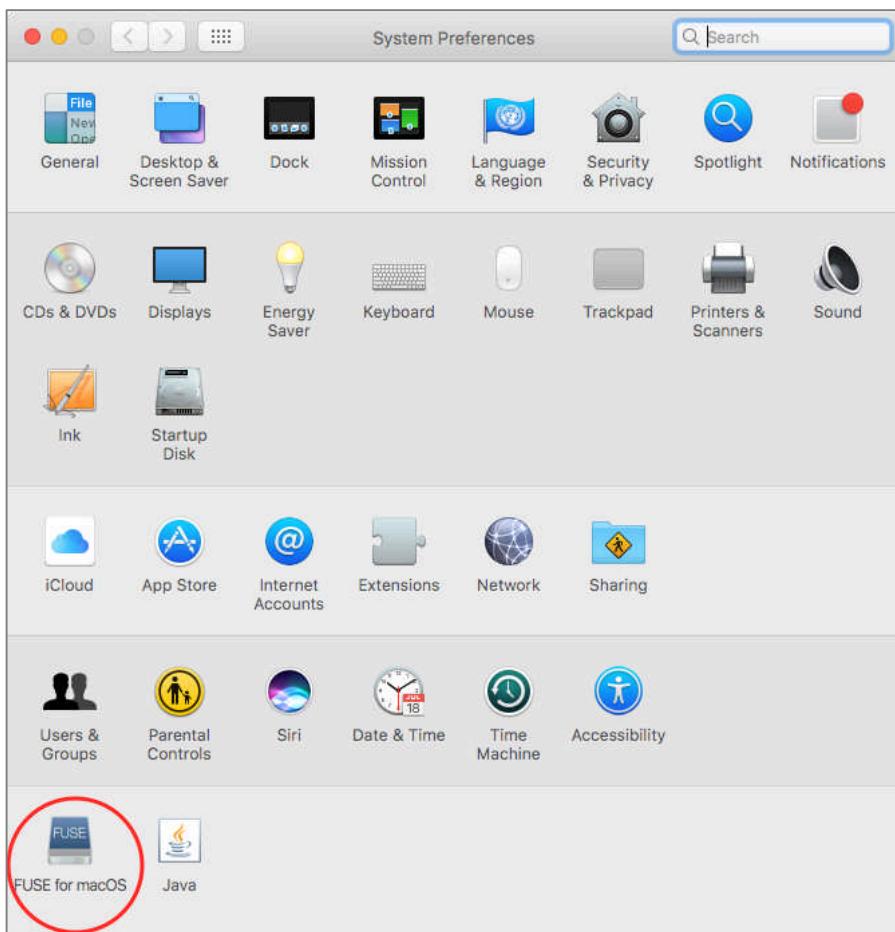
5. The *Install FUSE for macOS* installer welcome screen will appear. Select the *Continue* buttons until you see the *Custom Install on <hard drive>*. Enable both *FUSE for macOS Preference Pane* and *MacFUSE Compatibility Layer* check boxes, and then select the *Continue* buttons to complete the installation.





6. Verify FUSE for OS X has installed by opening *System Preferences*, and seeing its icon

17 Documents



7. Close System Preferences.

The *really* easy part is done. Now on to the easy part—installing VeraCrypt.

17.6.2 Assignment: Download VeraCrypt

In this assignment you will install VeraCrypt.

- Prerequisite: Installation of FUSE for OS X (the previous assignment)

17 Documents

1. Open a web browser to <https://veracrypt.codeplex.com>.
2. Click the Downloads tab (not the Downloads button). Selecting the tab allows you to select which version to download.

The screenshot shows the VeraCrypt project page on CodePlex. At the top, there's a navigation bar with links for Register, Sign In, and a search bar labeled "Search all projects". Below the header is the VeraCrypt logo and name. A horizontal menu bar includes links for HOME (which is highlighted in blue), SOURCE CODE, DOWNLOADS, DOCUMENTATION, DISCUSSIONS, ISSUES, PEOPLE, and LICENSE. Under the HOME link, there are "Page Info" and "Change History (all pages)" options. To the right of the menu, there are "Follow (474)" and "Subscribe" buttons. The main content area has a section titled "Project Description" with a paragraph about the software being based on TrueCrypt 7.1a and developed by IDRIZ. On the right side of this section is a search bar for "Wiki & Documentation". Below the description is a large purple "download" button. At the very bottom of the page, there's a decorative footer element consisting of several colored bars.

17 Documents

3. From the *OTHER AVAILABLE DOWNLOADS* area, select *VeraCrypt MacOSX Setup*. The installer will download.

Screenshot of the VeraCrypt project page on CodePlex.

The page shows the following details:

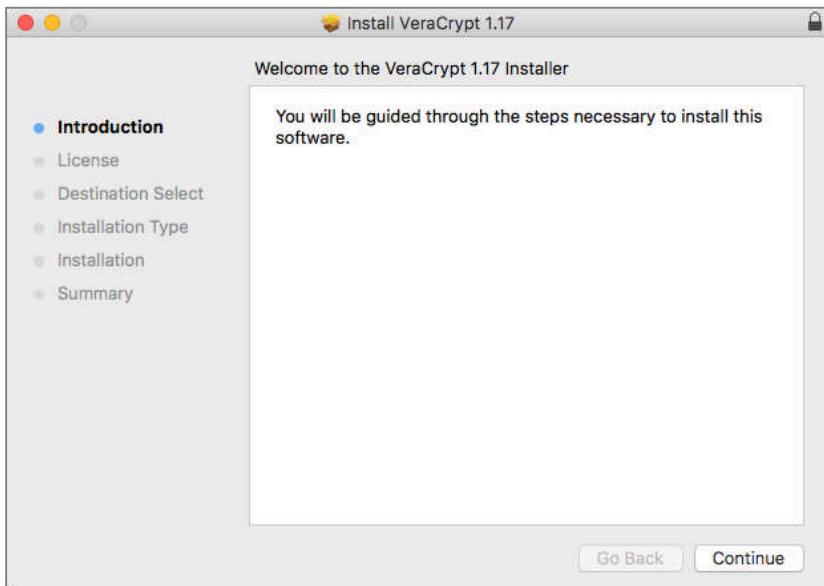
- Project Name:** VeraCrypt
- Downloads:** Aug 17, 2016
- Rating:** ★★★★☆ Based on 4 ratings
- Reviewed:** 4 reviews
- Downloads:** 6494
- Change Set:** 33185bf2fff2
- RECOMMENDED DOWNLOAD:** VeraCrypt version 1.18 (application, 19392K, uploaded Wed - 4177 downloads)
- OTHER AVAILABLE DOWNLOADS:**
 - VeraCrypt Linux Setup 1.18 (application, 16658K, uploaded Wed - 563 downloads)
 - VeraCrypt MacOSX Setup 1.18 (application, 8917K, uploaded Wed - 278 downloads)
- OTHER DOWNLOADS:**
 - Released | Planned:** VeraCrypt version 1.18 (Aug 17, 2016, Stable) ★★★★☆
 - VeraCrypt version 1.17 (Feb 13, 2016, Stable) ★★★★★
 - VeraCrypt version 1.16 (Oct 7, 2015, Stable) ★★★★★
 - VeraCrypt version 1.0f-2
- Release notifications:** Sign in to display notification settings.

4. Locate the downloaded installer, and then double-click to open the disk image.

- Double-click to launch the *VeraCrypt_Installer.pkg* inside of the mounted disk image.



- The installer opens. Follow the on-screen instructions to complete the installation.

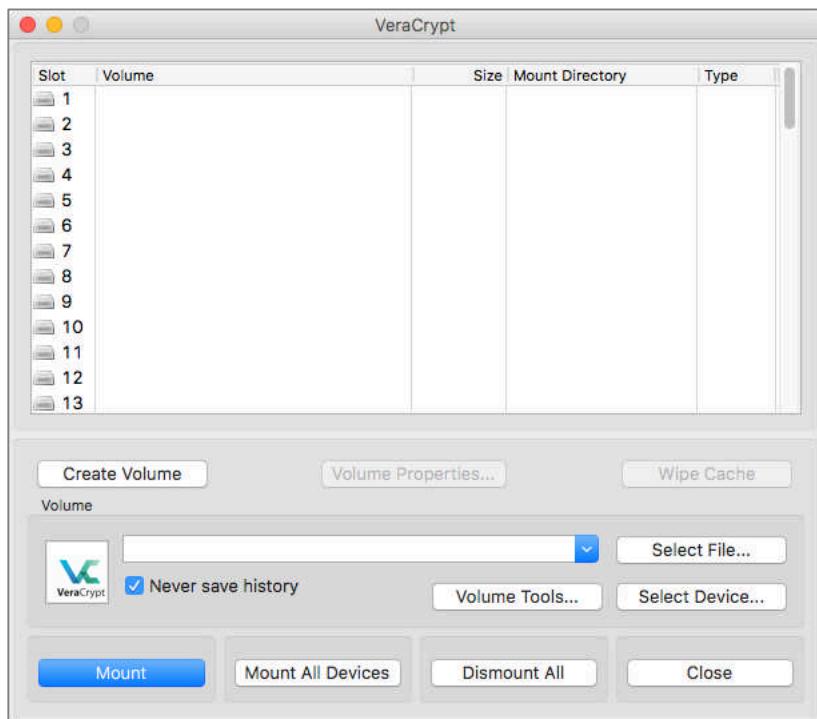


That's all there is to the installation.

17.6.3 Assignment: Configure VeraCrypt

As with most applications, it helps to view and configure VeraCrypt preferences before using it. In this assignment, we will examine VeraCrypt preferences.

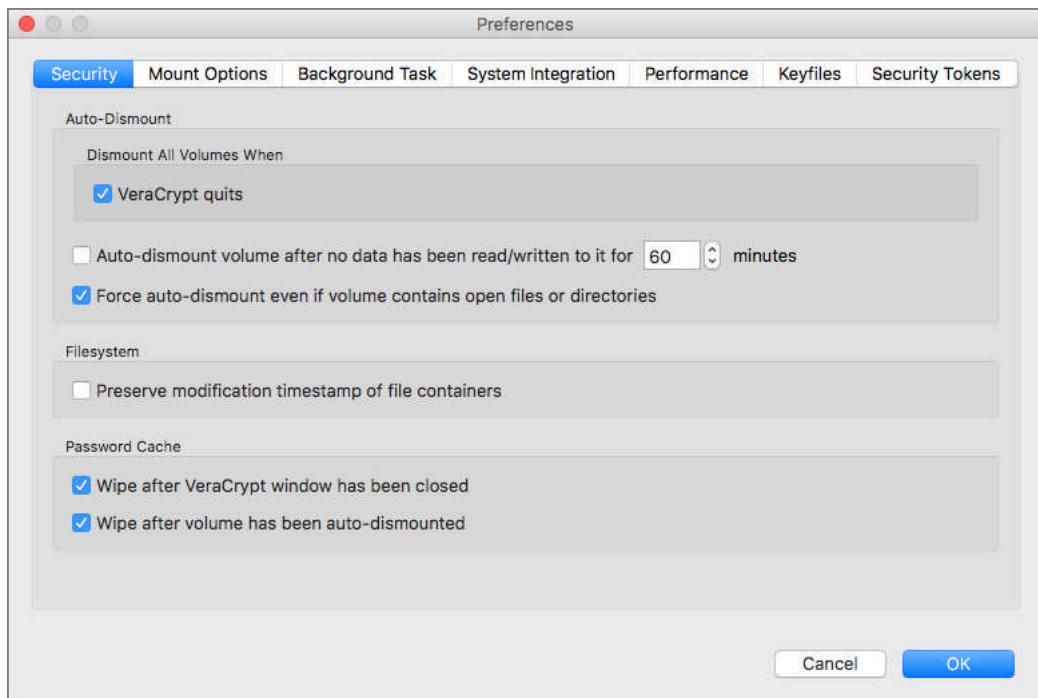
1. Open VeraCrypt.



2. Select the *VeraCrypt* menu > *Preferences*.
3. Select the *Security* tab. Most of the options may be configured to taste. The exception is *Preserve modification timestamp of file containers*, which should be *disabled* if the containers will be used with cloud-based file storage service

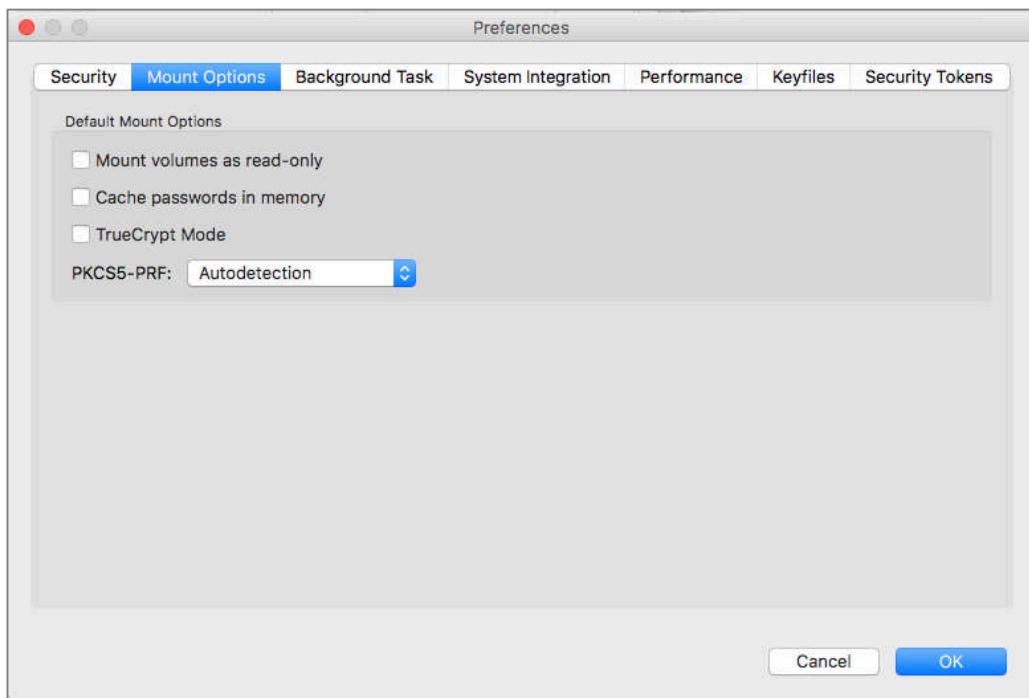
17 Documents

(DropBox, Google Drive, SugarSync, etc.) as it will conflict with the service's ability to update the timestamp.

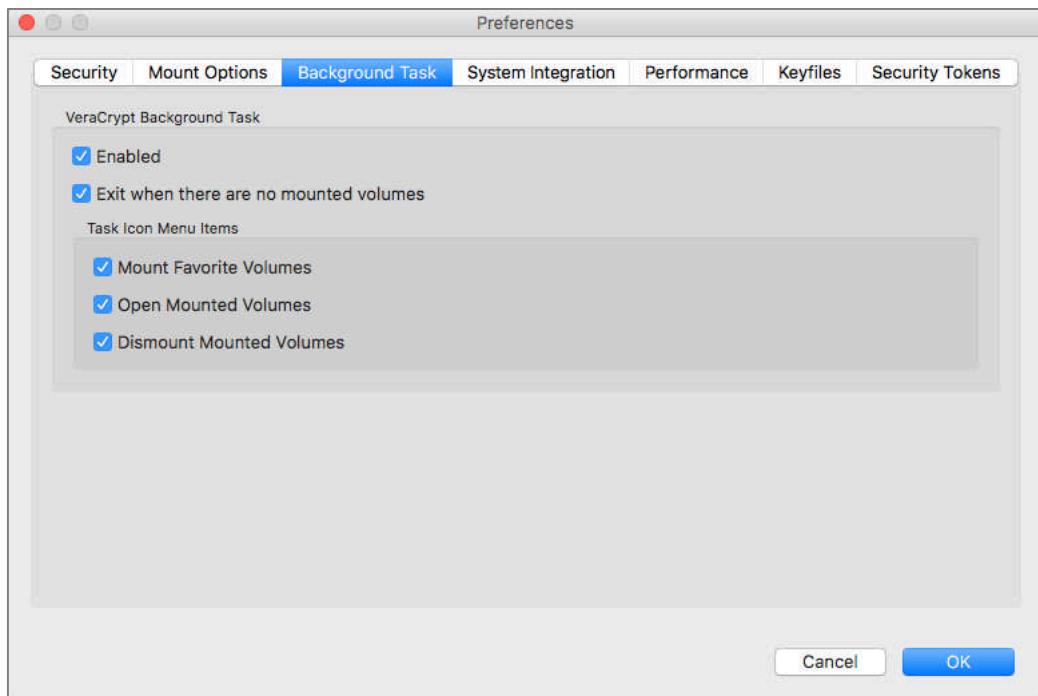


4. Select the *Mount Options* tab.

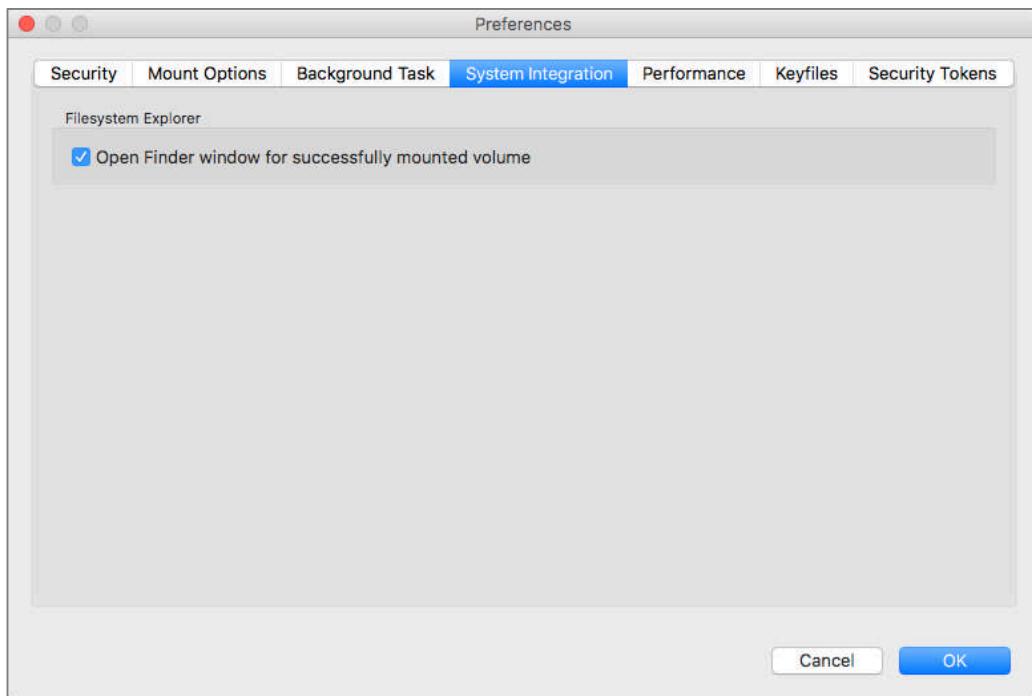
- *Mount volumes as read-only* if left unchecked will prevent accidental editing or deletion of the container contents.
- *Cache passwords in memory* if left unchecked will provide higher security against hackers gaining access to container passwords.
- *TrueCrypt Mode* option should be left unchecked unless you will be using software that can only work with the older TrueCrypt mode..



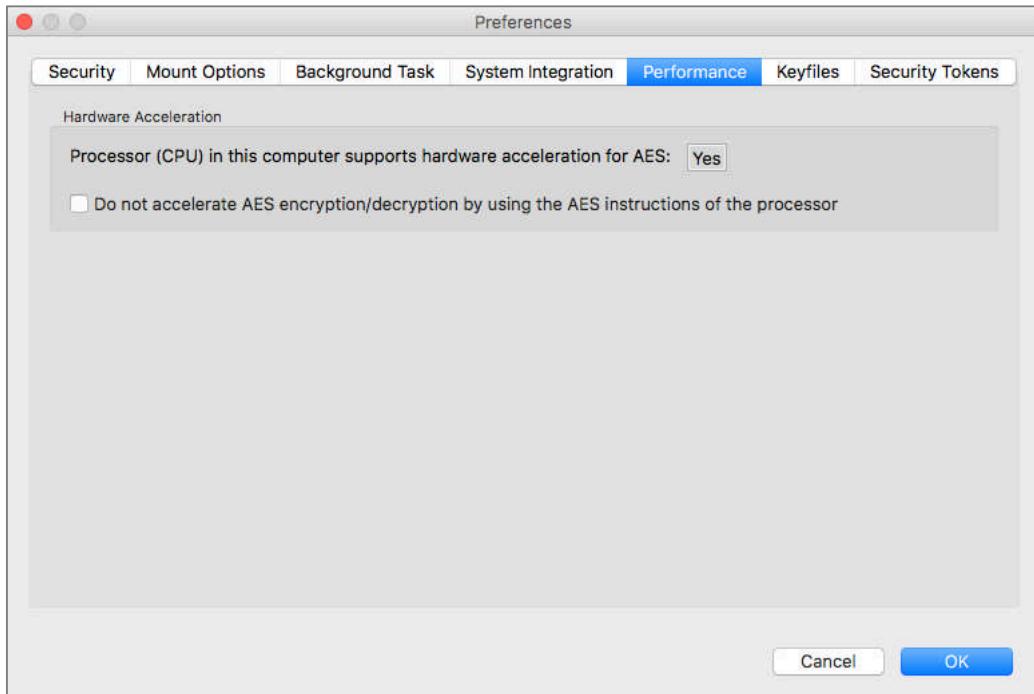
5. Select the *Background Task* tab. All options may be configured to taste. Listed below are my settings.



6. Select the *System Integration* tab. You may configure to taste. Listed below is my setting.



7. Select the *Performance* tab. If your computer supports hardware acceleration of AES encryption protocols, you will probably want to leave the checkbox disabled. Doing so will improve encryption and decryption up to 4 fold.



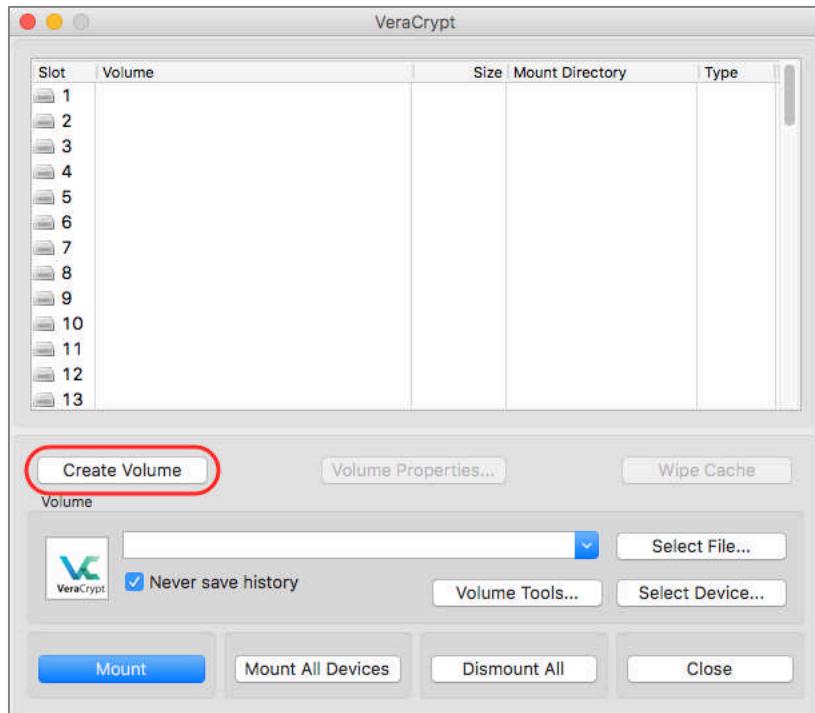
8. The *Keyfiles* tab is an advanced option. Please see the VeraCrypt online documentation <https://veracrypt.codeplex.com/documentation> for additional information.
9. The *Security Tokens* tap is an advanced option. Please see the VeraCrypt online documentation <https://veracrypt.codeplex.com/documentation> for additional information.
10. Close the VeraCrypt Preferences window.

We are now ready to create our first encrypted VeraCrypt container!

17.6.4 Assignment: Create a VeraCrypt Container

Although we will cover the basics of using VeraCrypt, you may find it useful to dive deeper into the topic⁵.

1. Open the *VeraCrypt* application, located in the /Applications folder. Then select the *Create Volume* button.

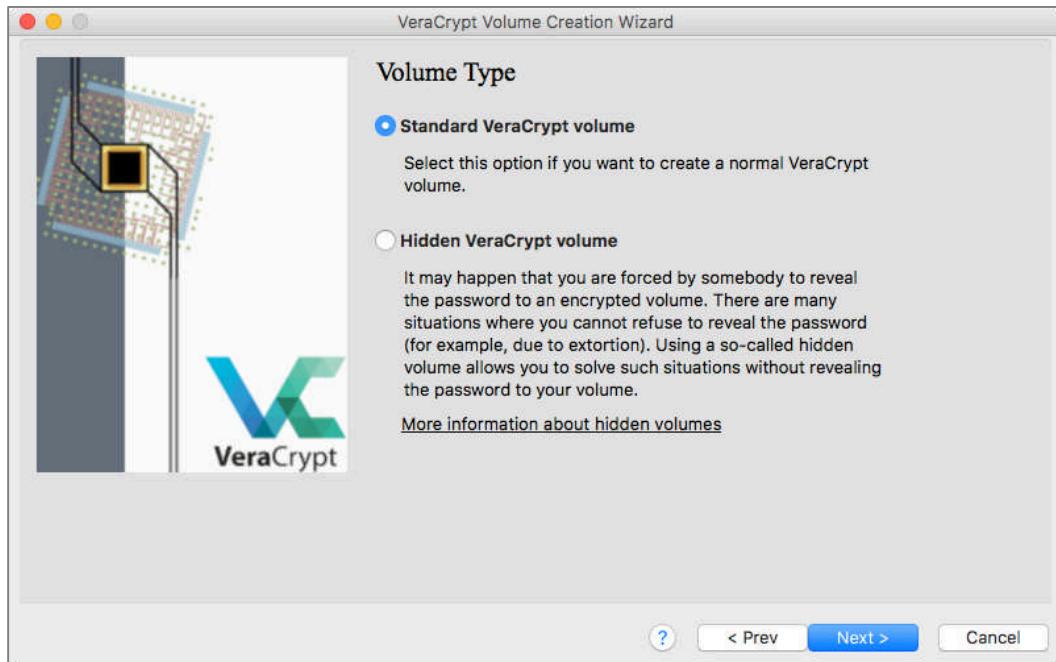


⁵ <https://veracrypt.codeplex.com/documentation>

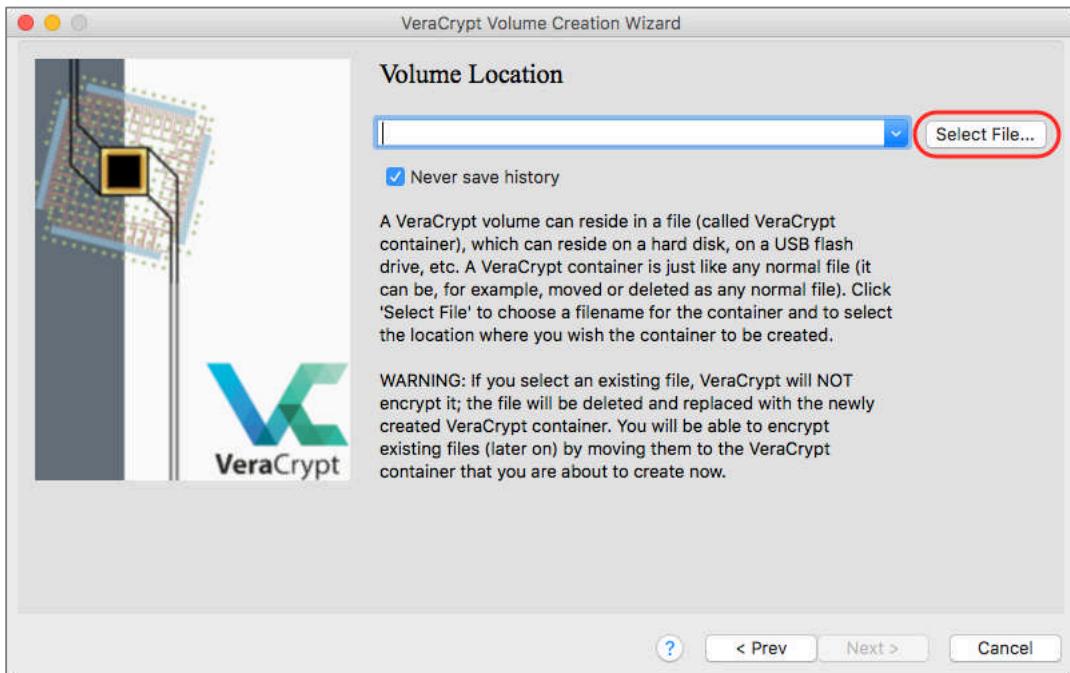
2. To create an encrypted container, at the *VeraCrypt Volume Creation Wizard*, select the *Create an encrypted file container* radio button, and then select the *Next >* button.



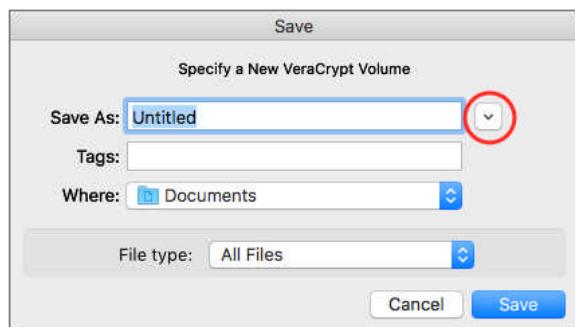
3. At the *Volume Type* window, select the *Standard VeraCrypt volume* radio button, and then select the *Next >* button.



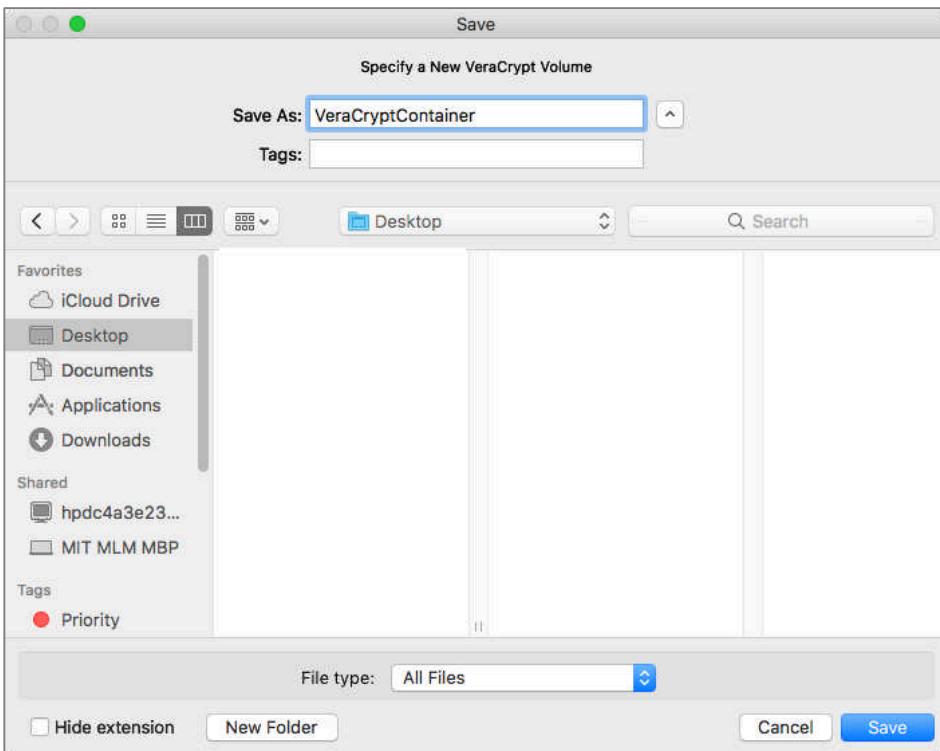
4. At the *Volume Location* window, select the *Select File...* button.



5. When the *Save* window appears, select the *Disclosure arrow* to the right of the *Save As* field. This will expand the window, making it easier to select where to save the container.



17 Documents

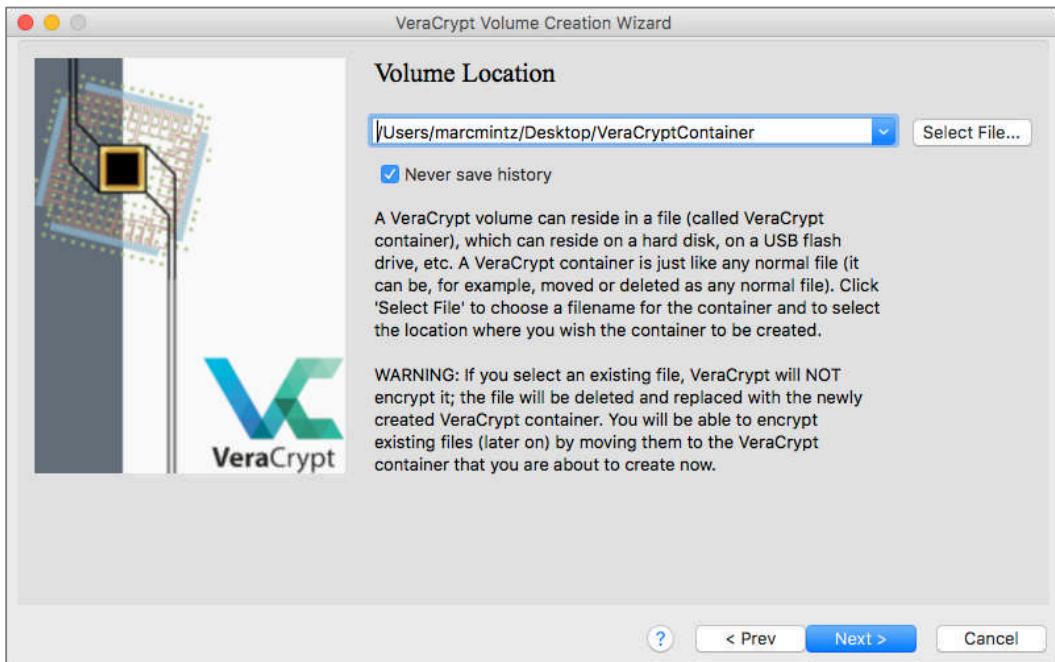


6. In the *Save As* field, enter a name for your container. For this assignment, use *VeraCryptContainer*.

Navigate to where you wish to save your container. For this assignment, use the *Desktop*.

7. Click the *Save* button.

8. When returned to the *Volume Location* window, select the *Next >* button.

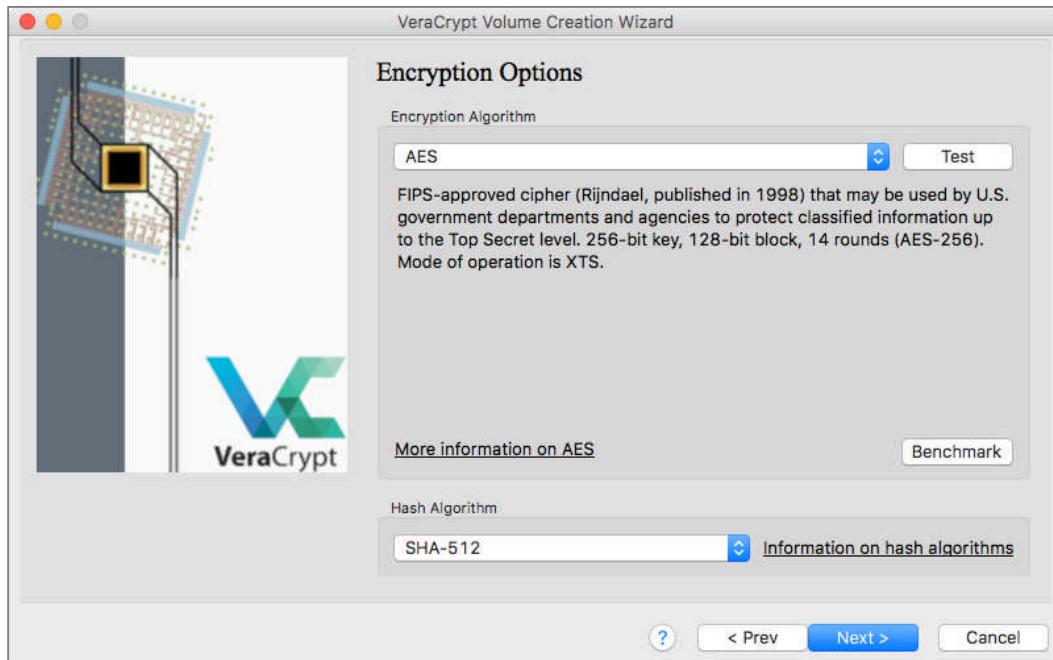


9. In the *Encryption Options* window, configure as below:

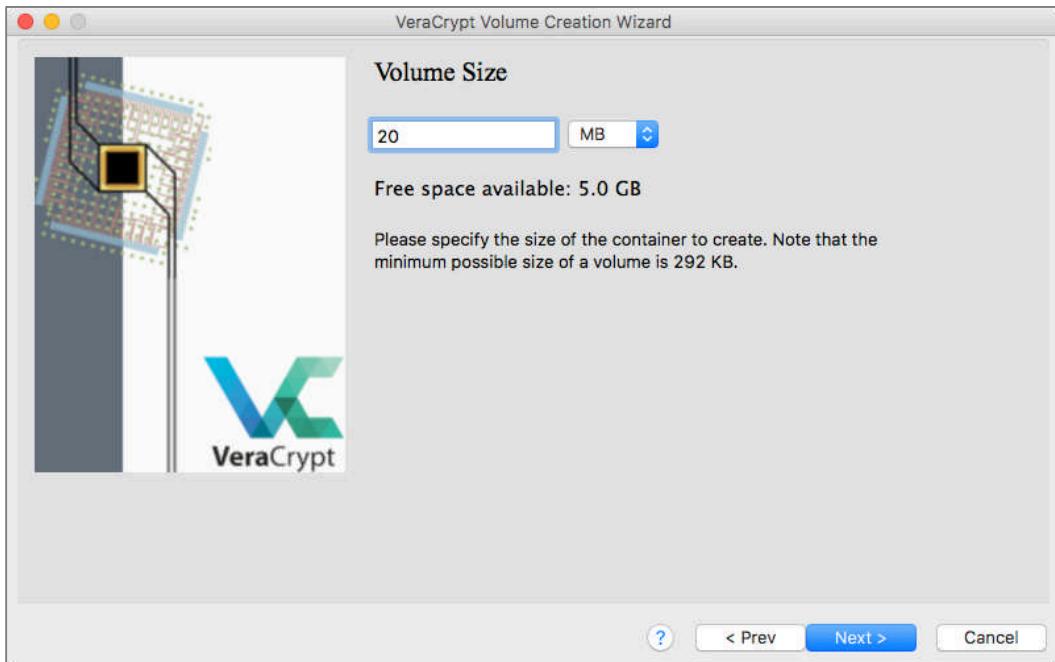
- From the *Encryption Algorithm* pop-up menu, select your desired option. AES is the industry standard, however, as the NSA and NIST were involved with its acceptance, some experts recommend selecting another option.
- From the *Hash Algorithm* pop-up menu, select the desired option. SHA was developed by the NSA, so some experts recommend selecting

Whirlpool. For our example, we will use the industry standards—AES and SHA-512.

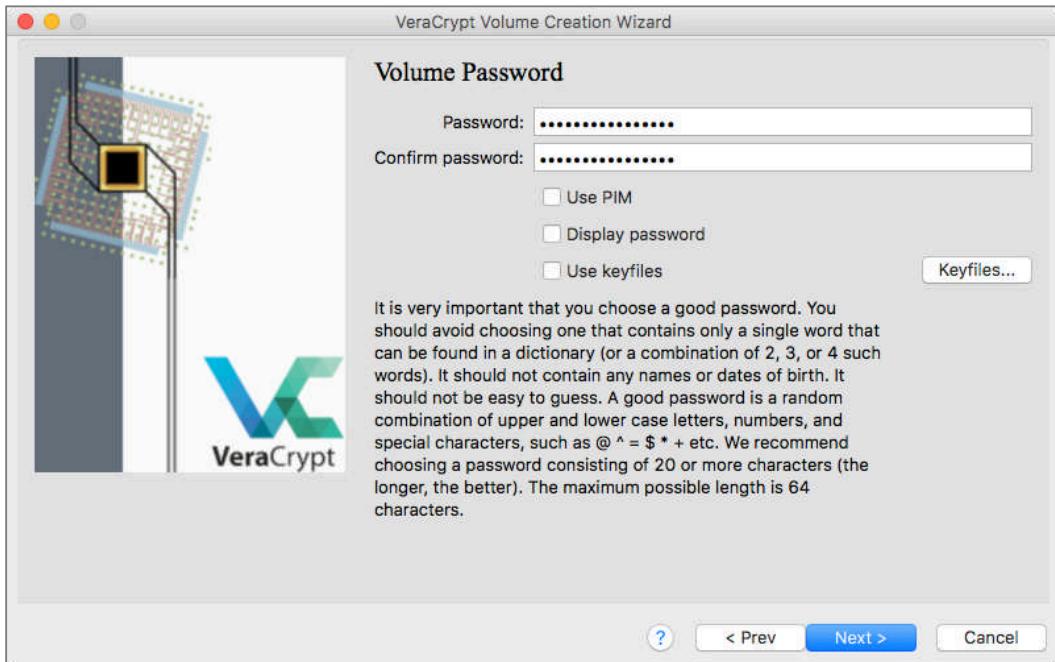
- Select the *Next >* button.



10. In the *Volume Size* window, set the size of your container. If you intend to email the container, keep in mind that each email provider has hard limits on the maximum file size that may be sent or received. If you intend to save the container to a storage device such as a thumb drive, keep in mind that a storage device needs approximately 20% free space for the directory and housekeeping needs. For this assignment, set *Volume Size* to 20MB, then select the *Next >* button.

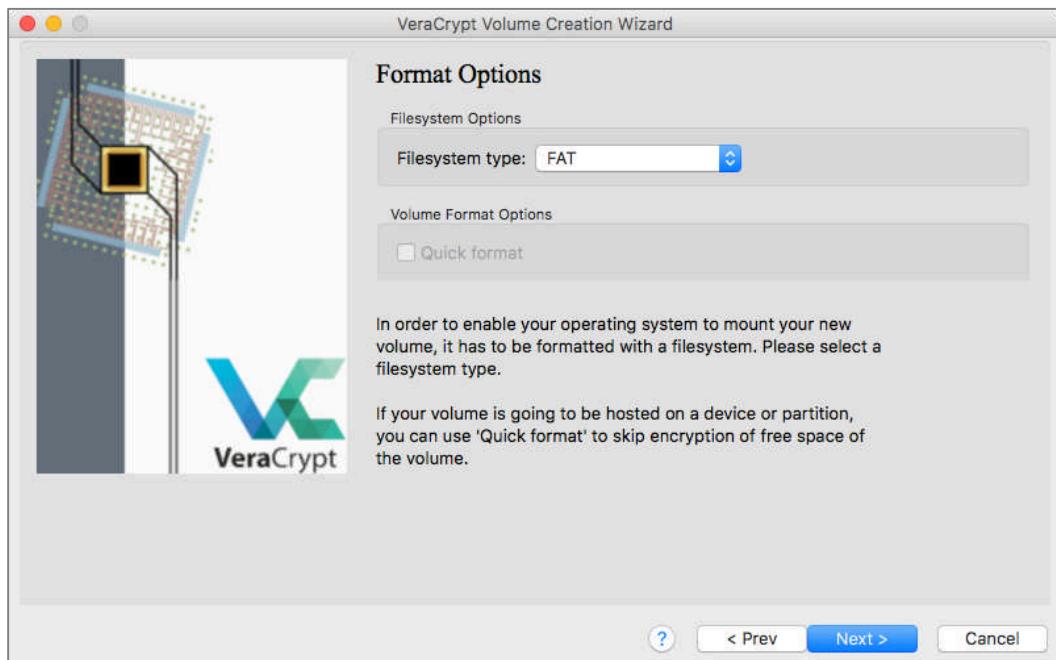


11. At the *Volume Password* window, in the *Password* and *Confirm Password* fields, enter a strong password for the container, and then select the *Next >* button.

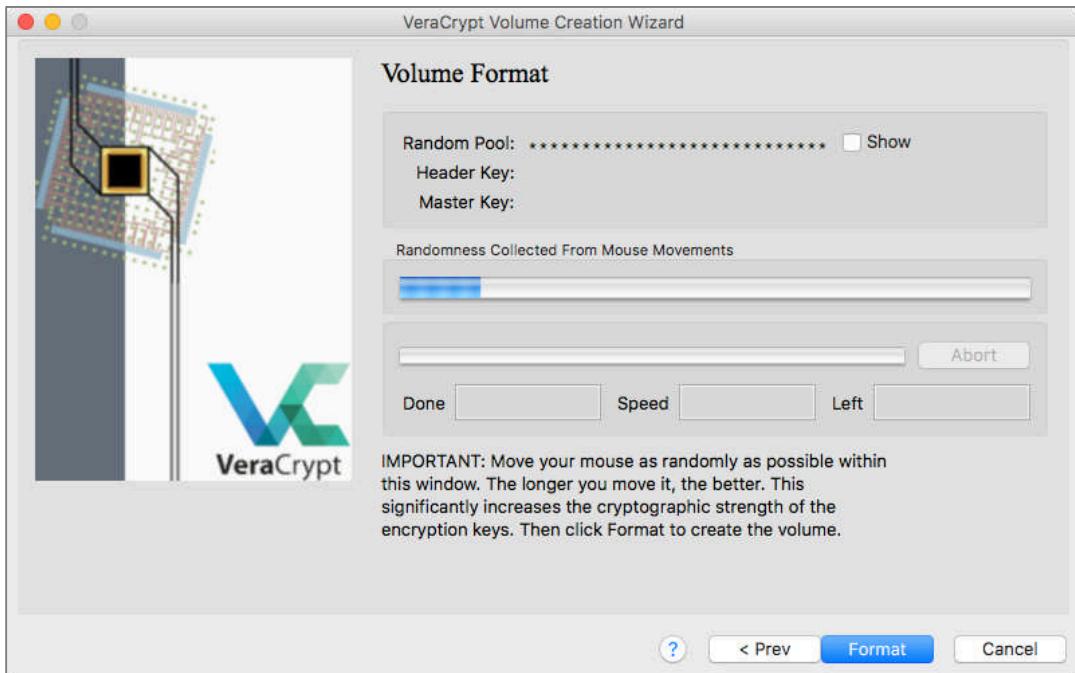


12. At the *Format Options* window, from the *Filesystem type* pop-up menu, select the desired option, and then select the *Next >* button. For this assignment, the *Filesystem type* is **FAT**.

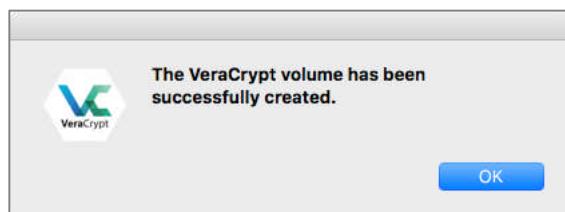
- **FAT** offers full compatibility for Linux and Windows use. macOS can read and write to FAT, but one should not hold macOS applications here as they may not function properly.
- **Mac OS Extended** offers full compatibility for macOS. Linux and Windows users are unable to read this format without the assistance of 3rd-party system add-ons.



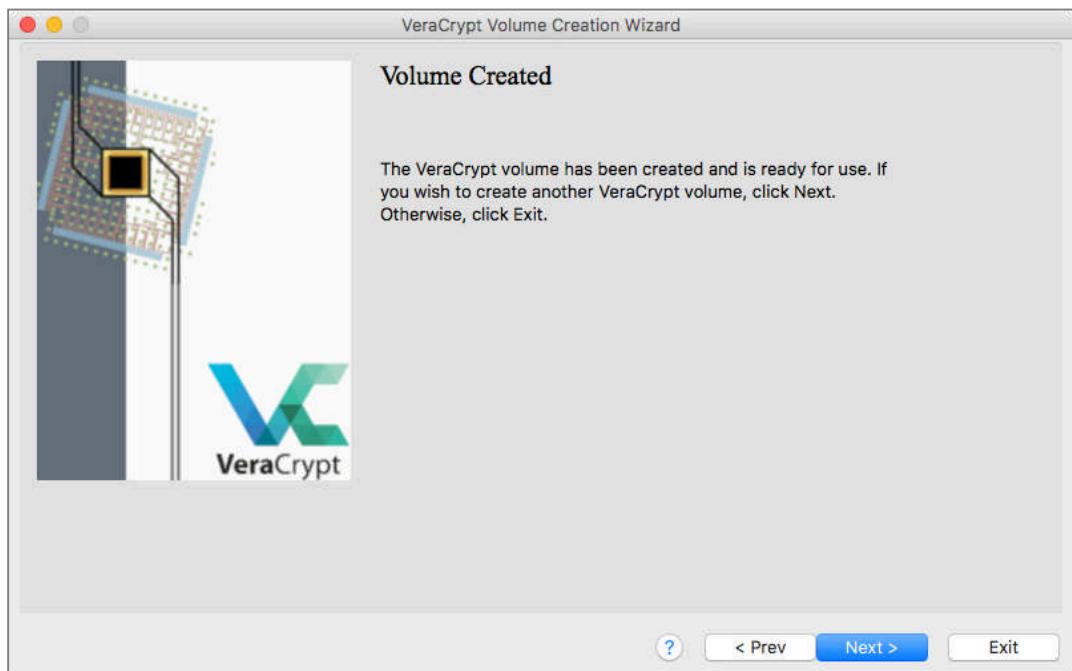
13. At the *Volume Format* window, move your cursor as randomly as possible within the window for at least 30 seconds, and then select the *Format* button.



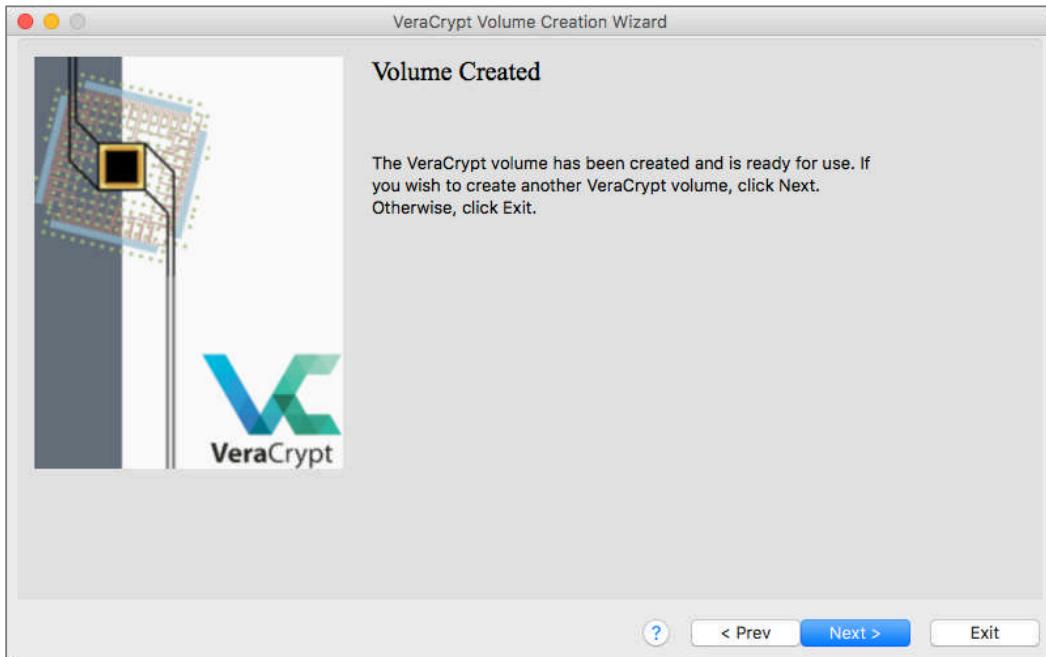
14. Once the container encryption has completed, the *Success* alert appears. Select the *OK* button.



15. At the *Volume Created* window, select the *Next >* button.



16. You will find yourself back at the start of the process, with VeraCrypt assuming that you wish to create another container. You may select the *Cancel* button to exit the process.



17. You will now find, at the location you specified earlier, the encrypted container.

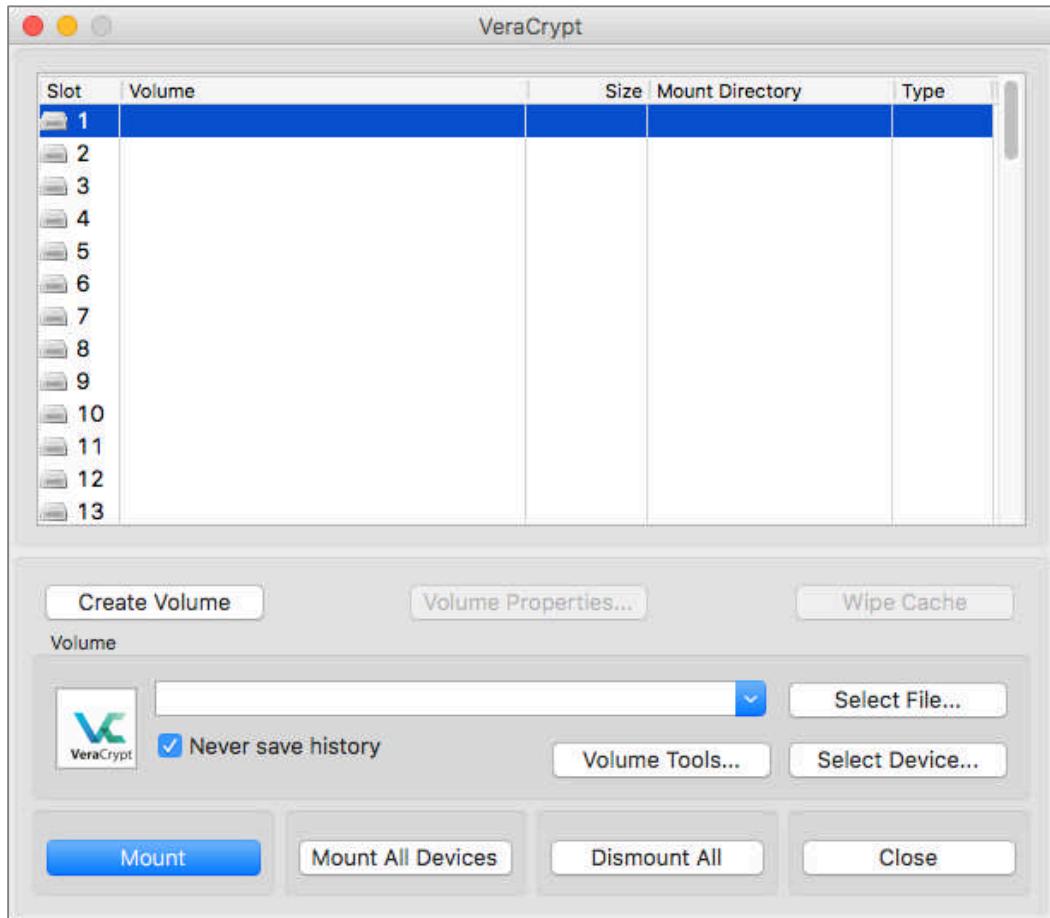


Congratulations, you have created your first truly spy-class encryption!

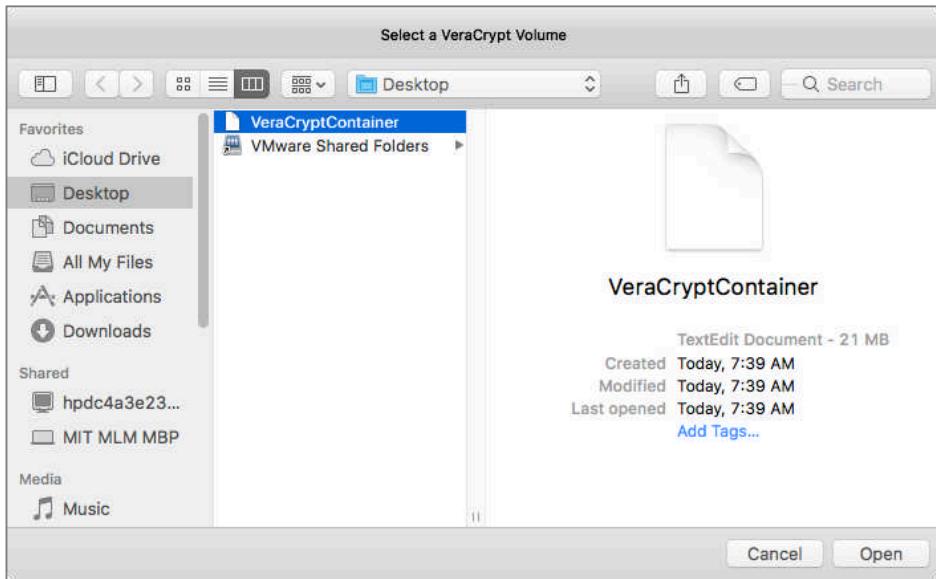
17.6.5 Assignment: Mount an Encrypted VeraCrypt Container

Once you have a VeraCrypt container, you will eventually need to open it to read the contents, add to the container, or make edits to the files. In this assignment, we will mount the VeraCrypt container, which gives you access to all of its data.

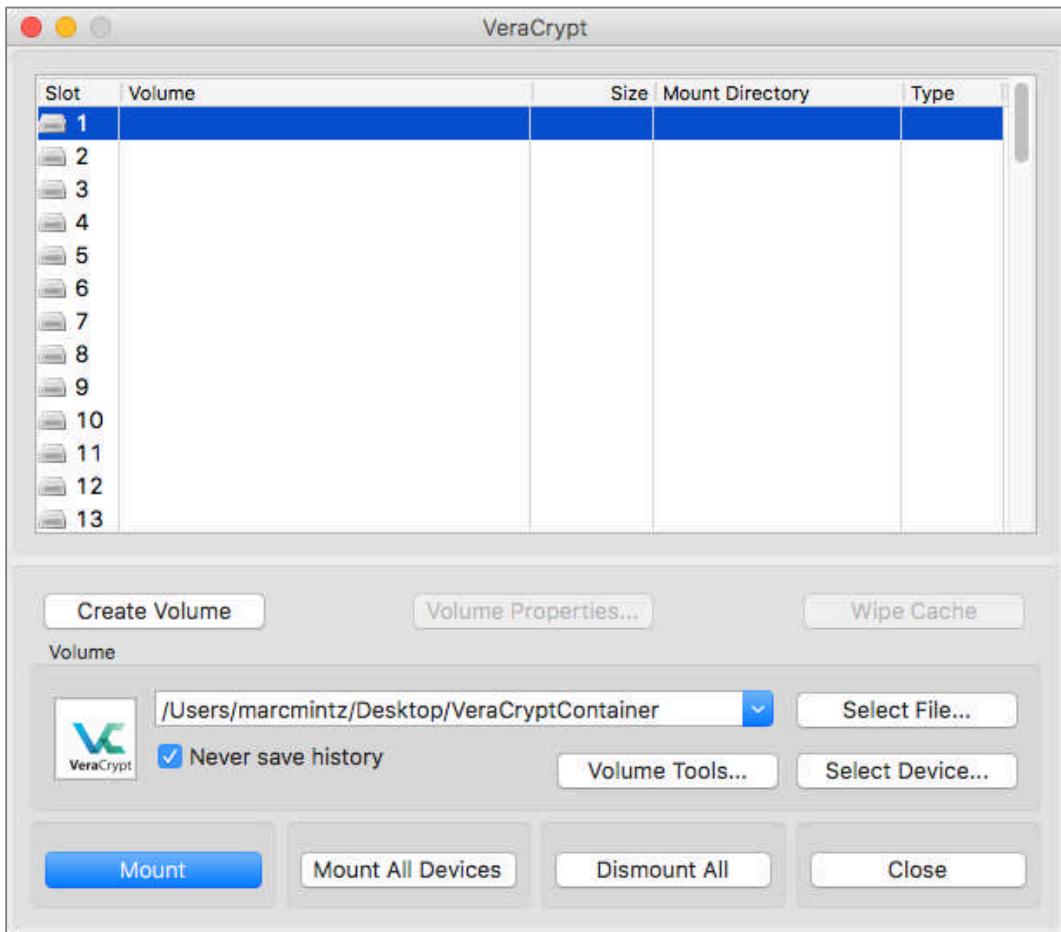
1. Open *VeraCrypt*, and then select one of the *Slot* numbers along the left side bar. This will become the temporary number of the VeraCrypt container to be mounted. Select the *Select File...* button.



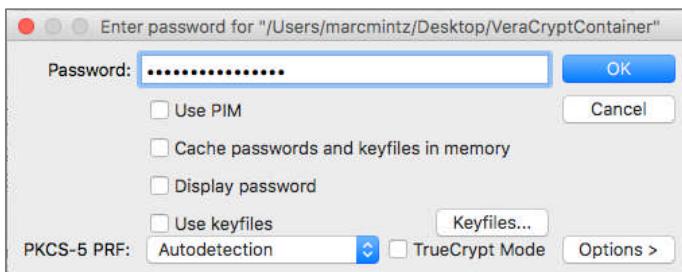
2. Select the *Select File...* button. The standard *Open* window appears. Navigate to the folder holding the target container. Select the container, and then select the *Open* button.



3. In the VeraCrypt window, select the *Mount* button.



4. The *Enter password* window appears. Enter the password assigned to the container, and then select the OK button.



5. On your Desktop you will see the mounted volume, named *Untitled*. Double-click to open the volume.



6. You may rename the mounted volume as you would any other item.
7. You may drag and drop or save files and folder into the container.
8. To unmount, return to the VeraCrypt window, and then select the *Dismount* button. The mounted volume will disappear from the Desktop.

A screenshot of the VeraCrypt application window. The main interface shows a table of mounted volumes. In Slot 1, there is a listed volume with the path "/Users/marc/Desktop/VeraCryptCo...". The size is 19.8 MB, the mount directory is "/Volumes/veracrypt", and the type is Normal. Below the table are several buttons: "Create Volume", "Volume Properties...", and "Wipe Cache". Under the "Volume" section, there is a dropdown menu set to "/Users/marc/Desktop/VeraCryptContainer", a checkbox for "Never save history" which is checked, and buttons for "Select File...", "Volume Tools...", and "Select Device...". At the bottom of the window are four large buttons: "Dismount" (highlighted in blue), "Mount All Devices", "Dismount All", and "Close".

Slot	Volume	Size	Mount Directory	Type
1	/Users/marc/Desktop/VeraCryptCo...	19.8 MB	/Volumes/veracrypt	Normal
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				

17 Documents

OMG... You *really* are doing high-end security work now! This container may be copied to a thumb drive, optical disc, DropBox, Google Drive, or other Cloud-based storage, and remain secure.

17.7 Review Questions

1. Microsoft Office 2016/Office 365 use AES 256-bit encryption. (True or False)
2. Microsoft Office for Mac is limited to a maximum of _____ characters for the encryption password.
3. Adobe Acrobat 9 and higher use _____ encryption.
4. Disk Utility can create encrypted disk images readable by both macOS/OS X and Windows. (True or False)
5. The Zip protocol can create very secure encrypted archives. (True or False)
6. VeraCrypt can create encrypted containers readable by Android, iOS, macOS/OS X, and Windows. (True or False)

18 Voice, Video, and Instant Message Communications

Surveillance technologies now available—including the monitoring of virtually all digital information—have advanced to the point where much of the essential apparatus of a police state is already in place.

- Al Gore¹

¹ https://en.wikipedia.org/wiki/Al_Gore

18.1 Voice, Video, and Instant Messaging Communications

Every time you send or receive a text message, phone call, or videoconference on your computer or mobile device, the conversations and metadata are stored by third parties. The carriers (Verizon, AT&T, etc.) for each party have the ability to intercept any traffic that crosses their networks, which may also extend to any third parties that work with your carrier, such as contractors, or subsidiaries.

Aside from the telecom companies themselves, your local and federal government are monitoring in dragnet style snooping.

Online voice & video services such as Facebook messenger and Google Hangouts are more secure in transit between your computer or device and their servers, but because your conversations are stored on their hardware without end-to-end encryption, there is no guarantee of privacy.

So how can you communicate easily and securely using your computer and mobile device? The common options are:

- *FaceTime*: If you are to videoconference between another iPhone, iPad, or macOS/OS X user, you can use the built-in FaceTime app. FaceTime is fully encrypted, Apple does not have a back door, so neither does a criminal or government.
- *Skype*: Skype is Microsoft's premier video conferencing solution that offers voice, video chat and desktop sharing for up to 25 people in a group. Recently setting a record for over 35 million people online simultaneously, Skype is one of Microsoft's core technologies, and is bundled into Windows, XBOX, and Windows mobile.

It is well known that Skype allows Microsoft and several major governments to listen in on conversations as well as the potential to gain access to files and metadata on the user's computer. As a result, Skype should be treated as a completely insecure service that any number of organizations and governments have access to.

- *Google Hangouts:* In the past several years, other proprietary alternatives to Skype have surfaced, most notably is Google Hangouts. Hangouts tightly integrates Google's social network, Google+, along with Chat, Screen Sharing, and integration with other Google services into a plugin based application. Hangouts is free, and supports up to 10 users simultaneously with any free Google account. Google Business accounts support up to 15 users.

Like Skype, Hangouts has many privacy implications. Google Hangouts doesn't have end-to-end encryption, and in a recent online interview with Google's director for law enforcement and information security, it was revealed that Governments, law enforcement and Google itself have access to your chats, and calls.

Secure Alternatives

If you are interested in cross-platform, end-to-end encrypted, voice and video conferencing solutions, there are several alternative services that provide encrypted calls and work with many existing open source clients.

Wire² is our choice for end-to-end encrypted voice, video, instant messaging, and group communications. Wire provides end-to-end encrypted communications between macOS/OS X, Android, iOS, and Windows. Although not open source, the developers have made their encryption and privacy protocols open for inspection.

² <https://wire.com/>

18.2 HIPAA Considerations

If your instant messaging needs include HIPAA compliance (meeting the Joint Commission guidelines), then the rest of this chapter does not apply to you.

HIPAA is concerned about securing *Protected Health Information* (PHI) from leakage, but at the same time, requires that instant messaging have an audit trail. This requires that all messaging be logged to a centralized server. Should the need arise, the log can be reviewed.

In addition, HIPAA requires that the vendor be willing to sign a *Business Associate Agreement*³ (BAA). As doing so puts the vendor at some level of potential liability should their service or software be found to be responsible for leakage of protected health information, you will not find free or inexpensive software that meets HIPAA compliance requirements.

For most readers and students of this work, the desire is to leave *no* record of an encrypted conversation. This is a far more difficult task, with very few options. And most of our readers have no need of a BAA.

Should you have the need for HIPAA compliance, you will have a few dozen options to choose from.

³ <http://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html>

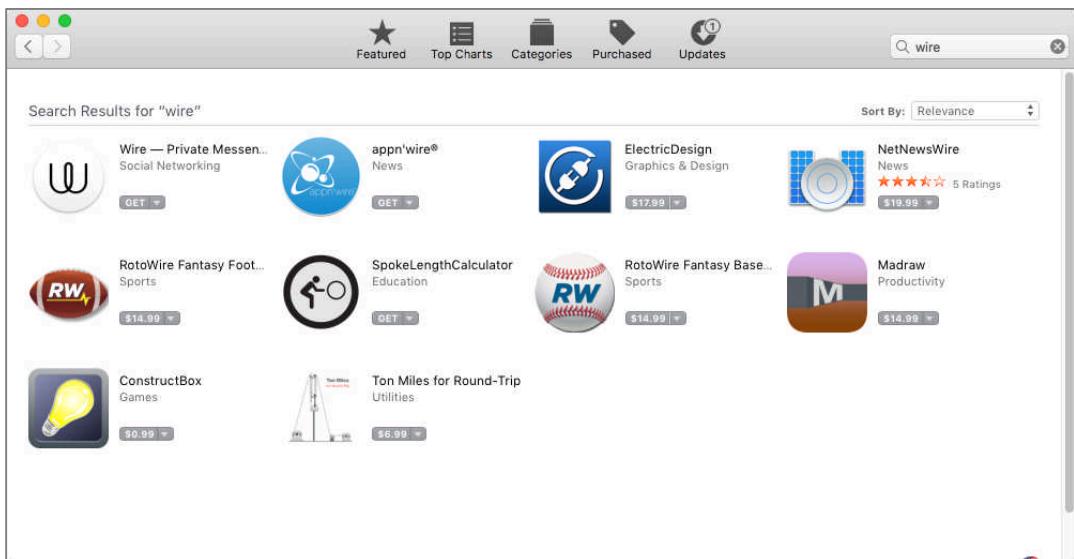
18.3 Wire

Wire is a free platform for peer-to-peer (no centralization) and group secure, end-to-end encrypted communications using instant messaging, voice, and video.

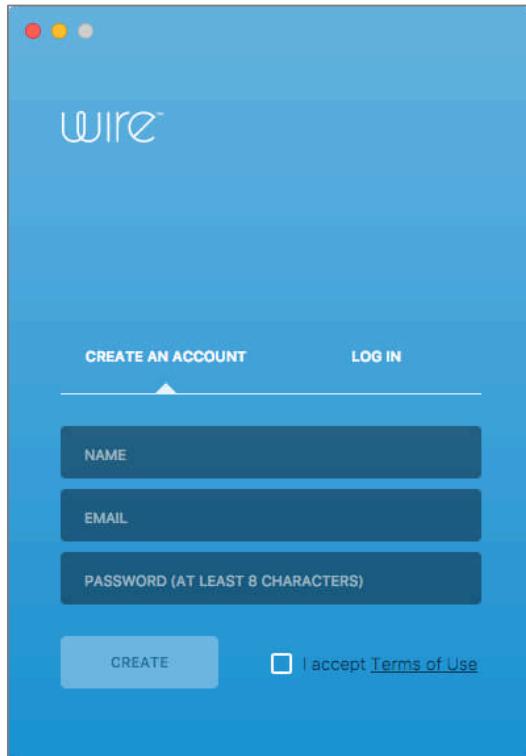
18.3.1 Assignment: Install Wire

In this assignment you will download and install the Wire client for macOS. This will allow you to make fully secure, encrypted instant messaging, voice calls, and video conferences with friends and business associates.

1. Open the *App Store* app, and then search for *Wire*.
2. Click the *Get* button for *Wire—Private Messenger*, and then click *Install App*.

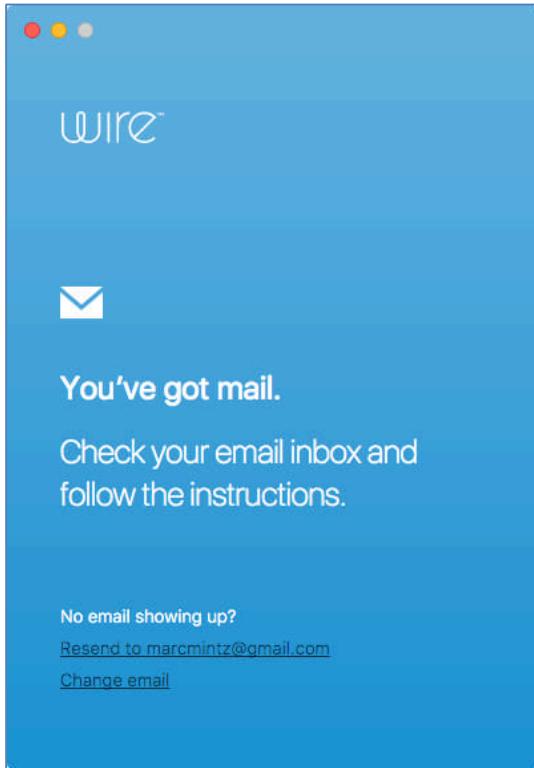


- When the download completes, open Wire. The Wire home window appears.



- Enter your *Name*, *Email*, create a strong *Password*, enable the *I accept Terms of Use*, and then click the *Create* button.

5. At the *You've got mail* window, check your email.



6. You will have an email from Wire. Click the *Verify* button.

The screenshot shows an email from Wire. The subject line is "Wire". The recipient is "Marc Louis Mintz" with the message "Your Wire Account". The email body starts with a large blue 'W' logo, followed by "wire.com". It greets the user with "Hello," and states that "marcmintz@gmail.com" was used to create a Wire account. It asks the user to verify their identity as "Marc Mintz". A prominent blue "VERIFY" button is centered below the text. Below the button, a note says "Click the button above to verify your address. You won't be able to use Wire until you do." It also provides a link for users who can't click the button: "<https://wire.com/verify/?key=ckCHTwCjYHu8OGy-P3BP1GNBRGcR3Ktq0QcPdERNAE=&code=uwlSpl3LxdVdmUPbX4nQU6ajaG8AKKv>". At the bottom, there are links for "Privacy Policy · Report misuse" and "© Wire Swiss GmbH. All rights reserved."

Wire
To: Marc Louis Mintz
Your Wire Account

wire.com

Hello,

marcmintz@gmail.com was used to create a Wire account. We want to verify that you are indeed **Marc Mintz**.

VERIFY

Click the button above to verify your address. You won't be able to use Wire until you do.

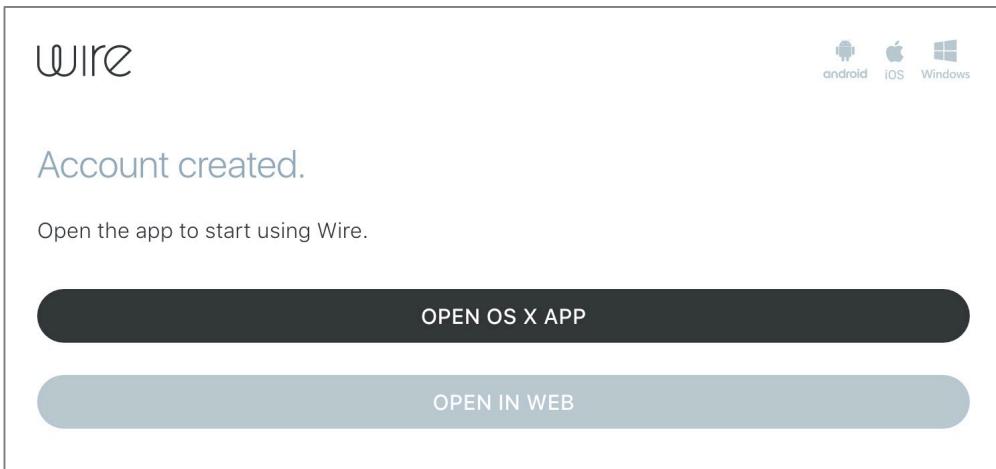
If you can't click on the button, use this link:

<https://wire.com/verify/?key=ckCHTwCjYHu8OGy-P3BP1GNBRGcR3Ktq0QcPdERNAE=&code=uwlSpl3LxdVdmUPbX4nQU6ajaG8AKKv>

If you didn't create a Wire account using this email address, please [contact us](#).

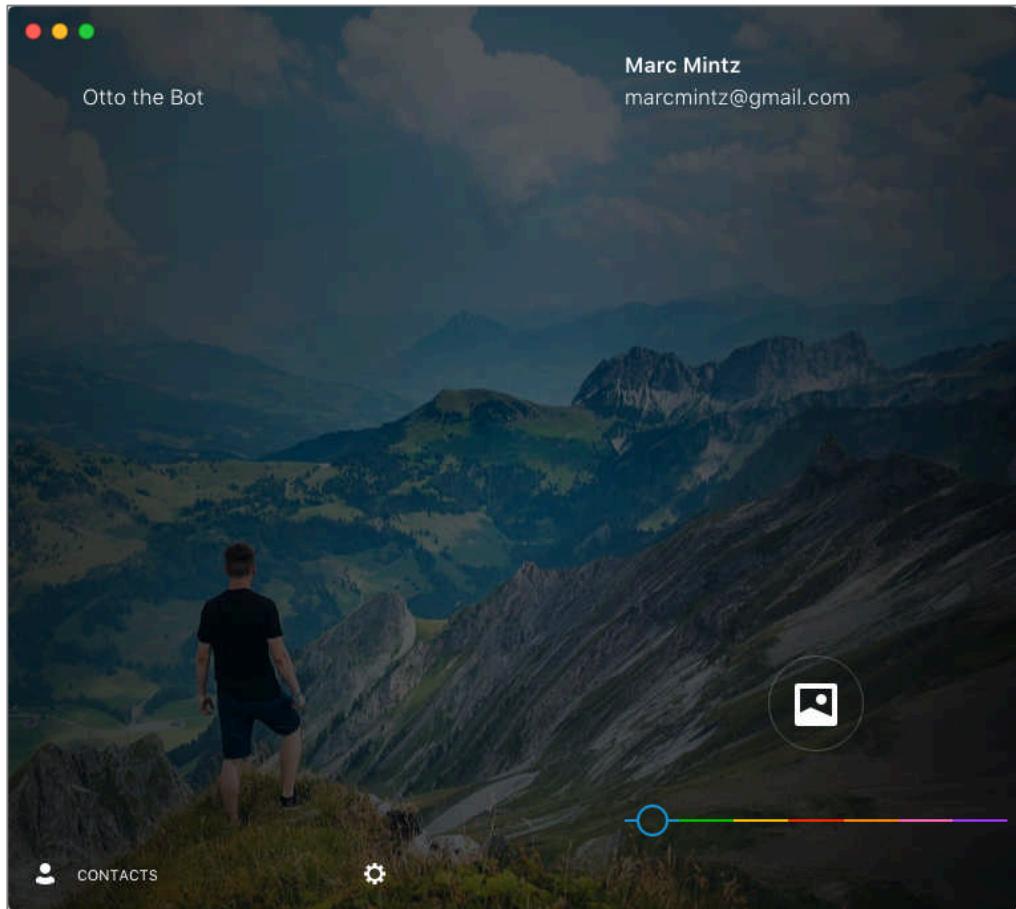
[Privacy Policy](#) · [Report misuse](#)
© Wire Swiss GmbH. All rights reserved.

7. At the *Verified* window, select *Open OS X App* (or *Open in Web* if you prefer to use a web interface.)



8. Wire opens, asking if you would like to change the background image. For now, select *Keep This One*.

9. The Wire main window opens.

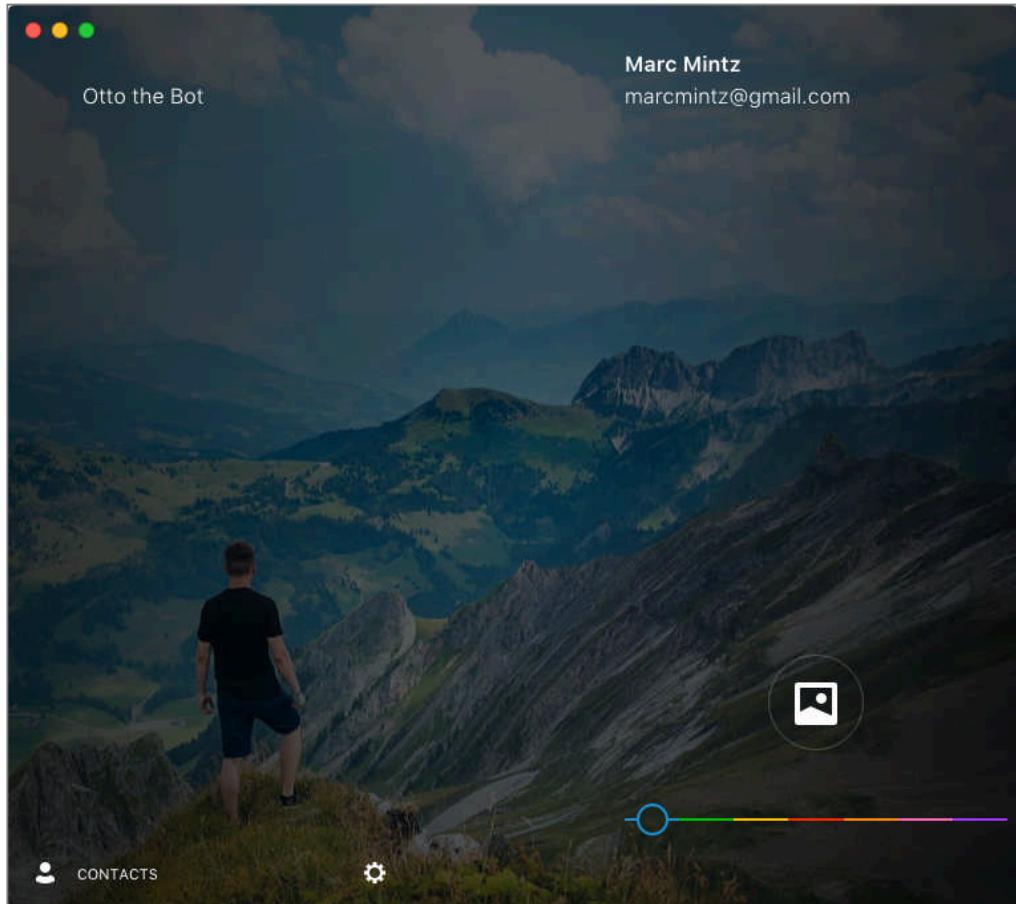


18.3.2 Assignment: Invite People to Wire

Before you can communicate with someone else using Wire they must also have that app installed.

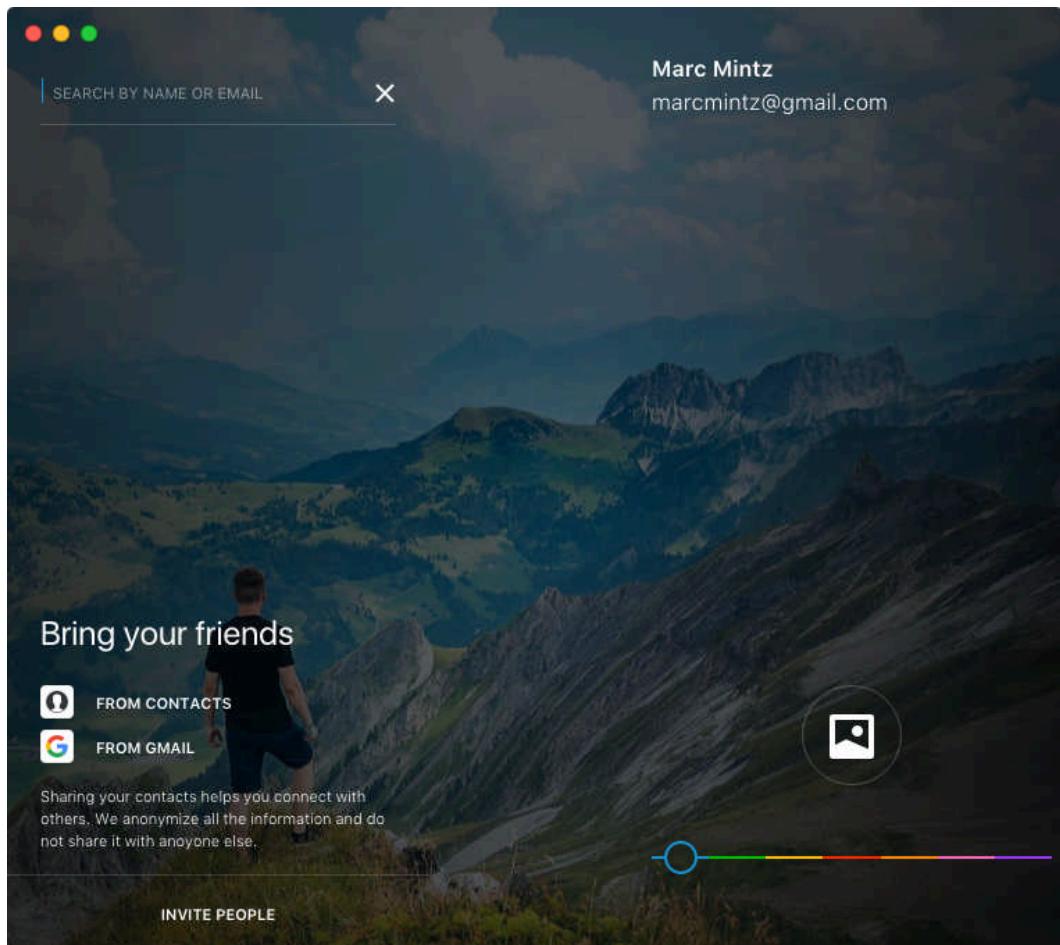
In this Assignment you will invite someone to install Wire and create an account.

1. Open Wire. The home window appears.

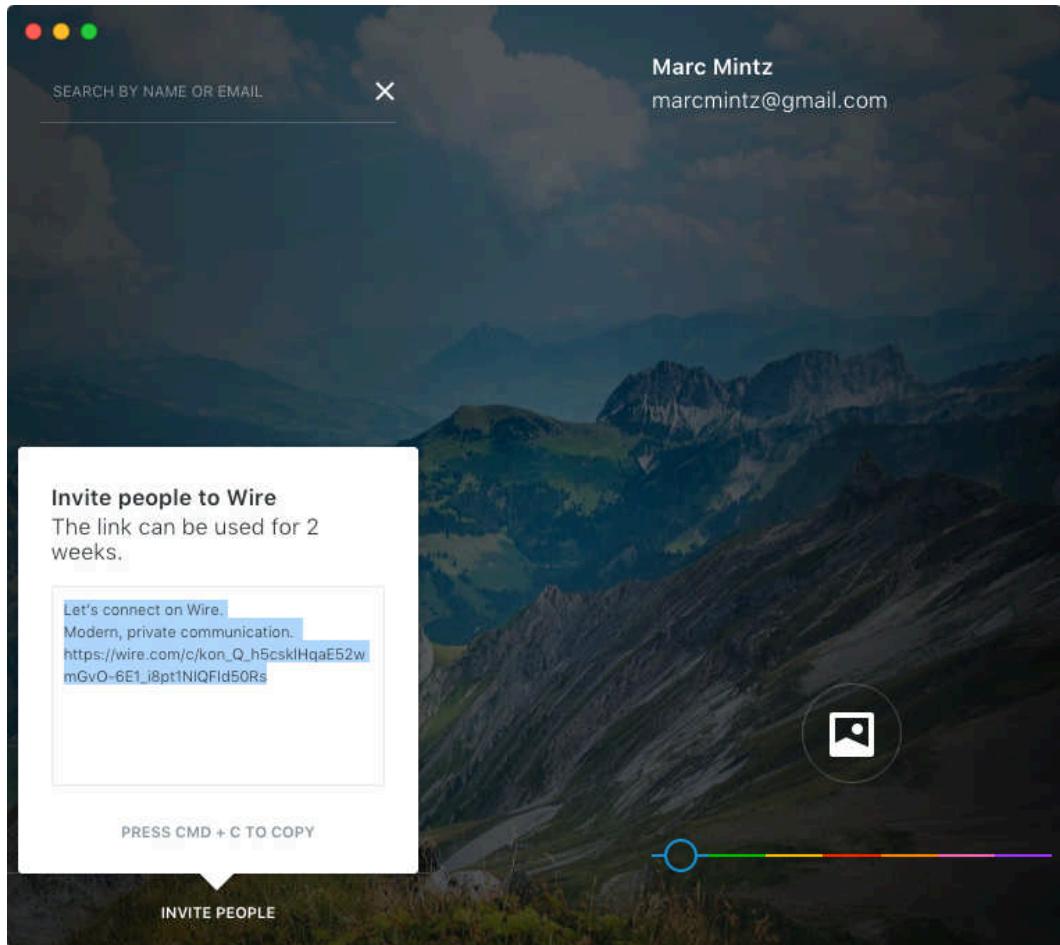


2. Click on *Contacts* in the bottom left corner.

3. Click on *Invite People*.

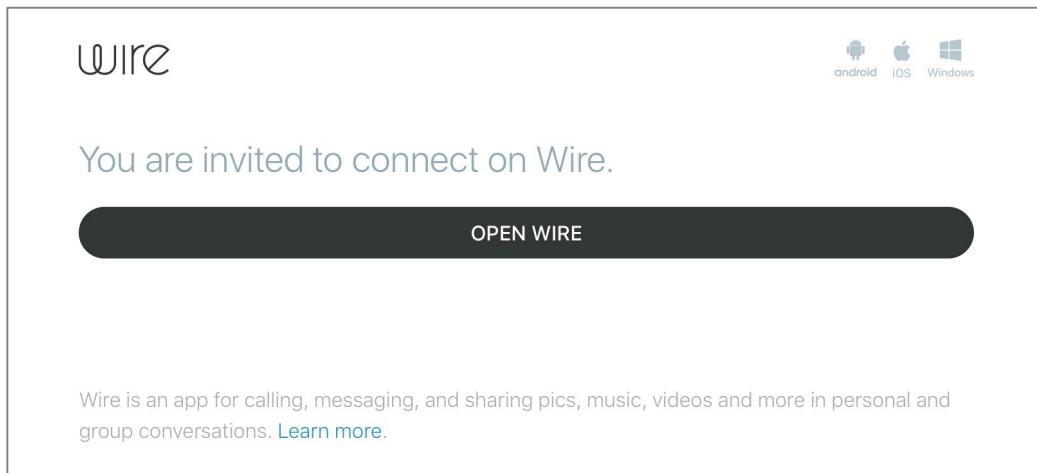


4. From the pop-up window, copy the selected text.



5. Open your email app, create a new email addressed to everyone with whom you would like to securely communicate, paste the link in the body of the message, and then send the email.

6. When the recipient(s) received your email, and then click on the link, their browser will open to Wire, inviting them to connect with you.
 - Note: The web-based version of Wire only works on Google Chrome, Mozilla Firefox, Opera, and MS Edge. Safari and Explorer users will have to open a different browser.



7. When the recipient clicks the *Open Wire* button, they are taken to the Wire *Create An Account* page.

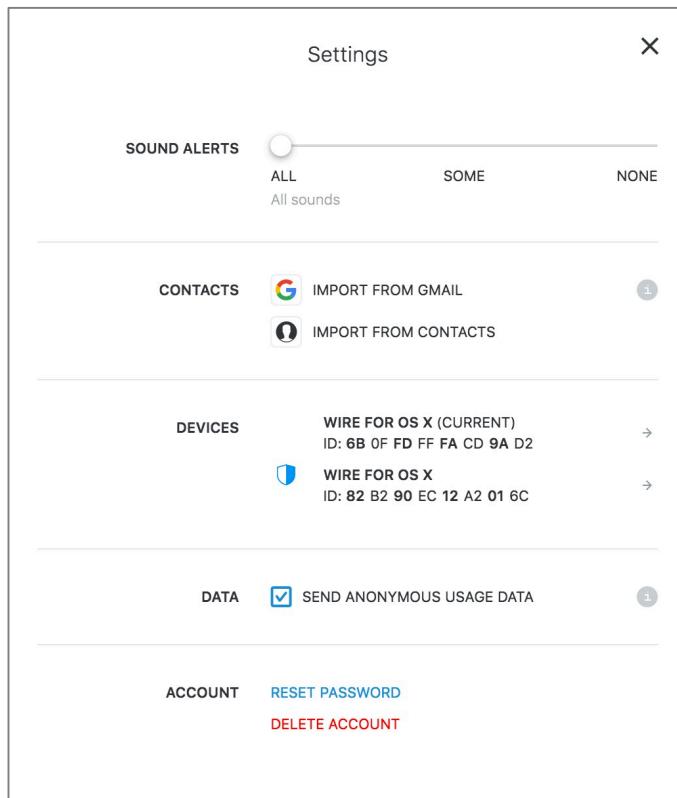
Once the other person has Wire, the two of you may communicate securely.

18.3.3 Assignment: Import Contacts Into Wire

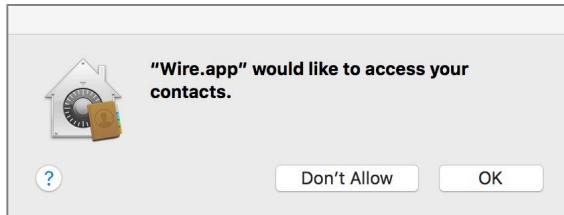
Wire allows you to import your contacts into the Wire contacts database. All you need is someone's phone number to reach out to them with Wire.

In this assignment you will import your contacts into Wire.

1. Select the *Wire* menu > *Preferences*.



2. Select from where you wish import your contacts. For this assignment, I'm selecting *Import From Contacts*. At the dialog box, select the *OK* button.



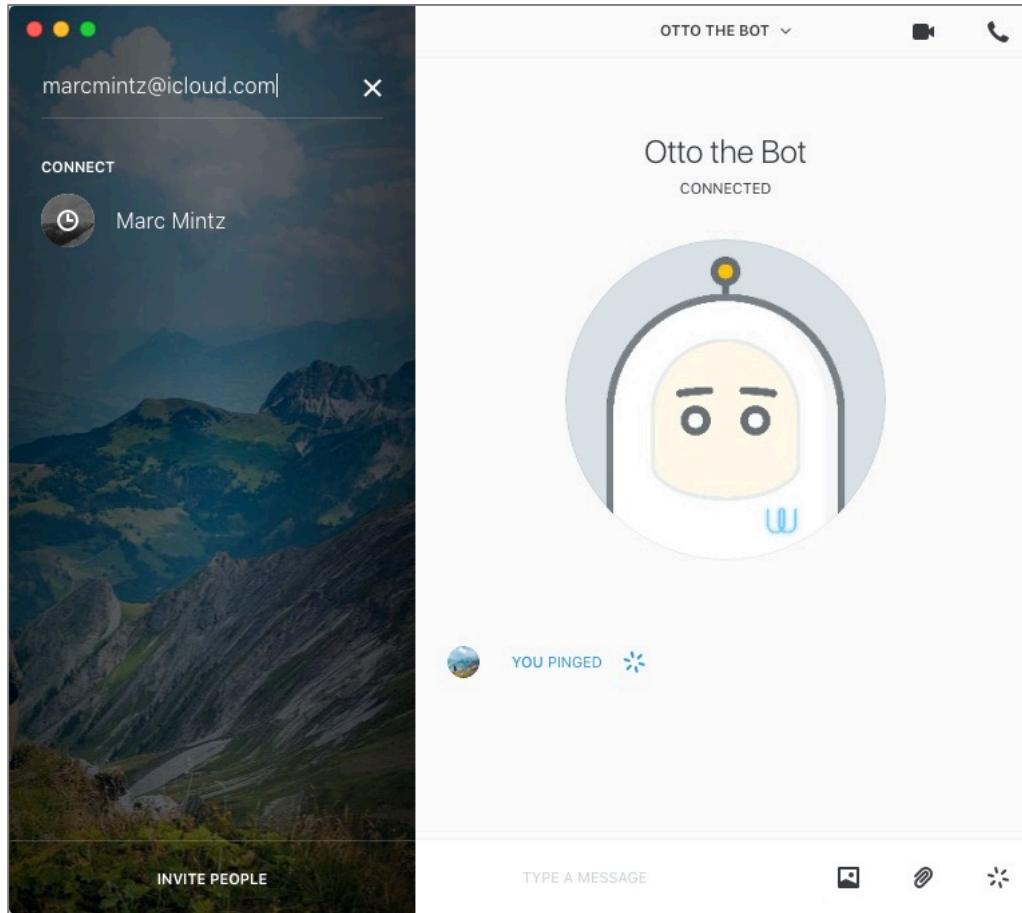
That's it! Your Wire.app is set up and ready to go

18.3.4 Assignment: Secure Instant Message a Wire Friend.

In this assignment, you will instant message your new Wire friend.

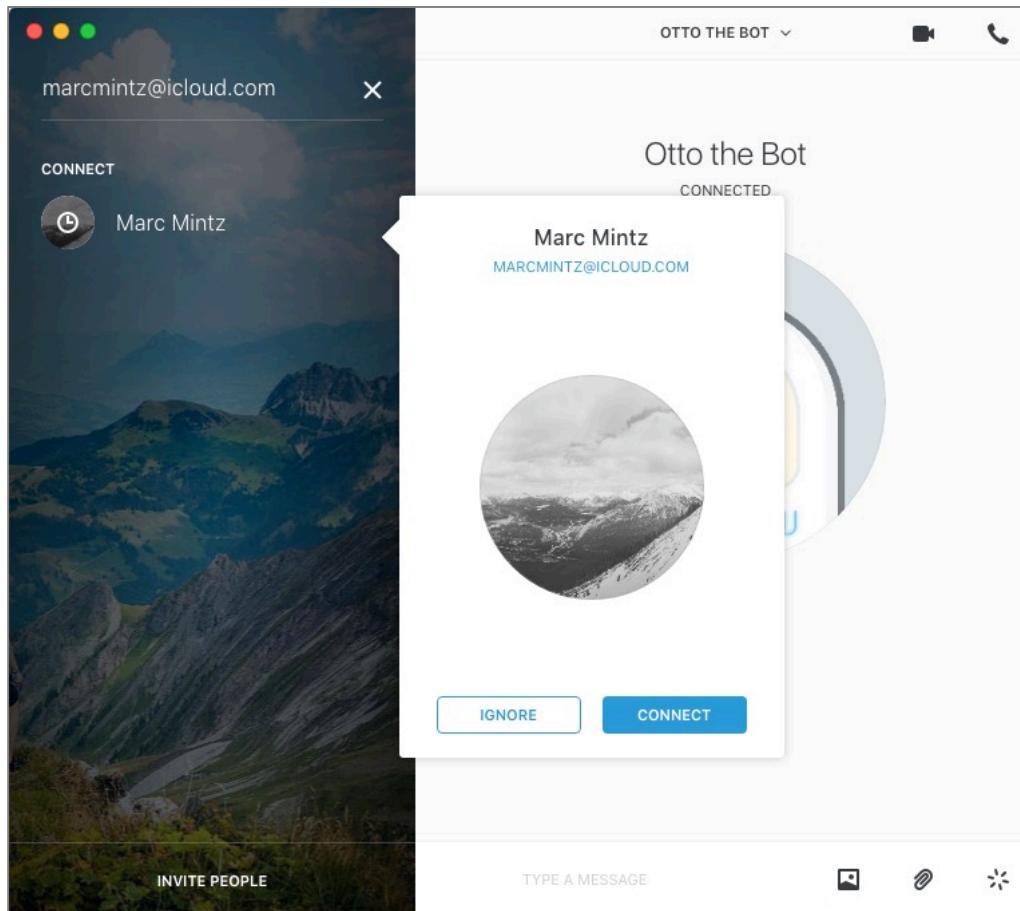
1. Open the *Wire.app*.
2. From the side bar, select a friend. If you don't currently have any friends added, you can search for them by either name or email address. For this assignment, that will be step taken. In the top left corner of the app window or screen, enter the name or email address of the person you wish to communicate with. In this example, I'm connecting to *marcmintz@icloud.com*. Once the name or email address is entered, tap the

Enter or Return key. Any matching Wire users will display below. In this example, the Wire user just happens to share my name.

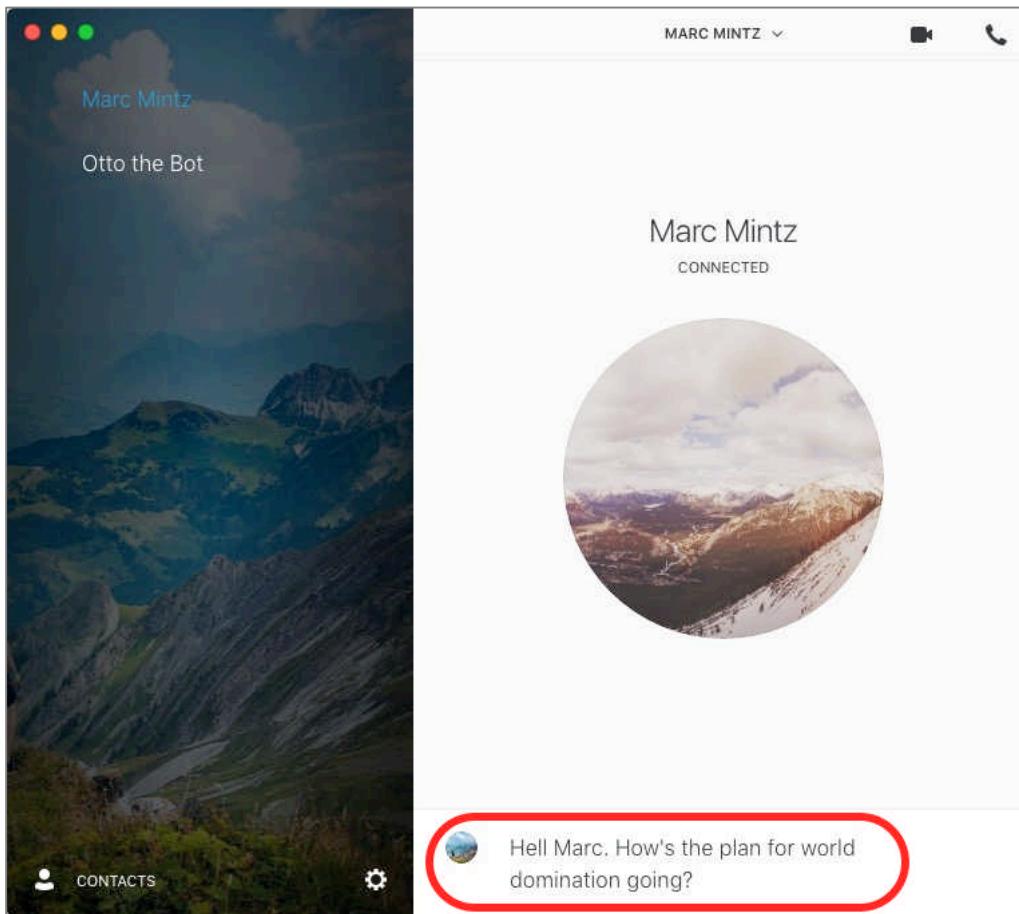


3. Click on the desired Contact.

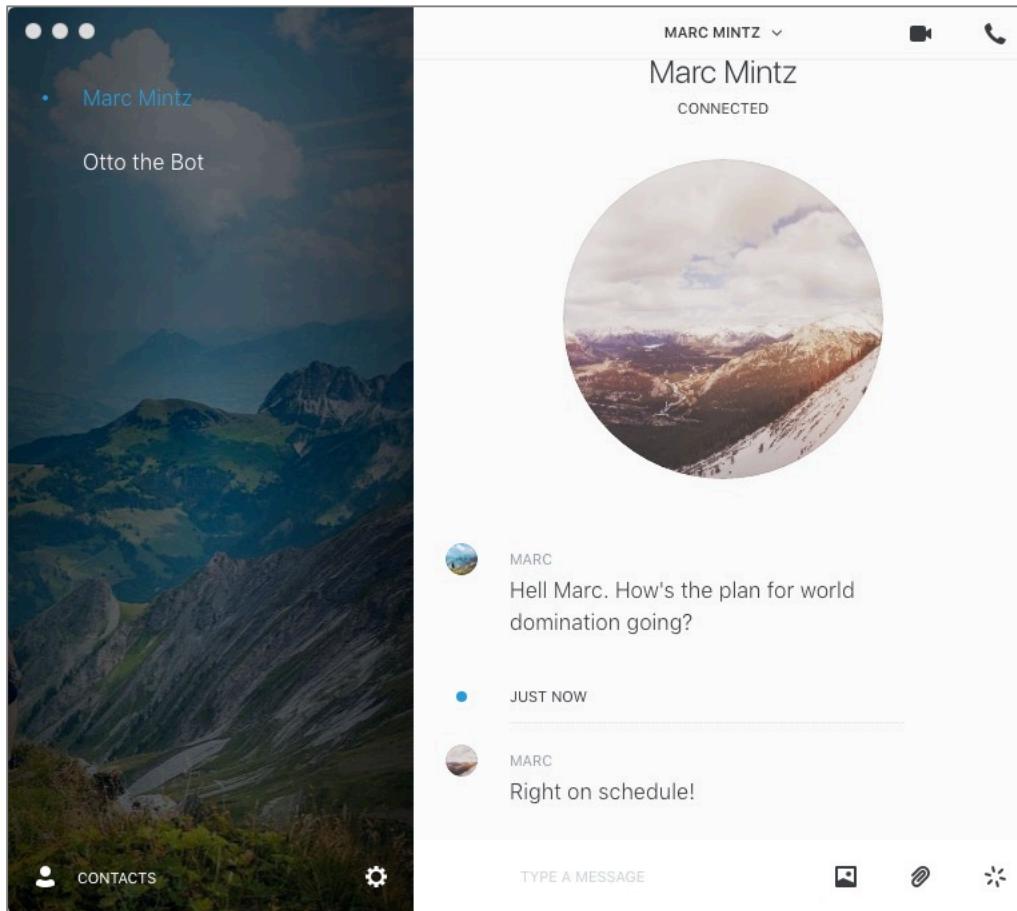
4. In the pop-up window with their name and email address, click the *Connect* button.



5. In the *Text* field at the bottom center of *Wire*, enter the message to be sent, and then tap the *Enter* or *Return* key.



6. Your message will appear immediately in the message field of your contact. In this example, the contact is running Wire in a web browser, and has entered their reply.

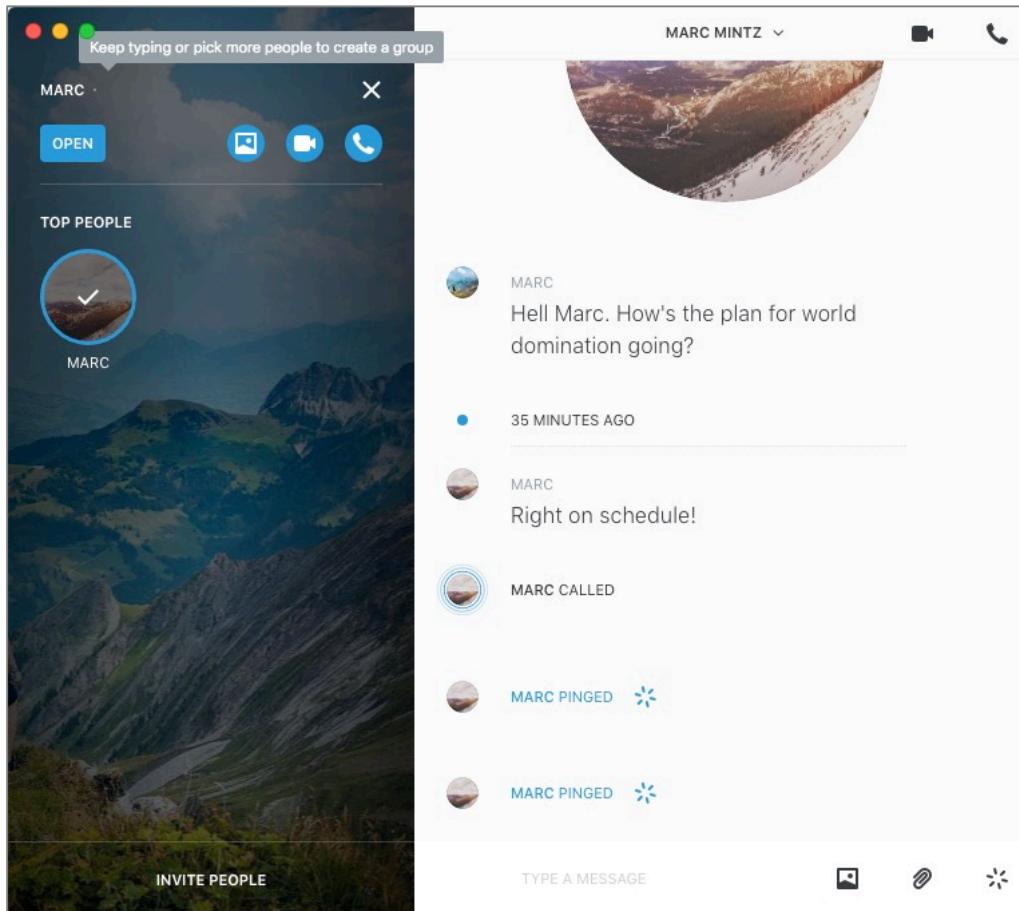


18.3.5 Assignment: Secure Voice Call a Wire Friend

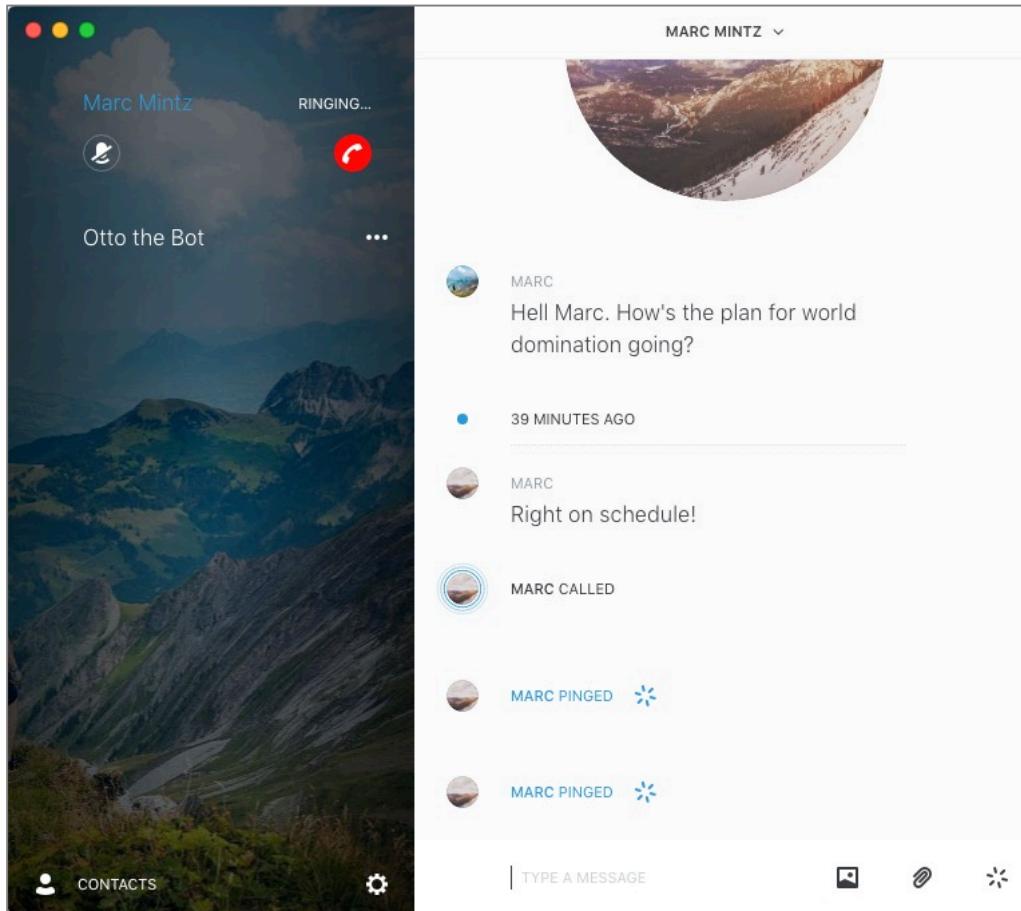
In this assignment, you will make a secure, encrypted voice call to one of your Wire friends.

1. Open *Wire.app*.
2. Select a Wire contact to call.

3. If this is a Wire contact you have communicated with before, there will be icons to instant message, video conference, or call just under and to the right of their name in the sidebar.



4. Click the *Phone* button to call. You will see a *Call ringing* message.



5. On your friends Wire device, they will hear their device ringing, and a Call invited message in Wire. if they wish to answer, they click the Phone icon.

6. The two of you can now speak in complete privacy—even better than Maxwell Smart's Cone of Silence⁴.



7. To disconnect, either party just clicks the Phone icon.

18.3.6 Assignment: Video Conference With a Wire Friend

Video conferencing works exactly the same with Wire as a voice call, except to click the *Video* button instead of the *Phone* button.

⁴ https://en.wikipedia.org/wiki/Cone_of_Silence

18.4 Review Questions

1. Instant messages sent via *Messages* between iOS and macOS are securely encrypted. (True or False)
2. There are currently no cross platform secure instant messaging applications available. (True or False)
3. When using Facetime between iOS and macOS computers, the communications are fully secure. (True or False)
4. Skype is fully secure between any devices. (True or False)
5. Google Hangouts has end-to-end encryption. (True or False)

19 Internet Activity

If you have built castles in the air, your work need not be lost; that is where they should be. Now put the foundations under them.

–Henry David Thoreau¹, *Walden*

- **Special Note:** We are most grateful to our VPN provider of choice for offering *Practical Paranoia* readers and students a special discount on their services. When registering for VPNArea, in the *Coupon* field, enter ***pparanoia*** to receive your discount at checkout.

¹ https://en.wikipedia.org/wiki/Henry_David_Thoreau

19.1 VPN–Virtual Private Network

In case you have been sleep reading through this book, let me repeat my wake-up call: *They are watching you on the Internet.* They may be the automated governmental watchdogs (of your own or another country), government officials (again, of your own or another country), bored staff at an Internet Service Provider or broadband provider, a jealous (and slightly whackadoodle) ex, high school kids driving by your home or office or sitting on a hill several miles away, or criminals.

Regardless, your computer and data are at risk.

Perhaps one of the most important steps that can be taken to protect you is to encrypt the entire Internet experience all the way from your computer, through your broadband provider, to a point where your surfing, chat, webcam, email, etc. cannot be tracked or understood. This is accomplished using a technology called *VPN–Virtual Private Network*².

² http://en.wikipedia.org/wiki/Virtual_private_network

19.2 Gateway VPN

There are two fundamental flavors of VPN. The most common is called a *gateway* VPN (mesh VPN is discussed later.) Historically, gateway VPN involved the use of a VPN appliance resident at an organization. Telecommuting staff are able to use the gateway so the Internet acts like a very long Ethernet cable connecting their computer to the office network. In addition, all data traveling between the user's computer and the gateway is military-grade encrypted. The downside to this strategy is that these appliances are relatively expensive (from \$600 to several thousand dollars), and they require significant technical experience to configure correctly.

In greater detail the concept works like this:

1. Your computer has VPN software installed and configured to connect to a VPN server at the office. This server is connected to your office network. macOS/OS X comes with VPN software built into the Network System Preferences that works with many of the commercially available VPN servers, including the most popular—Cisco. Other VPN servers require their own proprietary client software to be installed.
2. On your computer you open the VPN software and instruct it to connect to the VPN server. This typically requires entering your authentication credentials of user name and password, along with a long key.
3. The VPN server authenticates you as an allowed account and begins the connection between itself and your computer.
4. As you send data from your computer to the network connected to the VPN server (typically the regular business network), all of it is military-grade encrypted. When the data is received at the VPN server or at your computer, the VPN software decrypts it.
5. Once your data reaches the VPN server, it is then forwarded to the appropriate service on your organization's network (file server, printer, mail server, etc.)

Although this may sound a bit complex, all a user must do is enter a name, password, and key. Everything else is invisible. The only indicator that anything is

different is that speed slower than normal. This is due to the overhead of encryption/decryption process.

We can use this same strategy so that instead of securely exchanging data with our office server, we can securely surf the Internet. The workflow is just slightly different:

1. Your computer has VPN software configured to connect to a VPN server that is not associated with your office, but is just another server “on the Internet.”
2. On your computer you open the VPN software and instruct it to connect to the VPN server. If you are using our recommended software, it is pre-configured with all the settings necessary—nothing much more to do but launch.
3. The VPN server authenticates you as an allowed account and begins the connection between itself and your computer.
4. As you surf the web, all data is military-grade encrypted. When the data is received at the VPN server or your computer, the VPN software decrypts it.
5. Once your data reaches the VPN server, it is then forwarded to the appropriate service on the Internet.

Using this strategy (a VPN Internet server), all of your Internet traffic is military-grade encrypted between your computer and the VPN server. It is not possible to decipher any of your traffic (user names, passwords, data) or even the type of data coming and going.

One downside is that once the data exits the VPN server, it is readable. However, your data is intermingled with thousands of other users data, making the process of tweezing out your data a task that perhaps only the NSA can accomplish.

Another concern is that some VPN providers maintain user activity logs. This is law in most countries, so that government agencies are able to review who is doing what through the VPN. Ideally, you want to work only with a VPN provider operating in a country doesn’t require logs, and in fact, do not keep logs.

There are thousands of VPN Internet Servers available. Most of them are free. I don’t recommend using the free services for two reasons:

1. You get what you pay for (typically here today, gone tomorrow, unstable, etc.)

2. You don't know who is listening at the server side of things. Remember, your data is fully encrypted up to the server. But once the data reaches the server on the way to the Internet, it is readable. There needs to be a high degree of trust for the administration of the VPN server. I see no reason to have such trust with free services.

When determining the best VPN provider for your use, there are some key variables to look for:

- **Speed.** How fast is your Internet experience? Using VPN introduces a speed penalty due to the encryption/decryption process, as well as the need to process all incoming and outgoing packets through a server instead of point-to-point. VPN providers can reduce this penalty in a number of ways, including; faster servers, reducing the clients:server ratio, better algorithms, filtering content to remove advertisements and cookies, and faster server internet connections.
- **Logs.** Are logs kept on client activities? In many countries it is required by law that all Internet providers maintain logs of client activities. If so, although the logs may not record *what* you were doing, they keep a record of *where* you traveled. It is ideal to have a VPN provider that keeps no logs whatsoever.
- **Support.** VPN adds a layer of complexity to your Internet activities. Should something not work correctly, you don't want to be the one troubleshooting. Ideally, your VPN provider has 24/7/365 chat support. Even better if they offer telephone support.
- **Cross-Platform Support.** Most of us have more than one device. Perhaps a Windows and macOS/OS X computer, an Android phone, and an Apple iPad. It would be madness to have to use a different VPN product for each of these. Look for a provider that supports all of your current and potential devices.
- **Multi-Device Support.** Most, but not all, providers now offer from 3-5 concurrent device licensing. This allows your VPN service to be operational on all of your devices at the same time. Providers that offer only single-device licensing may be quite costly should you have multiple devices.
- **DNS-Leak Protection.** Although VPN encrypts all data that comes and goes from your device, before you can reach out to the Internet to connect to your

email, a website, or text, your device must connect to a DNS server for guidance on where to find the mail, web, or text server. If you are using your default DNS server (typically one by your Internet broadband provider, data between your system and the DNS server is not encrypted *and* is recorded. It is ideal if your VPN provider offered their own DNS servers. Using this strategy, then the data between your device and the DNS server is now either encrypted, or is not logged.

Right about now you may be asking yourself: *If VPN is so great, why doesn't everyone know about and use it?*

Great question! As with everything else in life, there is bad that comes with the good. Each person needs to weigh the pros and cons for each situation for themselves. I personally *always* have VPN active, but I'm *always* doing work! I hope you don't have that disease. There are two primary downsides to VPN. It slows down your Internet performance. Often by 50% or more. If all I want to do were to stream Netflix to my computer, I'd turn VPN off to reduce the pauses induced by a slow Internet connection. Second, if you have selected a VPN server outside of your home country, you may have unintended consequences due to the *Internet* servers thinking you are resident in that other country. For example, Google searches will be displayed in the language native to that country. This is actually considered a feature of the *Proxy Server* function built into VPN, and is used by those in restrictive countries to view news across the border that are normally filtered out by their home country.

19.3 VPNArea

One of our favorite VPN providers is *VPNArea.net*. Although they do not offer a free or trial option, their yearly rate is a reasonable \$59. With this you get servers in almost every country you can name, use on 5 devices, unlimited bandwidth, humans on the other end of the tech support call, and highly responsive bandwidth.

The dominant feature of VPNArea is it is registered in Bulgaria, with servers located in Switzerland. Switzerland national data protection laws are among the strictest in terms of protecting private data, and permitting a VPN provider to not keep logs of client traffic. Other differentiating features include the option to use OpenVPN, L2TP, or PPTP (OpenVPN would be our only choice), 7-day money back guarantee, and their list of over 10,000 alternate DNS servers so that you do not need to use those provided by your organization or Internet provider. This last option is important, as if you are using your ISP, Google, or other common DNS servers, your web travels are logged (called a *DNS Leak*). They also offer the upgrade to your own dedicated VPN server. This provides a significant speed boost as your server isn't timesharing with dozens or hundreds of other users.

19.3.1 Assignment: Create a VPNArea Account

In this assignment, you will create a paid account (with a 7-day cancellation policy) with *VPNArea.net*, and then configure VPN services.

- Note: VPNArea has extended a special discount to *Practical Paranoia* students and readers. When registering, enter *pparanoia* in the coupon field to get your discount.
- Note: As of this writing, the default VPNArea application, Chameleon, only works when logged in with an administrative account, not standard accounts. As it is a serious vulnerability to log in with an administrative account, contact VPNArea for a customized version of the 3rd-party VPN application, *Viscosity*. Viscosity is also available directly from the developer³ for \$9. The assignment

³ <https://www.sparklabs.com/viscosity/>

19 Internet Activity

for Viscosity is found later in this chapter. Email VPNArea at viscosity@vpnarea.com to request your personalized copy of viscosity after you have registered for your account.

1. Open a browser, visit VPNArea at <https://vpnarea.com>, and then select the *Get Started–Prices* button.



19 Internet Activity

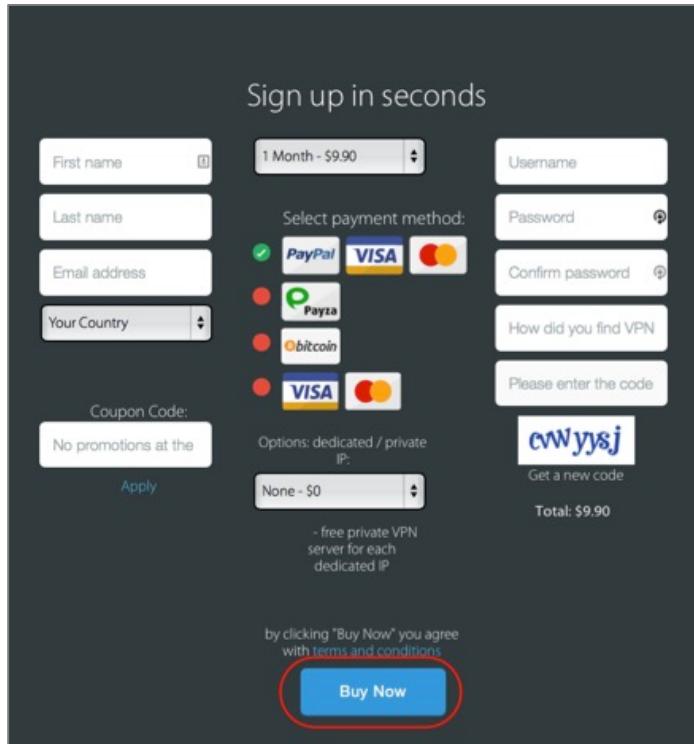
- After reviewing the available plans, click the *Buy Now* button for the desired plan.

	<u>1 month</u>	<u>1 year</u> <small>49% OFF</small>	<u>6 months</u>
Membership Price (comparison)	\$9.90 (\$9.90/mo)	\$59.00 (4.92\$/mo)	\$50.00 (8.33\$/mo)
Servers in <u>50 countries</u>	✓	✓	✓
Use on 5 Devices	✓	✓	✓
Unlimited bandwidth	✓	✓	✓
7 days money back	✓	✓	✓
   	✓	✓	✓
Instant Activation	✓	✓	✓
Dedicated IP option	✗	✓	✓
AES-256 encryption	✓	✓	✓
	buy now	buy now	buy now
			 Send a message

- Scroll down the page to the *Sign up in seconds* area. Enter all the requested information, remember to record your *Username* and *password*,

19 Internet Activity

4. In the *Coupon Code* field, enter *pparanoia* to receive your *Practical Paranoia* student and reader discount, and then click the *Buy Now* button.



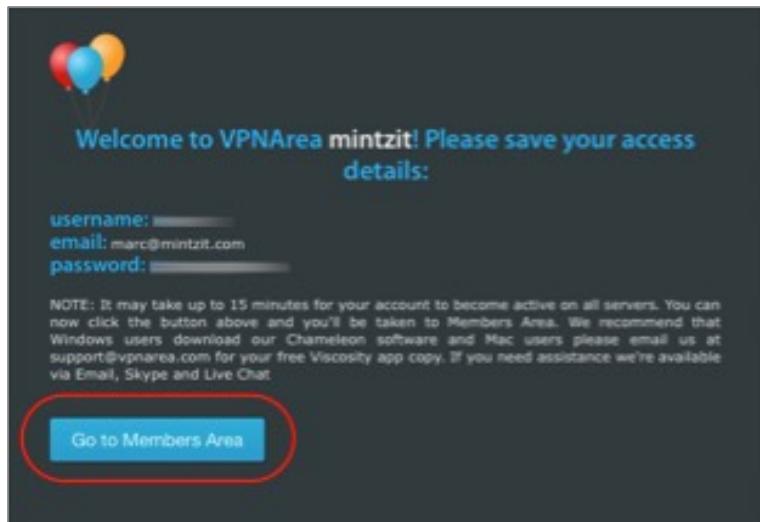
19.3.2 Assignment: Install VPNArea Chameleon

VPNArea has their own utility to interface with OpenVPN, named *Chameleon*. It is a powerful, yet very easy to configure utility. If there is a downside to it, it is that Chameleon requires that the user account be an administrator account. If you need or wish to log in as an administrator, use this assignment to install and configure Chameleon.

19 Internet Activity

If you need or wish to log in with a non-administrator account, VPNArea uses the 3rd-party utility *Viscosity*⁴. The assignment to install and configure Viscosity follows this one.

1. After your payment is processed, you are taken to the *Thank You* page. Select the *Go to Members Area* button.



⁴ <http://www.sparklabs.com/viscosity/>

19 Internet Activity

2. In the *Members Area* page, select the *Mac Yosemite / Lion / Mavericks* button.

The screenshot shows the 'Welcome to Members Area' page of the VPNArea website. At the top, there's a banner with the text 'mintzit don't forget to check the forum for news and updates!'. Below the banner is a navigation bar with links: 'Setup & HowTo', 'News & Updates', 'Servers Status', 'Chameleon', 'Change DNS', and 'Contact us'. A message at the top right says 'Your account will expire in: 365 days' with buttons for 'Renew', 'DEDICATED IP', 'CHANGE PASSWORD', and 'LOGOUT'. On the left, there's a 'NEW MEMBERS:' section with a callout bubble containing instructions: 'Hover on the logo of your Operation System and click "View Guide" to see the Instructions. Problems? Check our Support Forum'. Below this is a poll titled 'Where should our next server be?' with options: Finland, Denmark, Canada, 'Vote', and 'Results'. The main content area is titled 'VPNArea Setup instructions (OpenVPN)' and contains a grid of 12 cards, each representing a different system and its setup method:

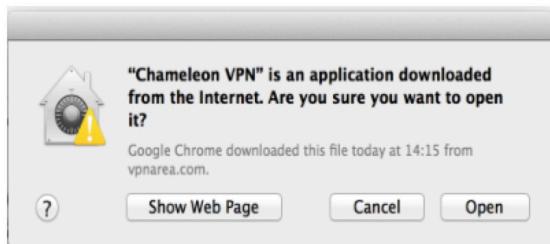
- Windows 8/7/Vista/XP - VPNArea Chameleon NEW
- Mac Yosemite / Lion / Mav - VPNArea Chameleon NEW (highlighted with a red border)
- Android - OpenVPN's software
- DD-WRT Routers - OpenVPN's software
- iOS - iPad - OpenVPN Application
- iOS - iPhone - OpenVPN Application
- Tomato Routers - OpenVPN's software
- Windows 7/Vista/XP - OpenVPN's software
- Mac Lion / Leopard - Viscosity App(pre-configured)
- Yosemite / OS X 10.10 - Tunnelblick App
- Ubuntu Linux - OpenVPN's software
- Debian Linux - OpenVPN's software

In this page will be complete setup instructions. They are repeated here.

3. For macOS, it is necessary to download the VPNArea VPN utility *Chameleon*. Select the *Setup File* button to download the file.
4. Once the *Chameleon* dmg file has downloaded, double-click to open it. Inside the virtual disk now mounted on your desktop will be the *VPNAreaChameleon.app*. Drag it into your *Applications* folder. This is important, as it will not function properly if located anywhere else.

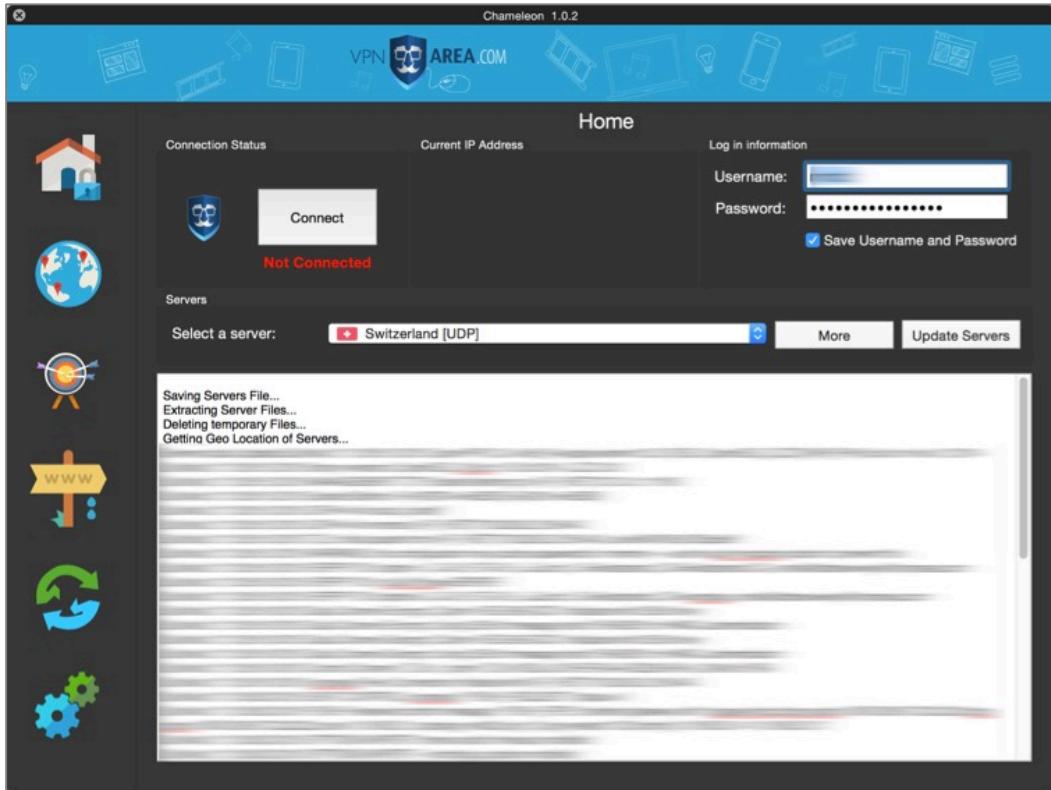
19 Internet Activity

5. Double-click to launch *VPNAreaChameleon.app* in your *Applications* folder.
6. If opening is blocked due to being from an unknown developer, open *System Preferences > Security & Privacy > General* tab, and then click the *Open Anyway* button.
7. If prompted to allow opening, select the *Open* button.

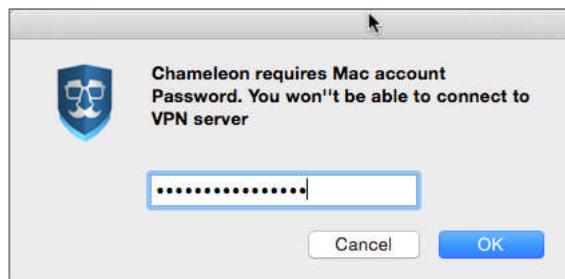


19 Internet Activity

8. *VPNAreaChameleon.app* will open. Enter your *Username* and *Password* as when you created your account, from the *Select a server* pop-up menu select a server, and then select the *Connect* button.

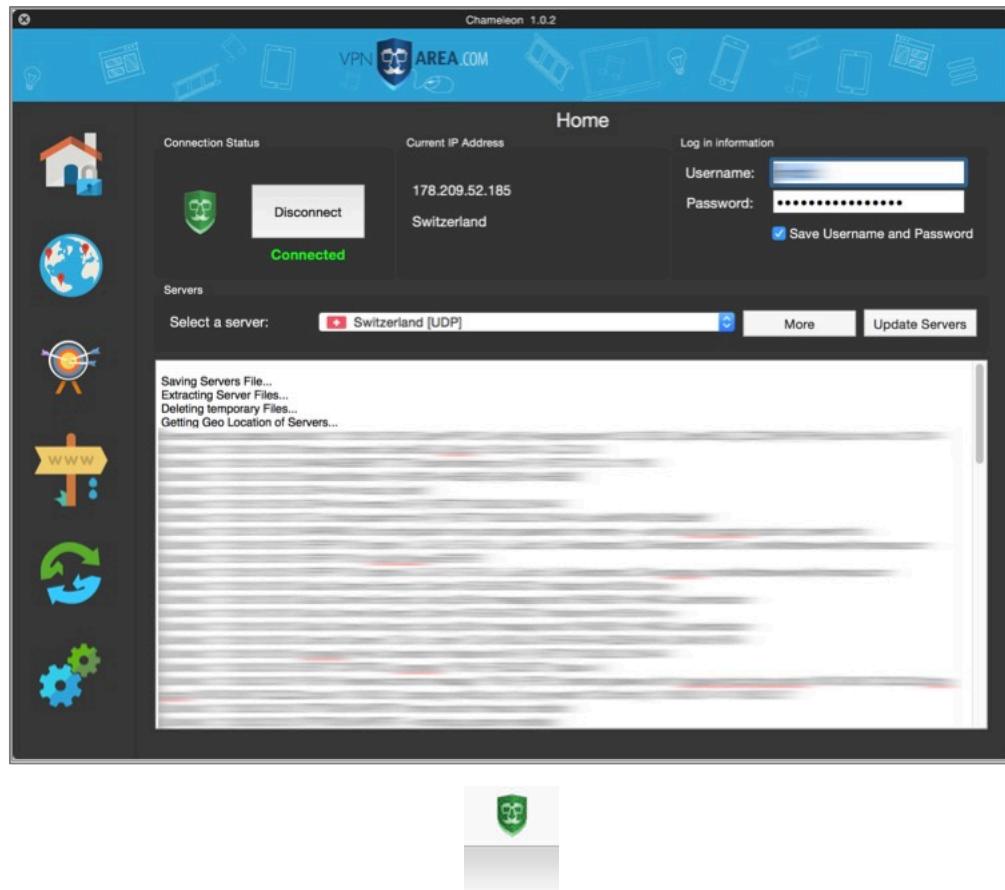


9. At the prompt for a password, enter your computer user account password, not your VPNArea password, and then select the *OK* button.



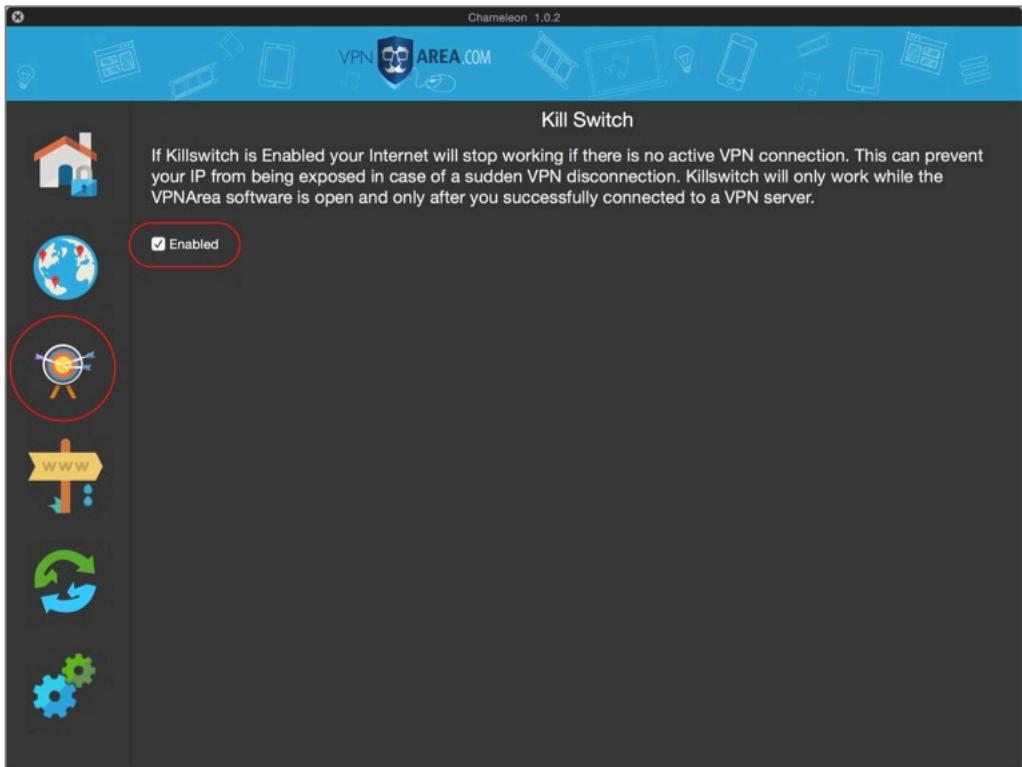
19 Internet Activity

10. When connected you will see the *Connection Status* change to *Connected*.
Also, the *Chameleon* menu item will change to green.



19 Internet Activity

- To add extra assurance that you will only ever use VPN when connecting to the Internet, from the *Chameleon* sidebar, select the *Kill Switch* icon, and then enable the *Enabled* checkbox.



- To reduce the possibility that your DNS activity is tracked or recorded (called a *DNS Leak*) by your organization or Internet provider, you will want to change your DNS Servers when connecting to VPN. With most other VPN providers, this must be done in the *System Preferences > Network > Advanced > DNS* pane. However, VPNArea makes this automatic! To find your desired DNS servers, open a browser and go to <https://vpnarea.com/front/member/dns>.

19 Internet Activity

You can get here manually from logging in to vpnarea.net, selecting *Members Area*, and then select *Change DNS*.

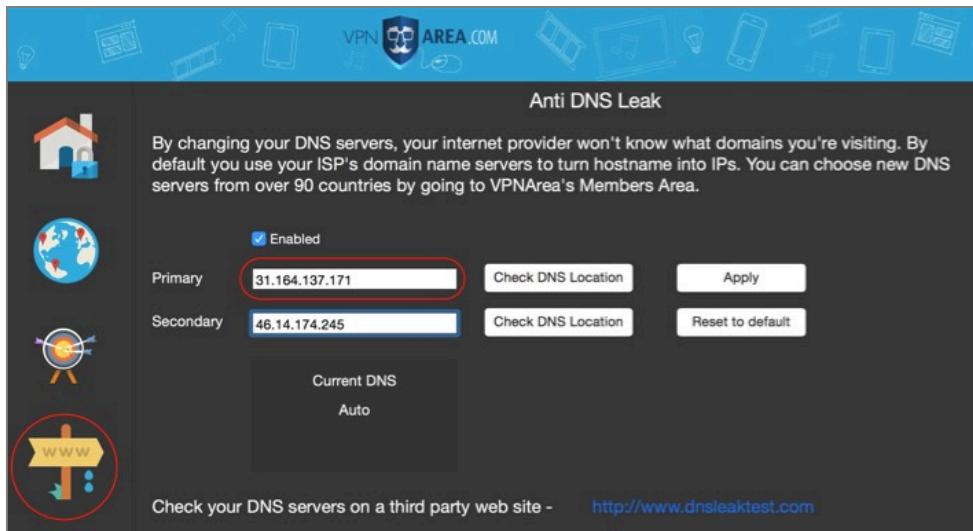
CHANGE DNS:
To prevent your Internet Provider from knowing what website names you're visiting replace your current DNS servers with some of those. This may have a slight negative or positive effect on the time required to initiate connection to a website.
Visit the Forum for a guide on how to change your DNS servers

IPv4/IPv6 Address	Hostname	Location	Software / Version	Checked at	Status	Whois
188.191.215.34		Moldova, Republic of		2015-03-02	valid	55 %
27.100.48.90	watv027100048090.watv.ne.jp.	Japan, Ashikaga		2015-03-02	valid	98 %
175.136.234.9		Malaysia, Kuala Lumpur		2015-03-02	valid	97 %
181.15.244.251	host251.181-15-244.telecom.net.ar.	Argentina		2015-03-02	valid	97 %
216.113.100.60		Canada	dnsmasq-2.40	2015-03-02	valid	92 %
89.216.55.115	cable-89-216-55-115.static.sbb.rs.	Serbia		2015-03-02	valid	98 %
31.164.137.171	xdsl-31-164-137-171.adslplus.ch.	Switzerland, Vevey	dnsmasq-2.52	2015-03-02	valid	98 %
218.44.154.28	mana.yakumo-net.jp.	Japan	8.4.7-REL-NOESW	2015-03-02	valid	98 %
70.59.180.20	arbitrary.quibble.com.	United States	9.10.1	2015-03-02	valid	98 %
118.97.150.171	171.subnet118-97-150.static.astin.net.telkom.net.id.	Indonesia		2015-03-02	valid	94 %
50.154.81.74	o-50-154-81-74.hsd1.fl.comcast.net.	United States, Fort Myers	[SECURED]	2015-03-02	valid	98 %
207.150.177.201	submit.standartered.com.	United States, Tampa		2015-03-	valid	98 %

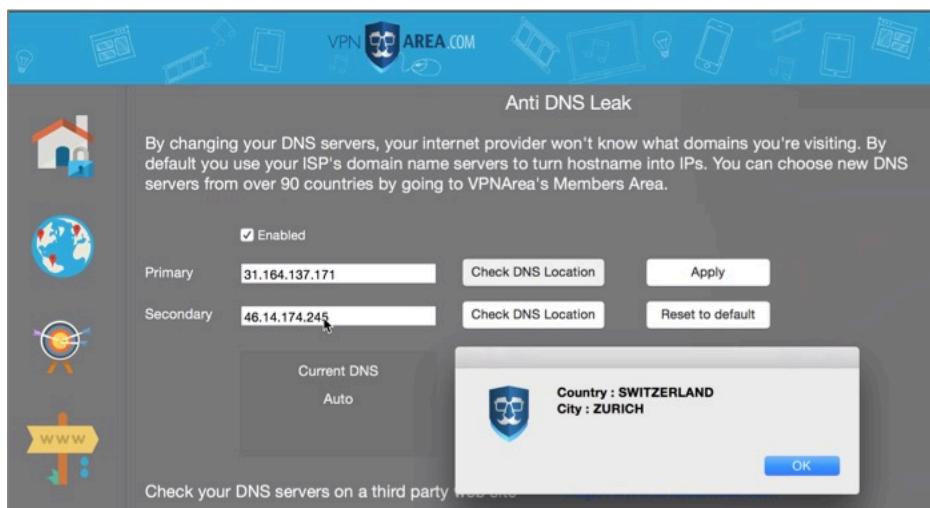
13. Scroll through the list to find a DNS server in the country of choice, and then copy the *IPv4* address from the left column.

19 Internet Activity

14. Select the *www Anti DNS Leak* icon from the *Chameleon.app* sidebar, click in the *Primary* field, and then *Paste*.

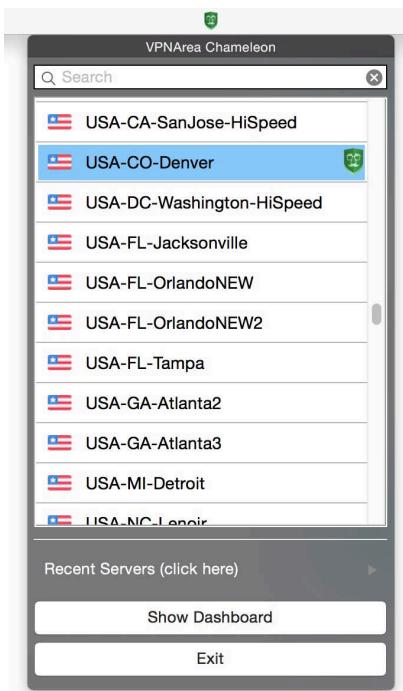


15. Repeat for another DNS server in your desired country, and then *Paste* in the *Secondary* field.
16. Click the *Check DNS Location* for each DNS server to verify it is working properly. When verified, click the *OK* button.



19 Internet Activity

17. Enable the *Enabled* checkbox, and then click the *Apply* button. Your computer is now using VPN with *Anti-DNS Leak* enabled.
18. If at any time you wish to change your VPN server or country, click on the *VPNArea* menu item, scroll through the list of servers, and then select the desired server.

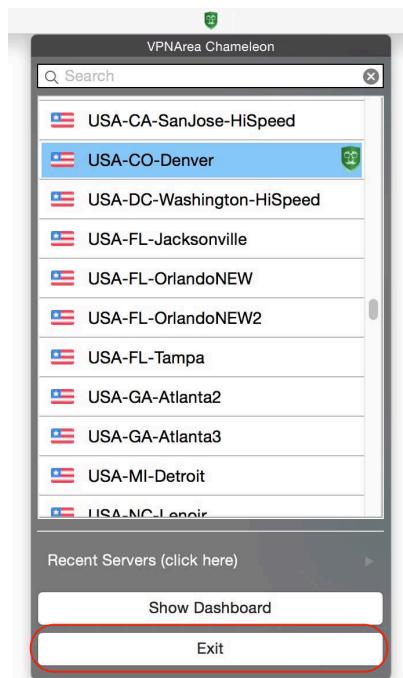


19 Internet Activity

19. The last piece of configuration is found by selecting the *Settings* icon in the *Chameleon* sidebar. Configure to taste. Shown below are my recommendations:



20. To turn VPN and Anti-DNS Leak off, click on the *VPNArea* menu item, and then select the *Exit* button.



21. When you wish to reactivate VPN, open *VPNArea Chameleon.app*. You can see that VPN is active when the *VPNArea* menu icon changes to green.

Congratulations! You have configured VPN so that any time you need complete privacy with your Internet communications, it is ready for you.

19.3.3 Assignment: Install Viscosity for VPNArea

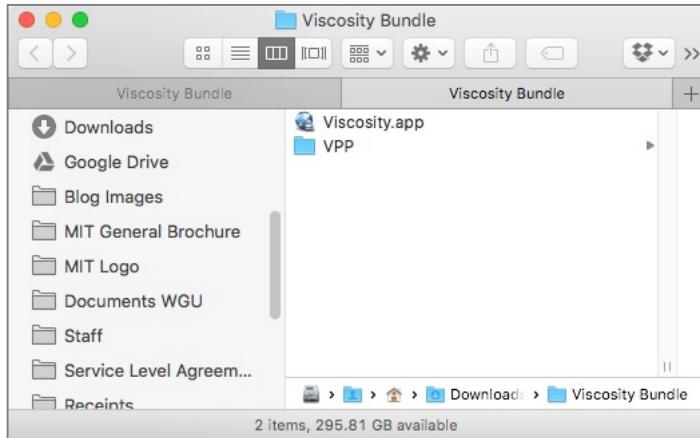
VPNArea uses the 3rd-party utility *Viscosity* as the front-end interface for OpenVPN for users who need or want to log in with a non-administrator accounts. If you need or want to log in as an administrator, VPNArea uses their own *Chameleon* utility to work with OpenVPN. If you will be logging in as an administrator, you may skip this assignment, and complete the previous one for Chameleon.

1. After completing registration for a VPNArea account, send an email to *viscosity@vpnarea.com*, requesting a copy of *Viscosity*. Include your email address and VPNArea account information.
 - Note: Viscosity may also be purchased from the developer, Sparklabs⁵.
2. Within 3 hours you will receive an email with a link to your customized version of Viscosity.
3. Click the link to download Viscosity.

⁵ <http://www.sparklabs.com/viscosity/>

19 Internet Activity

4. The Viscosity download will be named *Viscosity Bundle*, containing two items: the Viscosity.app, and the VPP folder.



5. Drag the Viscosity Bundle folder into your */Applications* folder.
6. Double-click the Viscosity.app, located in */Applications/Viscosity Bundle*.
7. The *Viscosity Helper Tool Installation* window opens. Select *Install*.



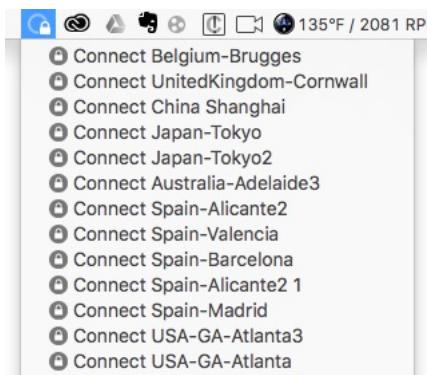
8. The *Welcome to Viscosity* window appears. You may close it as Viscosity is up and running without it.

19.3.4 Assignment: Create a Viscosity VPN Internet Connection

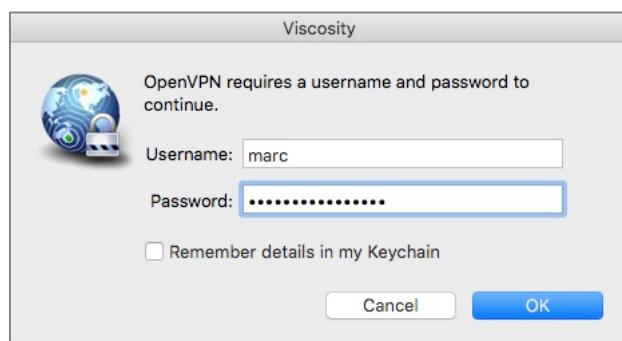
In this assignment, we will use the 3rd-party OpenVPN application *Viscosity* to create a secure VPN Internet connection through VPNArea.

19 Internet Activity

- Prerequisites: The previous assignments must have been completed to have an active VPNArea account, and Viscosity.app is installed on your computer.
1. Open Viscosity.app, located in */Applications*.
 2. From the menu bar, select the Viscosity menu icon  . The drop-down menu will display all available VPNArea servers. Select your desired server. As a general rule, the closer the server to your location, the faster your Internet service will be.



3. At the Viscosity authentication window, enter an administrator username and password, and then click OK.
 - Note: You may be logged in with either an Administrator or Standard user account, but you must enter Administrator credentials in this window.



4. Within a few seconds a notification alert will appear briefly announcing that your connection is complete.

5. To verify your VPN is working properly, open a browser to <https://whatismyip.com>. It will show your Internet IP address, as well as your geographical location, which is based on IP address. If all is working well, you will not have your normal public IP address, and your reported location will be somewhere else.

19.3.5 Assignment: Disconnect your Viscosity VPN Internet Connection

When you wish to have a native connection to the Internet instead of VPN, you will need to disconnect from your VPN provider. In this assignment we will disconnect from VPNArea while using Viscosity.app.

1. Click the Viscosity menu icon, and then from the drop-down menu, go to and select the server to which you are currently connected.
2. In a few seconds you will be disconnected.

19.3.6 Assignment: Configure Viscosity OpenVPN Utility

Viscosity is one of the few applications that is well configured by default, and you may not wish to change any setting. In this assignment, we will review the settings that we use at Mintz InfoTech, Inc.

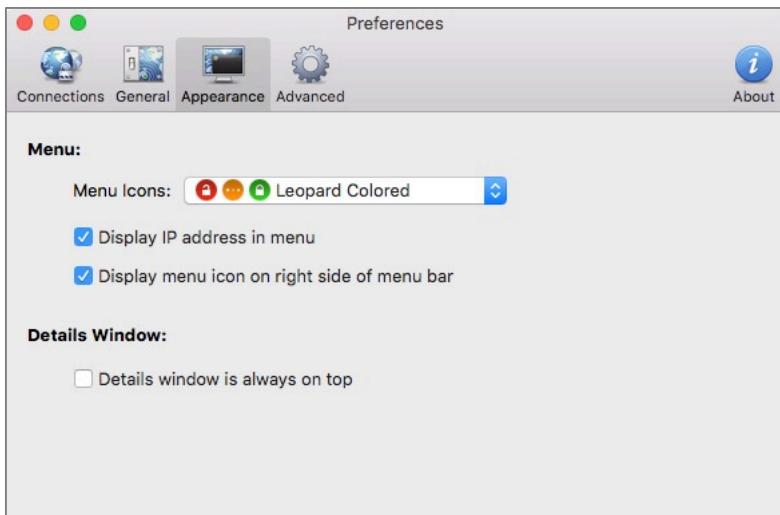
1. If Viscosity is not already running (it's icon cannot be seen in the menu bar), launch Viscosity, located in */Applications*.
2. From the Viscosity menu icon drop-down menu, scroll to the bottom and then select *Preferences*. The Preferences window opens.

19 Internet Activity

3. Select the *General* tab, and then configure as below:



4. Select the *Appearance* tab, and then configure as below:



19 Internet Activity

5. Select the *Advanced* tab, and then configure as below:



6. Close the Viscosity Preferences window.

Done!

19.4 Mesh VPN

Another way in which VPN can be configured is a *mesh* VPN. This strategy places multiple computers within the same virtual network regardless of where they are geographically located on the Internet. All the computers operate as if they are on the same physical network, and all traffic between each of the computers is military-grade encrypted. Mesh VPN is ideal for groups of people to exchange files, screen share, and access databases from each other, while maintaining full privacy from the outside world.

We now have software that enables mesh networks for a trivial cost. Keep in mind that VPN is only as secure as the provider, and the vendor of choice is a US company, subject to US federal laws and National Security Letters giving the NSA full access to logs and data crossing the vendor servers.

19.5 LogMeIn Hamachi

LogMeIn⁶ is a US-based company with a line of top-grade cloud services. They are best known for their *LogMeIn* remote support software, allowing technical support staff both attended and unattended access to client and server computers.

One of their lesser-known, but game-changing products is *Hamachi*⁷. Hamachi is a cloud-based VPN, completely eliminating the need for expensive VPN boxes. As if that weren't enough, it also allows for three different types of VPN configurations: Gateway, mesh, and hub & spoke. We will restrict discussion here to the mesh option.

As of this writing, Hamachi is free for use with 5 or fewer nodes (computers). Up to 32 nodes on one network is available for \$29/year. Up to 256 nodes on a network is available for \$119/year.

19.5.1 Assignment: Create a LogMeIn Hamachi Account

In this assignment, we will create a LogMeIn Hamachi account, so that we can deploy a free Hamachi network for up to 5 computers. Should you eventually need more computers on the network, your account can easily be upgraded at any time.

⁶ <https://logmein.com>

⁷ <https://secure.logmein.com/products/hamachi/>

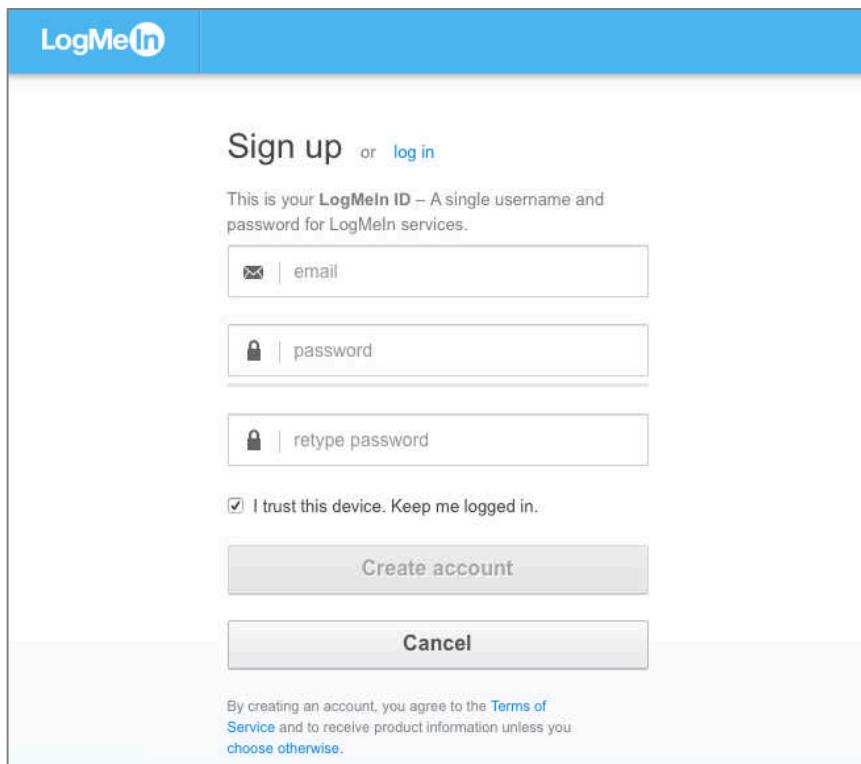
19 Internet Activity

1. Open a browser, and go to the Hamachi home page at <https://secure.logmein.com/products/hamachi/default.aspx>. The Hamachi home page opens. Click the *Sign up link*.



19 Internet Activity

2. Select the *Try it Free* button. In the *Sign Up* field, enter all requested information, and then select the *Create Account* button.



The image shows a screenshot of the LogMeIn sign-up page. At the top, the LogMeIn logo is visible. Below it, the word "Sign up" is prominently displayed, with a "log in" link nearby. A descriptive text states: "This is your LogMeIn ID – A single username and password for LogMeIn services." There are three input fields: the first for "email" (indicated by an envelope icon), the second for "password" (indicated by a lock icon), and the third for "retype password" (also indicated by a lock icon). Below these fields is a checkbox labeled "I trust this device. Keep me logged in." followed by a "Create account" button. A "Cancel" button is located below the "Create account" button. At the bottom of the form, there is a small note: "By creating an account, you agree to the [Terms of Service](#) and to receive product information unless you choose otherwise."

19 Internet Activity

3. In the *Complete Your Registration* page, enter all requested information, and then select the *Register* button.

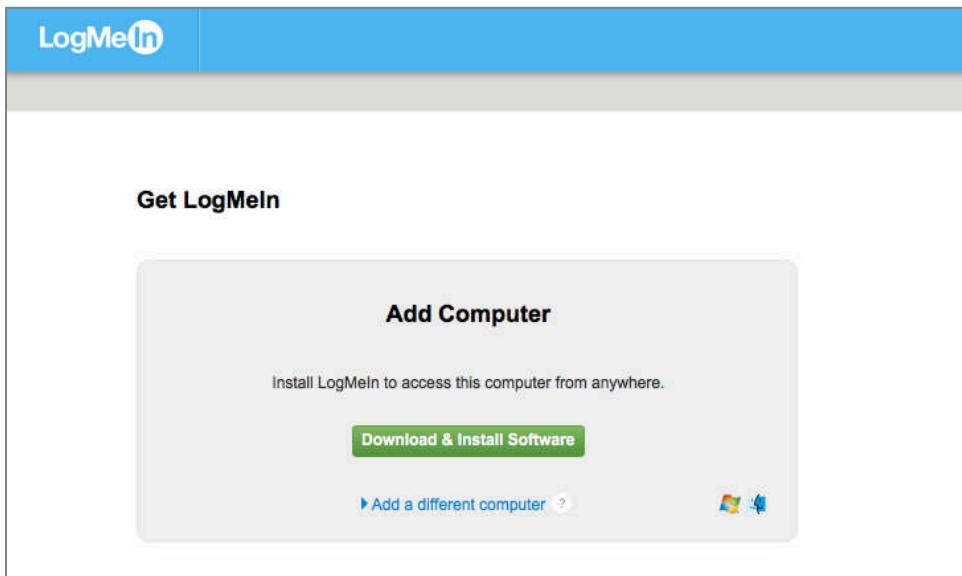
The screenshot shows a registration form titled "Complete your registration" from LogMeIn. The form fields are as follows:

- First Name: Marc
- Last Name: Mintz
- Title: President
- Phone Number: 5054530479
- Company: MIT
- Job Title: Outsourced IT Professional
- Computer Count: 51 - 100 computers

At the bottom, there are two buttons: a blue "Register" button and a "Skip" button.

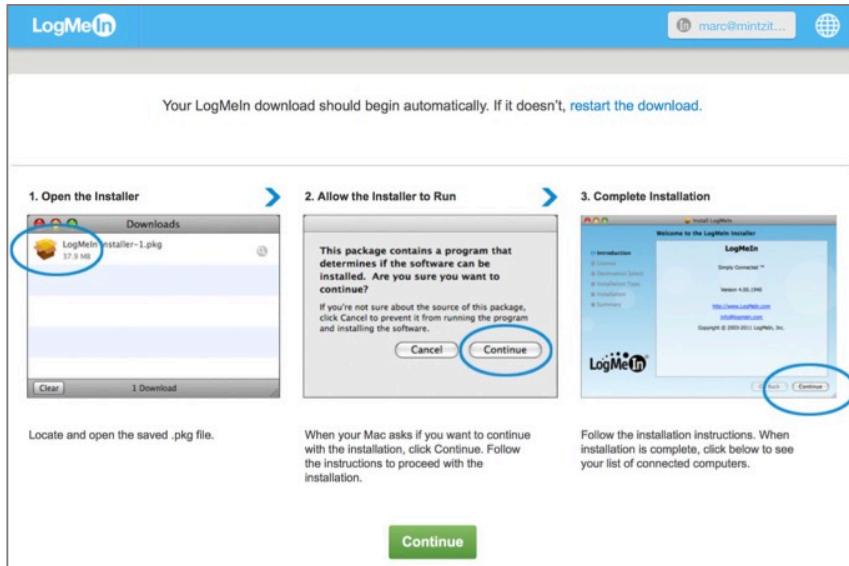
19 Internet Activity

- At the *Get LogMeIn* page, select the *Download and Install Software* button to install the software on this computer. If you don't need the software on this computer, but want to install on other computers, click the *Add a different computer link*, and then follow the on-screen instructions.



19 Internet Activity

5. The software will begin to download, and the guide page will appear. **Do not** select the *Continue* button quite yet.

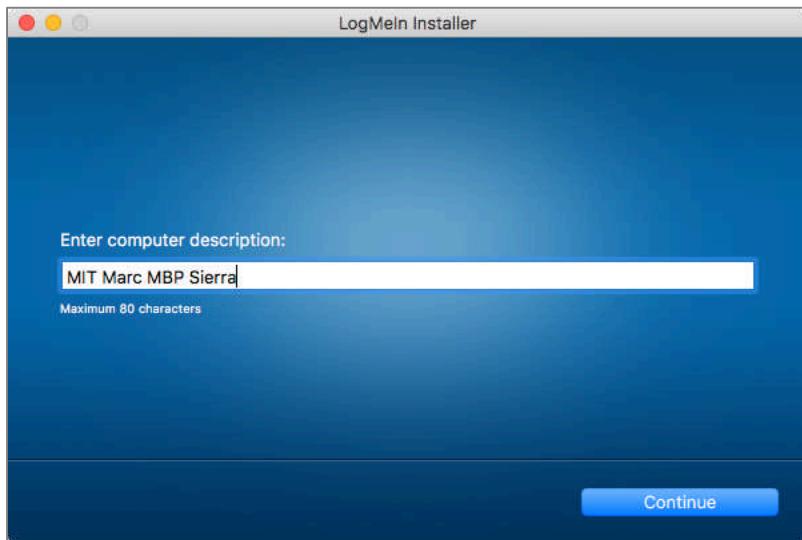


6. Go to your Downloads folder, and open the *LogMeIn Installer.app*. Enable the *I have read and agree...* checkbox, and then select the *Install* button.



19 Internet Activity

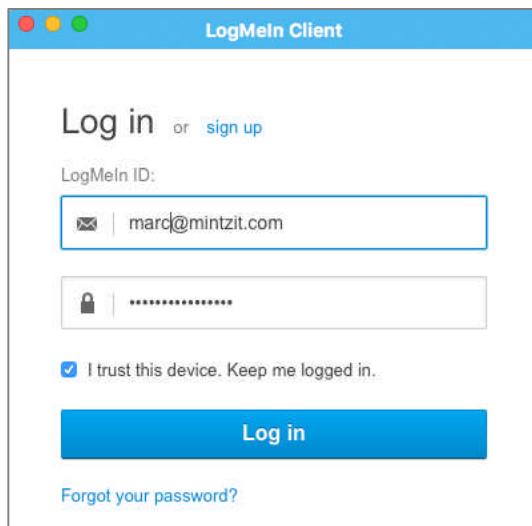
7. At the authentication prompt, enter an administrator username and password, and then select the *Install* button.
8. At the prompt, enter a name for your computer, and then select the *Continue* button.



9. At The *Installation Was Successful* pane, select the *Finish* button.

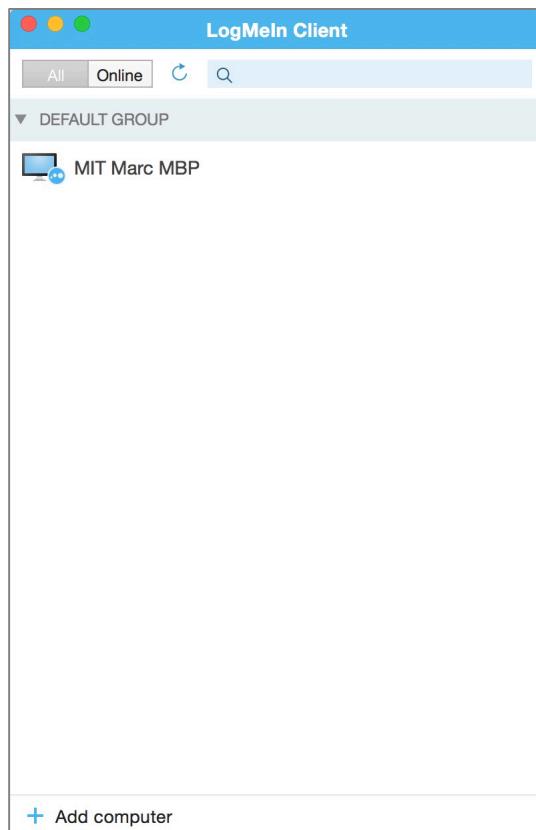
19 Internet Activity

10. The *LogMeIn Client Log In* window appears. Enter the same email and password used to create the account, and then select the *Log In* button.



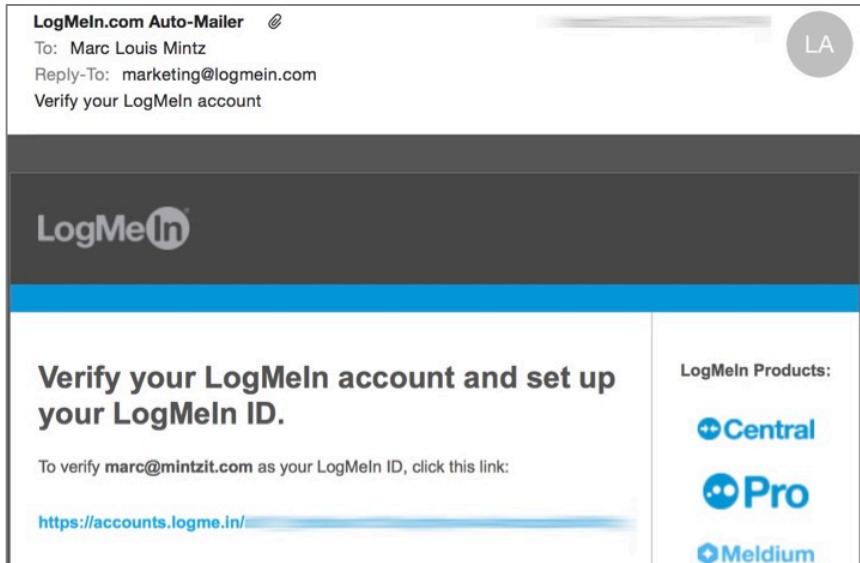
19 Internet Activity

11. The *LogMeIn Client* window will now display all users who are members of this network (currently, just yourself.) To add additional users, skip to step 13.



19 Internet Activity

12. Open your email to check for a verification message from LogMeIn. Click the reply link.



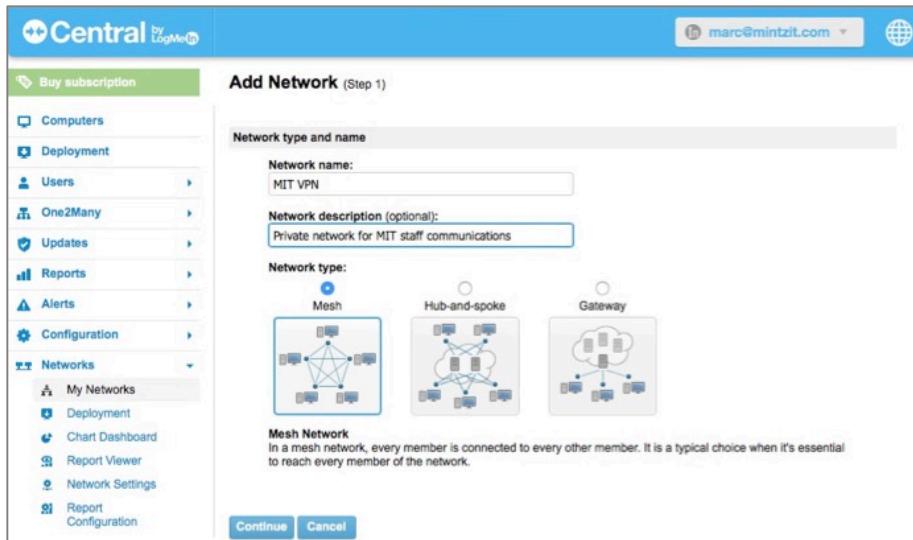
19 Internet Activity

13. Returning to your browser, in the *Hamachi* screen, select *Networks > My Networks*, and then select *Create Networks*.

The screenshot shows the LogMeIn Central dashboard. On the left, there's a sidebar with various menu items like 'Buy subscription', 'Computers', 'Deployment', 'Users', 'One2Many', 'Updates', 'Reports', 'Alerts', 'Configuration', 'Networks' (which is expanded to show 'My Networks', 'Deployment', 'Chart Dashboard', 'Report Viewer', 'Network Settings', and 'Report Configuration'), 'Backup', and 'Bulletin Board'. A yellow banner at the top right indicates 'Planned System Maintenance' on Saturday, April 18th, 2015, from 4:01 AM UTC to 4:31 AM UTC. Below the banner, there's a section titled 'Get Started Now with On-Demand VPN Connectivity' with three main options: 'Deploy Hamachi' (with a description: 'Deploy Hamachi to devices you want to connect.'), 'Creates Networks' (with a description: 'Set up virtual networks: mesh, hub-and-spoke or gateway.'), and 'Add Clients' (with a description: 'Network your devices. Manage them centrally.'). The 'Creates Networks' option is highlighted with a red rectangular box. At the bottom of the page, there's a 'Buy Hamachi Subscriptions' button and social media links for Facebook and LinkedIn.

19 Internet Activity

14. In the *Add Network* page, in the *Network Name* field, give your network a human-readable name, select the *Network Type* (in this example, we are creating a *Mesh* network), and then select the *Continue* button.

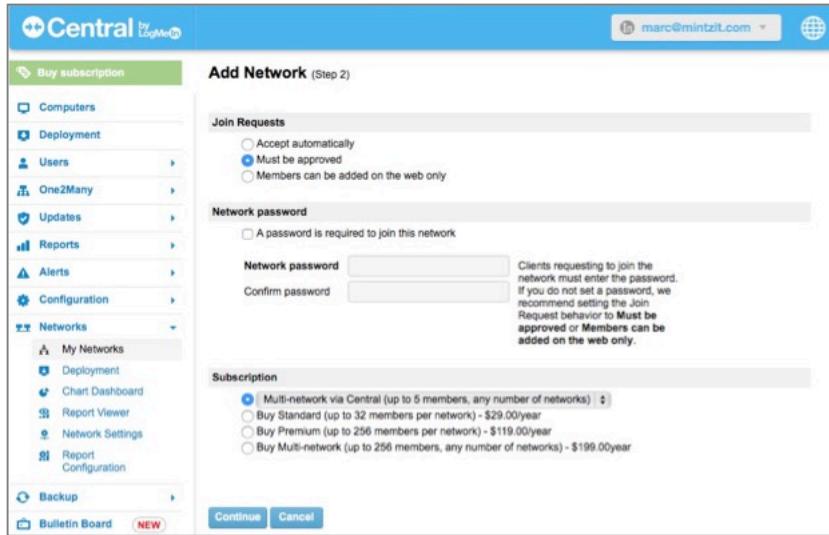


15. In *Add Network (Step 2)*, in *Join Requests*:

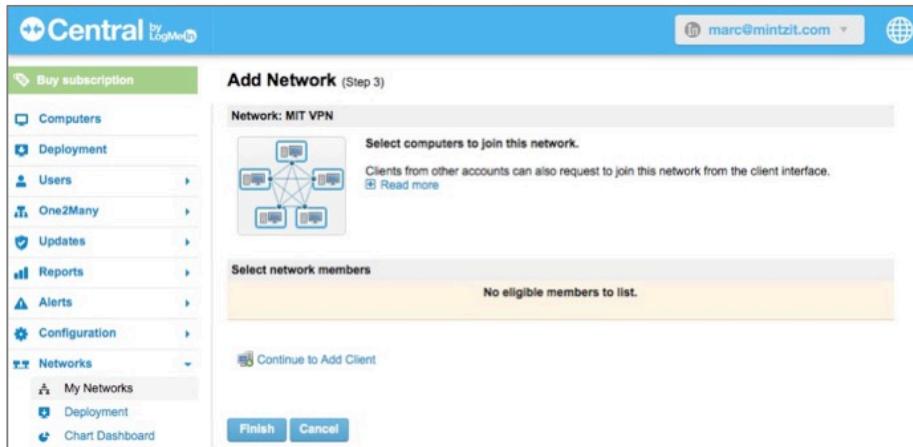
- In *Join Requests*, specify how users will be able to join the VPN network. If security is a concern, we recommend *Must be approved* in order to keep strangers out.
- In *Network password*, configure if a password is required to join the network. Assuming all user computers have strong passwords, and full-disk encryption, it would be extremely unlikely anyone other than the authorized user would be attempting network connection. However, if security is a concern, enable the password requirement, and then set a strong password.
- In *Subscription*, specify what subscription level is requested. For the purposes of this assignment, select *Multi-network via Control (up to 5 members, any number of networks.)*

19 Internet Activity

16. Select the *Continue* button.

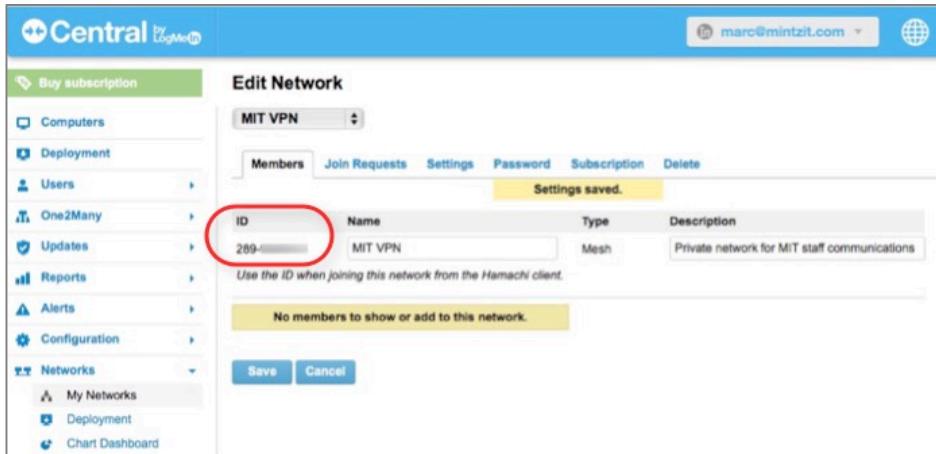


17. The *Add Network (Step 3)* appears. Select the *Finish* button.



19 Internet Activity

18. In the *Edit Network* page, make note of your network *ID*, as this will be used when joining the network. Select the *Save* button.



The screenshot shows the 'Edit Network' interface. On the left, there's a sidebar with various options like 'Buy subscription', 'Computers', 'Deployment', 'Users', 'One2Many', 'Updates', 'Reports', 'Alerts', 'Configuration', 'Networks' (selected), and 'My Networks', 'Deployment', 'Chart Dashboard'. The main area is titled 'Edit Network' with 'MIT VPN' selected. It has tabs for 'Members', 'Join Requests', 'Settings', 'Password', 'Subscription', and 'Delete'. A yellow bar at the top right says 'Settings saved.' Below it, there's a table with columns 'ID', 'Name', 'Type', and 'Description'. The first row shows '289-' in the ID column, 'MIT VPN' in the Name column, 'Mesh' in the Type column, and 'Private network for MIT staff communications' in the Description column. A note below says 'Use the ID when joining this network from the Hamachi client.' At the bottom, there are 'Save' and 'Cancel' buttons. The 'ID' field is circled in red.

Congratulations, your account is created and you are ready to add users to your mesh VPN network.

19.5.2 Assignment: Add Users to a Hamachi VPN Network

In this assignment we will add users to the Hamachi VPN network created in the previous assignment.

- Prerequisite: Completion of the previous assignment.
1. Open a browser and go to <https://secure.logmein.com>, and then login with your username and password. The *LogMeIn Central* page appears.

19 Internet Activity

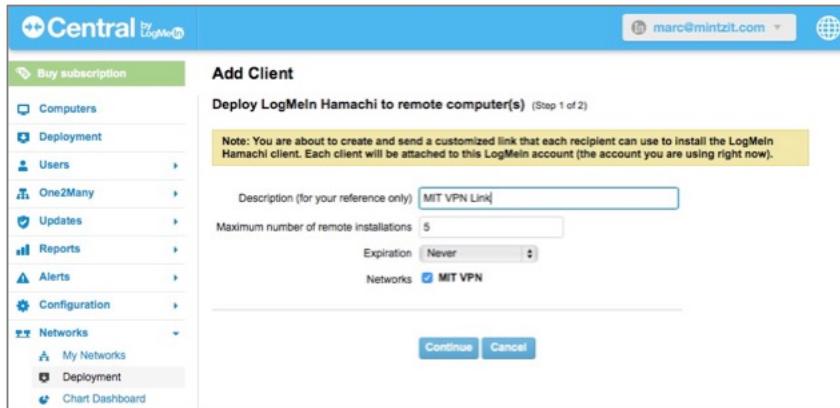
2. Select the *Networks > Deployment* link, and then select the *Add New Link* button.

The screenshot shows the Central by BigMech web interface. At the top, there's a navigation bar with a user icon and the email address 'marc@mintzit.com'. Below the header, on the left, is a sidebar menu with various options like 'Buy subscription', 'Computers', 'Deployment' (which is selected and highlighted in blue), 'Users', 'One2Many', 'Updates', 'Reports', 'Alerts', 'Configuration', 'Networks' (with 'My Networks' and 'Deployment' under it), and 'Chart Dashboard'. The main content area is titled 'Networks > Deployment' and contains two buttons: 'Add New Link' and 'Delete Selected'. A message at the bottom says 'You have no installation links.'

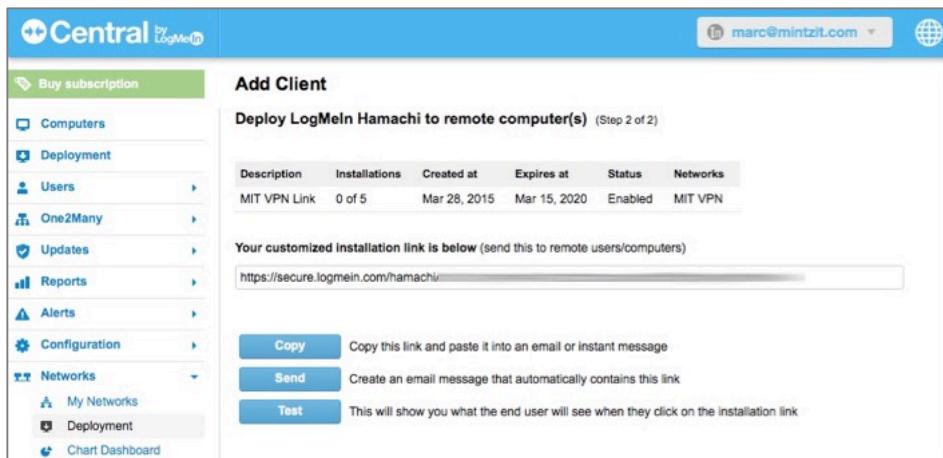
3. In the *Add Client* page, you will create a link that can be used to allow a custom installation of Hamachi.
 - In the *Description* field, enter information for your own reference.
 - In the *Maximum number of remote installations* field, enter, well, the maximum number of installations permitted (with a free account, this is 5.)
 - In the *Expiration* pop-up, specify when the link expires.
 - In *Networks*, enable the checkbox for the network this link will be used.

19 Internet Activity

4. Select the *Continue* button.



5. The *Add Client* link page appears. You have the option to *Copy* or *Send* the link. For our assignment, select *Send*.



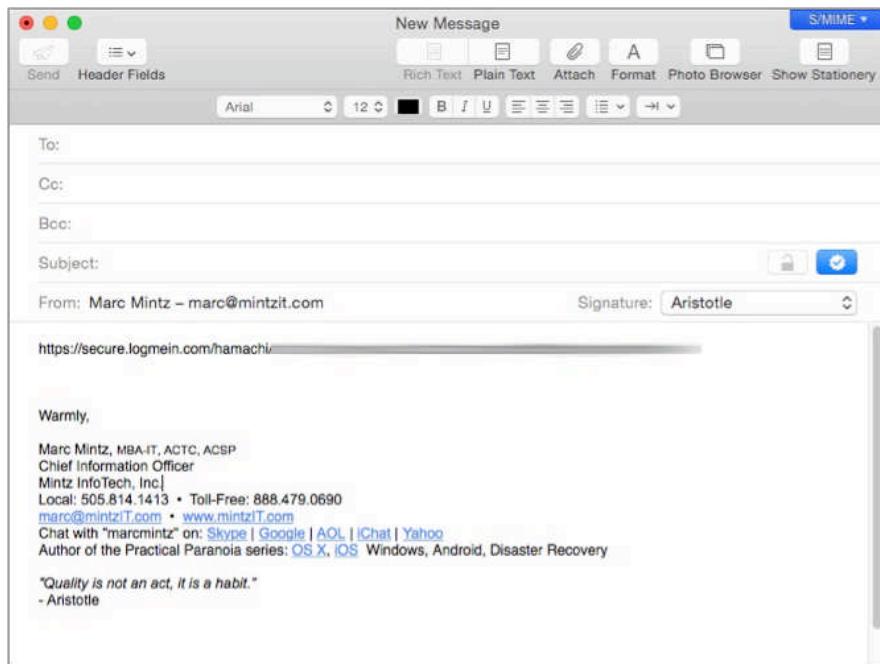
The default email client will open, with the link pre-entered in the body area, awaiting entry of recipient(s) and a message.

6. Enter recipient address(es).
7. Enter a subject.
8. Enter additional information in the body area explaining what to do next. Something like: *Listed below is a link to download LogMeIn Hamachi. This*

19 Internet Activity

software will allow all of us to create a private encrypted network within which we may continue our plans for world domination.

9. Send the email.



10. When the recipient clicks the link, they are taken to the *Hamachi Installer* page. Enable the *I have received this link from a trusted source* check box, and then select the *Continue* button.

Welcome to the LogMeIn Hamachi Installer

This will install the LogMeIn Hamachi client to this computer. Your Hamachi administrator will be able to change settings and manage your network memberships.

Hamachi is a secure virtual private networking (VPN) tool that allows your trusted IT support professional to set up a VPN over the internet, and bring your computer into that network. [Learn more about LogMeIn Hamachi.](#)

I have received this link from a trusted source

Continue

19 Internet Activity

11. At the *Download* page, select the *Download Now* button.



12. The *LogMeIn Hamachi Installer* will download. Once complete, launch the installer, enable the *I have read...* check box, and then select the *Install* button.

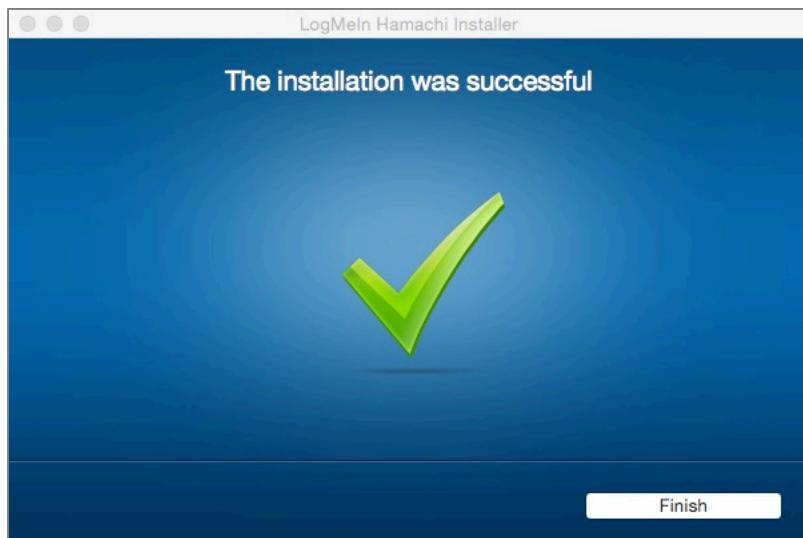


19 Internet Activity

13. The *Attach client to LogMeIn account* screen appears. Select the *Next* button.

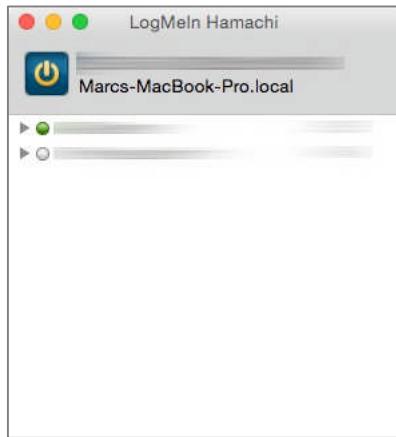


14. When the installation completes, select the *Finish* button.



15. Open *LogMeIn Hamachi.app*, located in */Applications/LogMeIn Hamachi*. In my case, there are networks that I currently belong to listed, one of which I am connected (the green button), and one I am not connected with (white button). Neither of which is the MIT VPN network (yet).

- If your target network appears in the *LogMeIn Hamachi* window with a green button, all is done!
- If your target network doesn't appear in the *LogMeIn Hamachi* window, we have a few more steps to complete.

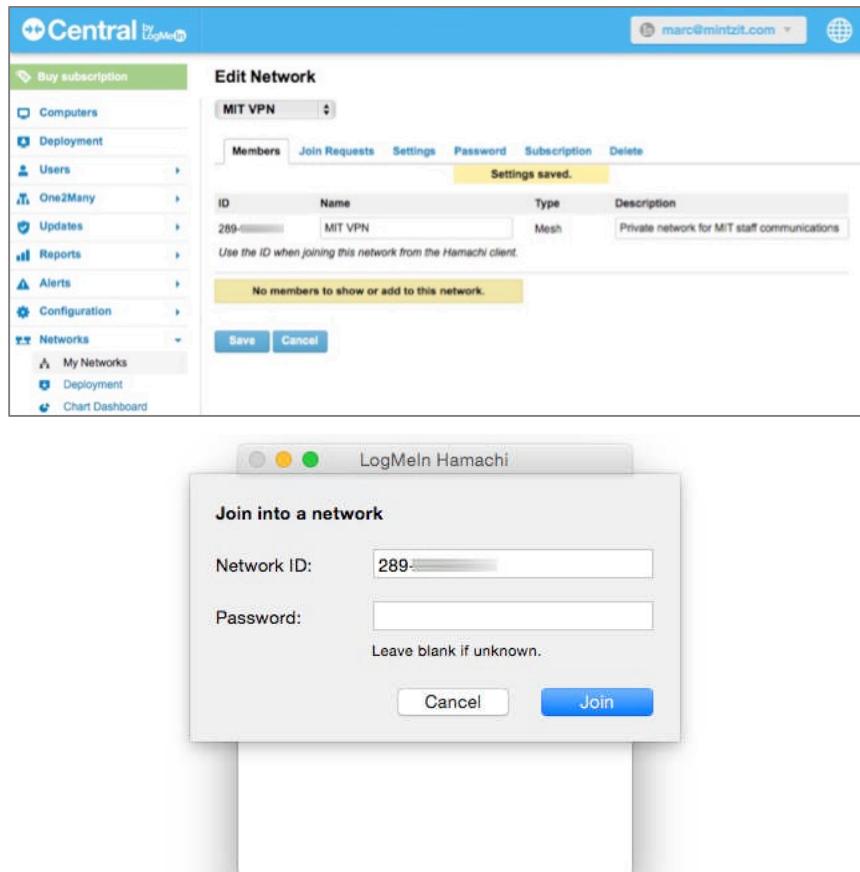


16. In LogMeIn Hamachi select *Network* menu > *Join an existing network...*

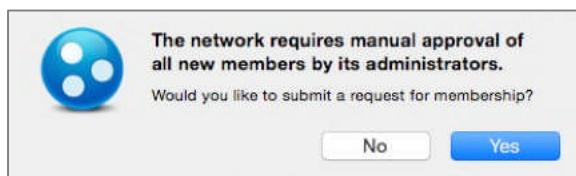


19 Internet Activity

17. Enter the *Network ID* as displayed in step 18 of the previous exercise, and then select the *Join* button.

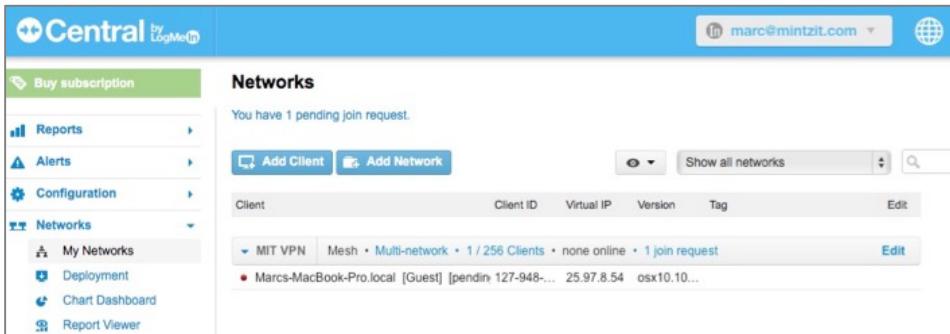


18. At the dialog box asking *Would you like to submit a request for membership?* Select the *Yes* button.



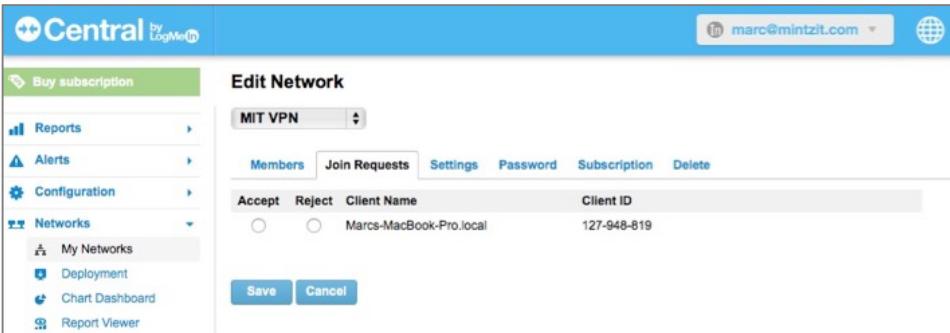
19 Internet Activity

19. Back at your computer, or the computer used to administer this network, in the *LogMeIn Central* page > *Networks* > *My Networks* will be found all of the users who have received and responded to their links from the previous steps. Select the *Edit* link.



The screenshot shows the 'Networks' section of the LogMeIn Central interface. On the left, there's a sidebar with 'Buy subscription' and links for 'Reports', 'Alerts', 'Configuration', and 'Networks'. Under 'Networks', 'My Networks' is selected. The main area is titled 'Networks' and displays a message: 'You have 1 pending join request.' Below this are buttons for 'Add Client' and 'Add Network'. A search bar and filter options ('Show all networks') are also present. A table lists clients with columns for 'Client', 'Client ID', 'Virtual IP', 'Version', 'Tag', and 'Edit'. One row is expanded to show 'MIT VPN' (selected), 'Mesh', 'Multi-network', '1 / 256 Clients', 'none online', and '1 join request'. Another row shows 'Marc's-MacBook-Pro.local [Guest] [pendin...' with 'Client ID' 127-948-819. An 'Edit' button is visible next to the expanded row.

20. In the *Edit Network* page, select *Join Requests*. If the pending join request is from someone who should join the network, select the *Accept* radio button. If they are someone who should not join the network, select the *Reject* radio button, and then select the *Save* button.



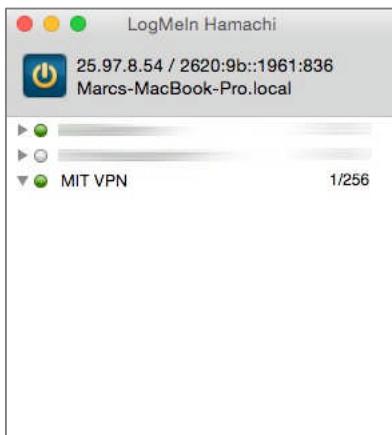
The screenshot shows the 'Edit Network' page for the 'MIT VPN' network. The sidebar is identical to the previous screenshot. The main area has a dropdown for 'Network' set to 'MIT VPN'. Below it, tabs for 'Members', 'Join Requests' (which is selected), 'Settings', 'Password', 'Subscription', and 'Delete' are shown. Under 'Join Requests', there are two radio buttons: 'Accept' and 'Reject'. Next to them are fields for 'Client Name' (set to 'Marc's-MacBook-Pro.local') and 'Client ID' (set to '127-948-819'). At the bottom are 'Save' and 'Cancel' buttons.

19 Internet Activity

21. In the *LogMeIn Central* page > Networks > My Networks > Members you will see that this user is now part of the group.

The screenshot shows the 'Edit Network' page for 'MIT VPN' in LogMeIn Central. The 'Members' tab is active. A table lists one member: ID 289-903-664, Name MIT VPN, Type Mesh, and Description 'Private network for MIT staff communication'. Below the table, a note says 'Use the ID when joining this network from the Hamachi client.' A list of current members shows 'Name: Marcs-MacBook-Pro.local [Guest], Client ID: 127-948-819, Tag: Details (Edit)'. At the bottom are 'Save' and 'Cancel' buttons.

22. Returning to the user who has just been accepted into the group, their Hamachi window will now reflect they are part of the network (the network appears in the window) and that they are actively joined to the network (green button next to the network name.)



Awesome! You have your first member of the VPN network. Of course you can't do anything with just one person. The value of VPN comes with additional members. Repeat the steps in this assignment to have at least one more computer part of your network, and then move on to the next assignment.

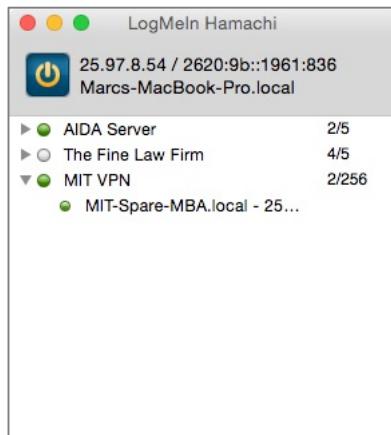
19.5.3 Assignment: File Sharing Within a Hamachi VPN Network

In this assignment we will file share within a Hamachi VPN network. Completing the previous assignment is a prerequisite.

In the typical macOS network environment, one Mac can see another Mac over the network using an automatic discovery protocol, *Bonjour*. This protocol isn't in effect over a VPN connection, so we will need a different method of accessing other computers for file sharing and other network activities.

Before we begin, please make sure the other computer has *System Preferences > Sharing > File Sharing* enabled, that SMB file sharing is enabled, and that you know a username/password allowed to file share.

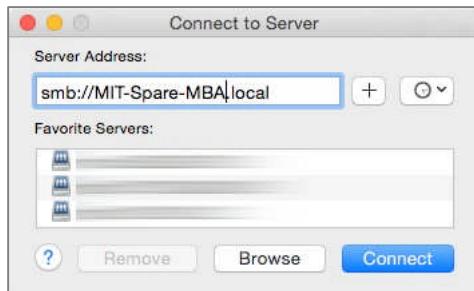
1. Launch *Hamachi*, and verify the target computer is showing as *Online*. In this example, the other computer is named *MIT-Spare-MBA.local*.



2. On your macOS/OS X computer, in the *Finder*, select the *Go menu > Connect to Server*. Enter *afp://<name of computer>* (to create an *Apple Filing Protocol*

connection), or *smb://<name of computer>* (to create a *Server Message Block* connection) and then select the *Connect* button.

- Although AFP⁸ is the legacy standard of communication between Apple computers. As of OS X 10.10, Apple is moving away from it in favor of SMB, the long-time Windows standard. SMB⁹ is the preferred protocol for macOS. You will likely have faster network throughput using SMB.



- When the *Authentication* window appears, select *Registered User*, and then enter your authorized *Name* and *Password*, and then select the *Connect* button.



⁸ https://en.wikipedia.org/wiki/Apple_Filing_Protocol

⁹ https://en.wikipedia.org/wiki/Server_Message_Block

4. The available volumes (sharepoints) will appear. Select the desired volume, and then select the *OK* button.



5. The volume will mount to your desktop. Double-click to open and navigate it just as if it were located on your physical network.
6. To file share, all you need do is drag and drop between your computer drives and the mounted volume.
7. When you are ready to disconnect from the remote computer, drag the mounted volume into the *Eject Dock* icon.

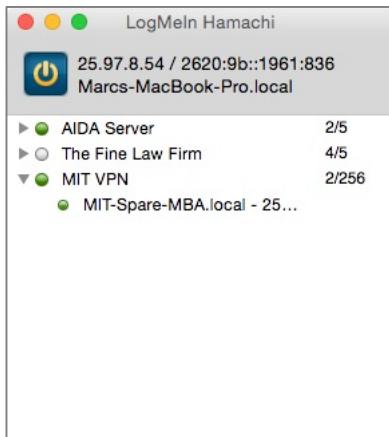
19.5.4 Assignment: Screen Share Within Hamachi VPN

In this assignment we will screen share within the Hamachi VPN environment. If you have followed the previous assignment, then screen sharing is almost identical to file sharing.

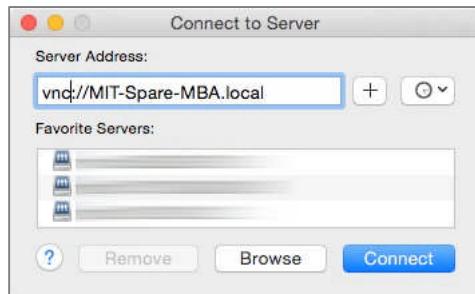
Before we begin, please make sure the other computer has *System Preferences > Sharing > Screen Sharing* enabled, and that you know a username/password allowed to screen share.

19 Internet Activity

1. Launch *Hamachi*, and verify the target computer is showing as *Online*. In this example, the other computer is named *MIT-Spare-MBA.local*.



2. On your macOS/OS X computer, in the *Finder*, select the *Go* menu > *Connect to Server*. Enter *vnc://<name of computer>* (to create a *Virtual Network Control* connection), and then select the *Connect* button.



19 Internet Activity

- At the authentication prompt, enter the authorized *Name* and *Password*, and then select the *Connect* button.

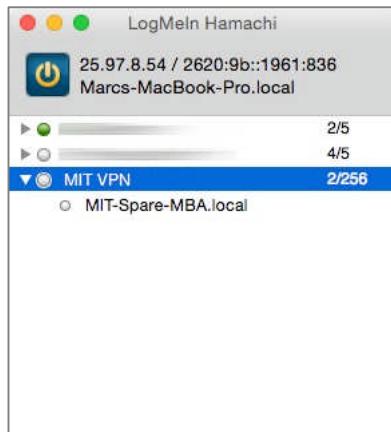


- The screen of the remote computer will appear. You will be able to control it with your mouse and keyboard.
- To exit out of screen sharing, close the *screen sharing* window.

19.5.5 Assignment: Exit the Hamachi VPN Network

In this assignment we will stop VPN so that we are no longer connected to the VPN network.

- On your computer, in the Hamachi window, right-click on the connected network name, and then select *Go Offline* menu. The network button will turn from green to white, indicating you are no longer connected.



19 Internet Activity

2. You may now *Quit LogMeIn Hamachi*.

Great work! You can now create a military-grade, encrypted network, on the fly, so that your friends or business associates can share files, screen share, etc. without fear of data or activities being spied upon.

19.6 Resolving Email Conflicts with VPN

Some email servers will send up a red flag and then block user access to email when the user switches to a VPN connection. This is a good thing as it indicates the email provider is highly sensitive to any possible security breach. In all cases there is a resolution available, although the steps to take will vary with each provider.

As an example I have outlined below what occurs when using VPN with a Gmail account, and how to gain access to your email after the blockage.

1. The user starts a VPN program to encrypt all data between the user's computer and the Internet.
2. The user attempts to receive Gmail.
3. Google sees attempted access from an unknown machine (the Proxy Server), and blocks access to the account.
4. Both an email and a text from Google are sent notifying the user of suspicious activity. Select the link in either message.
5. The first support file opens. Select the link.
6. In the authentication window, enter your email and password, and then select the *Sign In* button.
7. Another support window opens, explaining the next steps to take. Select the Continue button.
8. The final support window opens. Following the instructions, return to your email application and access your Gmail within 10 minutes. This will provide Google with the authentication to release your account.

19.7 Review Questions

1. VPN will encrypt all incoming and outgoing Internet traffic from the device it is installed on. (True or False)
2. VPN will hide or change your public IP address. (True or False)
3. Viscosity.app requires being logged in with an Administrator account. (True or False)
4. The software that can link multiple devices together into a VPN is named _____.
5. VPN stands for _____.

20 When It Is Time To Say Goodbye

Don't cry because it's over. Smile because it happened.

—Dr. Seuss¹

¹ https://en.wikipedia.org/wiki/Dr._Seuss

20.1 Preparing a Computer for Sale or Disposal

The time comes when all good things must come to an end. This is just as true for your beloved Macintosh. But, your Mac holds all of your documents, passwords, pictures, web browsing history, etc. Not the items you would like someone else to see. Even if you are tossing your damaged computer into the trash, there is the very real probability that someone will find it, remove the drive, and harvest all your data.

So before selling, giving away, or trashing your Mac, all data on the drive must be made inaccessible. There are two options:

- Securely erase the drive
- Physically destroy the drive

If you have to comply with DoD, DoE, NSA, or other top security regulations, you may have to physically destroy the drive. For the rest of us, we have a built-in application to securely erase a drive.

20.2 Secure Erase a Storage Device

If the storage device (SSD, hard disk drive, or flash drive) has been encrypted using FileVault 2, all that needs to be done is to unencrypt the storage device using Disk Utility (located in /Applications/Utilities/) by performing a reformat without encryption, and you have securely erased the device.

If the storage device (hard disk drive only, not solid state devices) has not been encrypted, Disk Utility provides the tools to erase magnetic drives (hard disk drives) to Department of Defense standards. Even though these same tools can be run on a solid state drive (SSD and flash drive), they are not 100% effective, leaving some of your data accessible. For this reason the DoD and all other governmental agencies generally do not permit the erasure of SSD's prior to sale, instead requiring the SSD to be physically destroyed. However, for use outside of DoD, first encrypting the SSD/flash with FileVault 2, and then unencrypting will provide a high level of secure erasure.

20.2.1 Assignment: Secure Erase a Storage Device

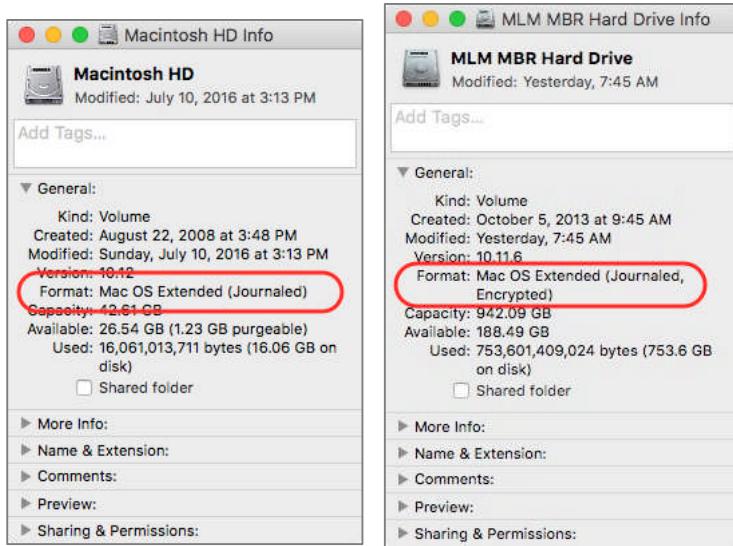
In this assignment, we will erase a drive which may or may not be encrypted with FileVault.

- Note: Do not do this assignment unless you intend to erase all of your data.

Determine if the drive is FileVault encrypted

1. Right-click on the drive, and then select *Get Info*.
2. In the *Get Info* window, examine the *Format* field. If it reads *Mac OS Extended (Journaled)*, there is no FileVault encryption. Skip to subsection below *Secure erase a non-encrypted storage device*, step 3. If it reads *Mac OS X Extended*

(*Journalized, Encrypted*), skip to the subsection below *Secure erase a FileVault encrypted storage device*.

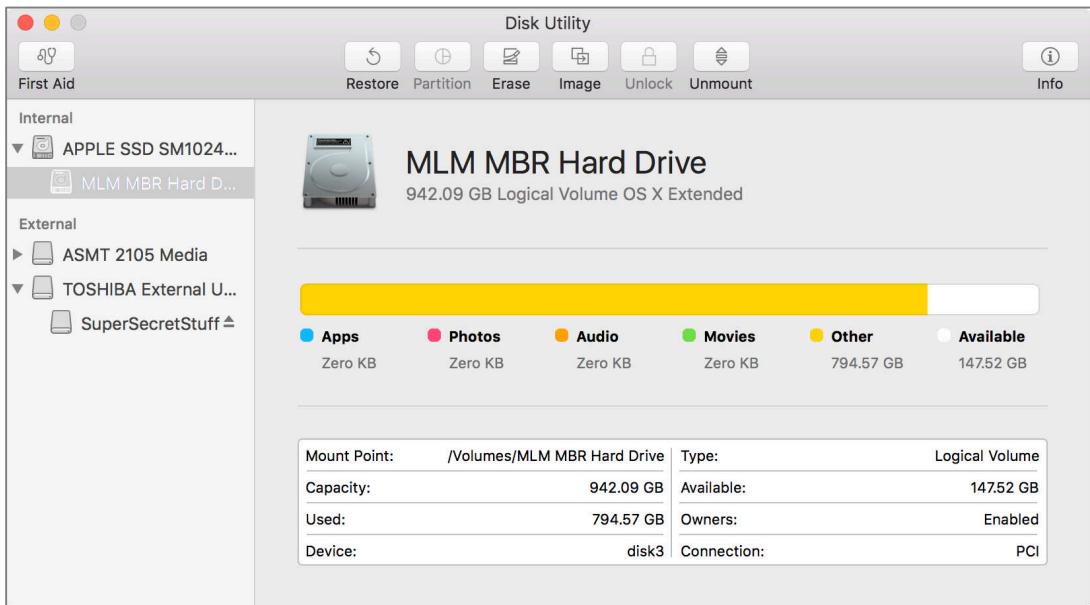


Secure erase a non-encrypted storage device

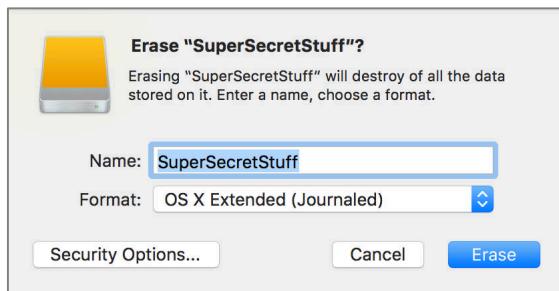
3. If you will be secure erasing a non-boot drive, open *Disk Utility* located in /Applications/Utilities, and then skip to step 6.
4. If you will be secure erasing a boot drive, restart your computer into *Recovery HD mode* by holding down the cmd+R keys immediately after restart.
5. At the *macOS/OS X Utilities* window, select *Disk Utility*.

20 When It Is Time To Say Goodbye

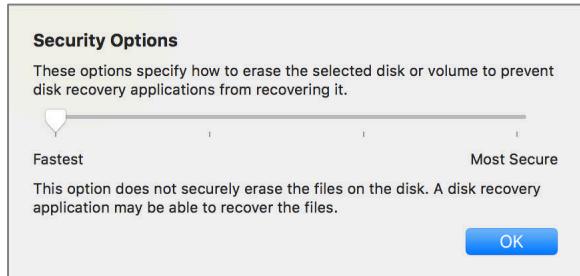
- From the sidebar, select the volume to be erased (indented names).



- From the toolbar, select the *Erase* button.
- From the *Erase* window, select the *Security Options...* button.



9. In the *Security Options* window, select your desired level of secure erase.



- *Fastest* only erases the directory structure, but leaves the data intact. It is trivial to recover data from such an erase procedure, but this only takes a few seconds.
- One tick to the right writes a single pass of zeros over the entire disk, directory and data. Depending on the disk size and speed, this may take from a few minutes to hours. Though this is considered secure, a determined hacker may be able to recover your data.
- Two ticks to the right meets Department of Energy (DoE) compliance regulations for security with a 3-pass erase over the entire disk. This will take 3 times longer than the single pass of zeros. Highly sophisticated hackers might be able to recover your data.
- *Most Secure* meets Department of Defense (DoD) compliance regulations for security with a 7-pass erase over the entire disk. This will take 7 times longer than the single pass of zeros. It is highly unlikely anyone but the government will be able to recover data from this procedure. If you have the time, this is the step to take.

10. Select the *OK* button, and then click the *Erase* button to start the erase process.

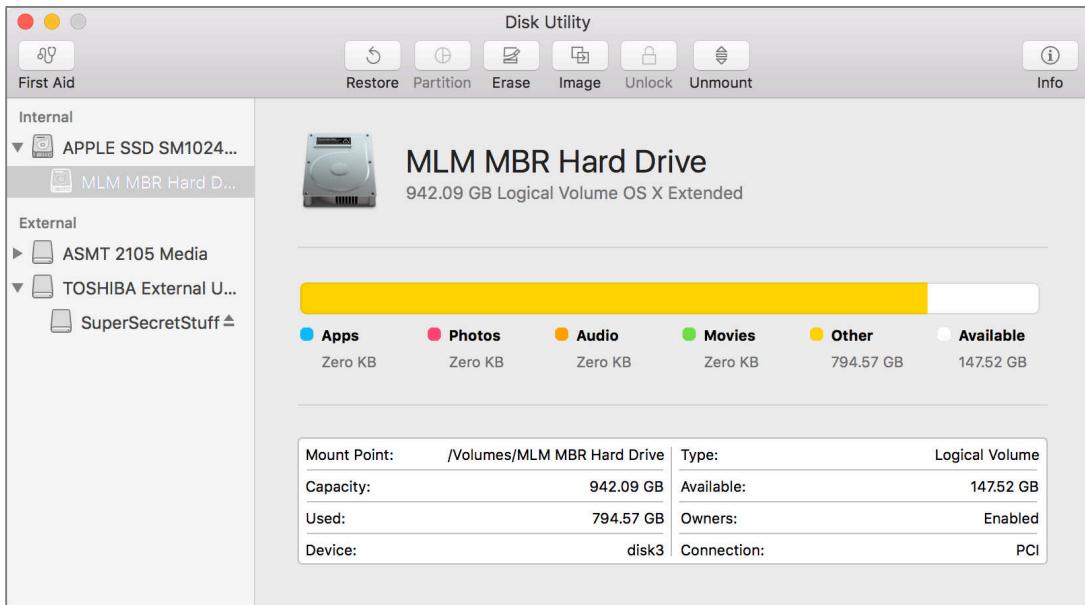
Done! The data on the drive is no longer readable.

Secure erase a FileVault encrypted storage device

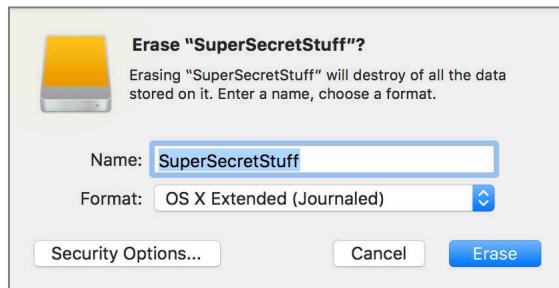
11. If you will be secure erasing a non-boot drive, open *Disk Utility* located in /Applications/Utilities, and then skip to step 15.
12. If you will be secure erasing a boot drive, restart your computer into *Recovery HD mode* by holding down the cmd+R keys immediately after restart.

20 When It Is Time To Say Goodbye

13. At the *macOS/OS X Utilities* window, select *Disk Utility*.
14. From the sidebar, select the volume to be erased (indented names).



15. If the target volume is in gray, select the *File* menu > *Unlock*. At the authentication window, enter the password of any user authorized to access this storage device.
16. From the toolbar, select the *Erase* button.
17. From the *Erase* window, in the *Name* field, enter the desired name for the storage device. In the *Format* field, select *OS X Extended (Journaled)*.



18. Click the *Erase* button.

20 When It Is Time To Say Goodbye

The process of removing the encryption while erasing provides full secure erase for the storage device.

20.3 Review Questions

1. To secure erase a boot device requires booting into _____.
2. When erasing a storage device, the *Fastest* option erases all directory information and data. (True or False)
3. If a storage device is using FileVault 2 encryption, it can be securely erased by reformatting without encryption. (True or False)

21 Miscellaneous

The nice thing about standards is that you have so many to choose from.

–Andrew S. Tanenbaum¹

¹ https://en.wikipedia.org/wiki/Andrew_S._Tanenbaum

21.1 Date and Time Settings

There are several reasons it is critical to keep your computer date and time accurate:

- If you are on a network with other computers, or use the services of a server, if your clock is off by more than a few minutes, you may be blocked as the other systems see this as a potential *man in the middle* attack.
- Should your computer become compromised by malware or criminal, it will be important to know the exact moment the penetration occurred.
- You don't want to be late to your Aunt Rose's dinner party. Noodle Koogle is best right out of the oven.

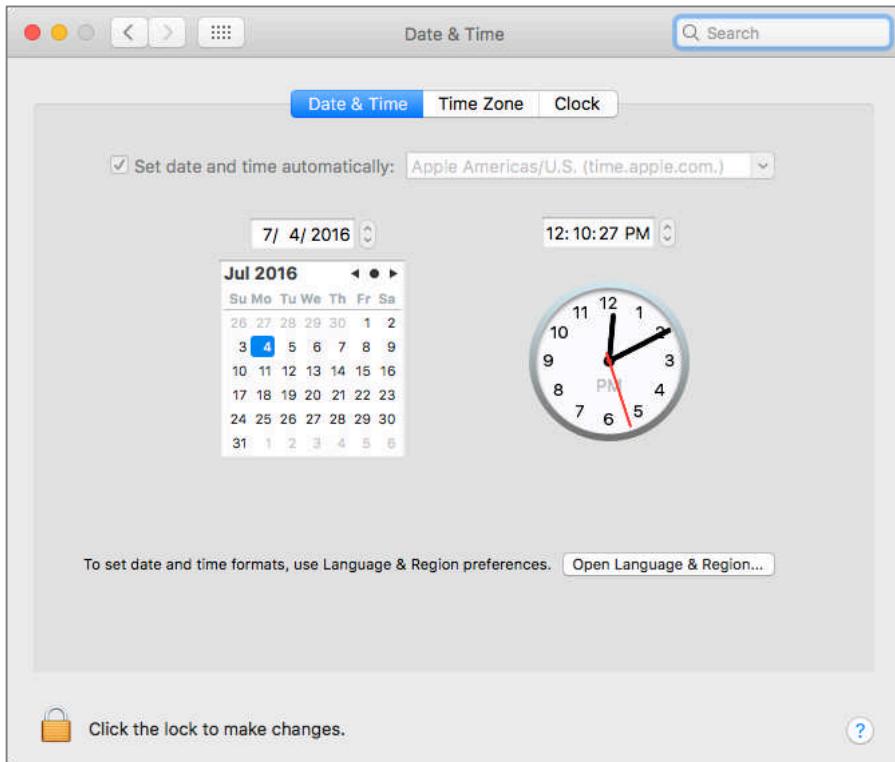
Fortunately, all Apple computers include the ability to automatically synchronize with Apple's atomic clocks, any International atomic clock, or any Network Time Protocol² (NTP) server you choose.

² https://en.wikipedia.org/wiki/Network_Time_Protocol

21.1.1 Assignment: Configure Date & Time

In this assignment you will configure your macOS computer to use the Apple NTP server.

1. Open *Apple* menu > *System Preferences* > *Date & Time*.



2. Select the *Date & Time* tab.
3. Click the *Lock* icon, and then authenticate.
4. Enable the checkbox *Set date and time automatically*.
5. From the *Set date and time automatically* pop-up menu, select the Apple NTP server closest to you.
 - Note: If you have an NTP server within your organization, you may enter either its IP address, or its Fully Qualified Domain Name in this field.
6. Close System Preferences.

21 Miscellaneous

Your computer will now automatically synchronize its time with the configured NTP server.

21.2 Hardware Components

Some hardware components may present a security risk to either the system or the organization that out-weighs their benefit. For example, the built-in camera included with a MacBook Pro is a convenience for those of us who enjoy video conferencing, but if that computer is part of a military base, the risk to security is too great to allow it to function.

When security needs are high, some hardware components may need to be disabled to ensure malware, hackers, or disgruntled staff cannot use the hardware to their evil ends.

Generally, there are two options to disable hardware: modify the hardware settings, or remove the Kernel Extension.

Modifying the hardware settings is the easiest option, but in many cases, either the user or malware/hacker is able to reverse the setting, re-enabling the hardware.

Removing the Kernel Extension does not always ensure the hardware is disabled, and will often be reinstalled during system updates.

Whichever path is taken, it is necessary to perform routine risk assessments to verify the hardware remains disabled.

Bluetooth Disable Via Settings:

In Terminal, enter on one line and then tap *Return* or *Enter key*:

```
defaults write /Library/Preferences/com.apple.Bluetooth.plist
ControllerPowerState -bool false
```

Bluetooth Enable Via Settings:

In Terminal, enter on one line and then tap *Return* or *Enter key*:

```
defaults write /Library/Preferences/com.apple.Bluetooth.plist
ControllerPowerState -bool true
```

Bluetooth Disable Via Kernel Extension:

Remove or rename the following files:

/System/Library/Extensions/IOBluetoothFamily.kext

/System/Library/Extensions/IOBluetoothHIDDriver.kext

Built-In Camera: Disable Via Kernel Extension:

Remove or rename the following files:

/System/Library/Extensions/IOUSBFamily.kext/Contents/Plugins/

AppleUSBVideoSupport.kext

/System/Library/Extensions/Apple_iSight.kext

/System/Library/Frameworks/CoreMediaIO.framework/Versions/A/Resources/
VDC.plugin

Firewire: Disable Via Kernel Extension:

Remove or rename the following file:

/System/Library/Extensions/IOFireWireSerialBusProtocolTransport.kext

Infrared: Disable Via Settings:

In Terminal, enter on one line and then tap *Return* or *Enter key*:

```
defaults write /Library/Preferences/  
com.apple.driver.AppleIRController.plist DeviceEnabled -bool false
```

Infrared: Enable Via Settings:

In Terminal, enter on one line and then tap *Return* or *Enter key*:

```
defaults write /Library/Preferences/  
com.apple.driver.AppleIRController.plist DeviceEnabled -bool true
```

Infrared: Disable Via Kernel Extension:

Remove or rename the following file:

/System/Library/Extensions/AppleIRController.kext

USB: Disable Via Kernel Extension:

Remove or rename the following file:

/System/Library/Extensions/IOUSBMassStorageClass.kext

Wi-Fi: Disable Via Settings:

In Terminal, enter on one line and then tap *Return* or *Enter key*:

```
networksetup -setairportpower en1 off
```

Wi-Fi: Enable Via Settings:

In Terminal, enter on one line and then tap *Return* or *Enter key*:

```
networksetup -setairportpower en1 on
```

Wi-Fi: Disable Via Kernel Extension:

Remove or rename the following file:

/System/Library/Extensions/IO80211Family.kext

21.3 National Institute of Standards and Technology (NIST)

NIST, part of the U.S. Department of Commerce, was established by congress in 1901 to improve our measurement systems. Sub-standard measurement systems were impeding the U.S. economic growth. This mission continues into the 21st-century by developing standards of measurement at the nanoscale through galactic scale.

NIST is also involved in developing standards for computer and IT systems. Some organizations—most particularly healthcare, financial, and legal—base much of their cybersecurity measures on NIST recommendations.

As of the time of this writing, NIST had just released their *Draft NIST Special Publication 800-179 Guide to Securing Apple OS X 10.10 Systems for IT Professionals: A NIST Security Configuration Checklist*³. This publication details how NIST recommends configuring the security of OS X 10.10 (and presumably macOS) computers.

Following the steps outlined in *Practical Paranoia*, you will likely pass a NIST-based security audit. That said, if your organization is held to NIST protocols, you will be held accountable for knowing them from the NIST perspective, and reading their guide is mandatory.

21.3.1 NIST-Specific Security Settings

The settings that NIST may require for your environment, but were either not mentioned or are otherwise recommended in *Practical Paranoia* include the following, prefaced by the NIST publication section number:

- 6.3.2.5 Fast User Switching. Off.

³ http://csrc.nist.gov/publications/drafts/800-179/sp800_179_draft.pdf

- 6.3.4 Password Policies. NIST recommends setting a maximum password age, minimum password length, minimum password complexity, preventing use of past passwords.
- 6.3.5 Session Locking. Set screen saver to start after 20 minutes of idle time.
- 6.3.6 Credential Storage. Change the Keychain password so that it is different from the login password. Set Keychain to lock when the screen saver starts.
- 6.3.8 Sudo. Restrict use of the sudo command to a single Terminal session. In Terminal, enter:
`echo "Defaults_tty_tickets" >> /etc/sudoers_`
- 6.3.8 Sudo. Force authentication for each invocation of the sudo command (default is to force authentication once every 300 seconds). In Terminal enter:
`echo _Defaults timestamp_timeout_=0" >> /etc/sudoers`
- 6.4.1 Audit Policies and Tools. Details the need for constant monitoring of log files.

22 The Final Word

If you have followed each of the steps outlined in this book, your computer now is secured to a level higher than even the NSA requires for its own staff. Although this won't prevent one of the bad guys from stealing your computer, it will prevent them from accessing your data. And since you have at least one current backup at the home or office, and one on the Internet, you are still in possession of the items with *real* value—your data, and peace of mind.

Mintz InfoTech, Inc. macOS Security Checklist

I have included the checklist that all of us at Mintz InfoTech, Inc. use when performing Security Checks for our clientele. This same checklist should be used to ensure your own system is fully hardened.

Data Loss

- Time Machine active and encrypted
- Time Machine password recorded
- Carbon Copy Cloner backup active and encrypted
- Internet-based backup active (CrashPlan or CrashPlanPro recommended)
- Integrity test Time Machine backup monthly
- Integrity test Carbon Copy Cloner backup monthly

Passwords

Critical

- Strong account passwords
- All passwords recorded
- All challenge questions and answers recorded

Optional

- Harden the Keychain with a different password than the user account password
- Harden the Keychain with a timed lock
- Synchronize Keychain across macOS/OS X and iOS devices through iCloud
- Synchronize Passwords across Android, iOS, macOS/OS X, and Windows devices with LastPass
- Password Manager in use (LastPass recommended)

System and Application Updates

Critical

- All OS updates installed
- All application updates installed
- Configure App Store to automatically install updates

Optional

- Install MacUpdate Desktop to automate application updates

User Accounts

Critical

- All users log in with non-administrative accounts
- Create an administrative account whose credentials may be used for administrator tasks
- Root user not enabled
- Guest user account enabled, no file sharing access to any folders

Optional

- Application Whitelisting with Parental Controls enabled for all non-administrator accounts

Storage Device

- Enable FileVault 2 Full Disk Encryption

Sleep and Screen Saver

- Require Password after Sleep or Screen Saver

Malware

- Install antivirus software (Bitdefender recommended)
- Configure antivirus software for automatic updates

Firewall

- Enable the Firewall
- Close unnecessary ports

Firmware Password

- Firmware password enabled
- Firmware password recorded

Lost or Stolen Device

- Find My Mac active
- Guest User Log in enabled

When It Is Time to Say Goodbye

- Secure erase storage device

Local Network

Critical

- WPA2 with AES encryption for all Wi-Fi networks
- Strong password in use for Wi-Fi
- Wi-Fi password recorded
- No Ethernet hubs in use, only Ethernet switches
- Modems and routers power-cycled
- Modems and routers firmware updated
- Modems and routers checked for DNS Servers
- Modems and routers checked for Port Forwarding
- Modems and routers checked for DMZ

Optional

- MAC Address to Limit Wi-Fi Access
- RADIUS authentication used for Wi-Fi and Ethernet access

Web Browsing

Critical

- HTTPS Everywhere installed (if using Firefox or Chrome)
- Client educated on recognizing secure and unsecure web pages
- DuckDuckGo search engine used
- Adobe Flash updated (if installed)
- Java updated (if installed)
- User educated on web scams

Optional

- Private Browsing used
- Tor installed and configured

Email

- All email accounts using either SSL, TLS, or HTTPS
- User educated on how to recognize phishing attacks

Does the client need end-to-end email security?

If “No,” then skip this section. If “Yes,” as appropriate, set up with ProtonMail, S/MIME or GPG:

- Create a ProtonMail account for our client, and then educate client how to use ProtonMail.
Or:
 - Acquire a Class 1 or 3 S/MIME certificate, install on computer, and then educate client how to use and have others do same.
Or
 - Install GPG, and then educate client how to use and have others do same.

Apple ID and iCloud

- Create an Apple ID
- Implement Apple ID Two-Step Verification
- Two-Step Verification Recovery Key recorded
- iCloud account active on the computer
- Two-Step Verification enabled

Document Security

Does the client need secure documents?

If “No,” then skip this section. If “Yes”:

- Educate how to password protect Microsoft Office documents
- Educate how to convert to .pdf, then how to password protect .pdf documents
- Educate how to create password protected disk images
- Download, configure, and educate how to use VeraCrypt

Audio, Video, and Instant Message Communications

- Educate user that when instant messaging between macOS/OS X and iOS users with Facetime or Messages, all communications are secure
- If instant messaging with Android, Windows, or any OS other than macOS/OS X and iOS, install and educate how to use Wire

Internet Activity

- Consult with user the comparisons between VPN and Tor/Tails to determine the best fit for their use
- As appropriate, install VPNArea VPN account and configure its software

MintzIT macOS Security Checklist

- Educate the client how to use VPN software
 - Or
- Create a Tails bootable thumb drive
- Educate the client how to use Tor/Tails
- Install LogMeIn Hamachi Mesh VPN

Change History

20160906, v1.1:

- Minor clean up
- Replaced Protonmail for SendInc in the Email chapter

20160901, v1.0.2:

- Minor clean up

20160801, v1.0.1:

- Minor typographical clean up
- Creation of forking for both a Student and Instructor book versions
- Replaced Wire for uTox in the Voice, Video, and Instant Message Communications chapter
- Removed Review Answers from the student version

20160801, v1.0:

- Initial release

Index

- 802.1x 229, 231
access point 232
administrative 122, 128, 129, 131, 193
administrator ..52, 120, 122, 128, 129, 131, 213, 215, 236
AES 70, 231, 504, 510, 629
Airport 33, 235, 236, 238, 244, 248, 250
Al Gore 525
Andrew S. Tanenbaum 617
Android 490, 553
Anonymous Internet Browsing.... 338
antenna 228
anti-malware 110, 131, 170, 171
Antivirus 170, 174, 175, 180, 181, 183
App Store..... 110, 222, 454
Apple ID ... 66, 87, 110, 218, 222, 453, 454, 455, 456, 457, 463, 465, 475
Application Updates 111, 115
Assignment .36, 40, 42, 43, 49, 53, 63, 71, 74, 77, 81, 83, 86, 87, 92, 101, 102, 109, 111, 115, 122, 126, 127, 129, 132, 143, 145, 150, 151, 153, 154, 155, 159, 162, 174, 193, 196, 206, 207, 212, 218, 222, 233, 235, 239, 244, 251, 261, 266, 278, 283, 284, 286, 289, 290, 291, 292, 293, 294, 296, 298, 300, 302, 303, 304, 307, 308, 313, 314, 316, 317, 323, 327, 329, 338, 349, 368, 373, 375, 380, 383, 389, 395, 401, 403, 405, 409, 411, 415, 421, 430, 441, 445, 448, 455, 465, 467, 479, 482, 485, 488, 489, 491, 495, 499, 505, 517, 529, 534, 539, 540, 544, 547, 555, 558, 569, 570, 572, 576, 589, 599, 601, 603, 609, 619
Aung San Suu Kyi 363
AV Comparatives..... 170
Avira..... 172
Backblaze 35
backup..... 32, 33, 34, 35, 42, 53, 222
Backups..... 42
Ban Ki-moon 149
Benjamin Franklin 275
Bitdefender....171, 174, 177, 180, 183
Blog..... 27
Boot Camp 170, 171
broadcasting..... 212, 228
Carbon Copy Cloner.... 34, 36, 43, 44, 45, 49, 50
Carbonite..... 35
Certificate Authorities 414
Chameleon560, 563, 564, 566, 568
Cisco..... 62
CISPA..... 23
Clear History..... 292
clone 34, 47, 48, 49, 50, 51, 52, 53, 54, 55

Index

- Comodo 415, 419, 421, 428, 430, 431, 442, 443
Computer theft 32
Cookies 289, 317
crack 62
CrashPlan 35, 627
Criminal activities 32
Deep Web 360
Disk Decipher 490
Disk Utility 36, 485
DMZ 260
Do Not Track.316, 317, 318, 323, 324
DoD 608, 609, 612
DoE 608, 612
Dr. Seuss 607
DuckDuckGo 289, 290, 291
Ed Snowden 360
EDS 490
EFI Chip 206
Elayne Boosler 205
Elbert Hubbard 161
Email 101, 363, 367, 368, 374, 380, 383, 388, 394, 395, 397, 409, 411, 414, 415, 416, 417, 419, 422, 423, 439, 440, 442, 443, 444, 605
Encrypt ... 51, 277, 405, 407, 408, 479, 482, 485, 488
Encrypted Data Store 490
encrypted email 367, 372, 388, 389, 445, 446, 447, 448
encryption 52, 53, 152, 157, 228, 230, 233, 276, 367, 373, 374, 409, 450, 478, 479, 482, 486
Entropy 32
Erase 221, 609
Ethernet 218, 228, 229
Facebook..... 27, 62
Facetime..... 526
FAT 514
FBI 23
FileVault 50, 51, 52, 152, 155, 157, 160, 212, 478, 609, 615, 628, 648, 656
FileVault 2 . 50, 52, 152, 155, 212, 478
Find My iPhone.... 219, 220, 222, 223, 224
Find My Mac..212, 213, 218, 220, 222
Find My Mac? 212
Fire..... 32
firewall .. 192, 193, 194, 195, 197, 198, 199, 232
FireWire..... 33, 34, 36, 150, 151
Firmware 205, 206, 207, 212, 261, 628
Firmware Password..... 157, 206, 207, 208, 628, 649
Flash 23
FUSE 491, 493, 494
Gateway VPN 551
General Douglas MacArthur 227
George Carlin..... 31
GNU Privacy Guard 374, 388
Google Hangouts..... 526, 527
GPA 389
GPG..... 388, 389, 391, 395, 396, 401, 402, 403, 409, 410, 411, 413, 414, 445, 448, 450
GPG Keychain Access . 395, 396, 401, 413
GPG Public Key..... 389
Gpg4win 389
GPGMail..... 403
GPGTools..... 389, 390, 395, 401
Gravity Zone 171, 174

Index

- Guest 121, 132, 212, 213, 214, 216, 218, 628
Hamachi 576, 577, 589, 590, 591, 592, 595, 598, 599, 601, 602, 603, 604
haystack 62, 63, 64
Henry David Thoreau..... 549
HIPAA 35
Honore de Balzac 169
Hot Corners 165
https... 62, 64, 276, 277, 278, 280, 281, 367, 368, 373, 374, 629
HTTPS Everywhere 277, 278, 340
Hypertext Transport Layer Secure 367
iCloud 65, 66, 67, 86, 87, 91, 156, 212, 218, 219, 453, 454, 455, 456, 458, 462, 465, 475, 630
Incognito Mode 283
infected 62
Insertion 228, 229, 240, 252
Integrity Test 42
Integrity Testing 53
iOS 86, 388, 414, 490
ipconfig 246, 247, 255, 256
iTunes 455
Java 23
Joseph Heller 19
Keychain 65, 68, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 91, 234, 393, 396, 401, 403, 420, 421, 444, 462, 464, 627
LAN 232
LastPass 63, 92, 101, 102, 103
Linux 336, 337, 388, 389, 490, 514
Local Area Network 232
LogMeIn 576, 580, 581, 583, 584, 585, 589, 591, 594, 595, 597, 598, 604
MAC Address 243, 250
Mac OS Extended 486, 514
MacKeeper 312
MacUpdate 111, 113, 114, 115, 116
MacUpdate Desktop 111, 113, 115
maintenance 33, 122
Malware 32, 122, 170
Managed with Parental Controls 121, 131, 132
MARC L. MINTZ 15, 19, 25, 26, 59
Mark Twain 119
Mintz's extrapolation of Sturgeon's Revelation 22
modem 232
Newsletter 27
NIST 21, 510, 623, 624
NSA ... 21, 60, 206, 207, 450, 510, 552, 575, 608, 625
NTP 618, 619, 620
Onion Sites 360
Parallels 171, 340
Parental Controls . 121, 131, 132, 133, 143, 144
passphrase 62
password.... 23, 52, 61, 62, 63, 64, 122, 128, 131, 152, 156, 206, 207, 212, 221, 222, 229, 230, 236, 238, 368, 373, 375, 454, 479, 485, 486, 487
permissions 122
PGP 388, 414, 450
phishing 23, 170, 365, 652
port 192, 260
Port forwarding 260
Ports 196

Index

- Power surges 32
Practical Paranoia Book Upgrades 28
Practical Paranoia Updates 27
Pretty Good Privacy 388
private browsing 283
ProtonMail 374, 375, 380, 382, 383
Public Key 388, 389, 394, 395, 401, 403, 409, 411, 445, 446, 447, 448
RADIUS 229
RAM-Resident Malware 260
Recovery HD 49, 50, 51, 207, 610, 612
Recovery Key 52
Root 120, 122, 125, 126, 127
router 232, 233, 239, 260, 261, 266
S/MIME 414, 415, 421, 430, 432, 437, 440, 441, 445, 446, 448, 450
Sabotage 32
Screen Saver 162, 165
screensaver 166
SEC 35
Secure Socket Layer 276
Seneca 107
Server 33, 228, 229
SHA 510
Sharing Only 121
Single User Mode 206
Skype 526, 527
sleep... 50, 53, 157, 162, 163, 164, 165, 166, 243, 283, 550
software 33, 35, 62, 122, 170, 228, 375
SSL 276, 368, 371, 374
Standard 121, 130, 132, 392, 507
Static electricity 32
stealth 196
switch 232
Symantec 23, 388
System Updates 107
Tails 336, 337, 338, 340, 359, 630, 631
Target Disk Mode 206
Terrorist activities 32
theft 23, 32, 33
Theodore Roosevelt 191
Theodore Sturgeon 22
thepracticalparanoid 446
Thomas Jefferson 59
Thomas Sowell 211
Thunderbolt 33, 34
Time Machine ... 33, 34, 36, 40, 41, 42, 627
TKIP 231
TLS 367, 368, 371
Tor. 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 348, 349, 359, 360, 629, 630, 631
TorBrowser 341, 347, 349
TrafficLight 183, 185, 186, 297
Trojan horses 23, 170
TrueCrypt 490, 501
Two-Step Verification ... 87, 454, 465, 630
USB 33, 34, 36, 150, 151
US-CERT 108
User Accounts 119
uTox 540, 542, 544
VeraCrypt 490, 491, 495, 499, 504, 505, 506, 507, 517, 518, 520, 521
virtual machine 170, 171, 340
Virtual Private Network 230, 277, 550
viruses 23
Viscosity 555, 559, 569, 570, 571, 572, 574
VMware Fusion 171

Index

- | | | | |
|-------------------|---|-------------------------|---|
| VPN..... | 230, 235, 277, 550, 551, 552, 553, 555, 560, 564, 567, 568, 569, 575, 576, 587, 589, 595, 598, 599, 601, 603, 605, 630, 631 | Wi-Fi | 23, 212, 218, 228, 229, 230, 233, 234, 235 |
| VPNArea | 549, 555, 560, 562, 564, 567, 568, 569 | William Blum..... | 477 |
| war driving | 23 | William Hazlitt | 453 |
| Water damage..... | 32 | Windows | 150, 170, 171, 172, 246, 255, 336, 388, 389, 490, 514, 553, 600 |
| Web Mail..... | 373 | Wire..... | 529 |
| WEP | 230, 233 | worms | 23, 170 |
| Whitelisting..... | 131 | WPA..... | 230, 231, 233 |
| | | WPA2..... | 230, 231, 233, 235, 238 |
| | | zero-day exploits | 24 |

Your Virtual CIO & IT Department

Mintz InfoTech, Inc.

when, where, and how you want IT

Technician fixes problems.

Consultant delivers solutions.

Technician answers questions.

Consultant asks questions, revealing core issues.

Technician understands your equipment.

Consultant understands your business.

Technician costs you money.

Consultant contributes to your success.

Let us contribute to your success.

Mintz InfoTech, Inc. is uniquely positioned to be your Virtual CIO and provide you and your organization comprehensive technology support. With the only MBA-IT consultant in New Mexico heading our organization, our mission is to provide small and medium businesses with the same Chief Information and Technology Officer resources otherwise only available to large businesses.

Mintz InfoTech, Inc.

Toll-free: +1 888.479.0690 • Local: +1 505.814.1413

info@mintzIT.com • <https://mintzit.com>

Practical Paranoia Security Essentials Workshops & Books

Best-Selling. Easiest. Most Comprehensive. Guaranteed.



This is an age of government intrusion into every aspect of our digital lives, criminals using your own data against you, and teenagers competing to see who can crack your password the fastest. Every organization, every computer user, everyone should be taking steps to protect and secure their digital lives.

The *Practical Paranoia: Security Essentials Workshop* is the perfect environment in which to learn not only *how*, but to actually *do* the work to harden the security of your OS X and Windows computers, and iPhone, iPad, and Android devices.

Workshops are available online and instructor-led at your venue, as well as tailored for on-site company events.

Each Book is designed for classroom, workshop, and self-study. Includes all instructor presentations, hands-on assignments, software links, security checklist, and review questions and answers. Available from Amazon (both print and Kindle format), and all fine booksellers, with inscribed copies available from the author.

Call for more information, to schedule your workshop, or order your books!

Mintz InfoTech, Inc.

Toll-free: +1 888.479.0690 • Local: +1 505.814.1413
info@mintzIT.com • <http://thepracticalparanoid.com>

