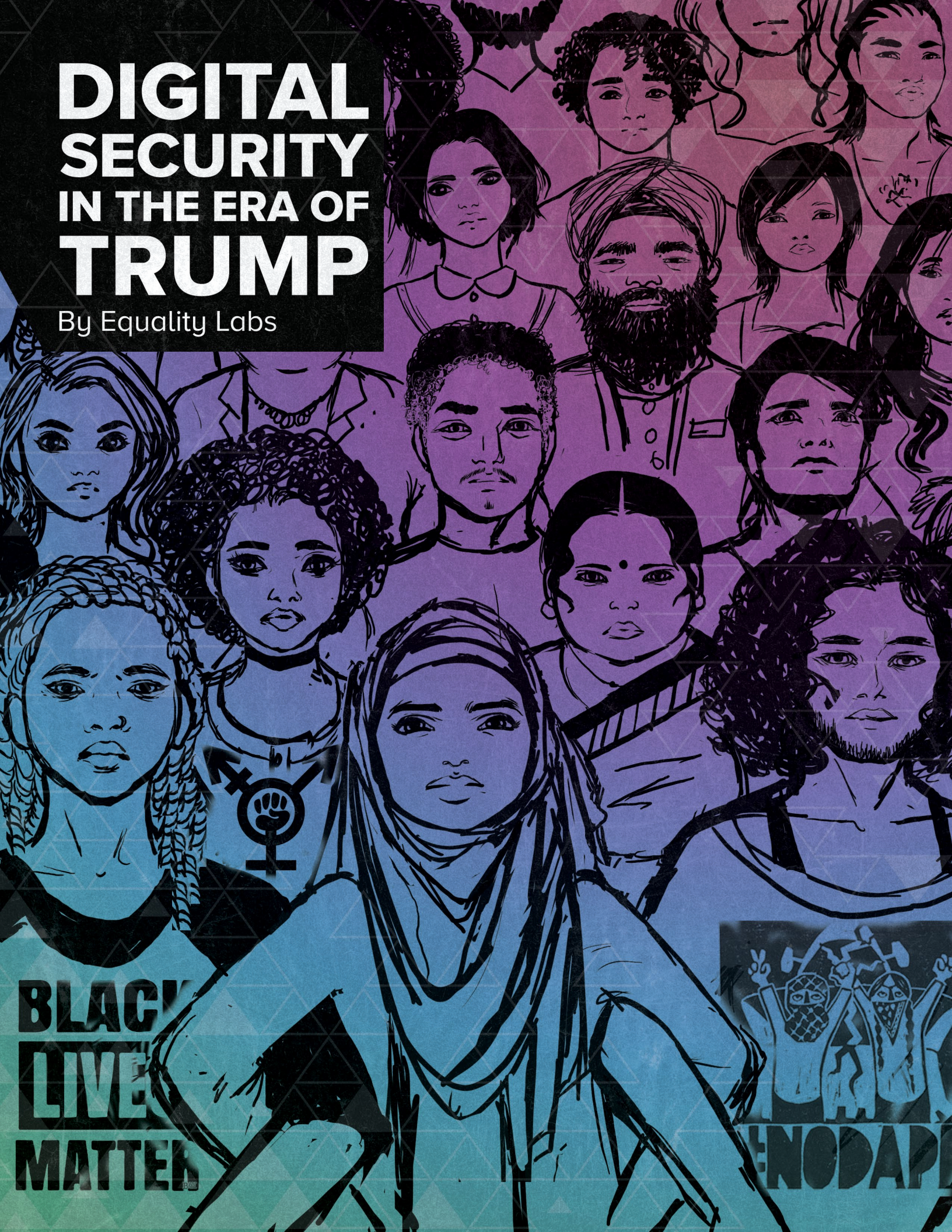
DIGITAL SECURITY IN THE ERA OF TRUMP

By Equality Labs



Credits: This curriculum is licensed under **Creative Commons** and is itself the remixing of the amazing work of many digital security experts round the world. We want to send special shout outs to Eva Galperin, Gemini Matt, Sandy Ordonez, Lyndsey Beck, Ryan Gerety, Michael Charbon and Matt and Isa **from Tor**.

This curriculum is a collective effort of Equality Labs and was compiled by Maari Zwick, Dalit Diva, DM Hommeee, and Kai

Designed by: Freedom Rios; illustrated by: Shrummi8

CONTENTS

WHY SHOULD WE CARE ABOUT SECURITY IN THE ERA OF TRUMP? 6
HOW TO USE THIS CURRICULUM 9
Legend 10
WHERE DOES THE U.S. STAND ON SECURITY ISSUES TODAY? 11
The Right to Privacy 11

WHAT IS DIGITAL SECURITY? 13
WHAT IS DIGITAL SECURITY 14
An Ecosystem of Digital Security 14
It's All About Harm Reduction Right Now 15
Sins of Security Compromise 16
How to Make a Risk Assessment 17
RISK ASSESSMENT MODEL 19
Threat Modeling Exercise

SECURE YOUR PHONE 22
A SECURE DEVICE IS ALWAYS THE FOUNDATION! 23
SECURE YOUR ANDROID 25
Lock Your SIM 25
Set Up Your Pin And Activate A Screenlock 26
Activate a Security Lock Timer 27
Android Encryption 27
Adjusting your Network Settings 29
Location Settings 29
- Hiding Caller ID 30

Updated Your Android 30
Applock for Androids 31
Dealing with Metadata on Photos 34
SECURE YOUR IPHONE 36
Activate Your Screen Lock 36
Activate Your Security Lock Timer 37
iPhone Encryption 38
Turn Off Location Services 39
ADDITIONAL SECURITY APPS FOR IPHONE 41
Guided Access for iPhone 41
Dealing With Metadata on Photos 43
- PixlMet for iPhones 44

SECURE YOUR COMPUTER 45
SECURE YOUR COMPUTER 46
Setting Up Users Accounts and Passwords 47
Disable Auto Login 50
Enable Full-Disk Encryption 50
Audit Your Security and Privacy Settings 54
Keep Your Computer's Software Updated 56
SECURING YOUR PC 57
Setting Up Users Accounts and Passwords 57
Turn On Your Firewall 58
Keep Your User Account Control Turned ON 61
Keep Your Windows Operating System Up to Date 62
Install a Traditional Antivirus for Reactive Protection 63
Device Encryption for PCs 63
Full Disk Encryption with Veracrypt 69

SECURE YOUR IDENTITY 70
PASSPHRASES REALLY ARE EVERYTHING 71
PASSPHRASE MANAGER 74
LastPass 75
KeePass X 76
1Password 77
SECURING YOUR GMAIL 80
GOOGLE SECURITY CHECK-UP 82
PRIVACY CHECK-UP 85
TWO-FACTOR AUTHENTICATION FOR GMAIL (2FA) 89
PROTECT YOURSELF FROM PHISHING 95
How Can You Identify Phishing Schemes? 95
Dealing With Phishing 97
HAVE YOU BEEN COMPROMISED? 99
Combat Trolling by Finding Your Data Online 100

SECURE BROWSING 101
NAVIGATING THE ONLINE: SEARCHING, BROWSING, AND EXTENSIONS 102
Browsers' Browser Browsers 102
Google Chrome 102
Mozilla Firefox 109
Internet Explorer 113
EXTENSIONS FOR A SAFER ONLINE SESSION 118
Privacy Badger 118
HTTPS Everywhere 119
Web of Trust 119
WHAT ABOUT SEARCH ENGINES? 121
DuckDuckGo 122

searX 122
startpage 122

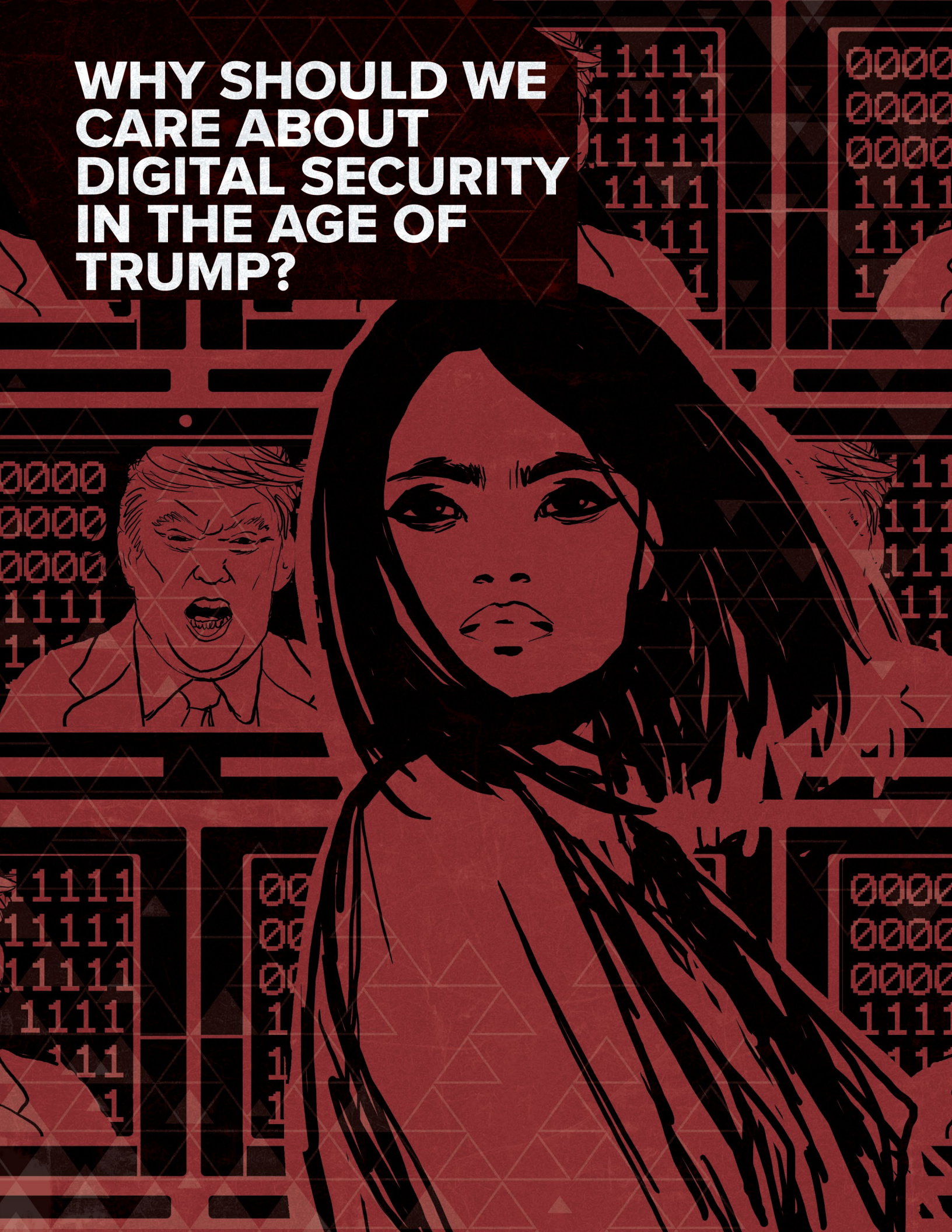
SECURE YOUR NETWORK 123
CONNECTING TO THE INTERNET—HOW DOES IT ALL WORK? 124
HOW WEBSITES ARE BLOCKED OR CENSORED 126
BROWSE THE INTERNET ANONYMOUSLY AND BYPASS CENSORSHIP 127
Tor 127
Virtual Private Networks (VPN) 131
Tor vs. VPN 134

SECURE YOUR SOCIAL MEDIA 135
SOCIAL MEDIA: BEING SMART, STAYING SAFE! 136
COMPARTMENTALIZATION: PERSONAL VS. PROFESSIONAL ACCOUNT SETTINGS 137
Facebook 137
Twitter 156
Instagram 161

SECURE YOUR COMMUNICATIONS 164
ENCRYPTION: THE PATH TO SECURE COMMUNICATION 165
SIGNAL 167
Signal for Androids and iPhones 167
Signal for Desktop—Chrome Extension 172
Safety Numbers—Signal 174
Disappearing Messages—Signal 177
SEMAPHOR 179
WHATSAPP 181
FACEBOOK MESSENGER 183
SENDING SECURE EMAIL USING ENCRYPTION 185
Using GPG Tools for MAC 187
GPG For Windows Using GNU Privacy Assistant 196
Safer Online Activism 101: Setting Up Social Media Accounts That Can't be Tracked 203

IN CONCLUSION 205
APPENDIX: MORE INFORMATION AND RESOURCES 206
GLOSSARY OF TERMS 209

WHY SHOULD WE CARE ABOUT DIGITAL SECURITY IN THE AGE OF TRUMP?



Fam, these are probably going to be some of the hardest years of our lives. And yes, it is going to get worse before it gets better.

Across the country we're all waking up and trying to understand what does the new administration mean for me. What will I lose, who else will be vulnerable, and yes, how can I fight.

At Equality Labs we believe we must begin the fight by understanding how we can fight safely, and how to protect ourselves and our communications.

We must also keep one another close, the strongest defense against Trump is a collective one rooted in community, self-care and accountability.

We have a president who is a **RAPIST, RACIST,** and **ISLAMOPHOBE**. He has done terrible, immoral things in his past, and now has the power to do many more.

Armed with a Republican-controlled Congress, we do not know how this administration will address protest. He is an unstable violent man who now has access to the destructive powers of the National Security Agency (NSA), the American military, and a nuclear arsenal.

THINK ABOUT THAT!

What comes next is beyond all understanding. There is no returning to the status quo. Our homes, our workplaces, our communities—even our families—will never be the same.

We must fight like our lives depend on it. **Because, in fact they do.**

This curriculum aims to present immediate common-sense measures to help activists learn how to protect each other and their movements.

While we are still unsure of what this change will bring, we should assume that surveillance and censorship will increase, and that the Trump Administration's tools and strategies will be more sophisticated than anything we've seen. These surveillance tools have existed for a while but were not used to their full potential under the previous Obama administration.

Additionally, we can expect that individuals fighting for progress will be targeted now more than ever before. While these prospects are overwhelming, the good news is that there are strategies and tools designed to help you avoid most surveillance successfully. We approach this new surveillance era with caution but also with Knowledge. This curriculum will help you make informed decisions about protective measures that can reduce your level of surveillance harm while helping you navigate new risks as they come up. There will never be a perfect silver bullet in terms of surveillance evasion but we believe we can help you feel safer as you organize because you know the

tools and you know your rights.

Trump's election campaign showed signs he would take the position of "erring on the side of (state) security" over people's rights.[1] We know that he has called for closing parts of the internet to protect against "Islamist propaganda".[2] He was also deeply critical of Apple over its refusal to unlock an iPhone implicated in a California shooting for the FBI.[3] And we can expect increased efforts to target Black and Brown communities using databases in predictive policing efforts that use algorithmic discrimination to go after those that are targets because they are "undocumented," "gang members," and/or—"criminals" regardless of whether or not such assumptions are true.

All of these issues must be considered in the context of Trump's majority in both houses of Congress. We know there will be members of his administration who will push harder than ever for "back doors" that allow the government to bypass data security measures like encryption. They can also easily expand the already bloated phone surveillance apparatus currently used by the NSA. Trump's words and actions have suggested that he would push for increased targeting of certain peoples. He has even suggested the creation of a "National Database of Muslims."[4] All of this has the tech world, legal, political experts, activists, and community members worried.

We also know many people in our diverse communities feel powerless and may even argue, "What's the point?" But, in fact, there are simple digital security steps you can take now to help protect you from most threats, and make the remaining threats very expensive for malicious actors to implement.

We hope this curriculum will create a foundation for an education in safety and resilience, and a pathway to bring this crucial conversation into your homes, organizations, and movements. Digital security is a process not a destination and we believe that together we can make all of us safer!

[1] http://www.cnn.com/2015/12/01/politics/donald-trump-nsa-surveillance/
[2] http://www.reuters.com/article/us-usa-election-cyber-idUSKBN13503H
[3] http://www.huffingtonpost.com/entry/donald-trump-apple_us_56c78150e4b0928f5a6bdd3e
[4] http://www.nytimes.com/politics/first-draft/2015/11/20/donald-trump-says-hed-absolutely-require-muslims-to-register/?_r=0

HOW TO USE THIS CURRICULUM

We hope this curriculum will arm you with basic digital security knowledge and effective, simple-to-follow pointers for staying safe. Read this material, come to the workshops, and refer to the curriculum whenever you need to. We will also be offering curriculum module updates at equalitylabs.org so visit us often!

THE CURRICULUM AND WORKSHOP SHOULD HELP YOU:

- Understand the history of surveillance in the United States
- Understand the basics of digital security
- Secure your phone
- Secure your computer
- Secure your network access
- Secure your browser
- Secure your identity
- Secure your social networks
- Secure your communications

LEGEND

This legend will help you identify the icons in this curriculum which highlight significant information.

NOTE: The pencil sign denotes important details that often will provide important background to comprehending the section at hand.

TIP: The lightbulb brings attention to important shortcuts or key concepts to help you make a task easier and faster or even both.

WARNING: When you see the warning sign, take note. These important notes stress actions to avoid that could make you vulnerable. These notes could also include actions that can keep you safer.

TASKS: When you see this checkmark you should be aware that you are being introduced to a key step that must be completed to ensure the security process being discussed is implemented correctly. Do not proceed to the next security task until you have completed the checkmark at hand as many steps are interdependent of each other.

WHERE DOES THE U.S. STAND ON DIGITAL SECURITY ISSUES TODAY?

THE RIGHT TO PRIVACY

The right to privacy is a powerful and necessary foundation of democracy. When the right to privacy is connected to the right to free speech and the right to assemble we have the three fundamental pillars of any functioning democracy. When any one of these pillars are compromised, democracy itself is at risk.

The right to privacy is our right to keep a domain around us. These domains include all those things that define our individuality, such as our bodies, home, property, thoughts, feelings, secrets, and identities. The right to privacy gives us the ability to choose which parts of these domains, others—most importantly, state and corporate entities—can access and empowers us to control the extent, manner, and timing of this use.

If a government strips us of privacy in our lives and in our communications, it can halt thoughts, innovations, movements, and political actions that differ from the mainstream. The feeling of being watched over creates a climate of fear that can end up leaving no room for public criticism or dissent. Such environments are not conducive to democracy or social change.

With the reality of a Trump presidency, we should expect an unobstructed furthering of

the state's rights in the face of our own.

The **Fourth Amendment** to the U.S. Constitution, alludes to the right to privacy, stating that:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue,

but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[5]

The goal of this provision is to protect people's right to privacy and freedom from arbitrary governmental intrusions. What we currently have in the U.S., is a broken policy framework where the law has failed into protect the rights of certain groups of citizens. Even more drastically, through the frame of "terrorism" the government has an unprecedented ability to surveil anyone who it deems a threat.

If we are really being honest, the right to privacy though has always been for the privileged. Since the U.S. was founded, its government has surveilled, policed, and imprisoned indigenous, black, and other communities of color as part of its policies of state control and to justify its settler colonialism.

From the slave pass, to lantern laws, to predictive policing we have to look at our current mass surveillance state not as an aberration, but rather as the next phase of **a continuing policy of state violence toward our communities.**

Communities like ours that are in the crosshairs of the current manifestations of mass surveillance must fight even harder for our rights to privacy.

If you are indigenous, black, Muslim, Latinx, undocumented, or LGBTQ you are seen as disposable by the government, your right to privacy has been eroded—or is non-existent. This increases exponentially if you have been part or are curently in the prison industrial complex.

Now, the whole country is experiencing what those of us from these communities have been saying for a long time:

SHIT IS REAL Y'ALL, and it's time to get to work!

[5] https://www.law.cornell.edu/constitution/fourth_amendment

WHAT IS DIGITAL SECURITY?

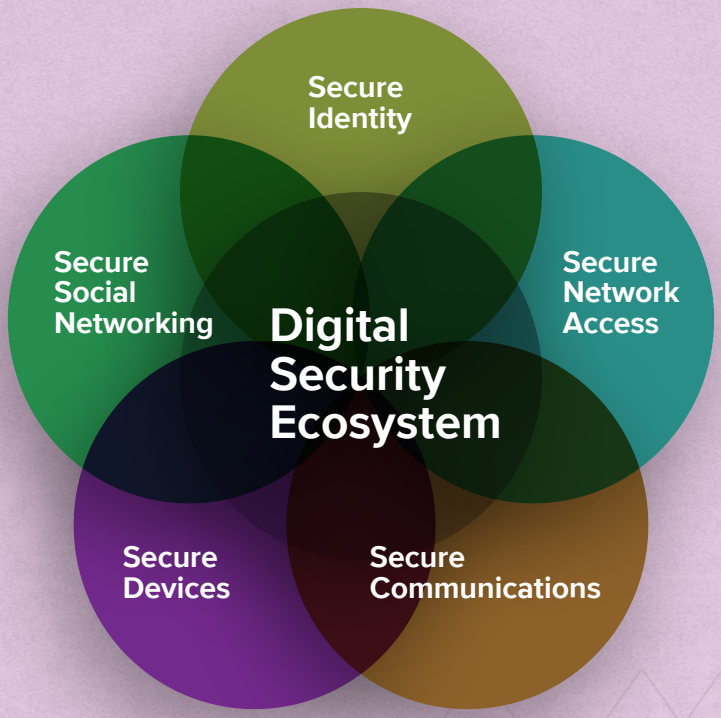
HOW TO USE THIS CURRICULUM

So, now that we know how big the problem is let's start with a definition: What the heck is **digital security** anyway?

> **Digital security** is a set of defensive practices and awarenesses that ensures that all your devices, data, communications, and identity markers are protected to minimize surveillance by entities or individuals that may directly or indirectly wish you harm.

AN ECOSYSTEM OF DIGITAL SECURITY

Digital security is part of a large ecosystem of thinking in regards to your safety. In this ecoystem each part works with the others to secure the whole. That is why we break down our modules into easily accesible part of this ecosystem.



The digital security ecosystem includes how you secure your devices and data, the way you access your network, and the means by which you protect your identity and communications. Each part of this ecosystem can be protected or it can becompromised. Our goal is to give you the tools to better understand this ecosystem and show you ways to use more disciplined practices that will help build your digital resilence.

While we are focusing only on digital communications, we encourage everyone to also think about physical and emotional threats, it's important to consider everything and to—always plan accordingly.

It's OK if this confusing! The more you start thinking about it on your own and with trusted friends the easier it will become. Promise! So let's begin.

TIP: Individuals that love their communities practice good digital security

IT'S ALL ABOUT HARM REDUCTION RIGHT NOW

In our journey toward better digital security, it is important to keep in mind that internet security solutions, programs, and services available on the internet can change their security settings and privacy policies without notice, possibly putting users at risk. New security updates, as well as viruses and malware, are launched every day. This means that what was secure yesterday may be vulnerable to attack today.

There is no alternative to staying aware, informed, and engaged **and most importantly fighting back as a community. You are only as safe as the discipline of your digital network.**

We also know that maintaining a secure environment can be hard work. At best, you have to change passwords, habits, and perhaps the software you use on your main computer or device. At worst, you have to constantly think about whether you are leaking confidential information or using unsafe practices.

Even when you know the problems, some solutions may be out of your hands. Other people may require you to continue unsafe digital security practices even after you explain the dangers. For instance, work colleagues might want you to continue to open email attachments from them, even though you know your attackers could impersonate them and send you malware. Or, you may be concerned that your main computer has already been compromised.

And you know what? All of that is ok. In order to become a digitally resilent community together we have to be patient, firm, and aware that digital security is a journey not a destination. This is why we use the harm reduction framework.

We will make mistakes, and we will also be getting stronger together. We want to be a learning

community that has patience and compassion for each other during this difficult time. So ask questions, ask them frequently, and know the work you begin today will only grow if you stay commited to digital resilence tomorrow.

SIGNS OF SECURITY COMPROMISE

Many people feel safe when, in fact, they already have a compromised digital ecosystems. Do you know what the signs of compromise could be? Here is a list of some examples:

- Passwords that change mysteriously.
- Private messages that appear to have been read by someone else.
- Websites that have become inaccessible from certain countries.
- New pop-ups constantly launch from your browser.
- Instances when your web browser redirects or crashes
- A rapid reduction of battery life, despite little-to-no use
- Instances when your cursor unexpectedly moves without your direction.
- Links from people you don’t know via Facebook, Twitter, WhatsApp, or e-mail.

If you have any of these symptoms don't panic. Just take your device to a trusted IT professional and have them take a look. Even if you don't have a security compromise these symptoms can also sometimes point to other serious problems on your machines. The point is to be aware and be proactive about problems so when a real threat arises you are ready.

HOW TO MAKE A RISK ASSESSMENT

Risk assesment is a skill that we use in many aspects of our lives. It is what we use when we think about what side of the street to walk on at night, whether we lock our doors in our houses and the numerous other calculations we make to balance risk with the effort it takes to protect ourselves from a threat.

Digital security is no different. By thinking through and mapping out the risks we face, we can make better decisions about how to stay safe and protect our friends and networks. When you take the time to create a risk assessment model for yourself or your organization/network you can:

- Identify your risks—specifically, the people or institutions that may pose a threat—and understand the various ways they could potentially target you.
- Understand your current or future vulnerabilities so you can account for them.
- Brainstorm how the vulnerabilities of the network(s) or organizations you are part of can affect you. For example, if you don't know the technical practices of an organization or network, you may want to rethink the sensitive information you share, it may not be adequately protected.

YOUR RISK ASSESSMENT

WHAT DO YOU WANT TO PROTECT?

WHO DO YOU WANT TO PROTECT IT FROM?

HOW LIKELY IS IT YOU WILL NEED TO PROTECT YOUR ASSETS?

HOW BAD ARE THE CONSEQUENCES IF YOU FAIL?

HOW MUCH TROUBLE ARE YOU WILLING TO GO THROUGH TO PREVENT THOSE NEGATIVE CONSEQUENCES?

While you are the best person to understand your own risk, make sure to research or talk to people who have a better understanding of your adversaries' capabilities. This is especially true about digital surveillance strategies and laws that may change quickly from one day to the next.

It is important to note that in managing risks to improve security there are always trade-offs. It's impossible to being 100% secure and digital security tools alone will not make you more secure. Ultimately, you will need to think deeply about your behaviors and practices.

Ask yourself a few questions:

What do you want to protect?
What do you have that requires protection? Some examples could include: personal information, sensitive communications, statistical reports, incriminating evidence, photographs, film, documentation of a movement, or written and oral histories of our communities.

Who do you want to protect it from?
The information you have may need to be protected from right-wing adversaries, the police, intelligence officers, movement infiltrators, and the state.

How likely is it that you will need to protect your assets?
What level of protection does your information need? How often are you exposed to a threat?

How bad are the consequences if you fail?
What can happen if the information you care about "leaks"? Could you lose the information completely? What does this mean for you as an individual, our organizations, movements, and our larger community?

How much trouble are you willing to go through in order to prevent those negative consequences?
For example, are you willing to tighten the security on your devices, learn more about digital security principles and use best practices?

Ultimately, by questioning your behavior you can reduce your digital imprint along with the amount of sensitive data you post online.

Let's do a risk assessment for one of the following scenarios. Before you begin, here are some quick definitions:

- **Threat:** An entity that can cause harm.
- **Adversary:** The opposition that poses this threat.
- **Asset:** Something of value that requires protecting.
- **Risk:** The likelihood of a threat to a vulnerable asset.

Consider who may present themselves as potential adversaries:

- A roommate
- A blogger with a grudge

- An employer
- The police department through an untargeted arrest at a protest
- Police or the FBI targeting you
- The NSA targeting you

Different adversaries have different capacities and therefore require different strategies for mitigating threats. For example, your employer may not break into your home, but they can monitor you at work. Your roommate may not set up a fake cell tower but could have direct physical access to your phone. A police arrest at a protest (generally) won't lead to a warrant for your email, but the police could get it directly from your phone on site.

RISK ASSESSMENT MODEL

Read the chart below to get an idea of how to think through your threat model. Some skills you may not understand quite yet. But return to this table as a model after you have gone through our training or read this curriculum handbook. You will find your understanding will change as you gain digital surveillance literacy. Some visit this page often or better yet make your own!

THREATS	RISKS	POSSIBLE ADVERSARIES	CURRENT CAPACITIES	CAPACITIES REQUIRED
Example 1: Someone is accessing my email.	• I've already shared my password. • My password is weak and the same across multiple accounts. • I have a habit of leaving my laptop unattended.	• Roomates • "Friends" • Infiltrators	• I will change my passwords so they are strong. • I will no longer share my passwords with anyone. • I won't keep my passwords in online documents or emails.	• I need to install a password manager so I can use strong and diverse passwords for different accounts. • I need to set up two-factor

THREATS	RISKS	POSSIBLE ADVERSARIES	CURRENT CAPACITIES	CAPACITIES REQUIRED
Example 2: My mobile phone is confiscated at Trump protest.	• I have a weak password on my phone lock or use fingerprint login. • I have sensitive contacts on my phone under their real names. • I use apps like Gmail, through which anyone who has physical access to my phone can read my email without a password.	• The police. • Private security guards. • Department of Homeland Security Officials.	• I can change my password so it's stronger. • I can remove the fingerprint login so I'm not compelled to use it unwillingly. • I can use pseudonyms for sensitive contacts. • I can leave my phone at home. • I can delete non-essential apps.	• I need to encrypt my phone.

THREATS	RISKS	POSSIBLE ADVERSARIES	CURRENT CAPACITIES	CAPACITIES REQUIRED
Example 3: Someone hacking my computer.	• I don't know the various ways they can hack into my computer, and I have sensitive information stored on it.	• List anyone who would want to hack into your computer:	• I can keep my operating system and software up to date, and encrypt the hard drive. • I can store sensitive files on a password-protected USB drive.	• I need to research the various ways in which someone can hack into my computer.

NOTE: If you're working with an organization, https://safetag.org has both an action guide and a curricula on risk modeling. If you want to think more about your organization's security culture, in addition to digital security, Ruckus has a great manual: http://pdf.resistrnc.org/RuckusSecurityCultureForActivists.pdf

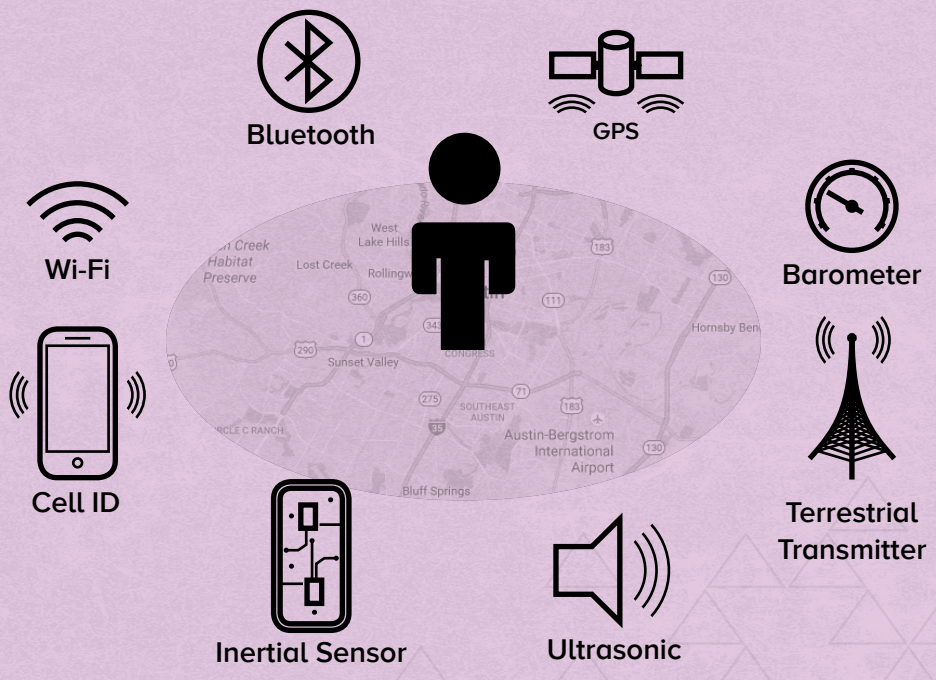
SECURE YOUR PHONE

A SECURE PHONE IS ALWAYS THE FOUNDATION!

Your phone is one of the most critical components of your digital ecosystem. Phones are essential to communication, strategizing, and community organization. Most people communicate primarily through their mobile phone, followed by their computers and tablets. However, for these very reasons, governments and corporations throughout the world use data collected through our phones to perform extensive surveillance.

As useful as it is, your phone can present pathways to serious violations of your privacy and security. Below is a graphic that shares all the different ways it collects and shares your personal data with cell phone service providers and phone manufactures. This vulnerability may allow governments and hackers to access information about your physical location at any time, **even when it's turned off**.

WARNING: Governments or malicious actors can turn on your phone's microphone and camera to listen to you even when the device is turned off?



Today, law enforcement agencies use technology that provide police with data about the identity, activity, and location of any phone that connects to targeted cell phone towers over a set span of time. A typical broad data search covers multiple towers and wireless providers and can net information from thousands of phones—without need for warrants.[10]

Organizations such as the American Civil Liberties Union (ACLU) and Electronic Privacy Information Center (EPIC), say that the power of even small-town police departments to quickly obtain cell phone data results in the erosion of privacy and the violation of Fourth Amendment protections against unreasonable search and seizure. But thanks to a unanimous Supreme Court decision in Riley v. California, this practice is now officially legal.[11]

In extreme circumstances, **to prevent all tracking of your location from your phone, shut it down completely and remove the battery. This is the easiest way to ensure that you can't be tracked**, But it comes at the price of not being able to use your phone at all. If you need access to any data on your phone, back it up to a computer before you power down your device.

If your phone's battery cannot be removed, place it in a **faraday bag,** which blocks transmission with its internal lining.[12] Not all faraday bags are created equal, so make sure you try it out before you put it into use in everyday life. You want to confirm that, at a minimum, cell and GPS services are blocked.

In addition to these scenarios, we face threats of information leaks during the everyday use of our phones. There are several simple safe practices that can be adopted to keep ourselves and our information safe. In the following section, we will explore a few of them.

NOTE: The "Secure Your Phone" section is broken up to address actions for Androids and iPhones separately. Please find the section that works for your device and begin.

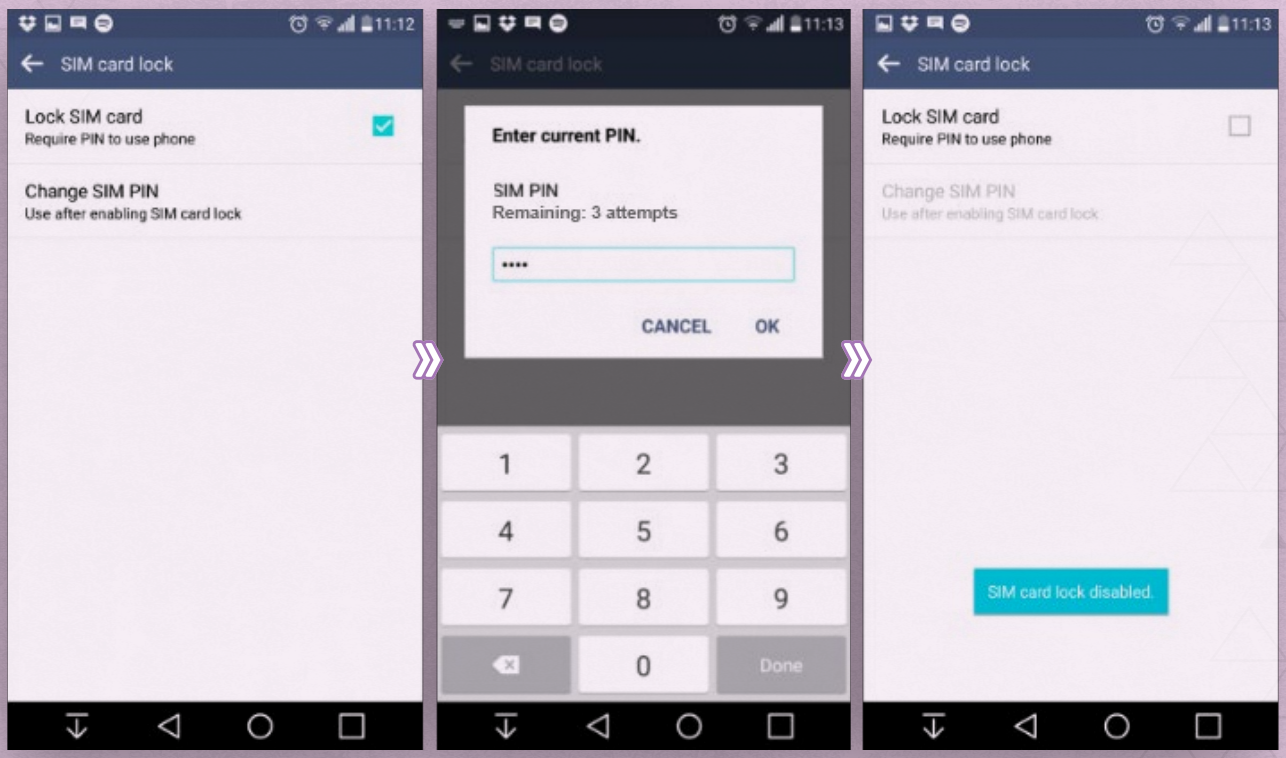
[6] http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/
[7] https://www.eff.org/deeplinks/2014/08/cell-phone-guide-protesters-updated-2014-edition
[8] https://www.amazon.com/Black-Hole-Faraday-Bag-Anti-tracking/dp/B0091WILY0

SECURE YOUR ANDROID

1. LOCK YOUR SIM

If your phone uses a SIM card, you can set a lock on the card so it cannot be used by anyone who does not know the code. If your SIM is stolen, this measure can protect your identity.

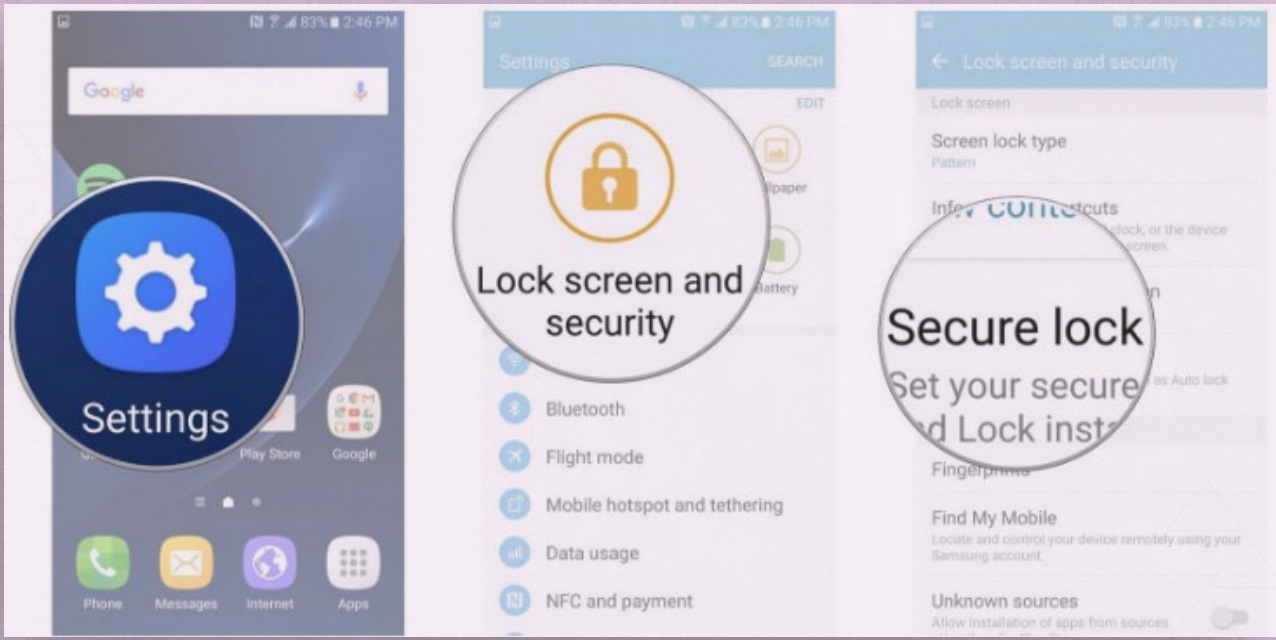
- Enable Lock SIM card by going to **Settings → Personal → Security → Set up SIM card lock**. Now, each time your phone is turned on it will require a PIN in order to unlock your SIM card. No one will be able to make calls using your device without the PIN.



2. SET UP YOUR PIN AND ACTIVATE A SCREENLOCK

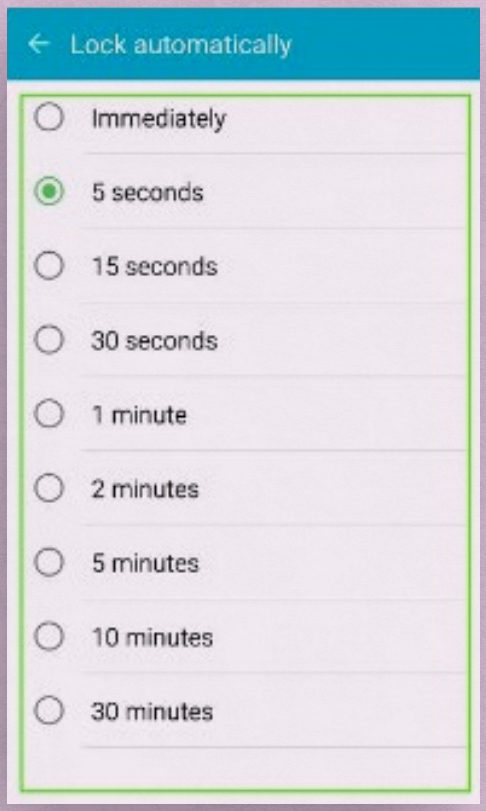
- Set up a screen lock by accessing **Settings → Personal → Security → Screen Lock**, to ensure that lists, pictures, and a code, pattern, or password need to be entered in order to unlock the screen.

We recommended using the PIN or password option, as these are more obstructive to law enforcement or adversaries than a fingerprint ID. This measure is particularly important in the event that you are faced with a casual search by police or other authorities.



NOTE: We highly recommend that people **DO NOT** use the fingerprint login, as you could be forced or manipulated into putting your finger on your screen. There are also more legal protections for the PIN versus the fingerprint login or even swipe access to one's phone. Finally it is never a good idea to give your biometric data like a fingerprint to a corporation if you can avoid it. So when in doubt use a PIN!

3. ACTIVATE A SECURITY LOCK TIMER



- Set the security lock timer, which will automatically lock your phone after a certain amount of time.
- Go to **Settings → Display → Sleep.** Different versions of the firmware use different names for this menu so you will have to find the one that matches your phone.
- Now select a time period that is appropriate to your usage habits in the pop-up menu that appears. The change will take place immediately.

For maximum security, always choose the shortest possible timeframe that suits you without becoming too taxing. You can always adapt your times to your activities as well. So if you use your phone for recipies keep security lock timer off, but then turn it back on when you resume regular activity. Use your risk assessment to figure out what makes the most sense for you.

4. ANDROID ENCRYPTION

With Androids, encrypting your phone is one of the best ways to protect your data if the device is ever stolen, seized, or confiscated. The purpose of encryption is to ensure that only someone who is authorized to access your phone's data will be able to read it using the decryption key.

When your phone is encrypted, its data is stored in an unreadable, seemingly scrambled form. If your phone is stolen, confiscated, or lost, this feature can protect data like your home address, email, bank accounts, communications, etc.

When you enter your PIN or your pattern on the lock screen, your phone decrypts the data, making it understandable and accessible to you. Without the encryption PIN or password, a malicious actor can't access your data. This is why Encryption is one of key building blocks of securing your phone.

NOTE: Before starting the encryption process, ensure your phone is backed up, fully charged, and plugged into a power source. This ensures that the encrypting process is not interrupted. If it is interrupted, and your data is lost or damaged, you will have a backup of all of your data.

- To begin encryption find out whether or not your Android has Encryption enabled. Some versions of Android come with Encryption already set up while others need to set it up manually. To discover where your phone is at please first visit **Settings → Personal → Security → Encryption**.

- If Encryption is enabled it will say it here clearly. If not then your next step will require you to set a screen lock password (described above).

- Once your PIN is selected make sure you phone is fully charged and backed up as you will not want to disturb the Encryption process. A back up also ensures that if anything goes wrong during encryption that your data is protected and your phone can be restored.

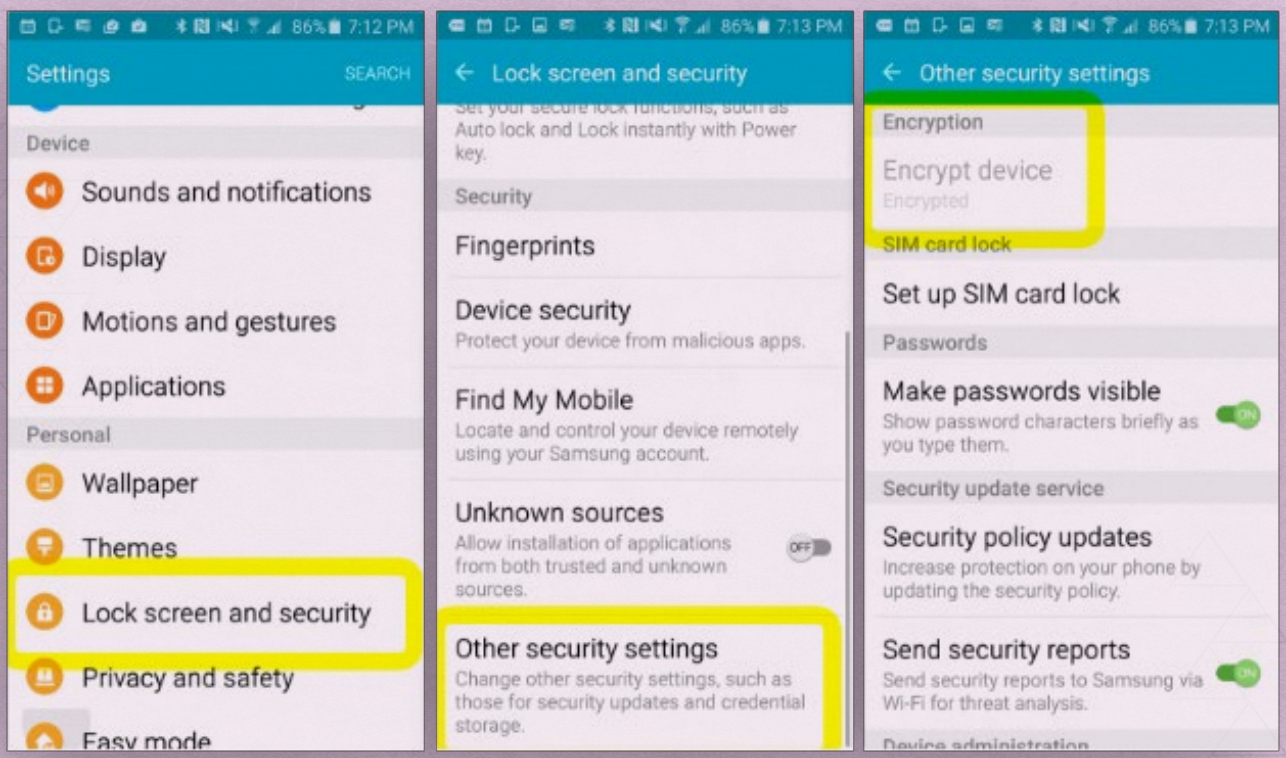
- Once the phone is ready and plugged in, please begin Encrypting by hitting Encrypt. The process should last anywhere from 30min to a couple of hours.

5. ADJUST YOUR NETWORK SETTINGS

We recommend keeping most networks turned off and only manually enabling them when necessary. One example is Bluetooth. Also, ensure that tethering and portable hotspots are switched off when not in use.

✔ Do so by accessing **Settings → Wireless & Networks → More → Tethering & Mobile Hotspot**.

If your device supports Near Field Communication (NFC), it will be switched on by default and must be disabled manually.



6. YOUR LOCATION SETTINGS

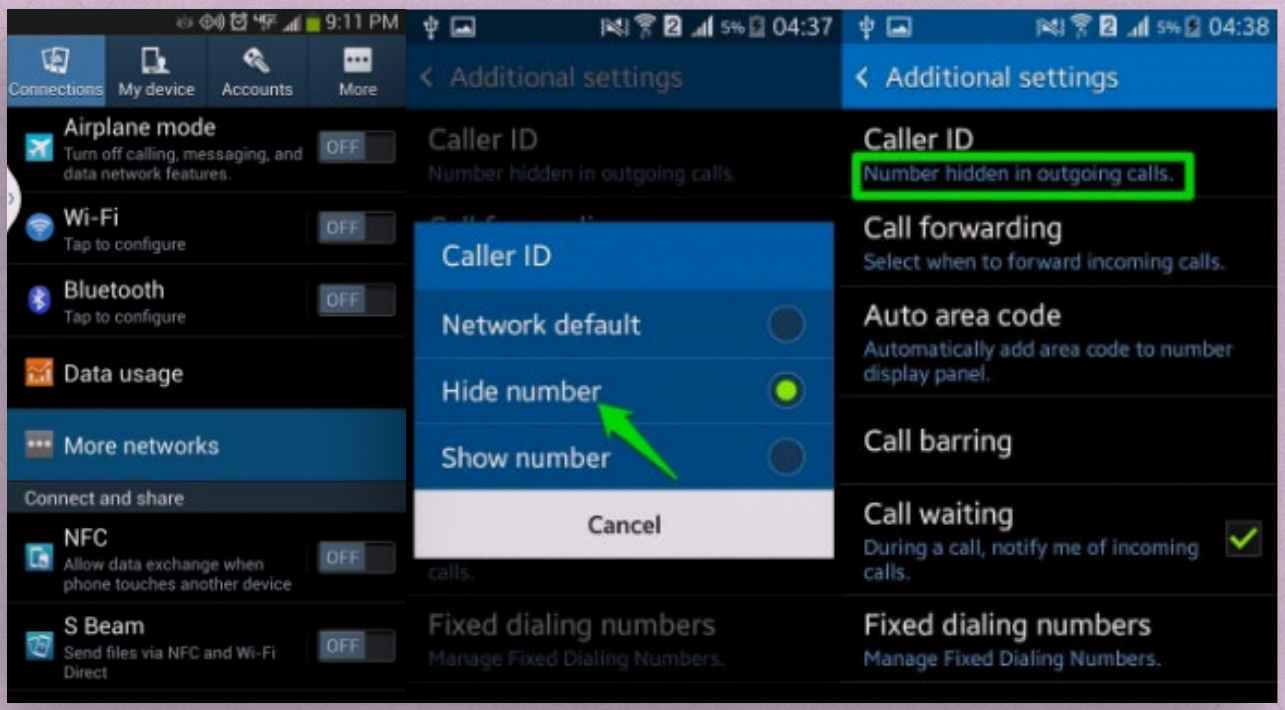
✔ Switch off wireless and GPS location (under Location Services) and mobile data (under **Settings → Personal → Location**)

NOTE: Only turn on location settings if necessary. When these services aren't running by default in the background, it reduces the risk of location tracking, saves battery power, and prevents unwanted data streams initiated by applications or your mobile carrier.

HIDING CALLER ID

You can hide your phone number from showing up to the person you are calling. However, you should note that your phone carrier and legal authorities will still have full access to logs showing who you called and when.

- Go to Settings and then tap on **Call → Additional Settings → Caller ID → Hide Number and it will be blocked**.



7. UPDATE YOUR ANDROID

To ensure that your phone remains secure, we strongly recommend you keep your software updated. There are two types of updates to check for:

- The phone's operating system: Go to **Settings → About phone → Updates → Check for Updates**[13]
- Individual apps you have installed: Open the **Google Play Store app**, and select My Apps from the side menu.

NOTE: It is important to always update your phone's software from a trusted location—such as your internet connection at home—somewhere like an internet cafe or coffee shop.

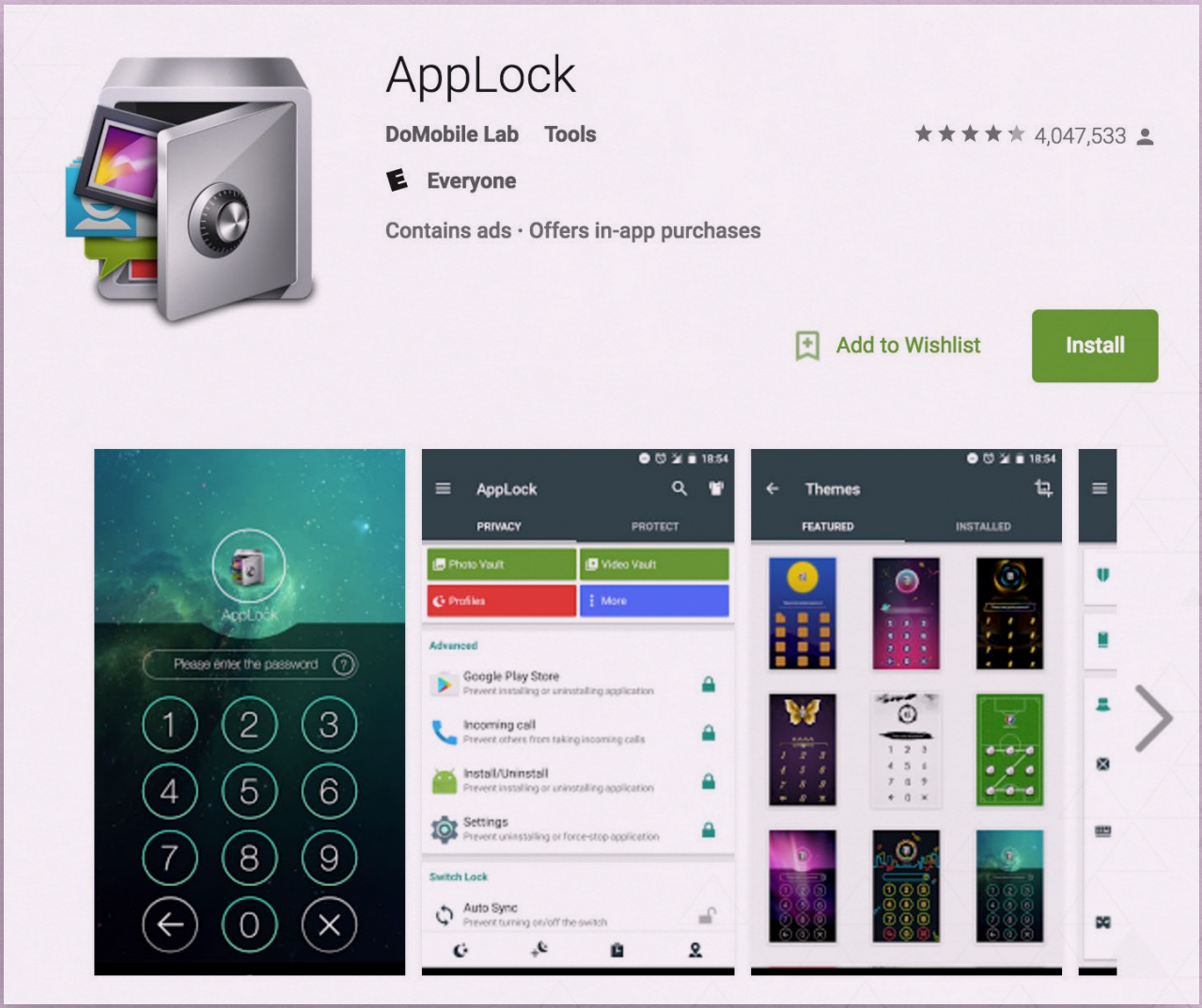
[9] https://videotron.tmtx.ca/en/topic/google_nexus6p/hiding_your_phone_number.html

1. APPLOCK FOR ANDROIDS

Security needs can arise in simple scenarios, such as keeping prying eyes out of certain apps. You might hand your phone to someone so they can make a call or look at a picture. You might be stopped by the police or have your phone confiscated. Once you turn your back, it's easy for that user to dig into your data.

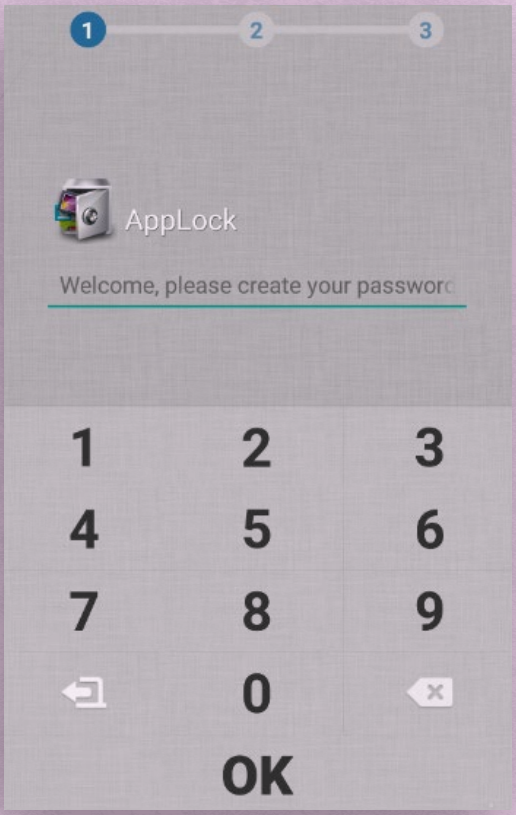
Fortunately, there are ways to keep certain applications readily available while others are locked down. Keeping a password lock on your phone prevents casual snooping through your contact numbers, texts, and data. In addition to requiring a passcode to unlock your phone, you can also download software that allows you to set a code for individual apps.

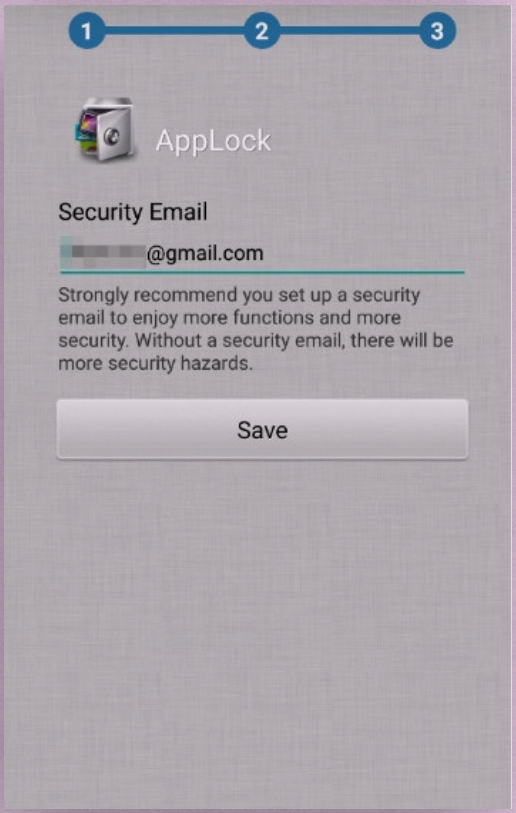
We recommend using **AppLock**[10] on Androids. AppLock is a free app that extends your phone's access controls to specific applications.



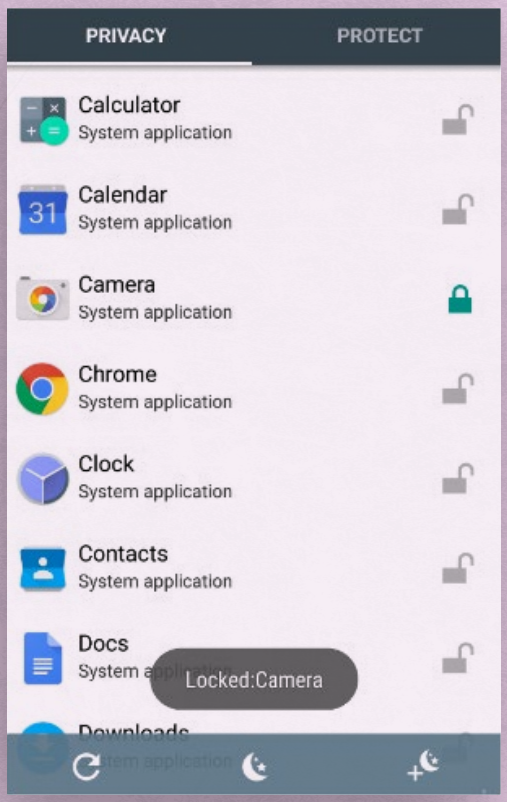
[10] https://play.google.com/store/apps/details?id=com.domobile.applock&hl=en

- Once you download, install, and open AppLock, you will be prompted to create a password. This is used whenever you re-open AppLock, as well as when you want to access any of the apps you will be protecting, so make sure it's a password you can easily remember. You'll also need to provide a security e-mail address.

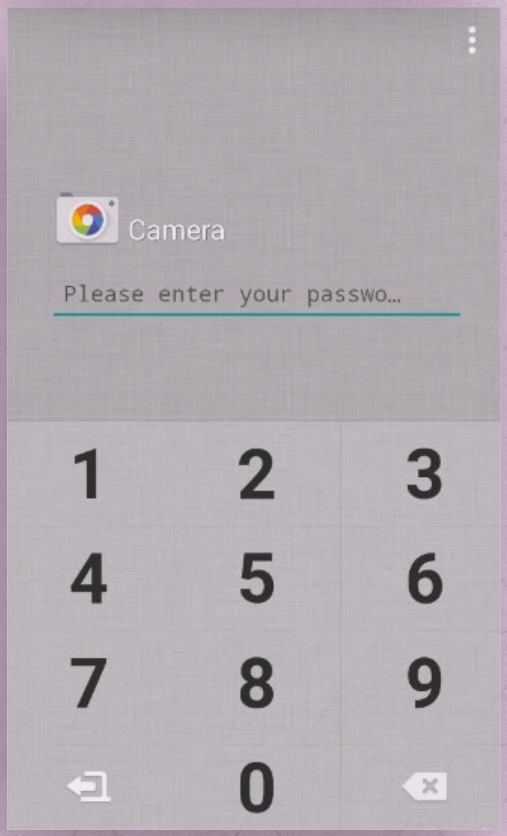




- After that, you are all set to start locking individual apps, such as Phone, Messenger, Facebook, and so on. If you want to lock the Camera app, for example, you'll simply tap the lock icon.



- Now it is locked, and if you want to access your phone's camera, you will be prompted to enter your passcode.



2. DEALING WITH METADATA ON PHOTOS

Photos we take on all electronic devices can often carry data that can be used to pinpoint our location and gather other information about us.

This information can be intercepted and gathered as part of the surveillance of our movements and habits. These details are often shared through something called **metadata** which is the additional details useful to categorizing, locating, or describing a file. Put simply, metadata refers to data about data.

Many of the files we use and create on our phones have metadata, including emails, text messages, and photos. So one of the ways we can secure our phones is by minimizing the metadata our phones share while we communicate.

The metadata in photographs are known as the **Exchangeable Image File Format,** or **EXIF.** This can reveal much about you, your subject, and where a photo was taken. Metadata embedded in a photo includes the following:

- Key identifying information, such as camera or cell phone user, GPS coordinates, and the time and date the photo was taken.
- Camera settings, including static information such as the camera model and make, and information that varies with each image such as orientation (rotation), aperture, shutter speed, focal length, metering mode, and ISO speed information.
- A thumbnail preview of the picture on the camera's LCD screen, in file managers, or in photo manipulation software.
- Descriptions of a photograph's content.
- Copyright information.

NOTE: Different versions of Android may have different ways to get to the settings described in this section. We describe the general method but do a little searching around the settings areas of your particular version of phone to make sure you achieve the same.

SWITCH OFF LOCATION TAGGING FOR YOUR CAMERA

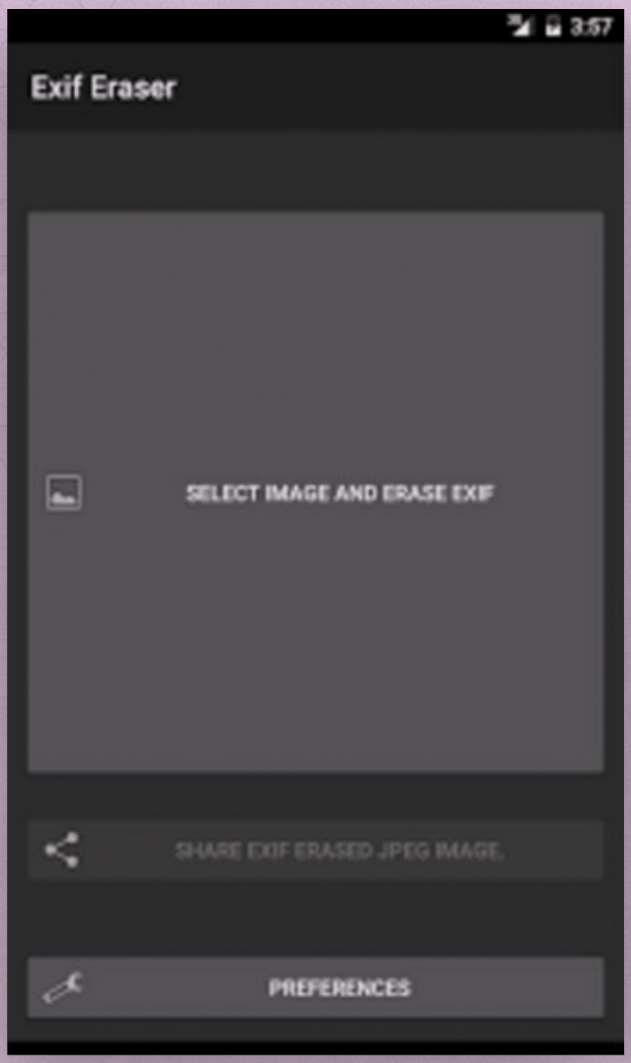
Android: Open the **Camera** app and tap the circle to the right of the shutter button. From the resulting menu, tap the **Settings** icon. Now, in the settings menu, tap the “Location” button. You can tell that geolocation is now disabled because of the icon overlaid on the options button.

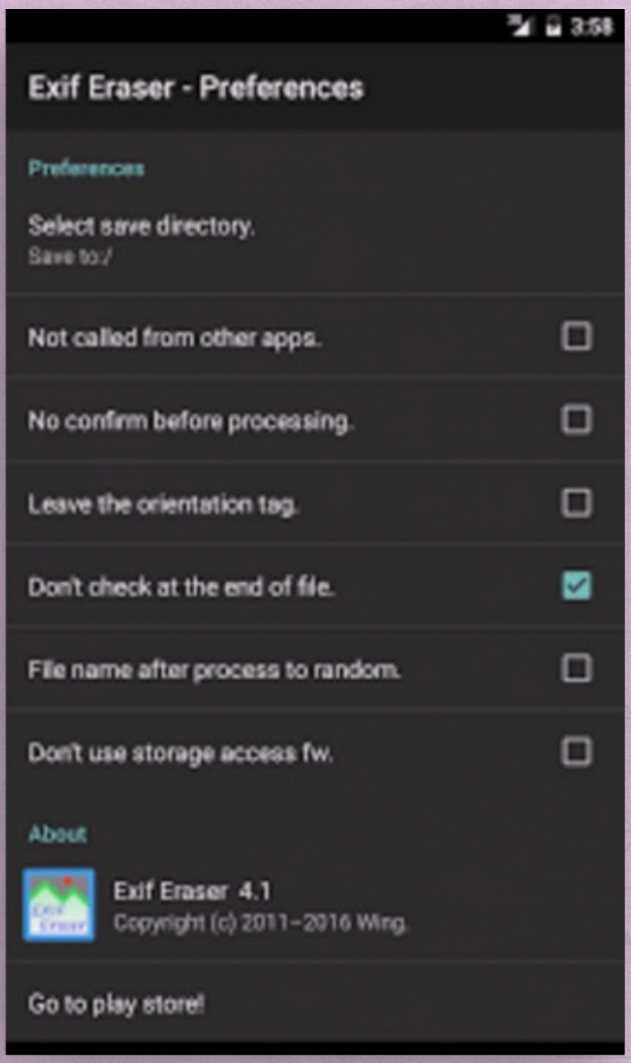
INSTALL A THIRD-PARTY APP FOR SCRUBBING METADATA FROM IMAGES

To remove (“scrub”) existing metadata from images we have taken on our Androids we can use third-party apps For Android we recommend installing and using **Exif Eraser**.

Exif Eraser for Android
After installing Simply pick one or more photos with EXIF information from Gallery or the app.

- Choose whether you want to replace the photo, create a new copy, or simply share the photo (e.g. to Facebook).
- Then, you are free to share your EXIF-free photos without compromising your privacy.



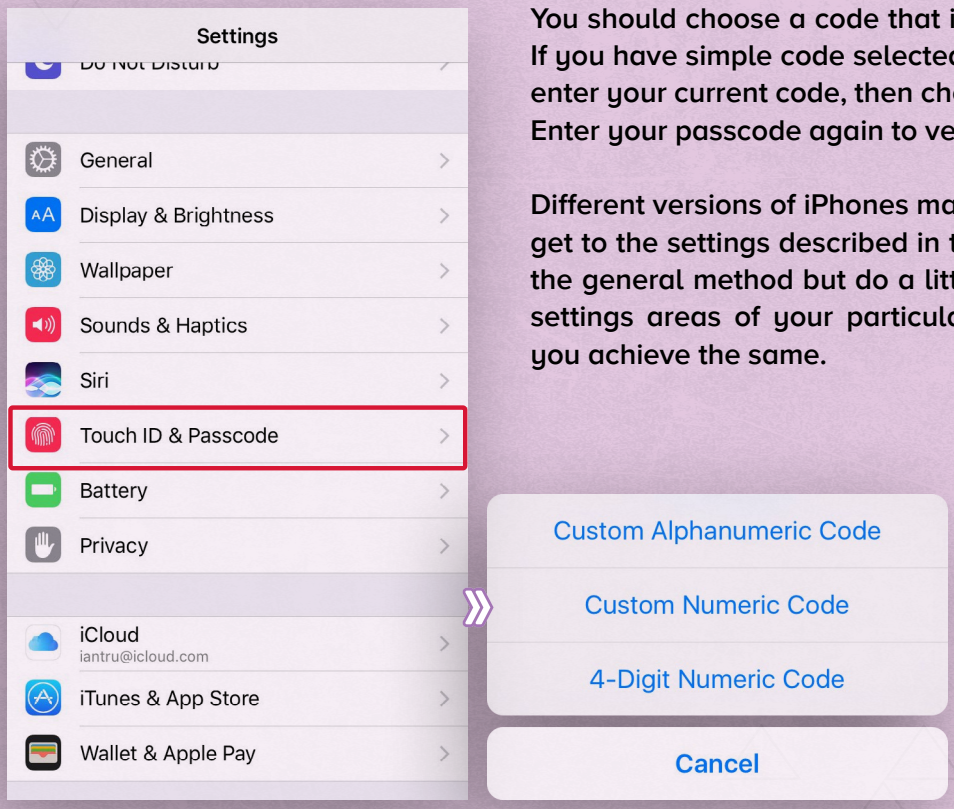


SECURE YOUR IPHONE

1. ACTIVATE YOUR SCREEN LOCK

First, set up a passcode. Some phones also allow you to set your fingerprint as your password through Touch ID.[11] We do not recommend setting up Touch ID, as you can be physically, unwillingly compelled to open your device. Instead, simply set a strong PIN.

- To set these up, go to **Settings → Touch ID & Passcode**. On devices without Touch ID, go to **Settings → Passcode**.
- Tap **Turn Passcode On**. Then, tap **Passcode Options** to switch to a four-digit numeric code, a custom numeric code, or a custom alphanumeric code.



You should choose a code that is at least six digits long. If you have simple code selected, tap Change Passcode, enter your current code, then choose a harder sequence. Enter your passcode again to verify and activate it.

Different versions of iPhones may have different ways to get to the settings described in this section. We describe the general method but do a little searching around the settings areas of your particular version to make sure you achieve the same.

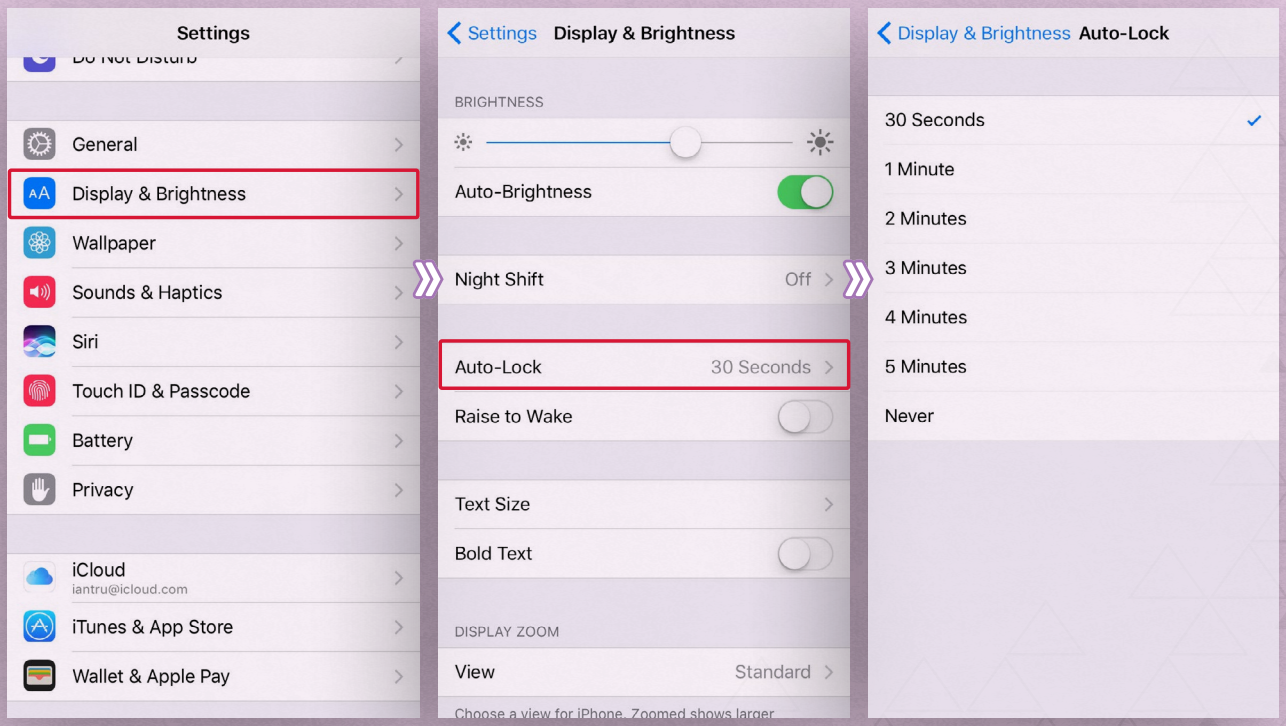
[11] http://www.pcadvisor.co.uk/how-to/mobile-phone/how-to-set-up-a-sim-lock-on-an-apple-iphone-3304041/

WARNING: We highly recommend that you DO NOT use a fingerprint login, as you can be unwillingly compelled to place your finger on the home button.

2. ACTIVATE YOUR SECURITY LOCK TIMER

- Go to the **Settings → Display & Brightness → Auto-Lock**.
- **Choose the time interval.** This means that, if you have not used your phone for the amount of time specified, it will automatically lock. Do not choose **"Never"**, as that will leave you vulnerable; instead, select an interval **between 30 seconds and one minute**.

  For maximum security, always choose the shortest possible timeframe that suits you without becoming too taxing. You can always adapt your times to your activities as well. So if you use your phone for recipies keep security lock timer off, but then turn it back on when you resume regular activity. Use your risk assessment to figure out what makes the most sense for you. If necessary, you can change it to a longer interval to complete a specific task, but make sure you change it back!
- If you are running iOS 9 or iOS 8, the lock screen option is available in **Settings → General → Auto-Lock → Time interval**.[12]



[12] http://www.howtoisolve.com/turn-on-off-change-auto-lock-screen-time-iphone/

3. IPHONE ENCRYPTION

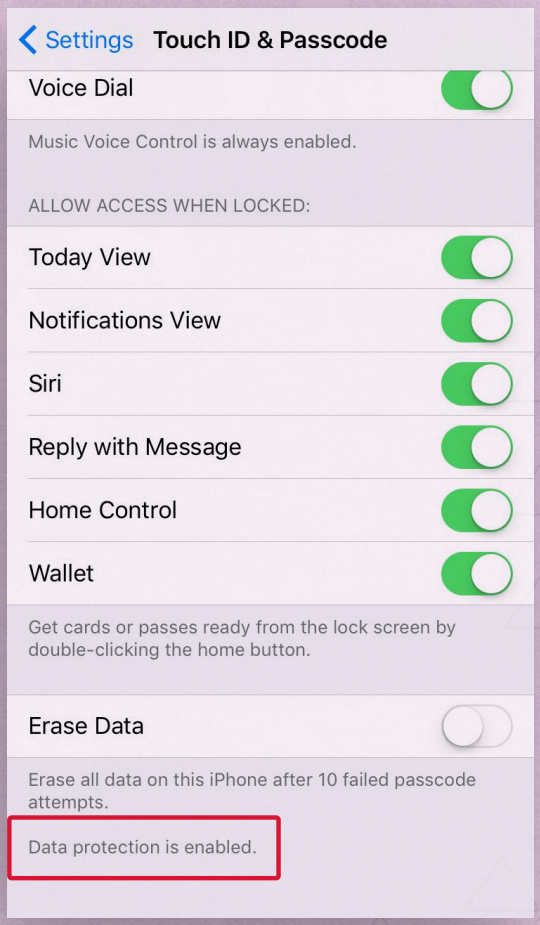
Encryption is essentially one of the best was to protect your phone's data if it is stolen, seized, or confiscated. The purpose of encryption is to ensure that only somebody who is authorized to access data will be able to read it, using the decryption key.[13]

With Androids, you must enable device encryption, but most modern Apple devices encrypt their contents by default, with varying levels of protection. However, to protect yourself from someone obtaining your data by physically stealing your device, you need to tie that encryption to a passphrase or code that only you know. The previous section explains how to set a passcode

Once your passcode is set your phone is now encrypted. What is crucial is then to **only** back up to your computer or hard drive and never to icloud. That way you retain maximum control of your data.

WARNING: Do not use iCloud to back up your phone. Always back up your content to a hard drive or your own computer. iCloud backups allow Apple and other third parties access to your data. For instance, if they recieve a subpoena to release your personal information to the authorities, there is no guarantee they will be successful guards of your content. That is a lot of trust to give to a corporation. Use your risk assessment to decide what is best for you. At Equality Labs we rarely give our data to corporations for this reason.

Once you've set a passcode, scroll down to the bottom of the Touch ID & Passcode Settings page. You should see a message reading **"Data protection is enabled."** This means that the device's encryption is now tied to your passcode, and most data on your phone will require that code to unlock.



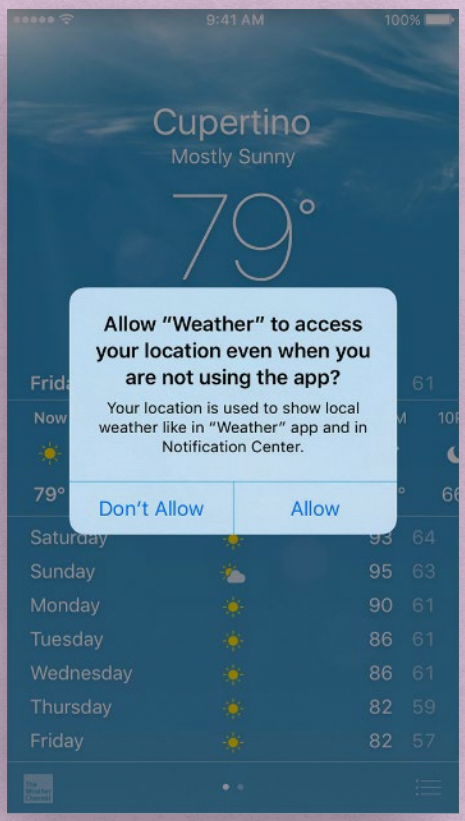
[13] https://ssd.eff.org/en/module/how-encrypt-your-iphone

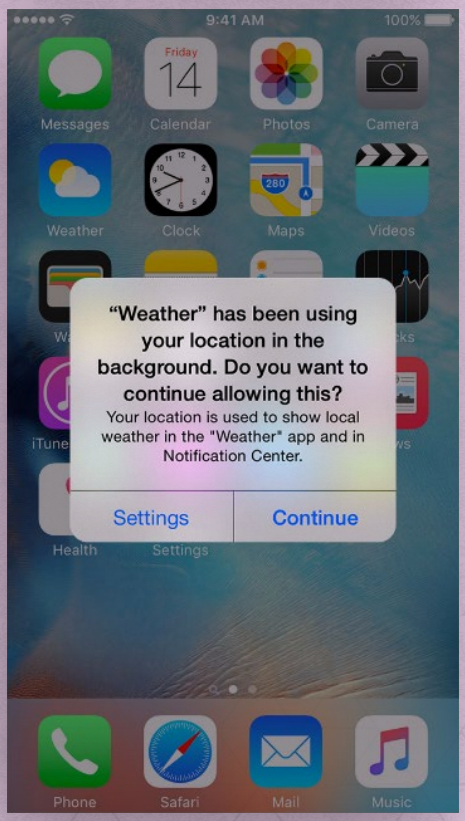
4. TURN OFF LOCATION SERVICES

The first time an app tries to access your location it will ask for your permission, even when it's running in the background. The app's developer may also explain how it uses your location.[14]

Some apps will ask to use your location only while the app is in use. An app is considered "in use" when you are actively using it in the foreground or when it's running idly in the background, which the status bar will indicate.

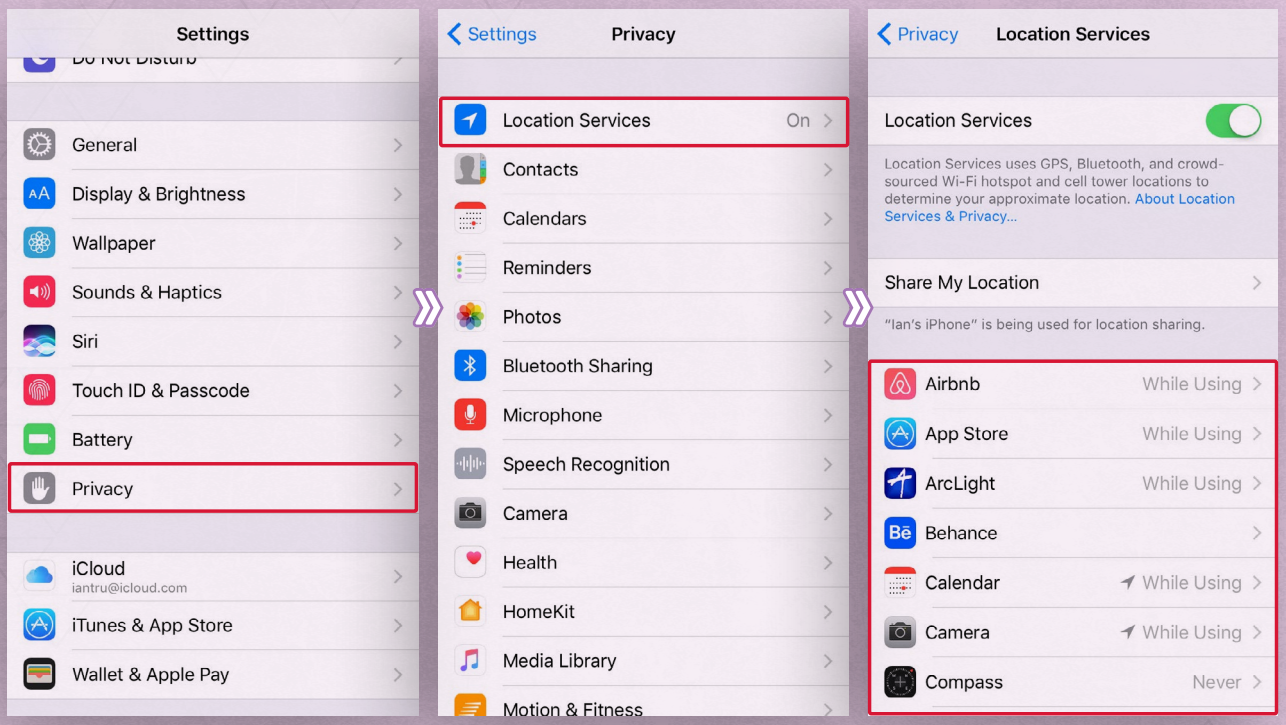
Other apps will ask for access to your location even when they are not in use. Your operating system will remind you which apps have this access with pop-up notifications, triggered when an app uses your location in the background.





[14] https://support.apple.com/en-us/HT203033

✔ You can control your phone's location settings at **Settings → Privacy → Location Services**. You can turn Location Services on either during the initial Setup Assistant process or later via the Location Services screen. After this, you will be able to control which individual apps and system services have access to your location data.



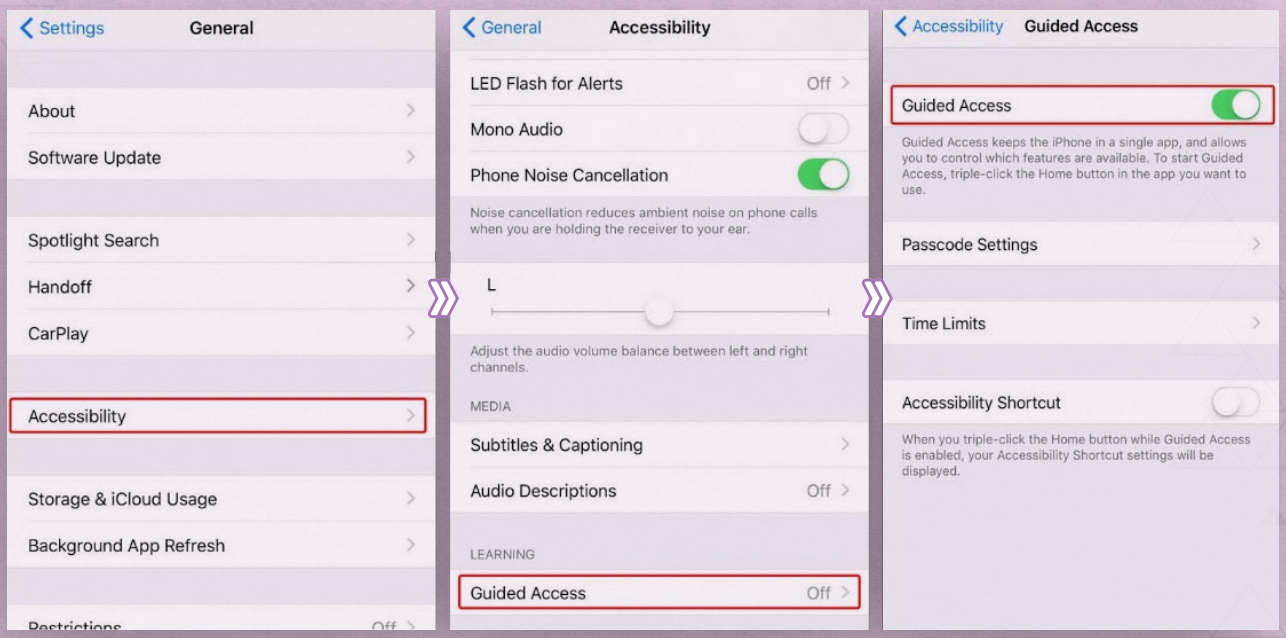
When Location Services are turned completely off, no apps can use your location in the foreground or background. This may limit applications like Maps and GPS requiring services like Uber or Lyft.

ADDITIONAL SECURITY APPS FOR IPHONE

1. GUIDED ACCESS FOR IPHONES

Apple provides a built-in feature to both hide and lock apps on iPhones.

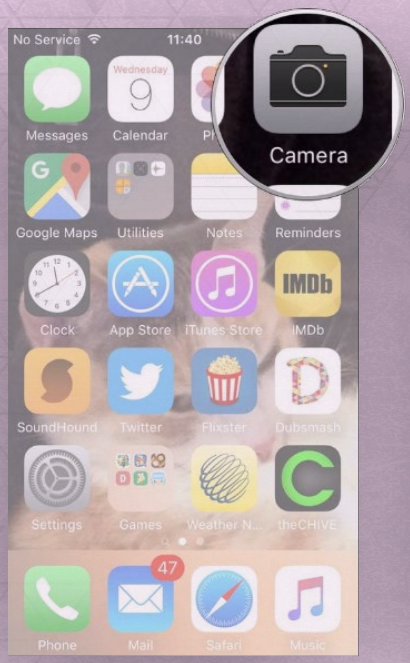
- Go to Settings and tap **General → Accessibility → Guided Access**. Under Guided Access, toggle Guided Access to ON.
- This will give you an option for—**Passcode Settings**. Now, you can set a Guided Access password.



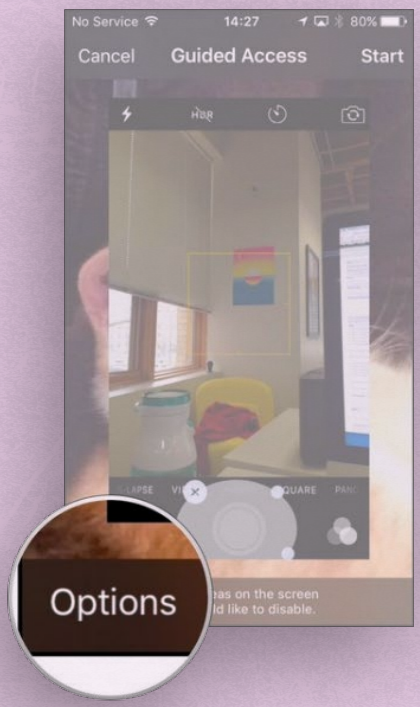
With this, you have successfully enabled the Guided Access feature and can now lock Apps. To do so, open the app you want to lock, for instance, the Camera app.

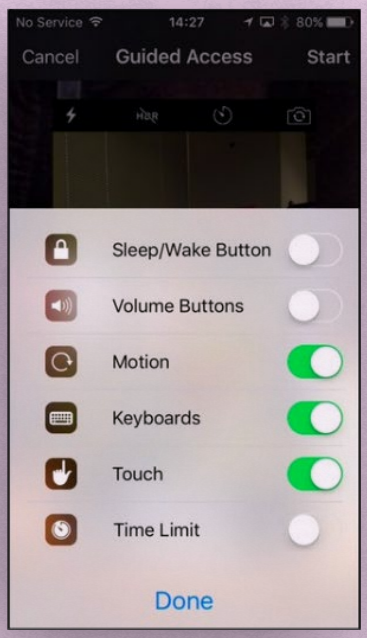
- Next, **triple-click the home button**. This will give you options to restrict features within an app, as shown below. This is the best part of this feature, you may have already seen apps that lock other applications, but the ability to lock specific features within an app is new and different. Simply circle any areas of the screen you would like to make inaccessible.[16]

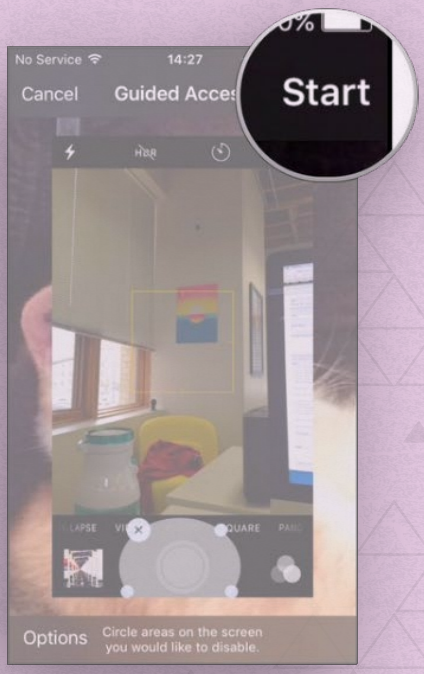
[16] http://www.imore.com/how-use-guided-access-iphone-and-ipad



✔ Tap on **Options** in the bottom left corner to choose whether you want to grant access to the **sleep/wake** button, **volume** buttons, touch screen, and motion. Tap **Done** to save your selections. Tap on **Start** at the top of the screen to begin Guided Access.







Once Guided Access is enabled, anyone trying to use or leave a specific app will require the passcode. Without the code, he or she will not be able to exit Guided Access.

2. DEALING WITH METADATA ON PHOTOS

Photos we take on all electronic devices can often carry data that can be used to pinpoint our location and gather other information about us.

This information can be intercepted and gathered as part of the surveillance of our movements and habits. These details are often shared through something called **metadata** which is the additional details useful to categorizing, locating, or describing a file. Put simply, metadata refers to data about data.

Many of the files we use and create on our phones have metadata, including emails, text messages, and photos. So one of the ways we can secure our phones is by minimizing the metadata our phones share while we communicate.

The metadata in photographs is known as the **Exchangeable Image File Format,** or **EXIF.** This metadata can reveal much about you, your subject, and where a photo was taken. Metadata embedded in a photo includes the following:

- Key identifying information, such as camera or cell phone user, GPS coordinates, and the time and date the photo was taken
- Camera settings, including static information such as the camera model and make, and information that varies with each image such as orientation (rotation), aperture, shutter speed, focal length, metering mode, and ISO speed information
- A thumbnail preview of the picture on the camera's LCD screen, in file managers, or in photo manipulation software.
- Descriptions of a photographs' content.
- Copyright information.

NOTE: Different versions of iPhones may have different ways to get to the settings described in this section. We describe the general method but do a little searching around the settings areas of your particular version of phone to make sure you achieve the same.

✔ SWITCH OFF LOCATION TAGGING FOR YOUR CAMERA

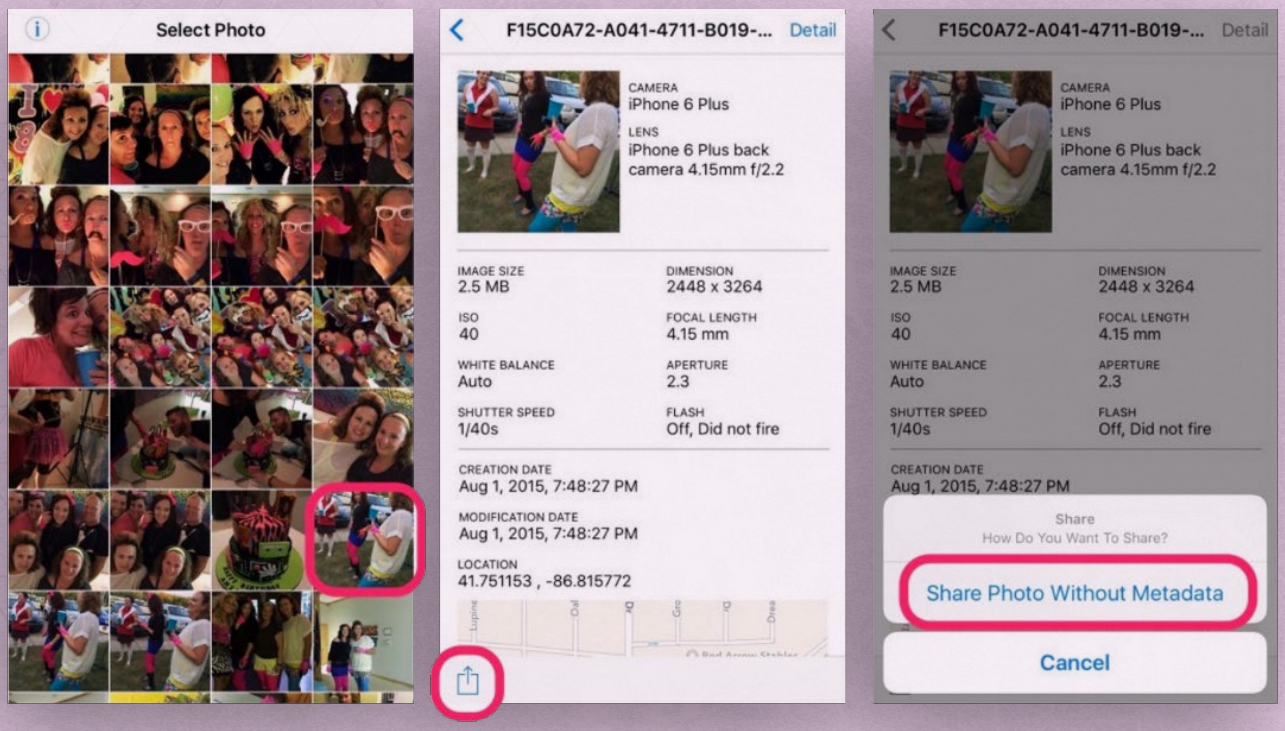
iPhone: Open the Settings app, then tap **Privacy**. Tap **Location Services**, find and tap **Camera** in the list of apps. Under, Allow Loaction Access, select **Never**.

✔ INSTALL A THIRD-PARTY APP FOR SCRUBBING METADATA FROM IMAGES

We recommend using **PixIMet** to remove (“scrub”) existing metadata from photos taken with your phone.

PixlMet for iPhones

This app works the same way. When you choose a photo, it shows you the saved metadata and allows you to share the photo to social media without this data.



NOTE: When removing metadata from a photo that is about to be shared, PixlMet makes a copy of the original photo and only removes metadata from the copy. The original file remains unmodified in your photo library.

SECURE YOUR COMPUTER

SECURE YOUR COMPUTER

Whether you are setting up a new machine or using using your day-to-day computer, it's a good idea to check your settings. In this section, we lay out some basics of computer security for both Macs and PCs. This section is broken down by operating system. In later editions, we hope to include sections on Linux, ChromeOs, and more, so stay tuned.

SECURE YOUR MAC

1. SETTING UP USERS AND PASSWORDS

It is good practice to set up different user accounts on your computer. For example, if one of your accounts is compromised by malicious software you can delete it so that it does not spread. This process helps to compartmentalise damage, allowing you to sandbox different activities on your machine. In general we recommend having an administrator account and several user accounts.

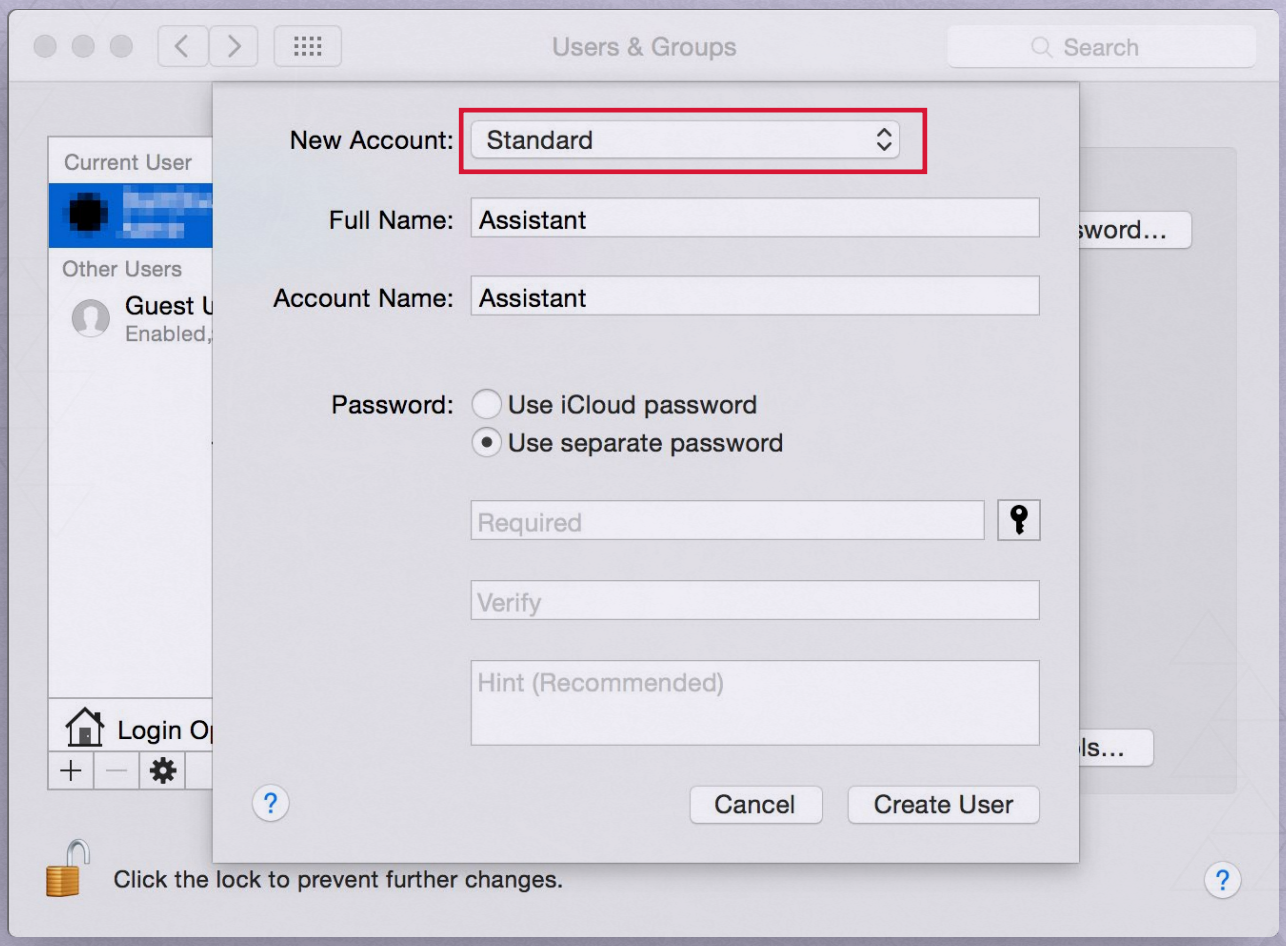
The **Administrator** account should be used to make large-scale changes, such as installing software or changing important settings. Only you or your organization's system administrator should have access. You can use another standard account for other everyday actions.

When using the **Standard** account, your computer will typically request an administrator's password as a permission when a user attempts to download, add software, or make changes. This approach will allow you to assess the resk.

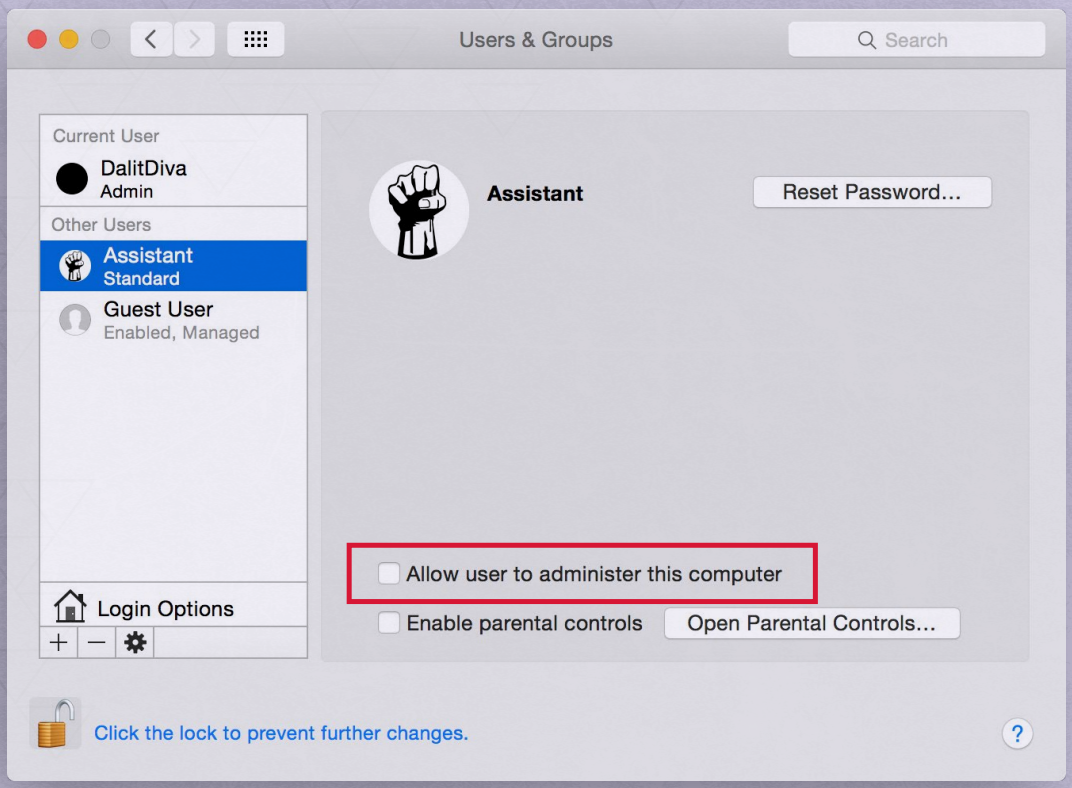
✔ To make this change, go to **Apple Menu → System Preferences → Users and Accounts**.

TIP: Always click the lock after you have selected your settings to make sure further changes require your password.

- Under this section, click on the **"+"** sign to create a new account. Select **Standard** and name the account.



✔ Make sure you keep the **"Allow user to administer this computer"** option **unchecked**.

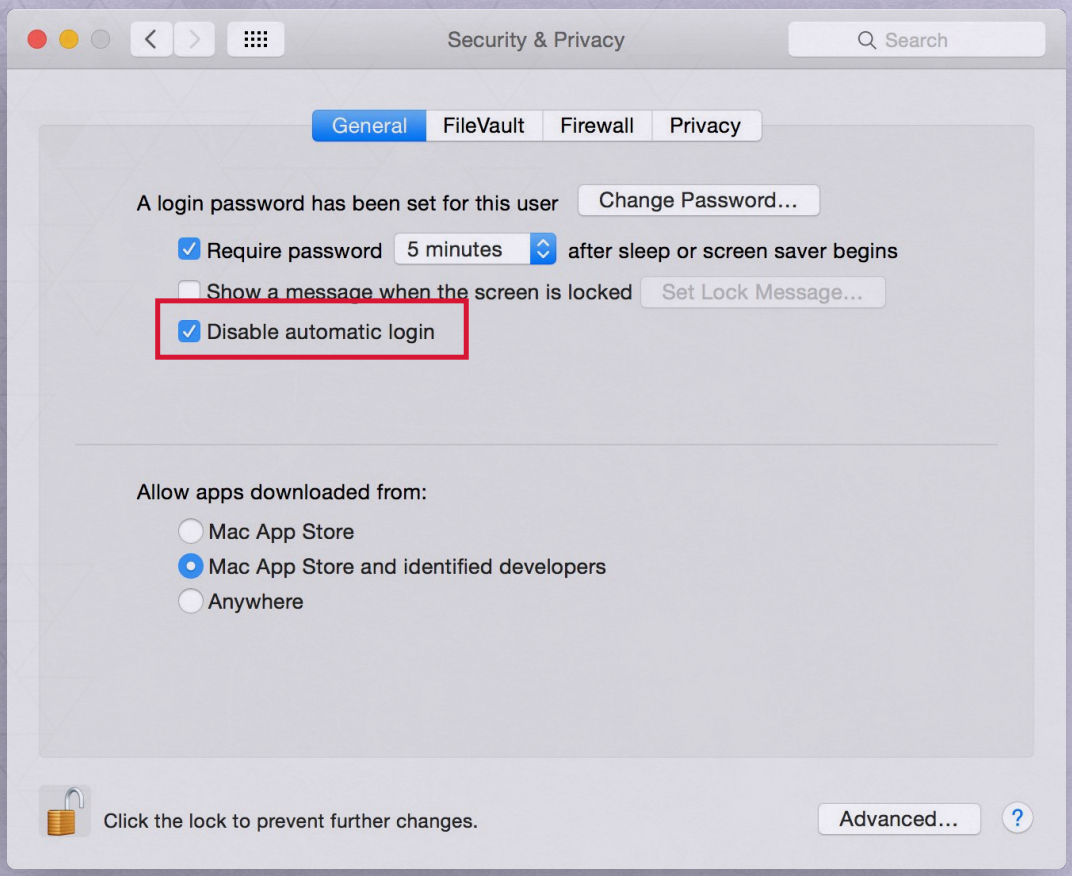


WARNING: If you did not select strong passwords, you will underride all other efforts to secure your computer. See the Secure Your Identity Password section for what makes a good password on page (71).

Also see page 72 and 73 on Rules for best passwords. If you don't want (or don't have time) to use a password manager or set a strong password, at least make sure you follow a few simple rules:

- The password should contain around 20 characters.
- Combine upper and lowercase locate, retrieve, and symbols.
- Don't use the same password for other accounts.
- Change your password at least every three months or more frequently based on your risk assessment.

TIP: Using a standard account ensures that a piece of malware that infects a limited account, won't do as much damage as one that infects an administrator account.



2. DISABLE AUTOLOGIN

Automatic login is the default setting on your computer. However, we highly recommend that you disable it, because anyone who has access to your computer will then be able to access your files. Don't leave yourself vulnerable, particularly if you work in an open office or in a space where multiple people might access your computer.

You can change this and tell your operating system to display a login screen when you start your computer.

- To do so, go to the **Security & Privacy** preferences under the **System Preferences** panel and click on the **General tab**. There, you will see an option to **Disable Automatic Login**.

3. ENABLE FULL DISK ENCRYPTION

The foundation of protecting your computer is encryption. Encryption scrambles your data so that no one can read its contents unless you have your password. While there are many ways to encrypt your hard drive Apple offers FileVault full disk encryption[17] as an easy option for you to begin encrypting. FileVault can encrypt your entire hard drive using a secure encryption algorithm.

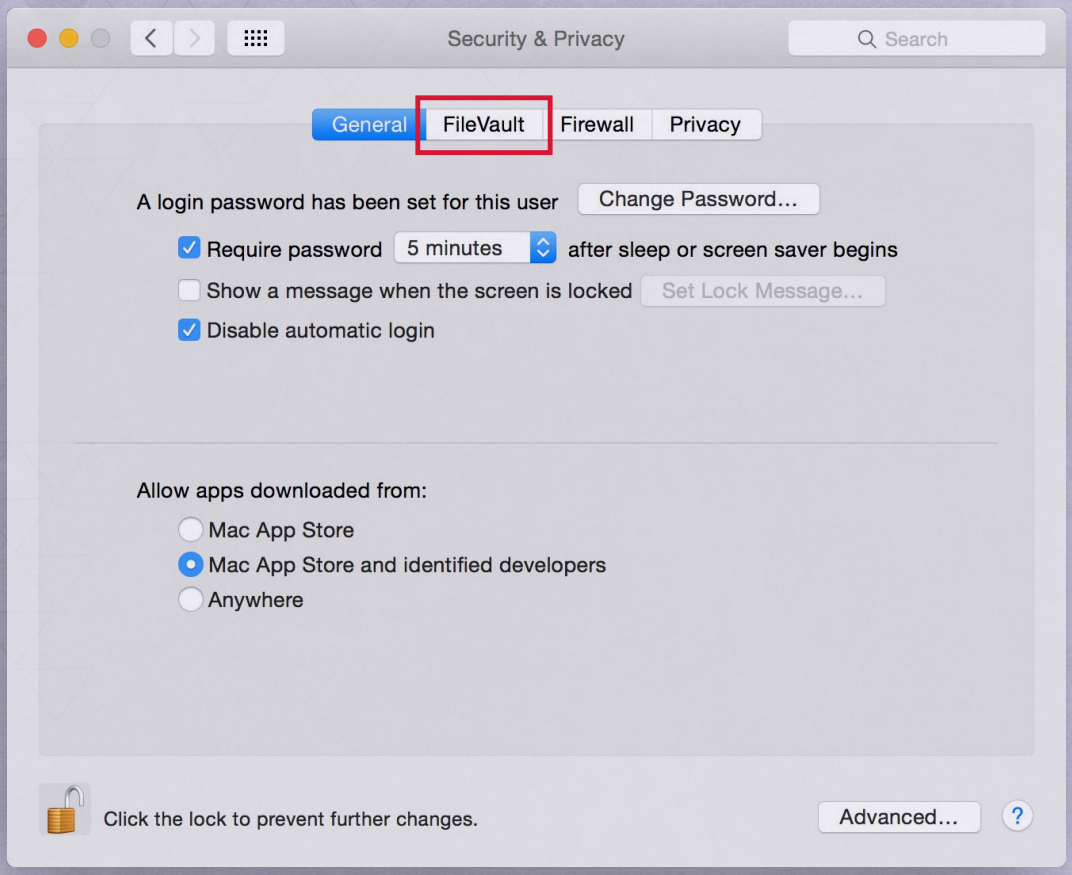
[17] https://www.intego.com/mac-security-blog/15-mac-hardening-security-tips-to-protect-your-privacy/

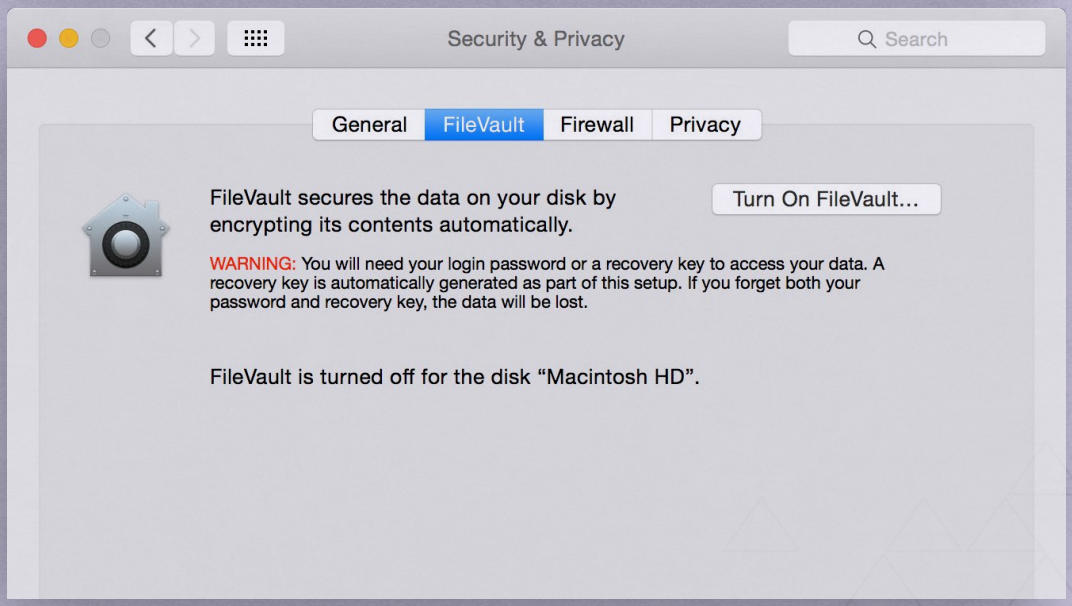
If you do not enable this feature on your Mac hard drive, anyone who manages to steal your computer can access any data on it.

With FileVault enabled, as soon as your Mac shuts down, its entire drive and data are scrambled and rendered inaccessible without your password. The drive's contents only unlock when an authorized user powers up the Mac and logs in. File Vault encryption is an absolutely necessary layer of protection so let's get started in activating it on your computer!

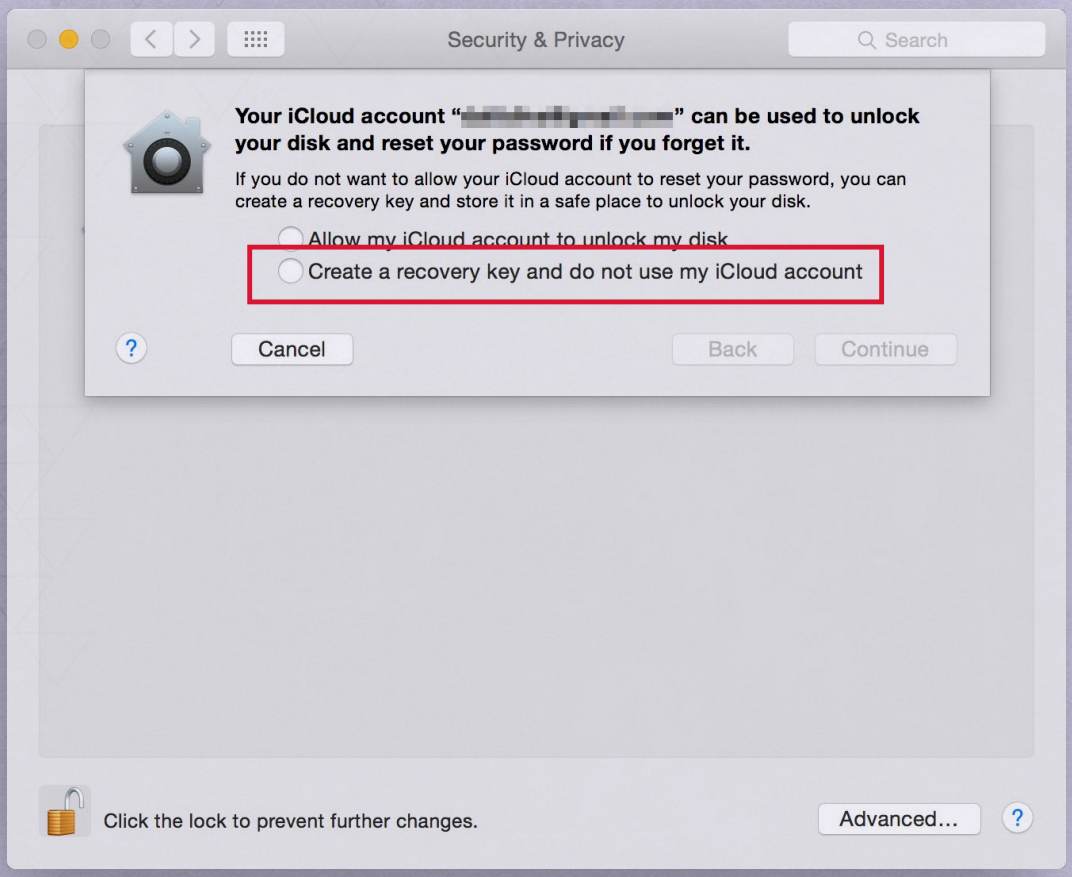
NOTE: Before beginning encryption make sure you have backed up all of your contents of your mac and that you are plugged in. That way if anything goes wrong you can restore your computer from your backup.

✔ Make sure you have logged into OS X with an **administrator's account**, then go to **System Preferences → Security & Privacy → FileVault**.

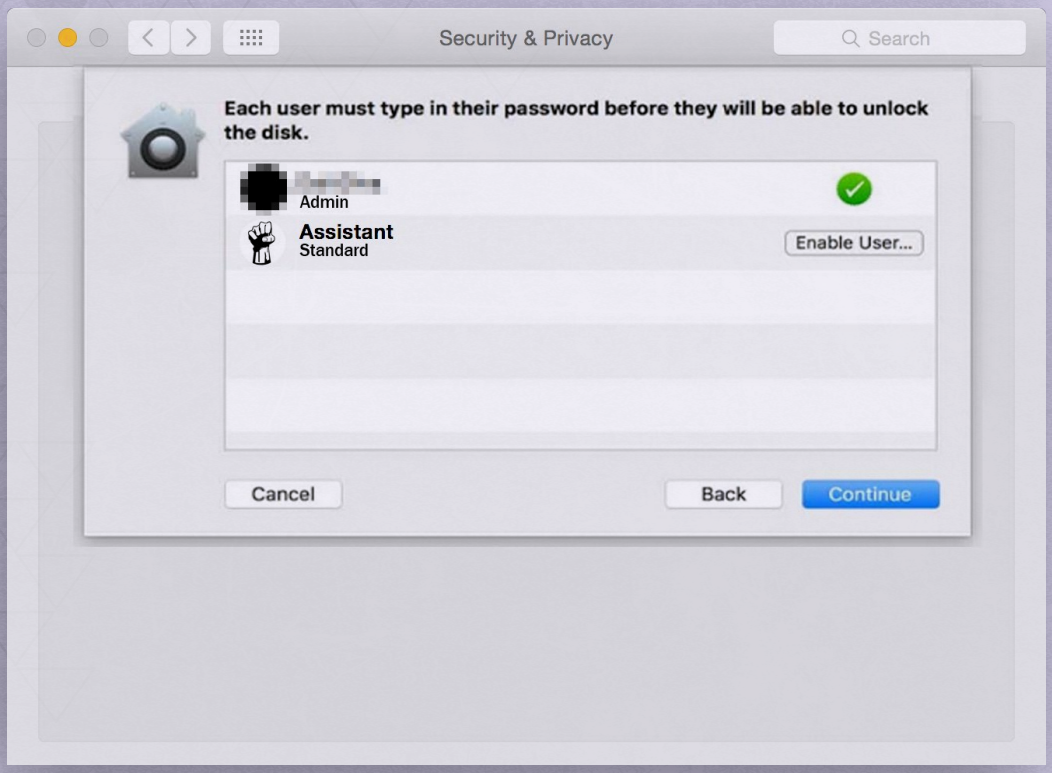




- You now have two options: Allow your iCloud account to unlock your disk, or to create a recovery key. **DO NOT CHOOSE THE ICLOUD OPTION!** This surrenders access to your drive to Apple when you might not want to grant this access.



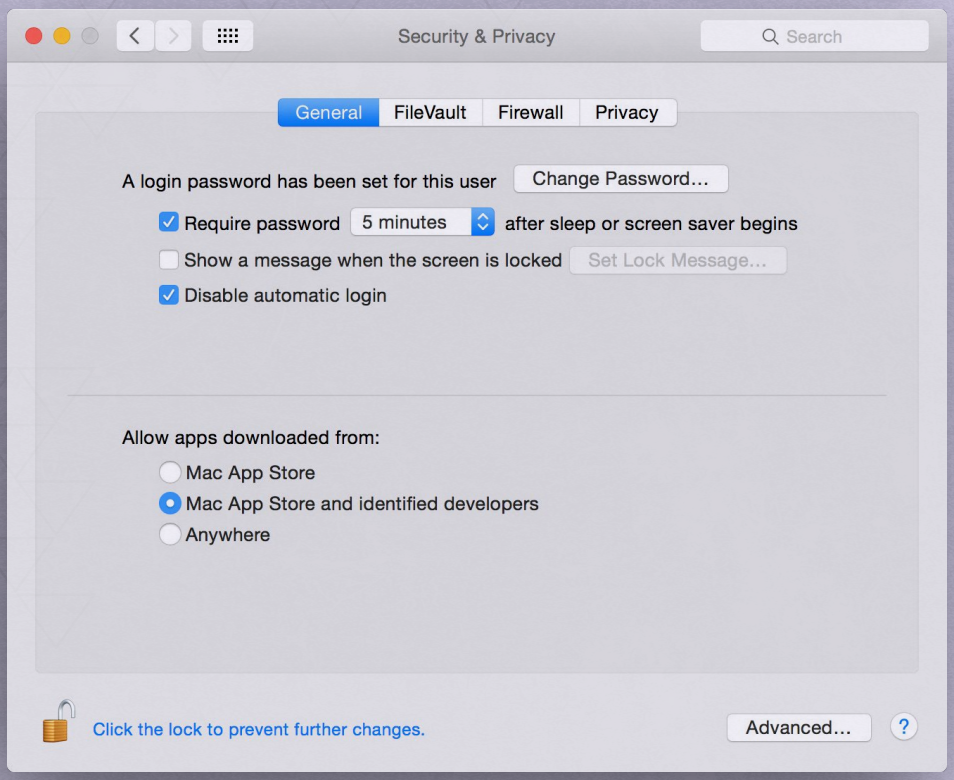
- Once there, press Turn on FileVault. Use the **“Create a recovery key”** option and write down **and save the key in a safe place**. Then click on **Continue**.

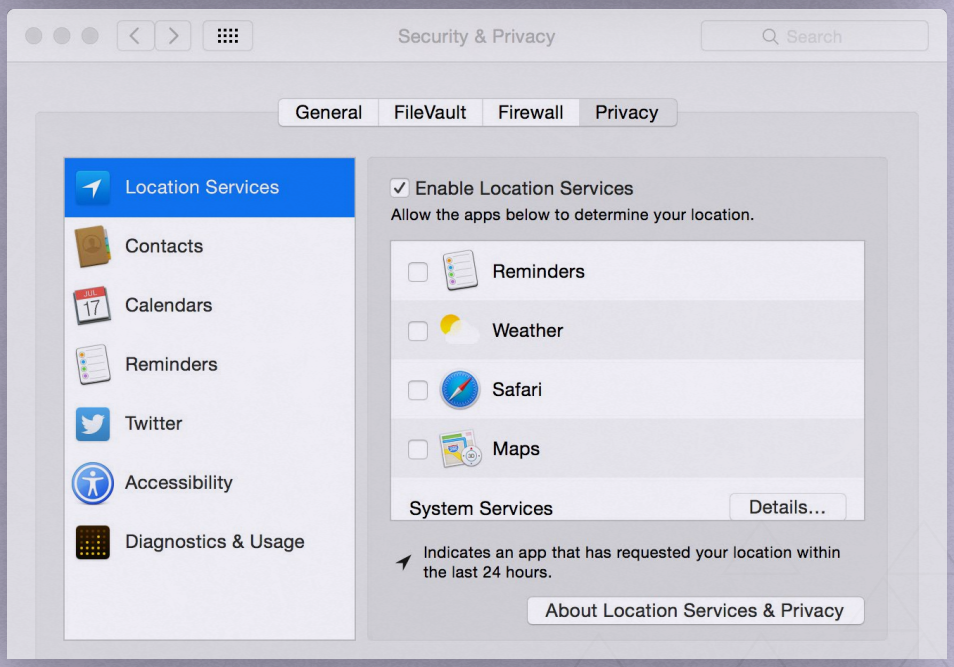


4. AUDIT YOUR SECURITY & PRIVACY SETTINGS

How comfortable are you with sharing your physical location with different apps? Do you even know which apps are receiving the changing details of your locations? A quick visit to System Preferences can reveal all.

To update these settings, click on **Security & Privacy** and choose the **Privacy tab**. Once there, you can choose **Location Services** and view whether they are enabled, and if so, which apps can access your location. To make changes to these settings, you may need to **unlock the padlock** by entering an administrator password.





5. KEEP YOUR COMPUTER'S SOFTWARE UPDATED

As always, it is important to keep your software up to date to thwart new security threats.

✔ Going to the **Apple Menu → App Store** will lead you to the software updates section.

SECURE YOUR PC

1. SET UP DIFFERENT USER ACCOUNTS AND PASSWORDS

It is good practice to set up different user accounts on your computer. For example, if one of your accounts is compromised by malicious software you can delete it so that it does not spread. This process helps to compartmentalise damage, allowing you to sandbox different activities on your machine. In general we recommend having an administrator account and several user accounts.

Windows grants a certain level of rights and privileges depending on what kind of user account you have. You may have a standard user account or an administrator user account.

The **Administrator** account should be used to make large-scale changes, such as installing software or changing important settings. Only you or your organization's system administrator should have access. You can use another standard account for other everyday actions.

We recommend using standard accounts for your computer to prevent users from making changes that affect everyone who uses it, such as deleting important Windows files necessary for the operating system.

When using the **Standard** account, your computer will typically request an administrator's password as a permission when a user attempts to download, add software, or make changes. This approach will allow you to assess the resk.

If you want to install an application or make security changes, Windows will ask you to provide the credentials for an administrator account.

TIP: Using a standard account ensures that a piece of malware that infects a limited account, won't do as much damage as one that infects an administrator account.

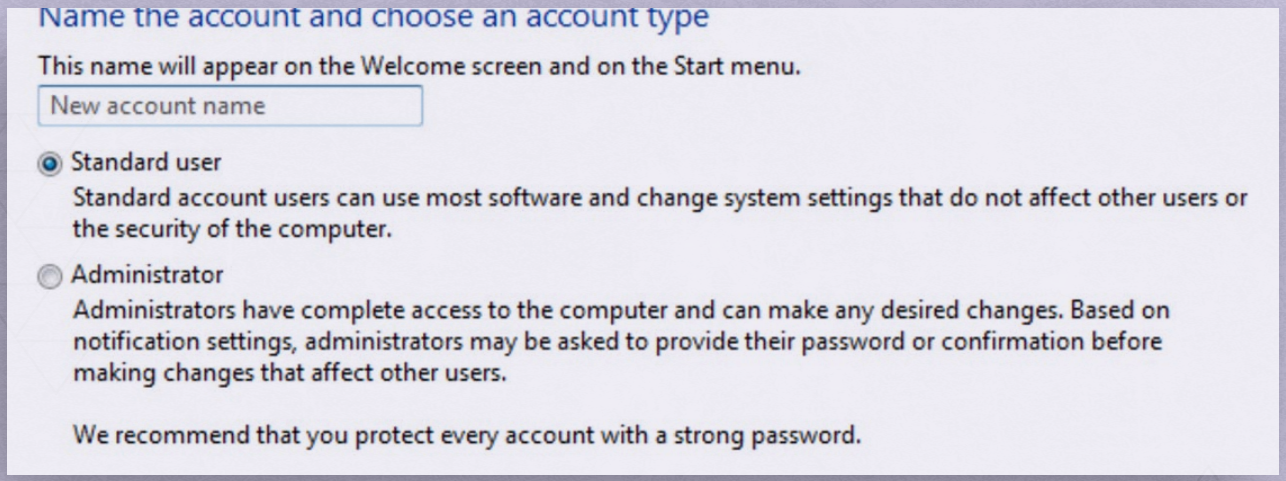
Also see page 71 on Rules for best passwords. If you don't want (or don't have time) to use a password manager or set a strong password, at least make sure you follow a few simple rules:

- The password should contain around 20 characters.

- Combine upper and lowercase locate, retrieve, and symbols.
- Don't use the same password for other accounts.
- Change your password at least every three months or more frequently based on your risk assessment.

✔ To create a new account on Windows 10, select **Start → Settings → Accounts → Family & other people → Add someone else to this PC**

✔ To create a new account on previous versions click **Start → Control Panel → User Accounts and Family Safety → User Accounts → Manage another account → Create a new account**.



2. TURN ON YOUR FIREWALL

One important defense for windows users is a Firewall, it is a piece of software and/or hardware that sits between a computer (or local network) and other networks (such as the Internet), controlling the incoming and outgoing network traffic.

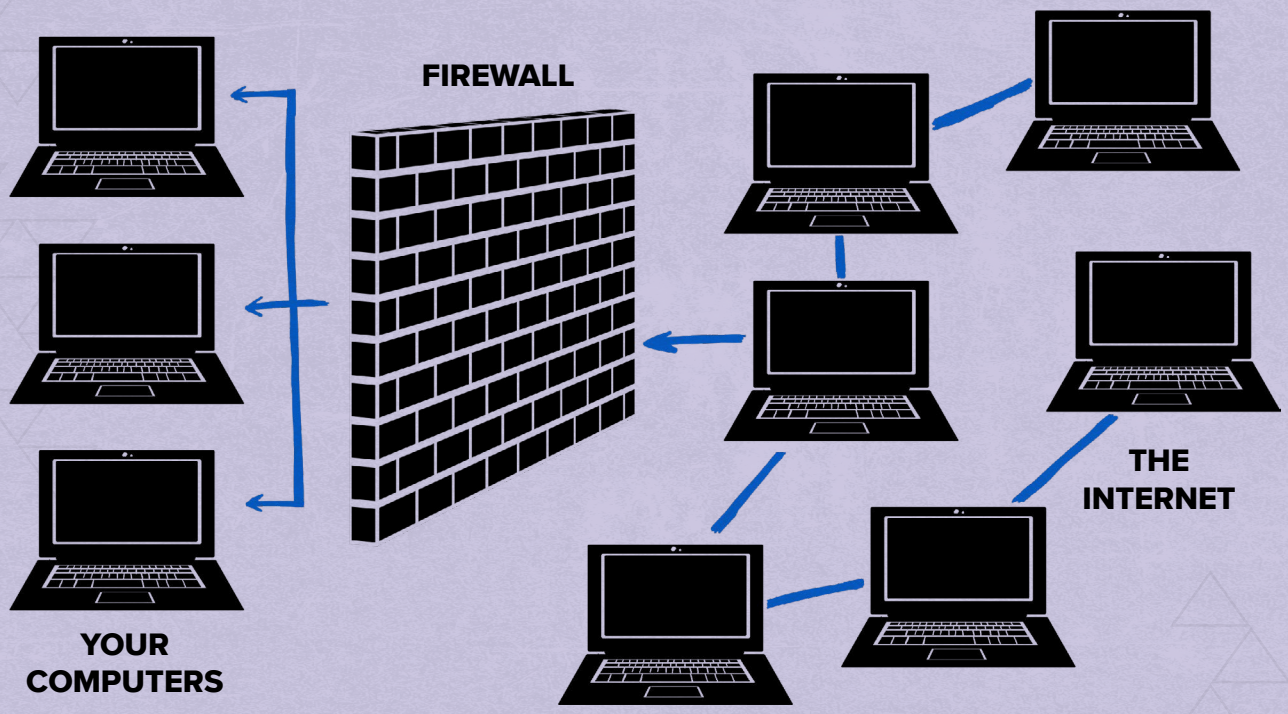
Without a firewall, anything can pass through your network. With a firewall, the firewall's rules determine which traffic is allowed through and which isn't.

This prevents people on the Internet from connecting to local network services on your computer. It also controls access to network services from other computers on your local network. That's why you're asked what type of network it is when you connect to one in Windows. If you connect to a Home network, the firewall will allow access to these services. If you connect to a Public network, the firewall will deny access.

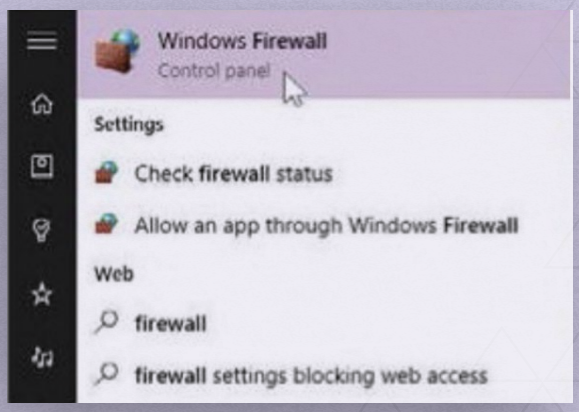
A firewall's main security purpose for home users is blocking unsolicited incoming network traffic, but firewalls can do much more than that. It can analyze all traffic reaching or leaving the network, making decisions on whether to block it or let it pass. For example, a firewall could

also be configured to block certain types of outgoing traffic, it can also log suspicious traffic or all traffic.

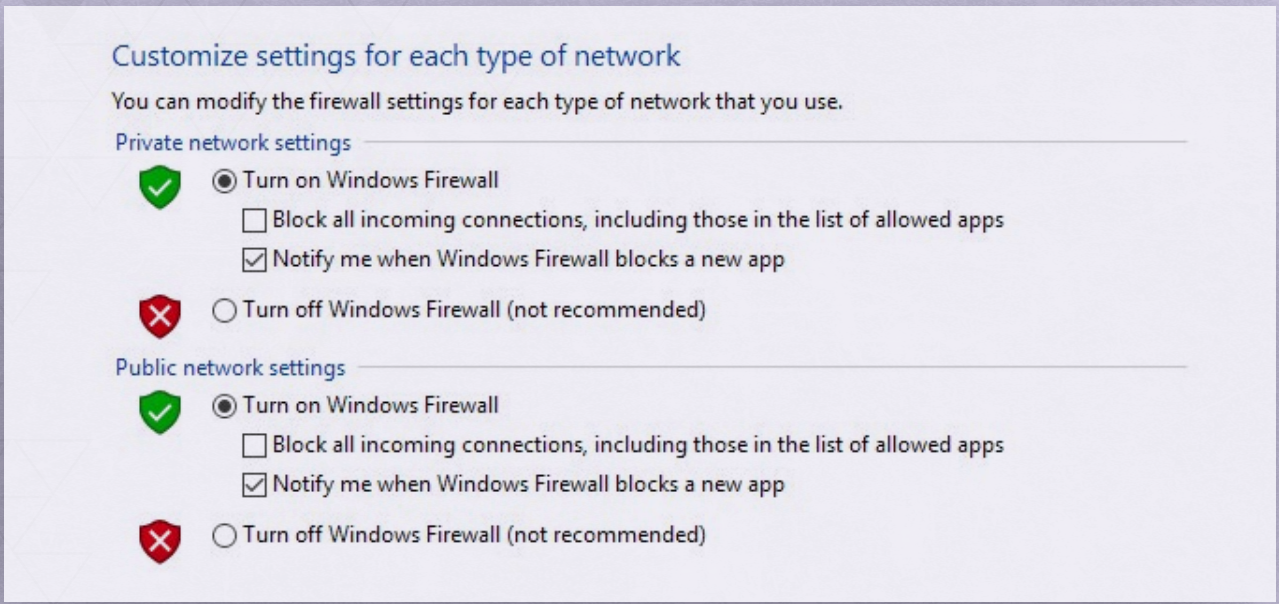
Firewalls can be anything from a piece of software running on your laptop (like the firewall included with Windows) to dedicated hardware in a corporate network. Such corporate firewalls could analyze outgoing traffic to ensure no malware was communicating through the network, monitor employee's Internet use, and filter traffic—for example, a firewall could be configured to only allow web browsing through the firewall, blocking access to other types of applications.



- You can find the Windows firewall in previous versions by going to **Start → Control Panel → System and Security → Windows Firewall**
- For Windows 10 users click on **Start** at the bottom left hand corner of the screen, type "firewall" into the search box, select "**firewall.cpl**"



- Check basic firewall settings, then ensure the firewall is turned on for private and public networks and that notifications are enabled.

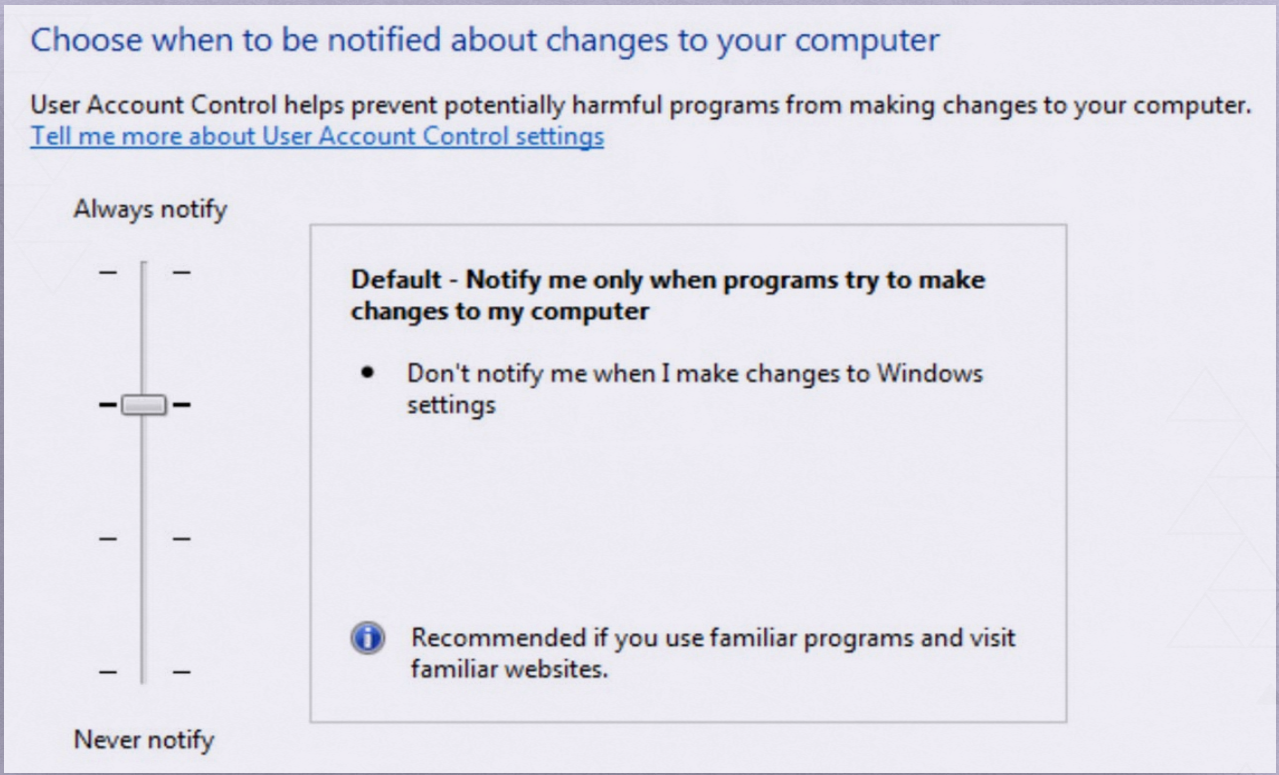


3. KEEP YOUR USER ACCOUNT CONTROL TURNED ON

Many users have the tendency to turn off **User Account Control** (UAC) after installing/reinstalling the Windows operating system. We don't recommend this. Instead of disabling the UAC, you can decrease the intensity level using a slider in the Control Panel.

UAC monitors the changes made to your computer. When important changes appear, such as installing a program or removing an application, the UAC pops up asking for administrator-level permission.

Should your user account be infected with malware, UAC helps you by keeping suspicious programs and activities from making changes in the system.



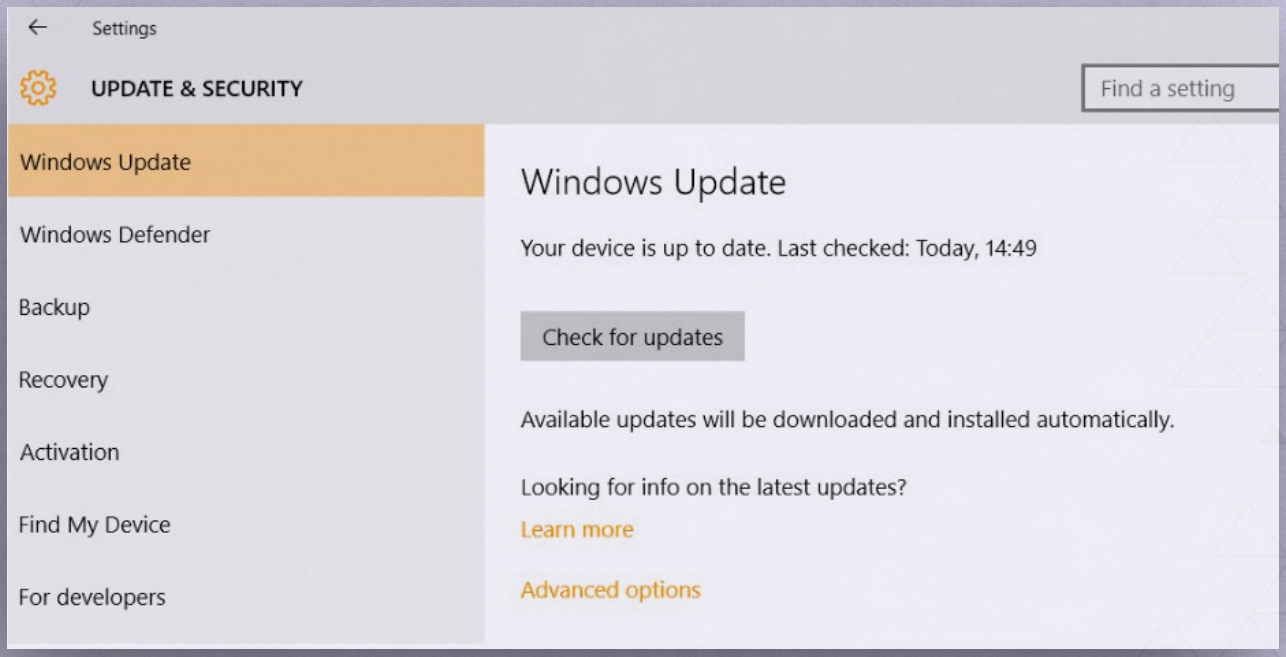
4. KEEP YOUR WINDOWS OPERATING SYSTEM UP TO DATE

The first important step is checking whether you have the latest security updates and patches available for your Windows operating system.

To get these security updates automatically, go to Control Panel and check whether automatic updating is enabled. Or, follow the stepsbelow:

- Access the search box in your Windows operating system, type **"update"**, and then select **Windows Update**.
- Select **"Change settings"**.
- Click **"Install updates automatically (recommended)"**, in case it is not already selected.

After the initial installation of available updates for your Windows operating system, keep the automatic option turned on to download and install important updates that can help protect your computer against new viruses and security threats. It's essential to install the latest security and stability fixes for your operating system, as hackers always try to benefit from these gaps.



5. INSTALL A TRADITIONAL ANTIVIRUS FOR REACTIVE PROTECTION

Use a known antivirus product from a **big security company**. It is important to have a reliable security solution on your system, which should include real-time scanning, automatic update and a firewall.

To find the best solution, check the antivirus test results in AV Comparatives, PC Magazine, AV-TEST, or Virus Bulletin and select the best solution for your system.

In case you choose to install a security product that doesn't include a firewall, make sure you have the **Windows firewall** turned on.

- To enable it, go to **Control Panel → Firewall → Turn Windows Firewall on or off**. Then, choose **Turn on Windows Firewall** for all options.

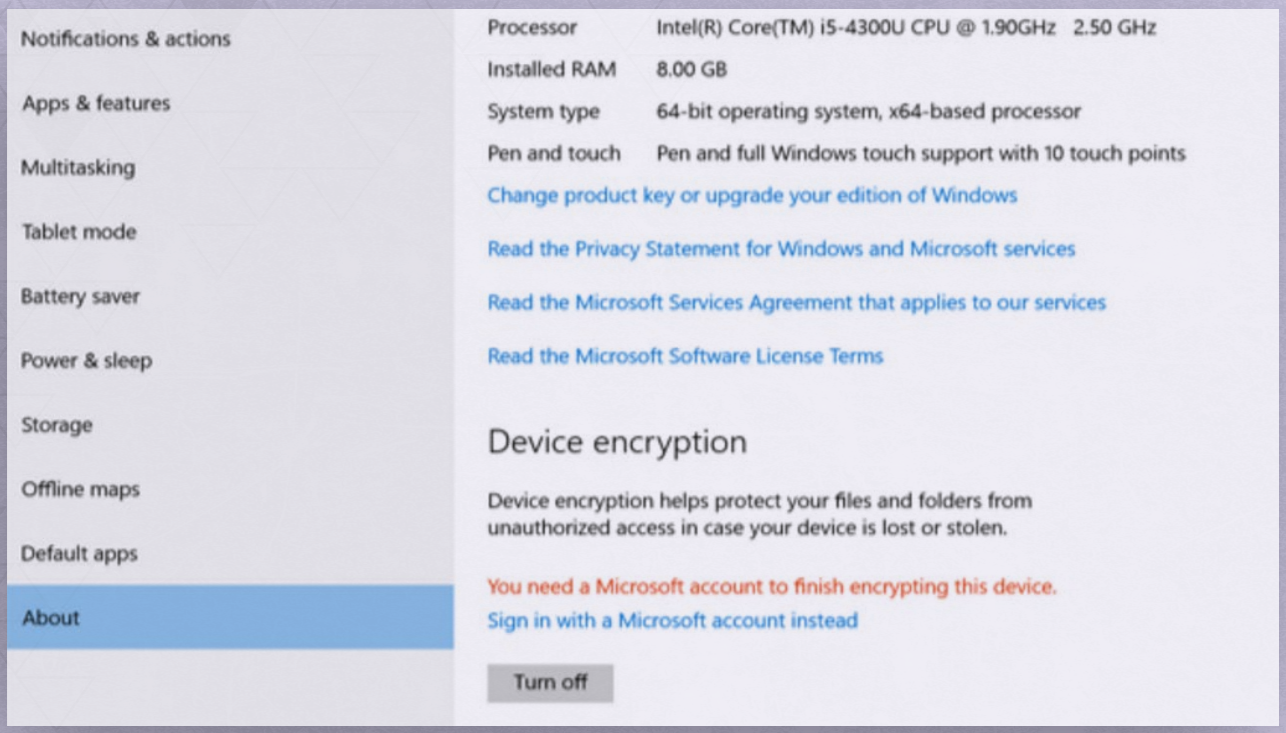
6. DEVICE ENCRYPTION FOR PCS

The foundation of protecting your computer is encryption. Encryption scrambles your data so that no one can read its contents unless you have your password. While there are many ways to encrypt your harddrive many new PCs that ship with Windows 10 will automatically have **Device Encryption** enabled. This feature was first introduced in Windows 8.1 and comes with specific hardware requirements.

With Windows Device encryption enabled, as soon as your PC shuts down, its entire drive and data are scrambled and rendered inaccessible without your password. The drive's contents only unlock when an authorized user powers up the PC and logs in.

This feature also has another limitation—it only encrypts your drive if you sign into Windows with a Microsoft account. Your recovery key is then uploaded to Microsoft's servers. This will help you recover your files if you ever can't log onto your PC but also allows Microsoft to have access to your content as well . (This is also why the FBI likely isn't too worried about Window's Device Encryption, but, for now, we're just recommending encryption as a means to protect your data from laptop thieves If you're worried about the NSA, you may want to use a different encryption solution like **Veracrypt.** We will have a separate unit on Veracrypt in the future so stay tuned.

- To check if Device Encry http://about.complex.com/ ption is enabled, open the Settings app, navigate to **System → About**, and look for a **"Device Encryption"** setting at the bottom of the **About** panel. If you don't see anything about Device Encryption here, your PC doesn't support it and it's not enabled.



NOTE: In addition to using this option for Windows, we also recommend **VeraCrypt**. It is a free software that allows you to encrypt your files. VeraCrypt is available for Microsoft Windows, Mac OS X, and GNU/Linux.

PC Encryption Using VeraCrypt

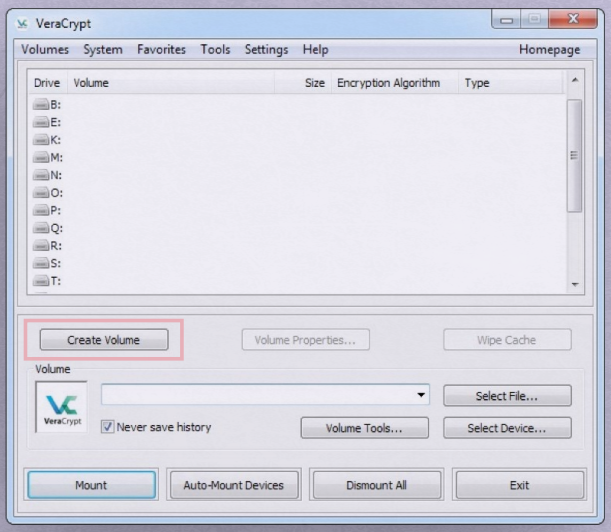
VeraCrypt is free software you can use to encrypt a whole disk, as well as a partition on a disk. You can download VeraCrypt from https://veracrypt.codeplex.com/releases/view/629329

Full disk encryption ensures that your whole computer cannot be turned on or accessed without a password. Read on to start using Veracrypt. As always with encryption processes please back up all your data and plug in to be safe.

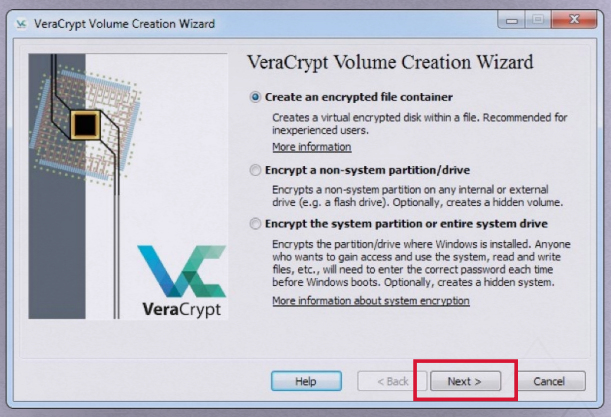
Create a Virtual Partition with Veracrypt (recommended for beginners)

Here, we will create a **Virtual Encrypted Partition**—a file on your hard drive that acts as a completely new, encrypted disk. You can think of this partition as a disk with a password—you can store whatever you like in the disk and the password will give it an additional layer of security.

- To start, open Veracrypt after you have installed it, and click the **“Create Volume"**

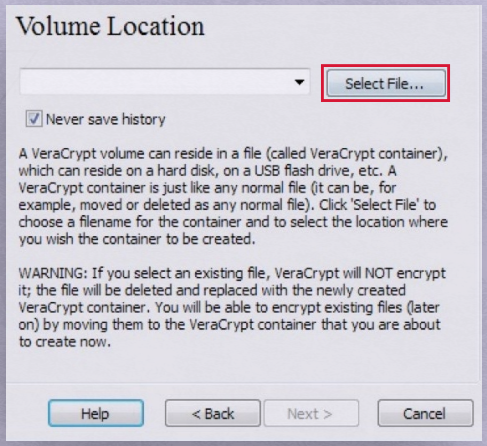


- Then check **“Create an encrypted file container”**

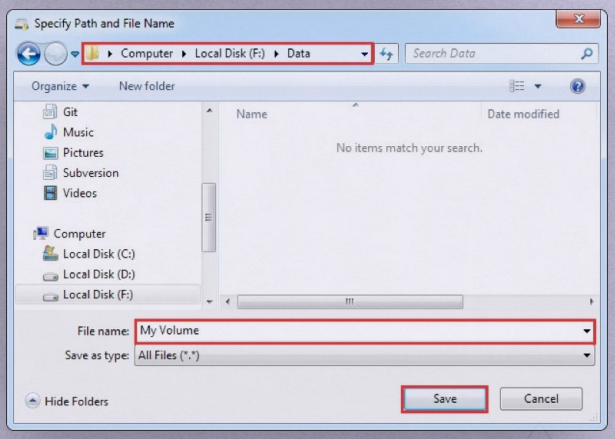


- For right now, we will create a **Standard Veracrypt volume**.

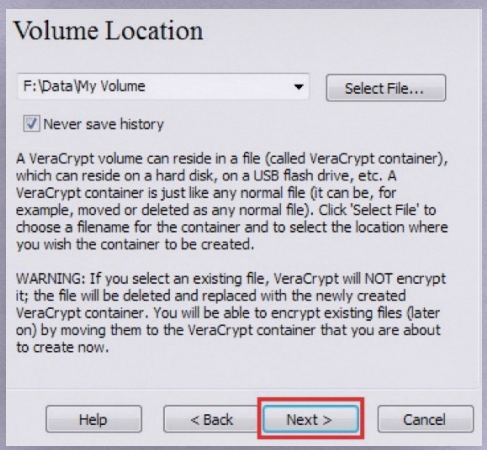
- Now choose **“select file”**. You will be prompted with an file explorer dialogue.



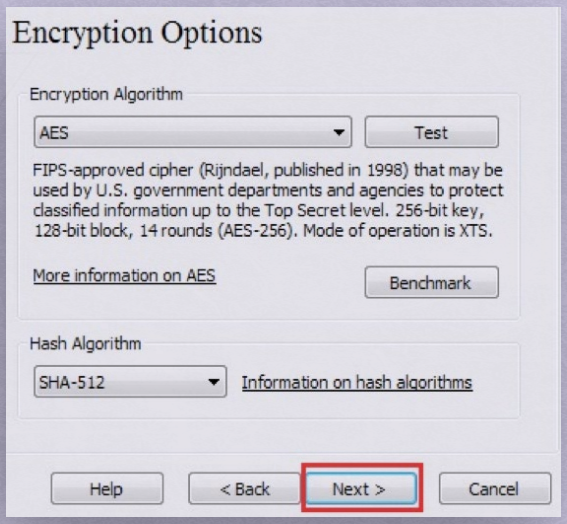
- In this step, we will be Creating a file that will store all your encrypted content. Later in the process, we will “mount” this file, so that it will show up looking like a folder or hard drive. But for now, select a location on your hard disk where this encrypted content will reside.



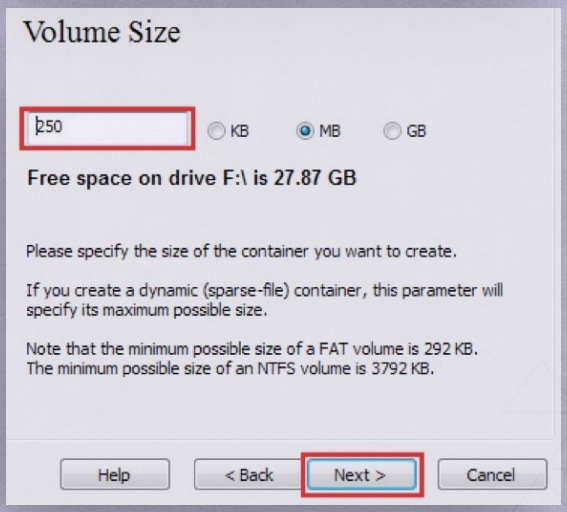
- Go ahead and click **Next** in this next step.



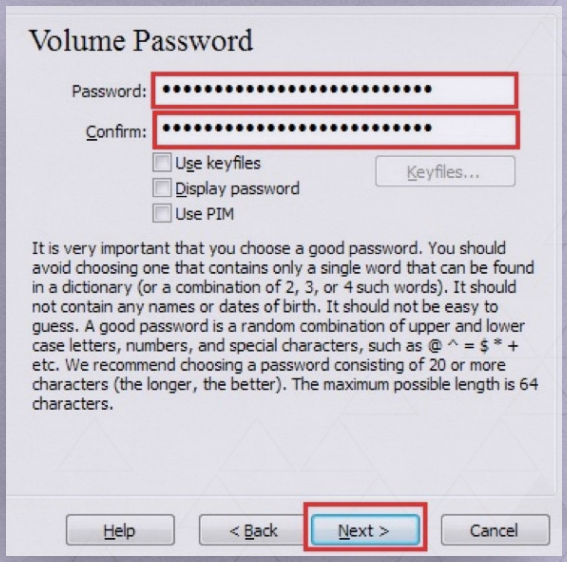
- In this next step, we choose which encryption techniques we should apply. Don't worry if this doesn't make sense, we can click "next" with the default options.



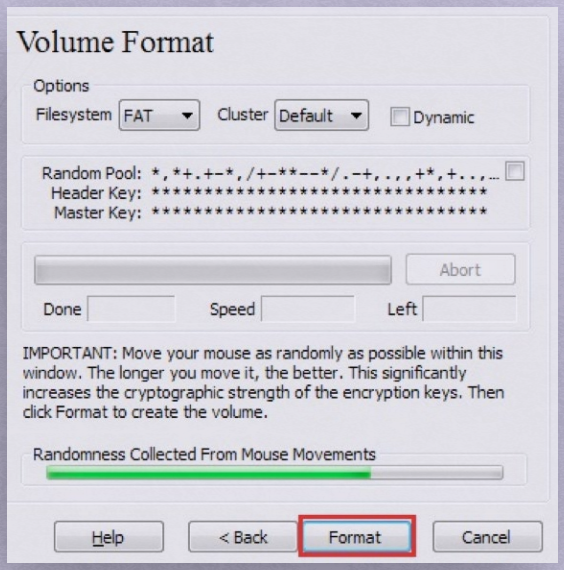
- In this step, you will need to choose how much of your disk space you want to dedicate to this encrypted segment. Make sure that you have that space available on your hard drive. Choose more space if you will be storing movies, video, audio, etc. You can dedicate less space if you are only encrypting text documents or photos.



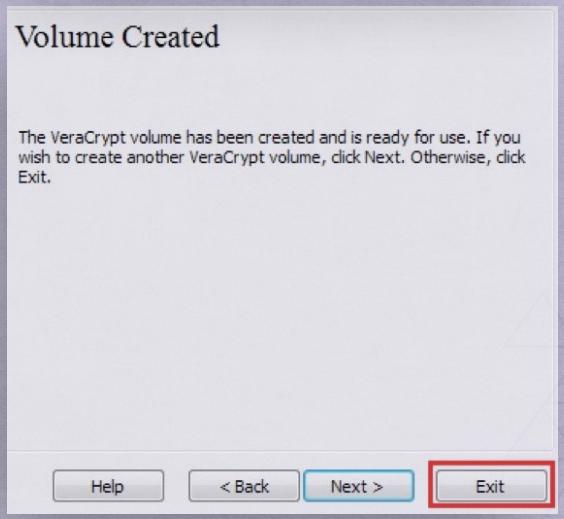
- Next, you will select a password. **Write this password down. Make sure it is a secure password as per the rules described elsewhere in this document.**



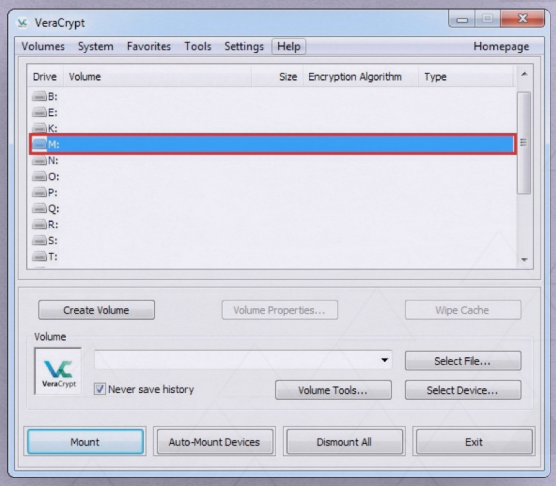
- Next, move your mouse around randomly for about 1 minute. This will generate “random noise” that will then be fed into the encryption in order to make it more un-crackable.



- At this point, you should see a volume successfully being created That is good, but we are not quite yet done.

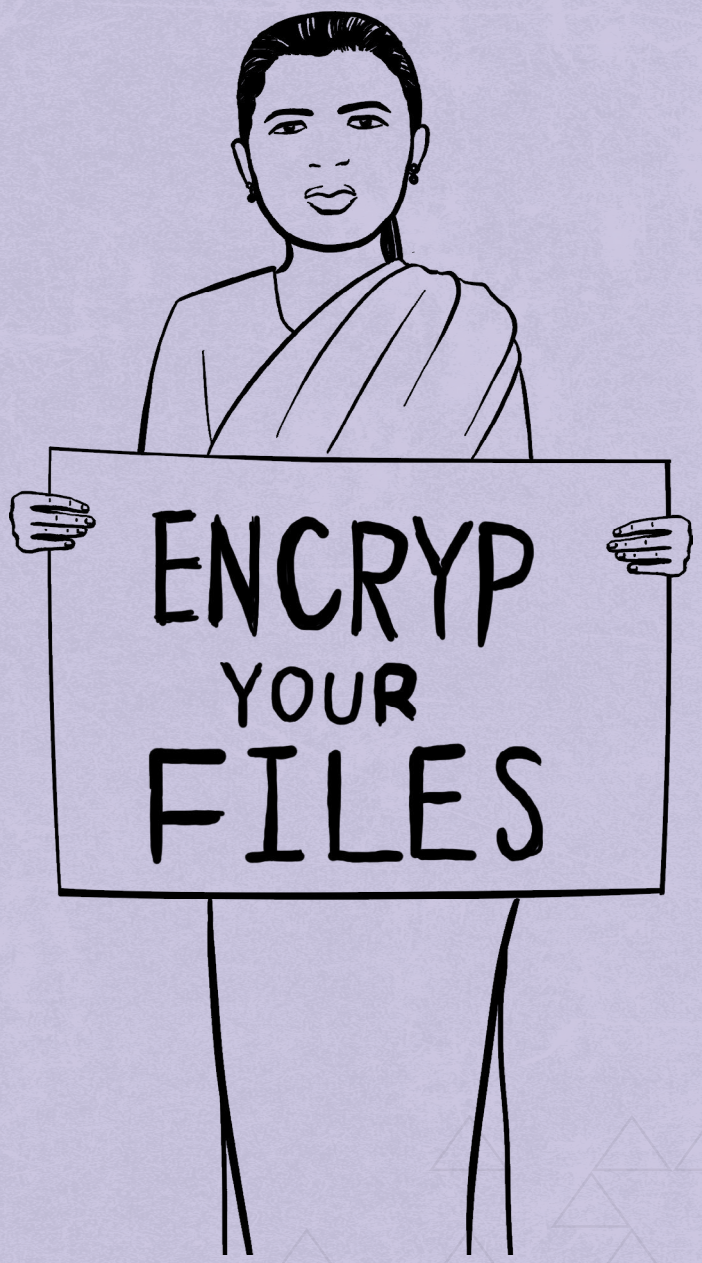


- Now, we are going to select an available drive letter in order to make the encrypted partition you just made visible as an extra hard drive. Go ahead and select any of the letters in the list and then click on **“Select File”**

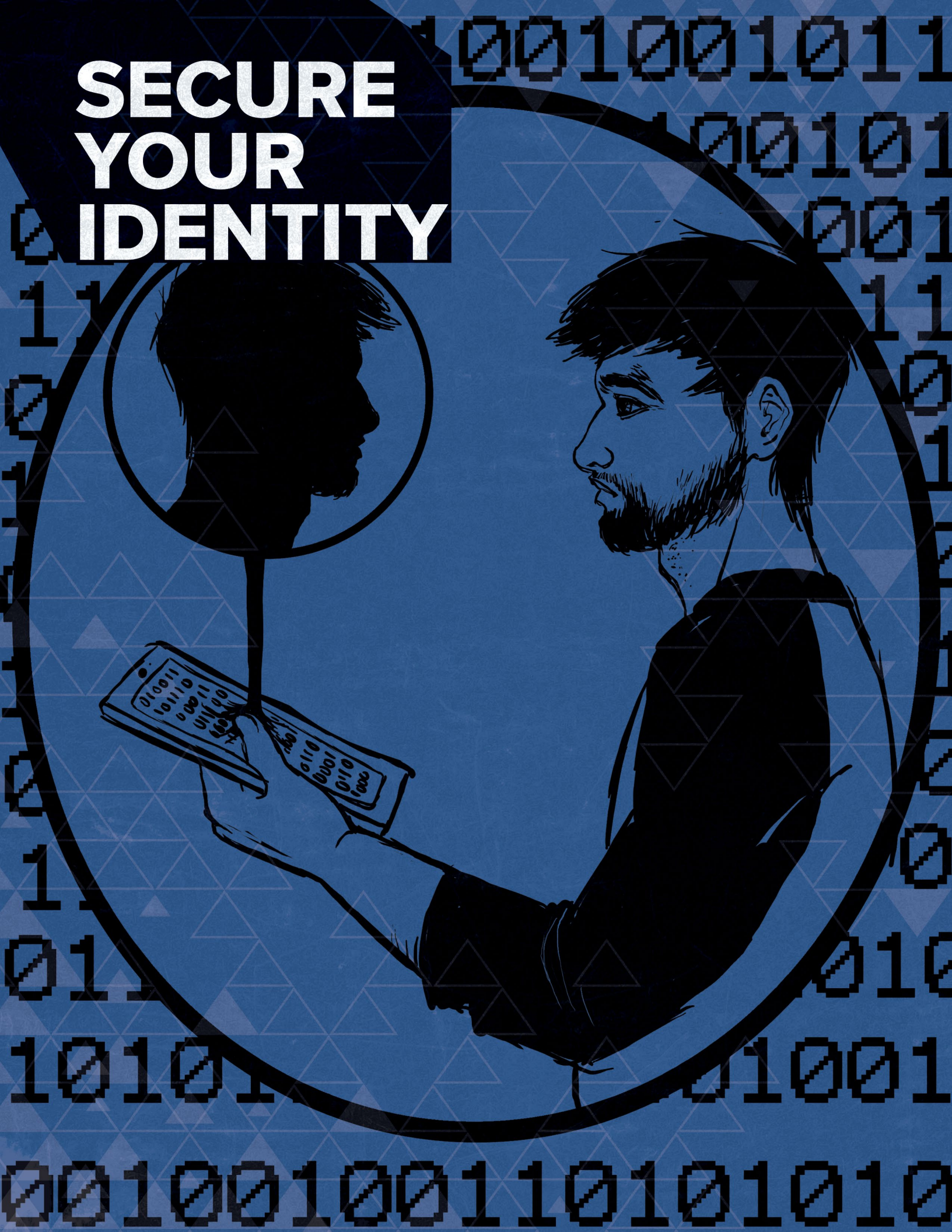


FULL DISK ENCRYPTION WITH VERACRYPT

- We do not recommend encrypting your whole disk with Veracrypt if you are a beginner. If you feel confident with your tech skills to troubleshoot, then proceed in this section. **You will need a USB Stick** to finish this process. You will also need to **Boot into your BIOS** and **Disable Secure Boot** in your BIOS.



SECURE YOUR IDENTITY



SECURE YOUR IDENTITY

We all perform many actions online on a daily basis which increases the amount of data we leave behind that can be used against us. Securing your identity means being aware of the locations your data lives, being aware of the data's vulnerabilities, and learning how you can begin to implement some very simple changes to ensure your identity remains protected. Here are some great tips, let's get started.

PASSPHRASES REALLY ARE EVERYTHING!

Good Passphrases are the Best Defense![18]

A "passphrase" is a long phrase used as a password, which is stronger than a secular word password. The increased length can allow for a greater number of possibilities, a passphrases made of randomly-chosen words can be both easy to remember and hard for someone else to guess, which is what we want.

Computers are now fast enough to quickly guess passwords shorter than ten or so characters—and sometimes quite a few more. That means short passwords of any kind, even totally random ones like nQ\m=8*x, or !s7e&nUY, or gaG5^bG, may be too weak, especially for settings where an attacker is able to quickly try an unlimited number of guesses. This is not necessarily true for an online account, where the speed and quantity of guesses will be limited, but it could be true in other cases (for instance, if someone gets ahold of your device and is trying to crack its encryption password).

[18] https://securityinabox.org/en/guide/passwords & https://www.eff.org/dice

To learn how to make a good passphrase we are going to follow the wonderfully easy workflow set up by our friends at the Electronic Frontier Foundation:

Step 1: Roll five dice all at once. Note the faces that come up without looking at the wordlist yet. (On our dice, the EFF logo is equivalent to rolling a one.)

Step 2: Your results might look like this reading left to right: 4, 3, 4, 6, 3. Write those numbers down.

Step 3: Open EFF's Long Wordlist [.txt] to find the corresponding word next to 43463.

Step 4: You will find the word "panoramic." This is the first word in your passphrase, so write it down.

Step 5: Repeat steps 1-4 five more times to come up with a total of SIX words.

When you are done, your passphrase may look something like this:

panoramic nectar precut smith banana handclap

Step 6: Come up with your own mnemonic to remember your phrase. It might be a story, scenario, or sentence that you will be able to remember and that can remind you of the particular words you chose, in order. For example:

The panoramic view, as I tasted the nectar of a precut granny smith apple and banana, deserved a handclap.

43453	pandemic
43454	pang
43455	panhandle
43456	panic
43461	panning
43462	panorama
43463	panoramic
43464	panther
43465	pantomime
43466	pantry
43511	pants
43512	pantyhose
43513	paparazzi
43514	papaya
43515	paper

Once you have made your passphrase please make sure of the following:

KEEP IT SECRET

Do not share your passphrase with anyone unless it is absolutely necessary. And, if you must share a passphrase with a friend, family member or colleague, you should change it to a temporary passphrase first, share that one, then change it back when they are done using it. Often, there are alternatives to sharing a passphrase such as creating a separate account for each individual who needs access.

MAKE IT UNIQUE

Avoid using the same passphrase for more than one account. That way if one passphrase is compromised hackers won't be able to exploit the rest of your acounts because you used your password for all of your online services. A good way to keep track of many unique and complex passwords is to use a password managers like Keepass X, Last Pass and 1pass.

KEEP IT FRESH

Change your passphrase on a regular basis, preferably at least once every three to six months based on your risk assessment. Some people get quite attached to a particular passphrase and never change it. This is a bad idea. The longer you keep one password, the more opportunity others have to figure it out. Also, if someone is able to use your stolen password to access your information and services without you knowing about it, they will continue to do so until you change the password.[19]

[19] https://securityinabox.org/en/lgbti-mena/passwords

PASSPHRASE MANAGER

These days we have accounts with a lot of companies. Emails, Social media accounts, online bank accounts and so on. One of the most important things you can do is not use one password for all accounts but generate different passwords for each of your individual accounts.[20]

NOW, YOU MIGHT BE SAYING WHHAA???????

But hear us out. This is actually a good thing. After all, your bank information is likely linked to many of your accounts, as well as your purchase history, media browsing habits, and a slew of other private information that you'd prefer protected. But if you're the kind of person who constantly forgets and resets passwords and usernames, or worse, recycles the same password you've been using for the past seven years, it's time for a password management tool. If a hacker discovers your password on a list they can then use it to access every tool in your life!

Passphrase managers actually become invaluable once you take the first step—they are an incredibly powerful improvement to your security, while also being very usable.

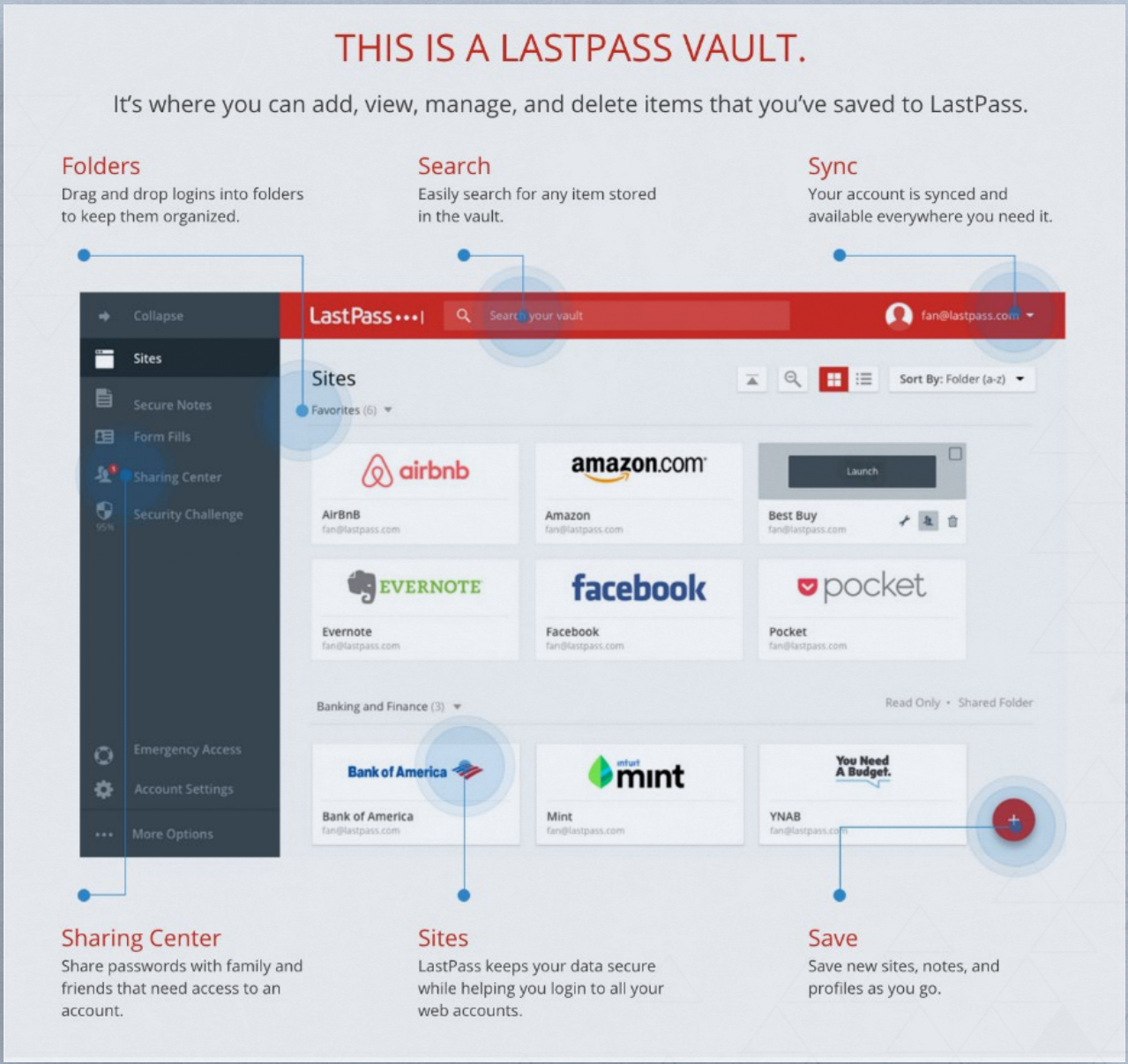
Passphrase managers store all your passwords, generate strong ones for you, and in general, the only password you have to remember is the one to open your password manager. So, make it a strong one.

[20] http://lifehacker.com/5529133/five-best-password-managers

LASTPASS

LastPass saves your passwords and gives you secure access from every computer and mobile device. You only have to remember one password—your **LastPass**[21] master password. Save all your usernames and passwords to LastPass, and it will auto login to your sites and sync your passwords everywhere you need them.

The benefit of LastPass is that it is super easy to use across all your platforms. The problem is that its ease of use comes with the caveat that LastPass is a corporation and your information is in their cloud. So balance its ease with your vulnerability and make your decisions for its use based on that. In general Last Pass is better then no Password Manager so please consider it

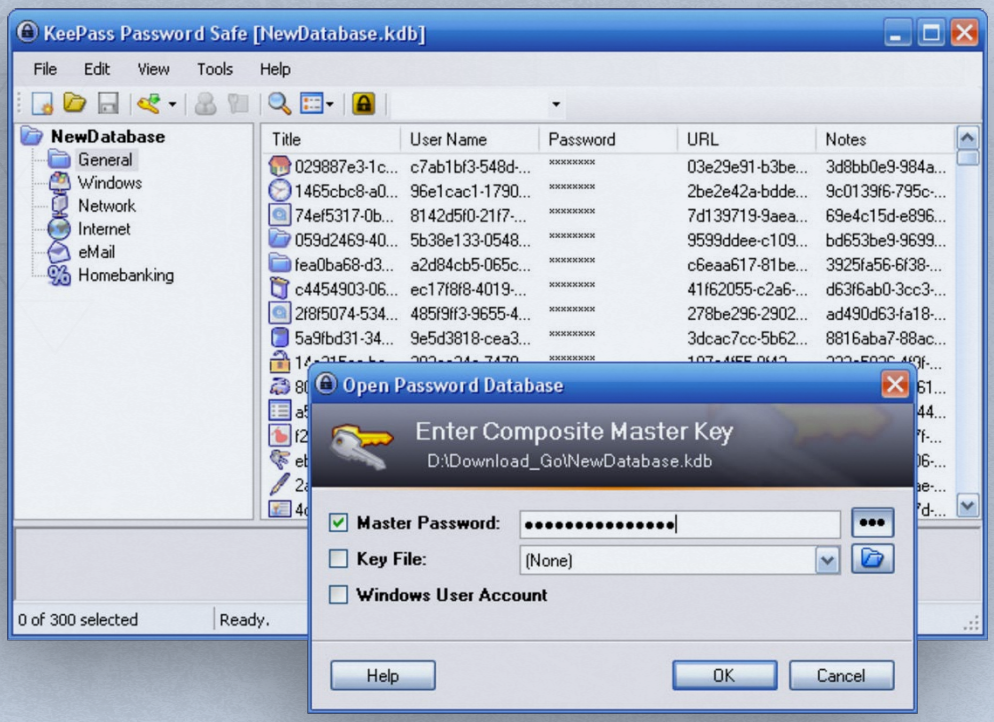


[21] https://lastpass.com/how-it-works/

KEEPASS X

KeePassX[22] Password Safe is another free, open source, lightweight, and easy-to-use password manager for Windows, Linux, and Mac OS X, with ports for Android, iPhone/iPad and other mobile devices. You can download it for PC's or Mac's here.

The benefits of KeePassX is that it is open source and is part of constellation of applications built by developers to support software independence. The challenges with KeePassX is the interface is confusing for beginners and there is not an easy way to sync KeePassX between your phone and your computer. That said, if you are willing to do a little work KeePassX can be one of your safest and most important autonomously implement password management solutions you could use.

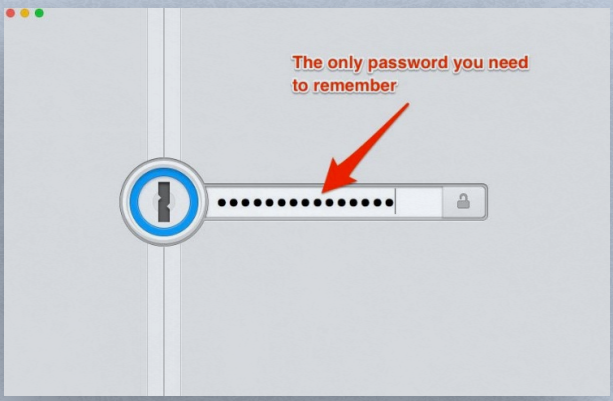


[22] https://www.keepassx.org

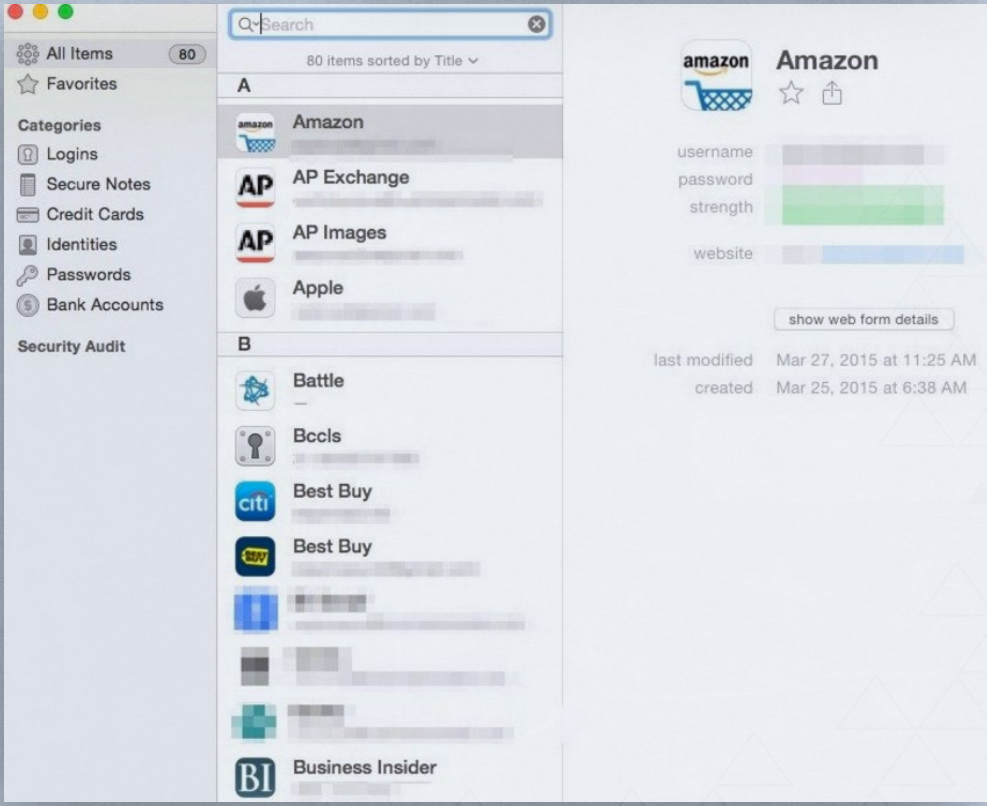
1PASSWORD

Like other password managers, 1Password enables you to sync your passwords across all of your devices using the same password vault. It is available for iOS, macOS, Android, and Windows.

When you first download the app from the App Store, you have to create an account. Same situation, one password will unlock all of your other passwords. It's all you need to unlock your confidential world on both desktop and mobile. **So make it good, and don't forget it**.



That will bring you into a dashboard where all your login information is stored. Here you can view and manage all the current user names and passwords you've saved.

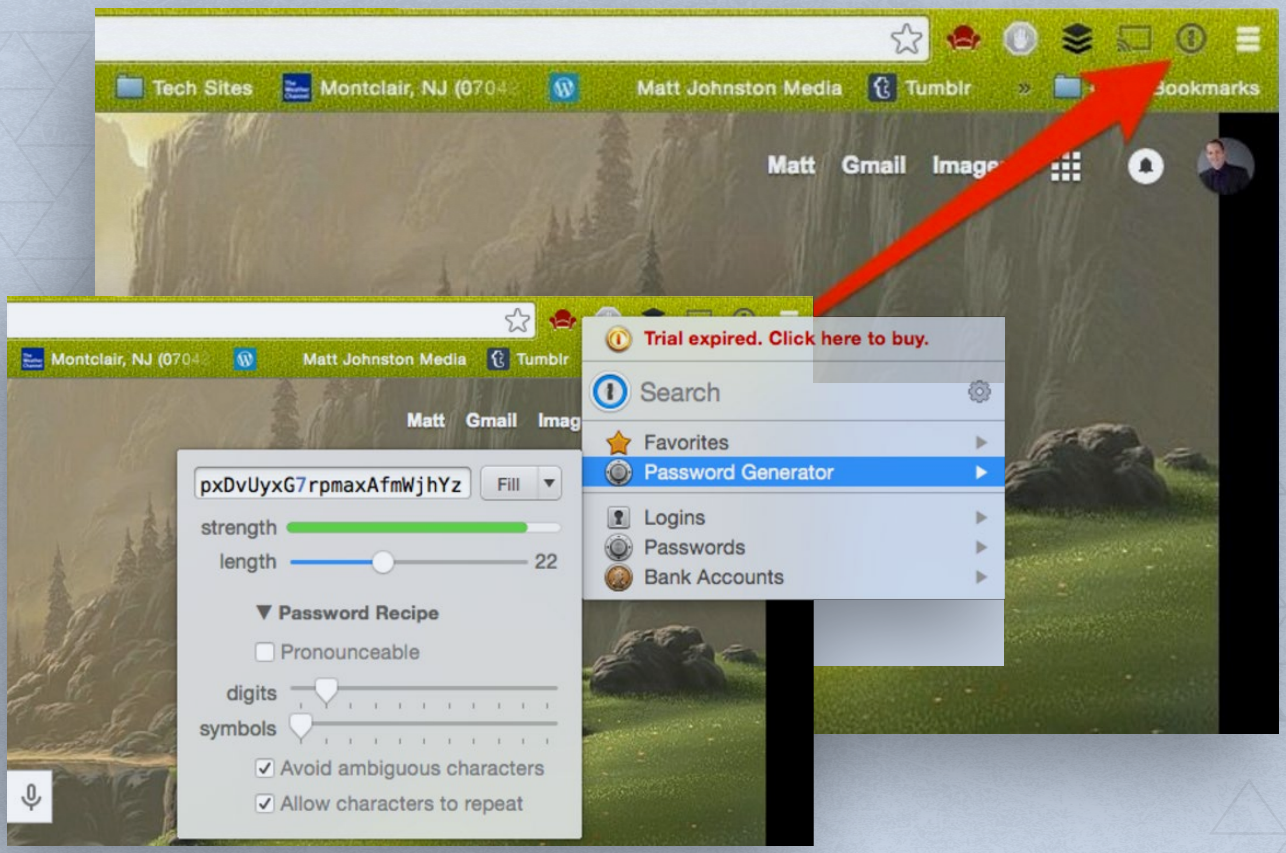


The secret to easily managing Login's is in a browser extension. You can get one for Chrome, Safari, Firefox or Opera.

Every time you're on a website where you need to input login information, you click this handy extension and tell it to fill in the information for you. The extension knows what site you're on and automatically fills in the blank fields.

The extension is also a hub for your whole password experience. In the drop down that opens, you can copy and paste passwords, view login information, and make complicated and hard-to-guess new passwords for all the sites you use.

Now there is no need to remember any passwords, just the one that gets you into the 1Password app.



The 1Password app has its own built-in browser that can take advantage of saved passwords, credit card information and more, but with the addition of Extensions in iOS 8, MobileSafari can use this information as well.

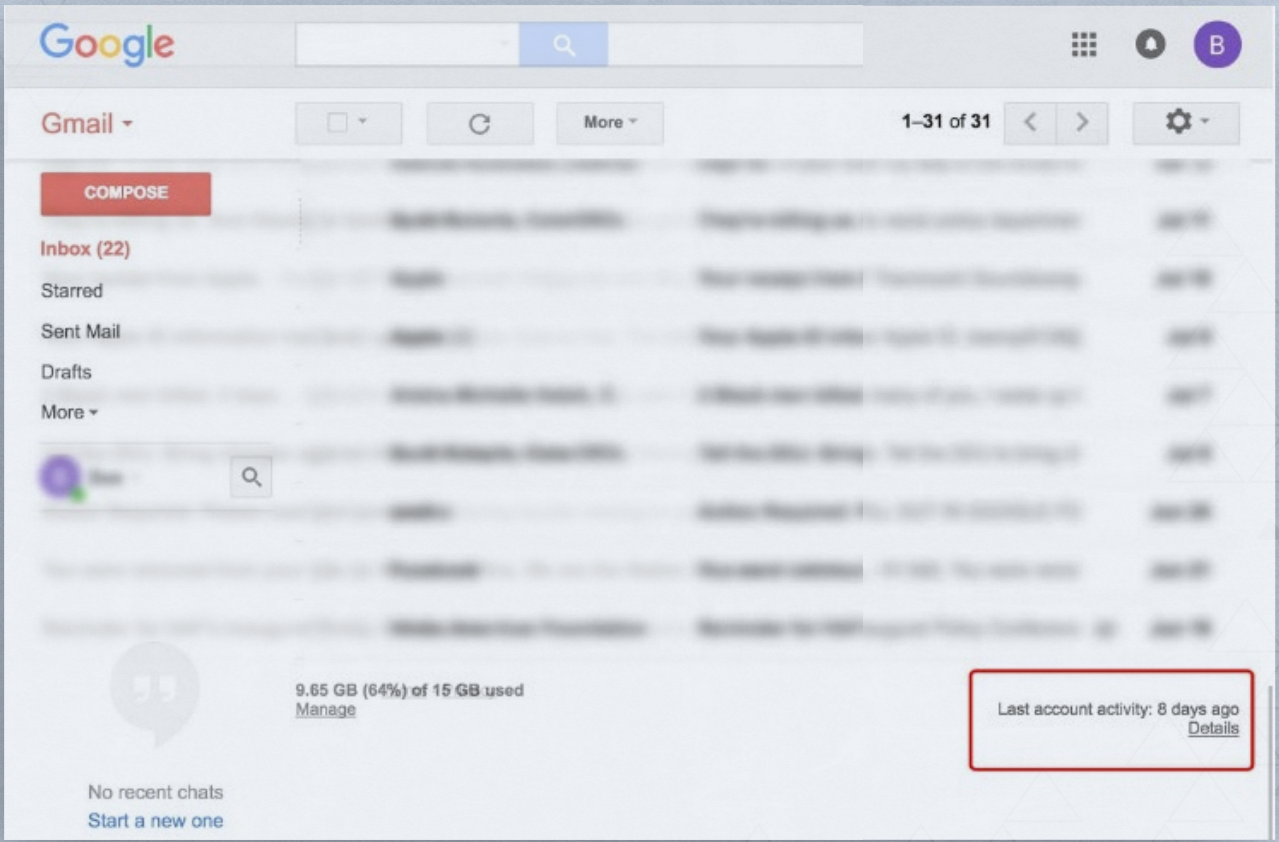
- If on a page with a login or other input field, simply tap the Share icon, then the iPassword icon. The app will ask for your master password, then it will fill in the requested information, just as it does on the Mac.

Apps also exist for Androids that work similarly. We recommend you sync your data across devices on a secure wi-fi network.

SECURE YOUR GMAIL

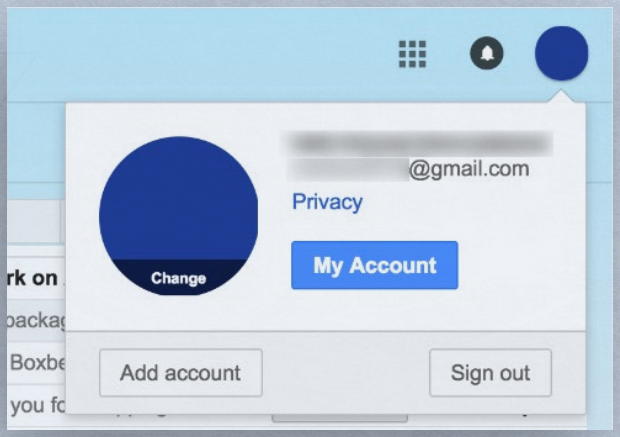
Google's Gmail is one of the most used web email apps in the world. This section helps us learn how to secure Gmail and how to identify if you are currently vulnerable. First, let's see whether your account has already been compromised.

- To check for signs of a hack, look at the bottom right hand side. It will tell you when the last activity on your account took place. Make sure the dates and times align with your use.
- Additionally, you can click on **"Details"** below to view a list of all the activity on your account.

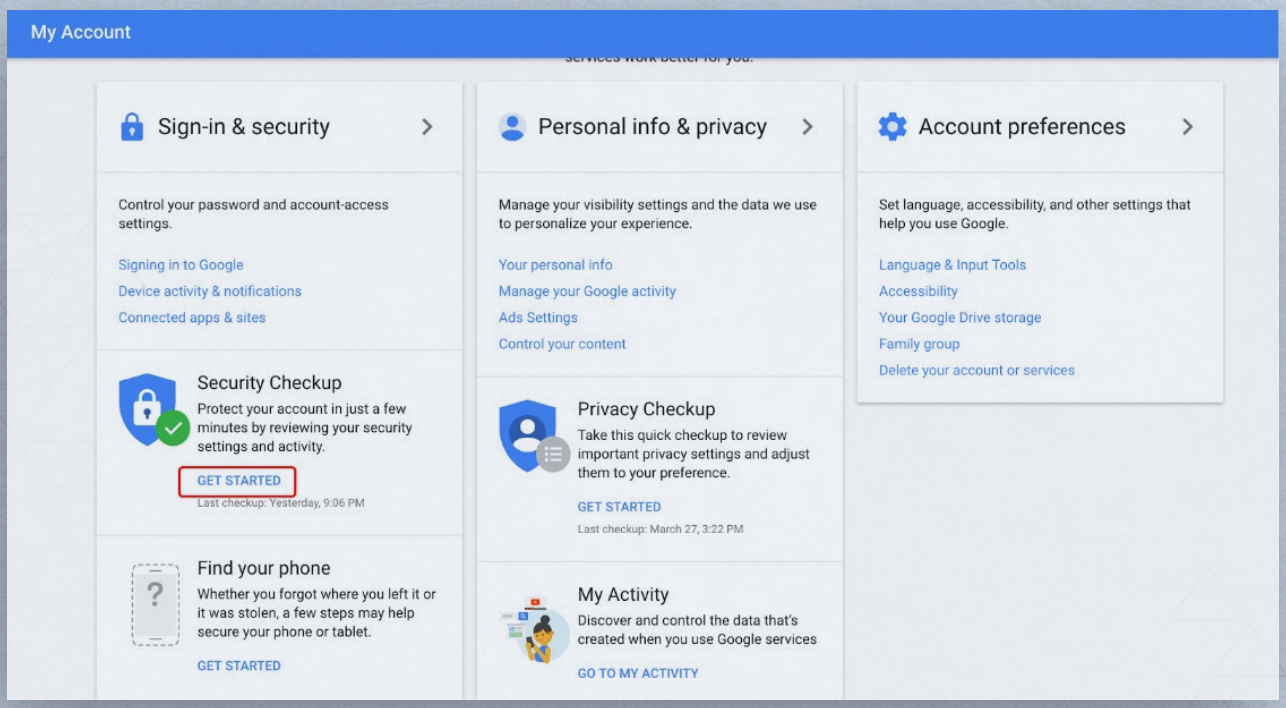


- To set your account security for gmail and your google accounts in general, click on your profile picture on the top of your gmail screen and click on **"My Account"**

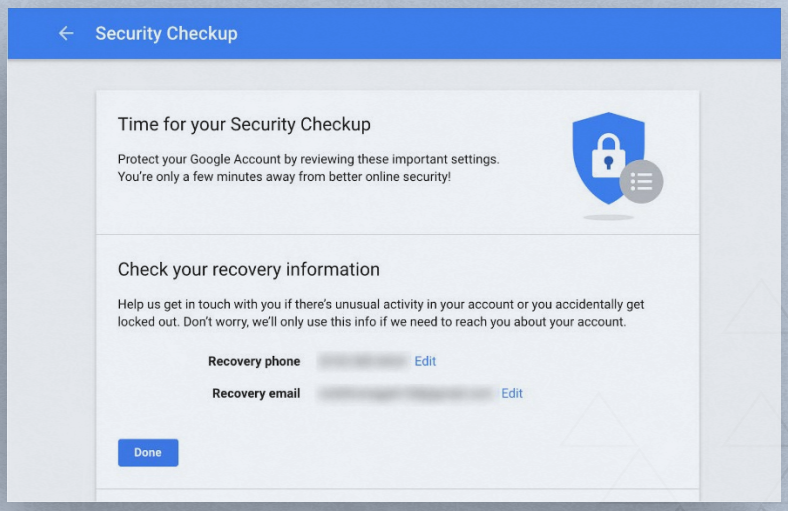
- You will be taken to a master settings page. Here you can make sure your basic settings are set to protect you. Fists, do an overall security check by clicking on **"Get Started"** under the **"Security Check Up"** option.



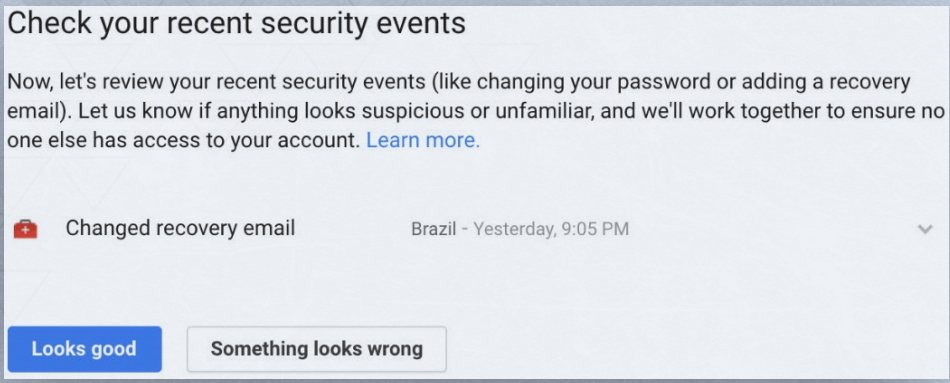
GOOGLE SECURITY CHECK UP



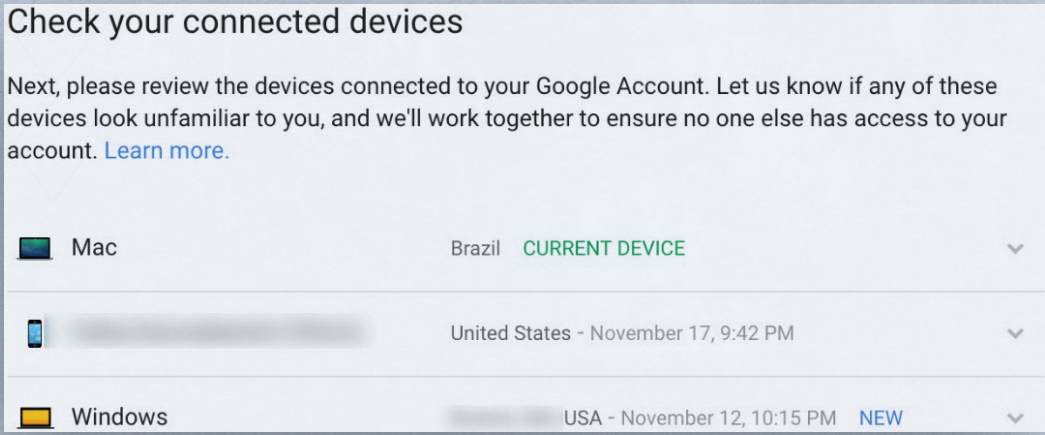
Check that your **recovery phone** or email are accurate and up-to-date. This will be useful in case you lose your passwords and entry into your account or if suspicious activity is detected on your account and Google wants to alert you.



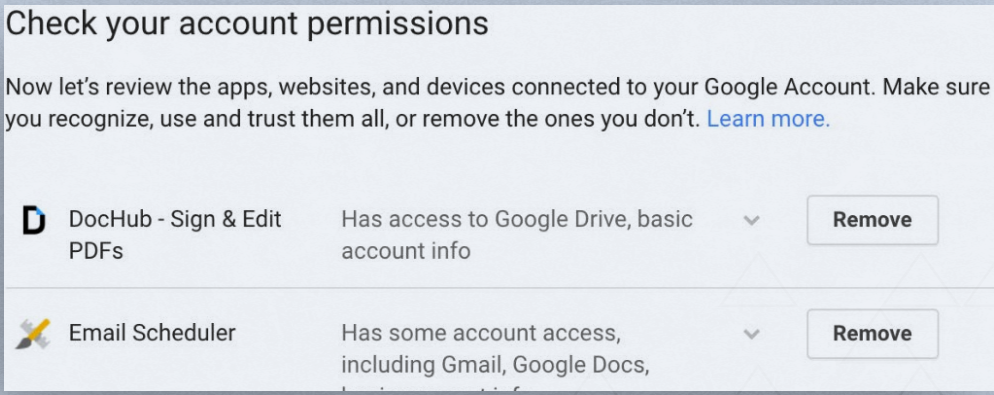
- Next, you can check that any recent changes made to the account settings were in fact made by you from a location you recognize.



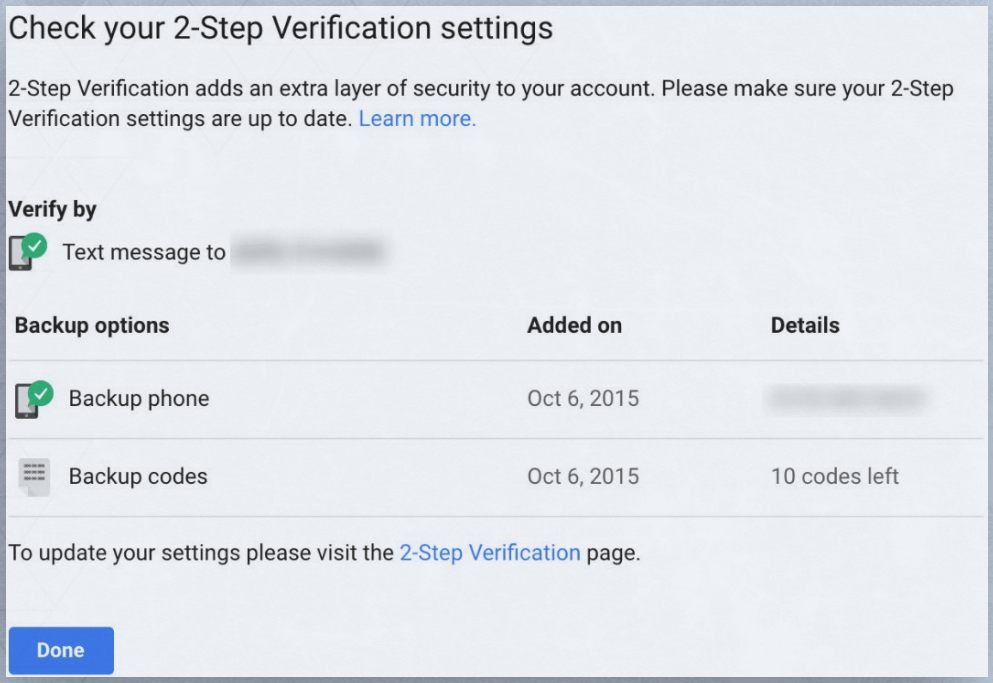
- Check that the devices from which you access your account look normal.



- Check that the apps you have allowed access to your gmail account are there as you specified. We strongly recommend you do not allow access to random apps that are less secure as they can compromise your security and gather data about you.

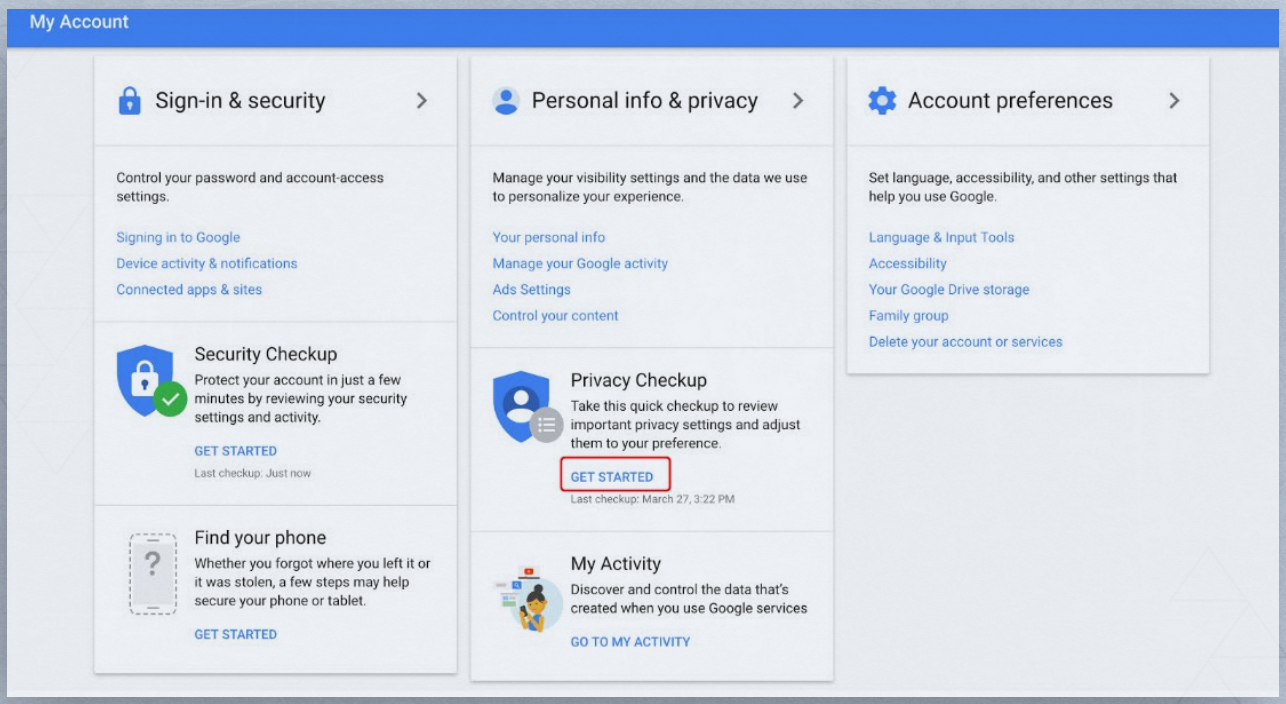


- Lastly, check your 2-step verification settings and make sure you have your backup codes. To see more on this, see page 90

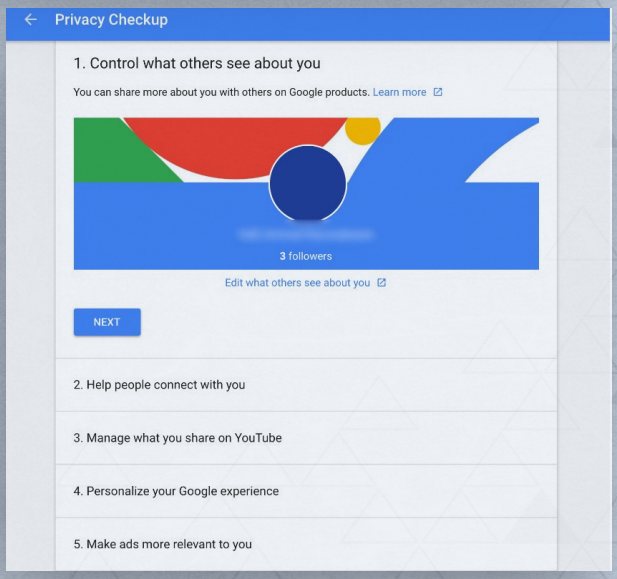


PRIVACY CHECK-UP

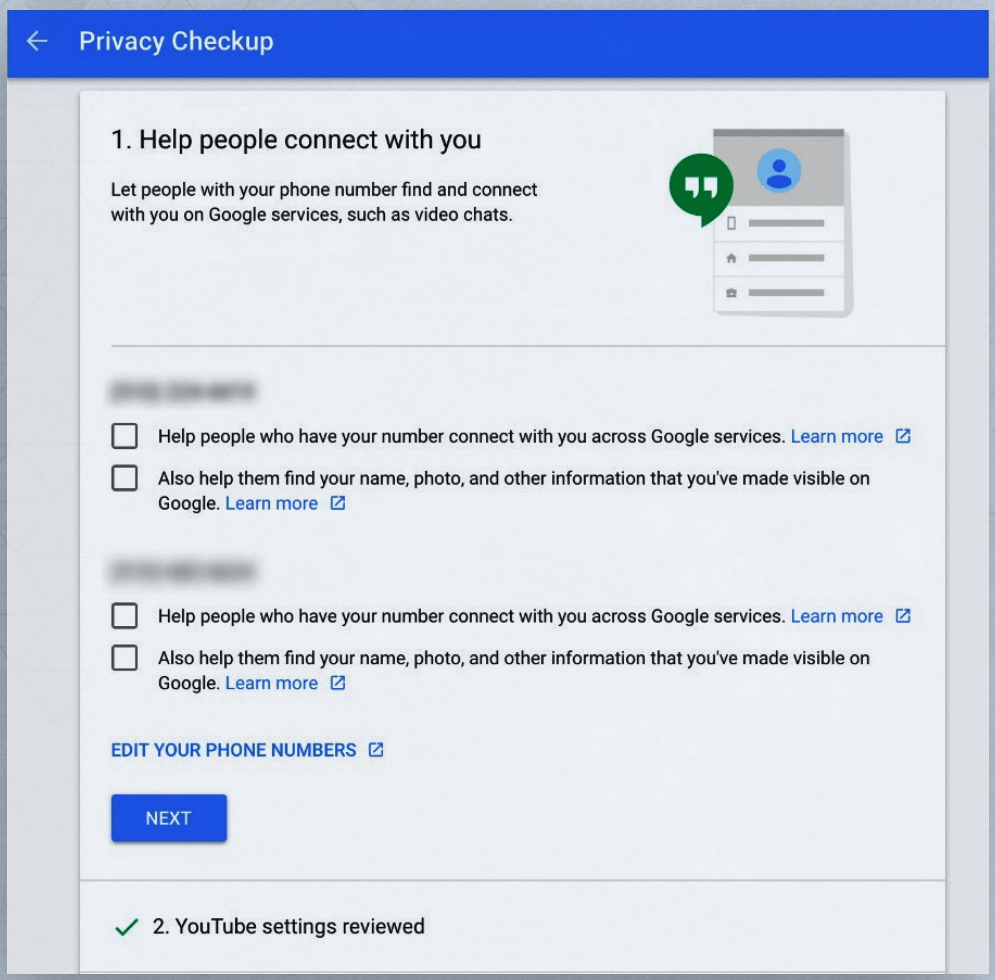
Now, back in your accounts page you can also perform a Privacy Check up.



- Click on it and choose settings that minimize your exposure to the internet in general

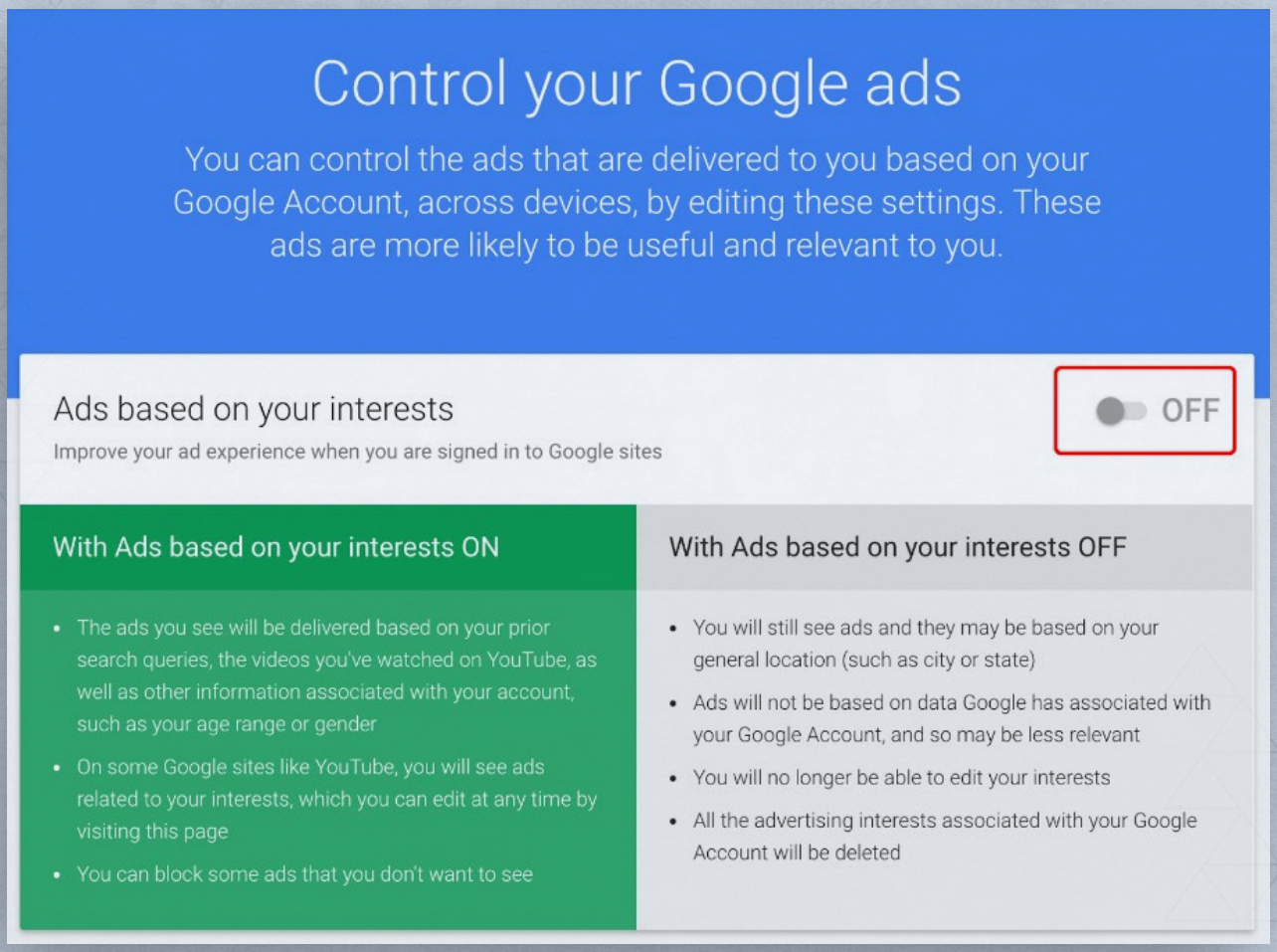


- For example, uncheck the following suggestions so that only people you give your phone number to can contact you.



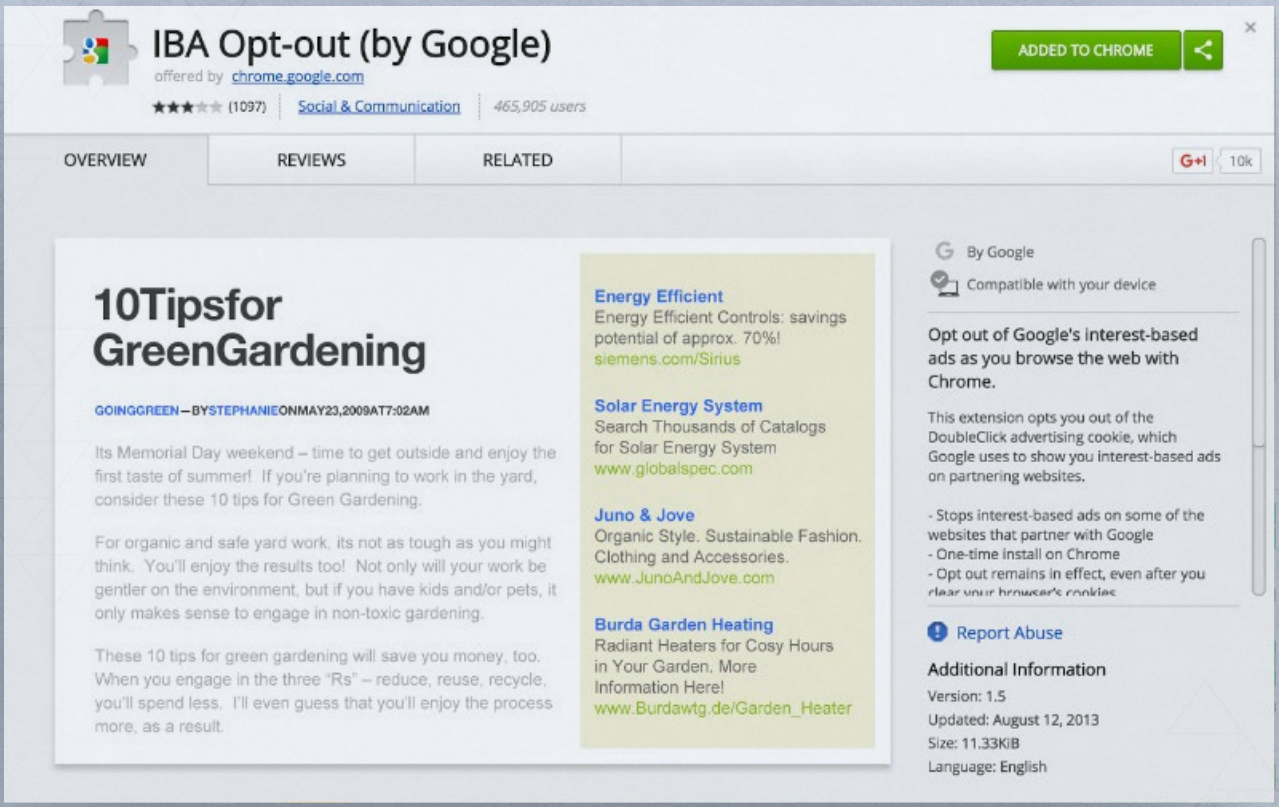
Google can collect information on you to send you **"personalized ads"**. This means that you may get ads that relate to your recent emails. For example, if you wrote to your mom about difficulties you were having with your health, Google may start showing you ads for relevant pharmaceuticals. We strongly recommend you turn this service off and protect your daily information.

✔ To do this you need to toggle the **"Opt Out"**, switch to the **"OFF"** position.



We recommend you get an **IBA Opt Out Extension** for your Google Chrome. This tells Google, you have opted out of being tracked for ads throughout your browser experience.

- To install this go to **Chrome → Windows → Extensions**. Scroll to the bottom of the page and click on **"Get more Extensions"**. Search for Google Opt out and Install.



TWO FACTOR AUTHENTICATION FOR GMAIL (2FA)

Because passwords can be phished, guessed, cracked, or acquired in other ways (like Keyloggers), you may want to consider adding another barrier to your accounts through two-factor authentication.

2FA as it's commonly abbreviated, adds an extra step to your basic log-in procedure. On your frequently visited accounts you typically enter your username and password once, and then you're done. This is categorized as a single factor of authentication. When you enable 2FA, it asks for two factors of authentication.[23] This factor can be code or even a physical dongle connected to your device.

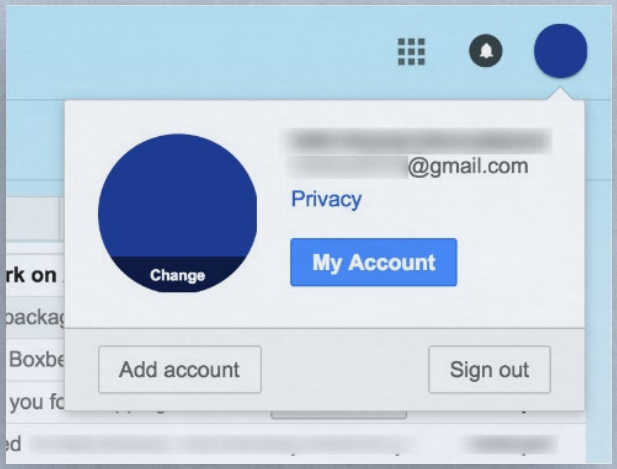
A common example of two-factor authentication is a bank card: the card itself is the physical item and the personal identification number (PIN) is the data that goes with it. Including those two elements makes it more difficult for someone to access the user's bank account because they would have to have the physical item in their possession and also know the PIN.[24]

Almost all online accounts and platforms not offer two-factor authentication. You can learn more and slowly implement 2FA by going to https://www.turnon2fa.com. You'll find tutorials for almost every platform you can think of and some you would even be suprised by. In either case you can never go wrong with 2FA so add it when you can!

NOTE: We will cover two factor authorization for Twitter and Facebook in the social networking section that follows.

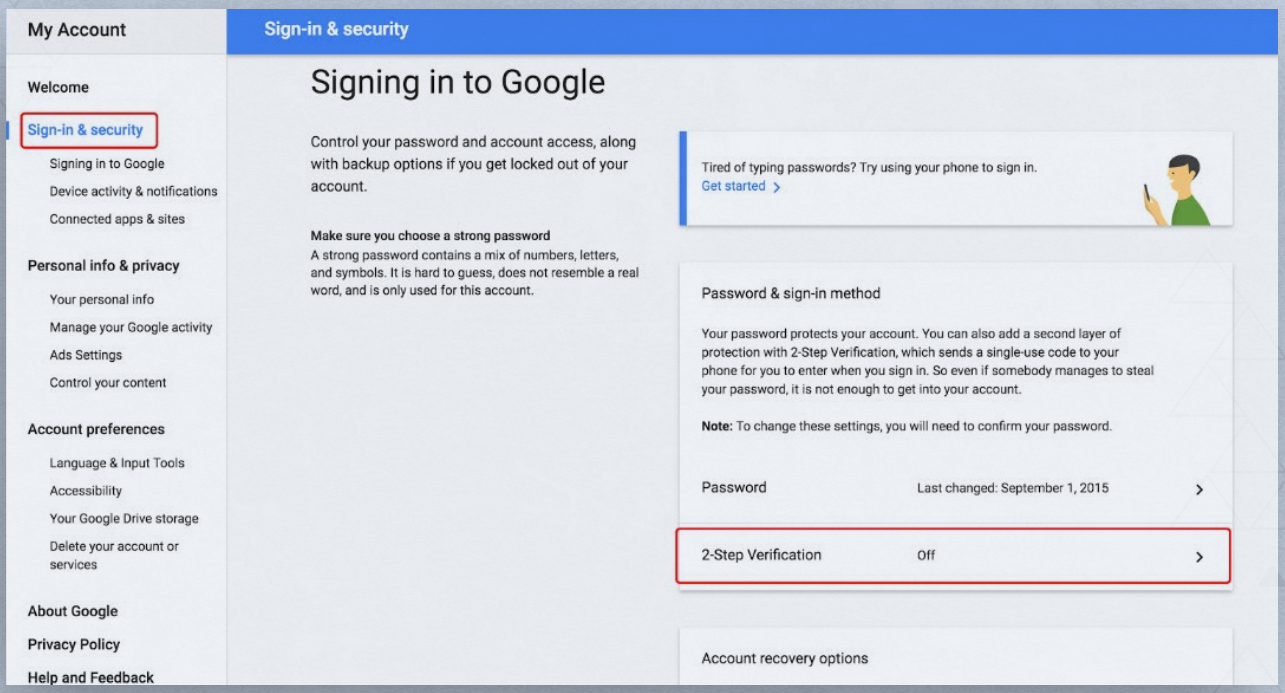
[23] http://gizmodo.com/its-time-to-enable-two-step-authentication-on-everythin-1646242605
[24] http://searchsecurity.techtarget.com/definition/two-factor-authentication

Most people only have—their password—to protect their account. With 2-Step Verification, if someone hacks your password, they will still need your phone or Security Key to get in.

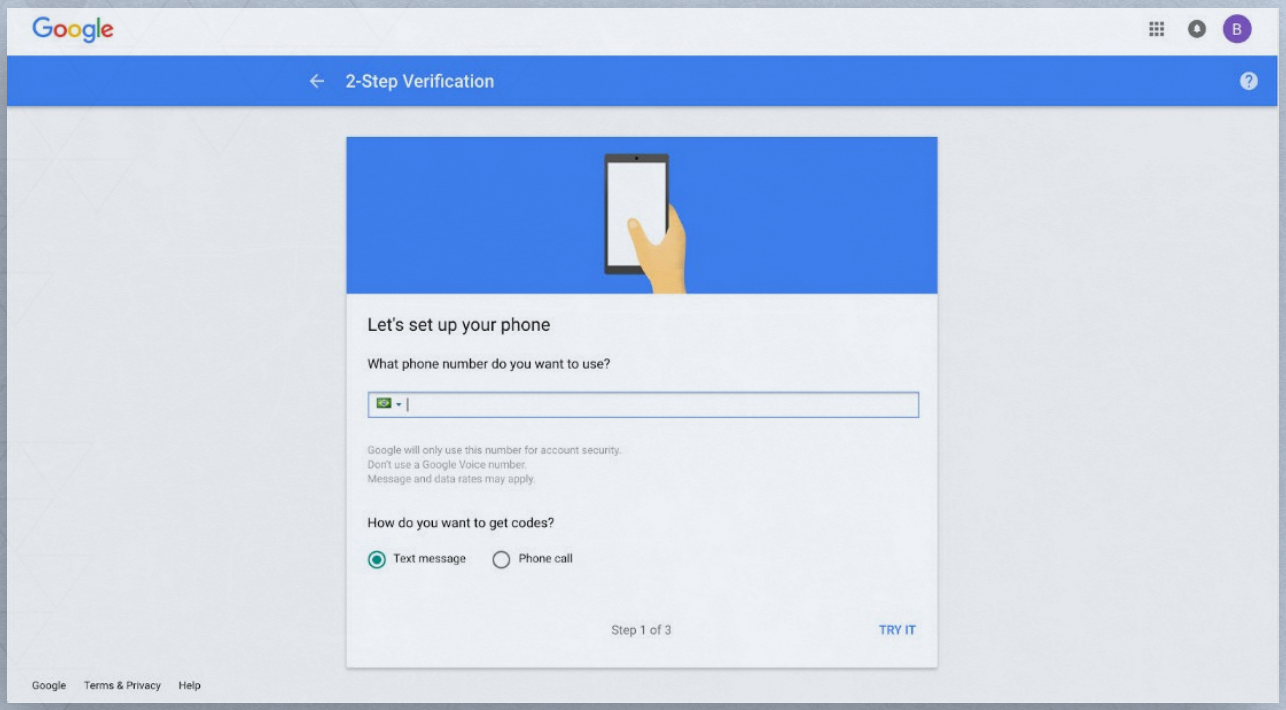


If turned on, signing in to your account will work a little differently:

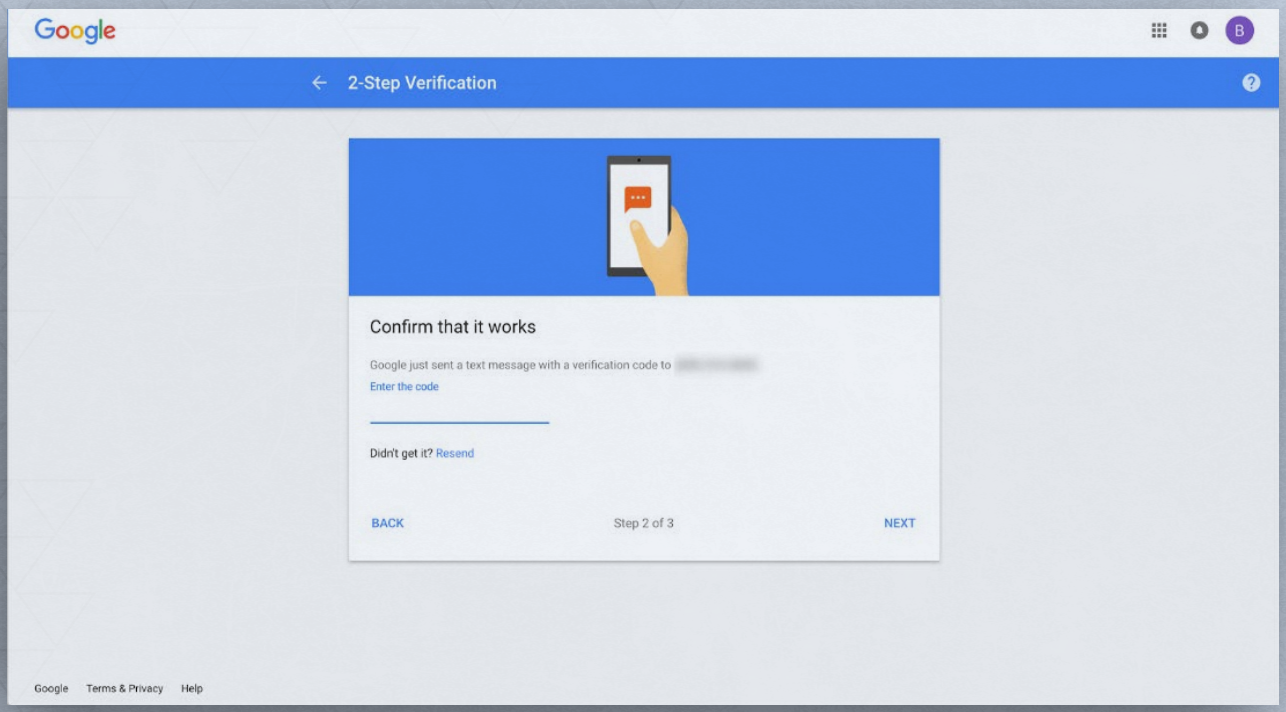
- Whenever you sign-in to Google, you'll enter your password as usual.
- You will be asked for something else. Then, a code will be sent to your phone via text, voice call, or our mobile app.
- To set up 2FA on your gmail account, go to your profile pic/icon on the top right and click on **"My Account."**, click on **Sign in and Security**. Then click to **turn 2FA on**.

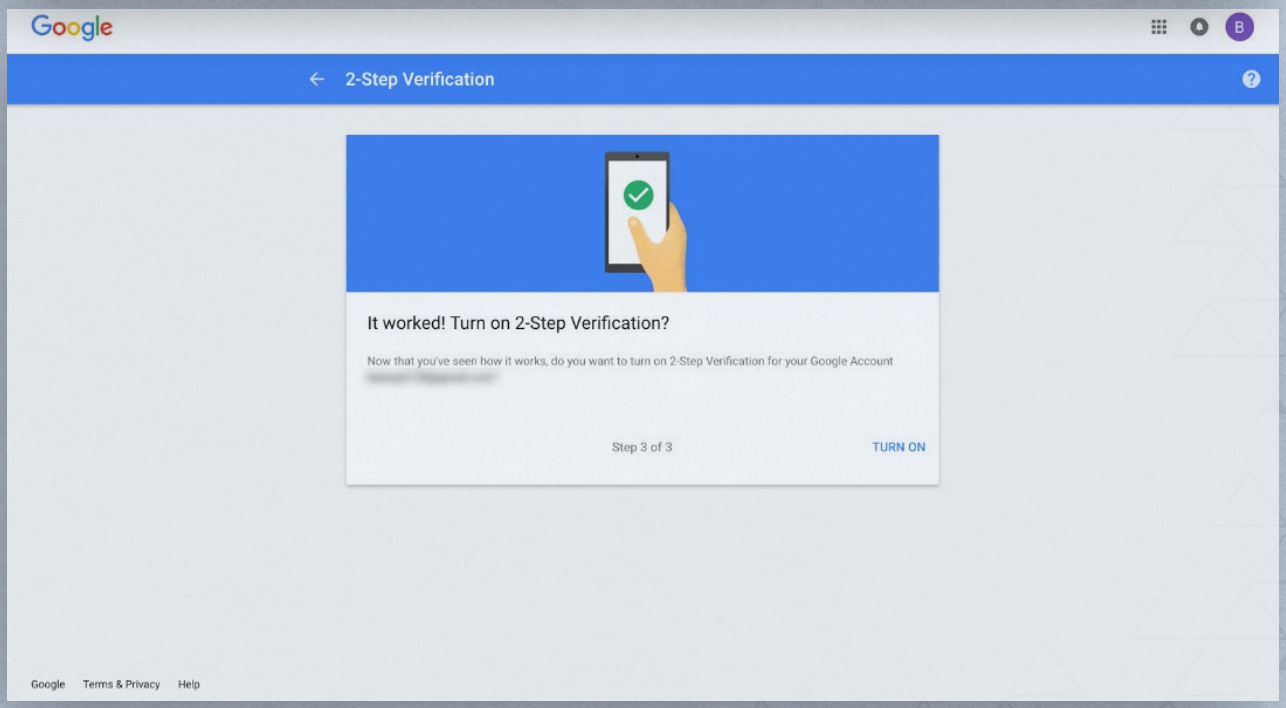


Google will ask you for your phone number to send you the verification codes. Once you enter the phone number, you will receive a **text with the secret code**.

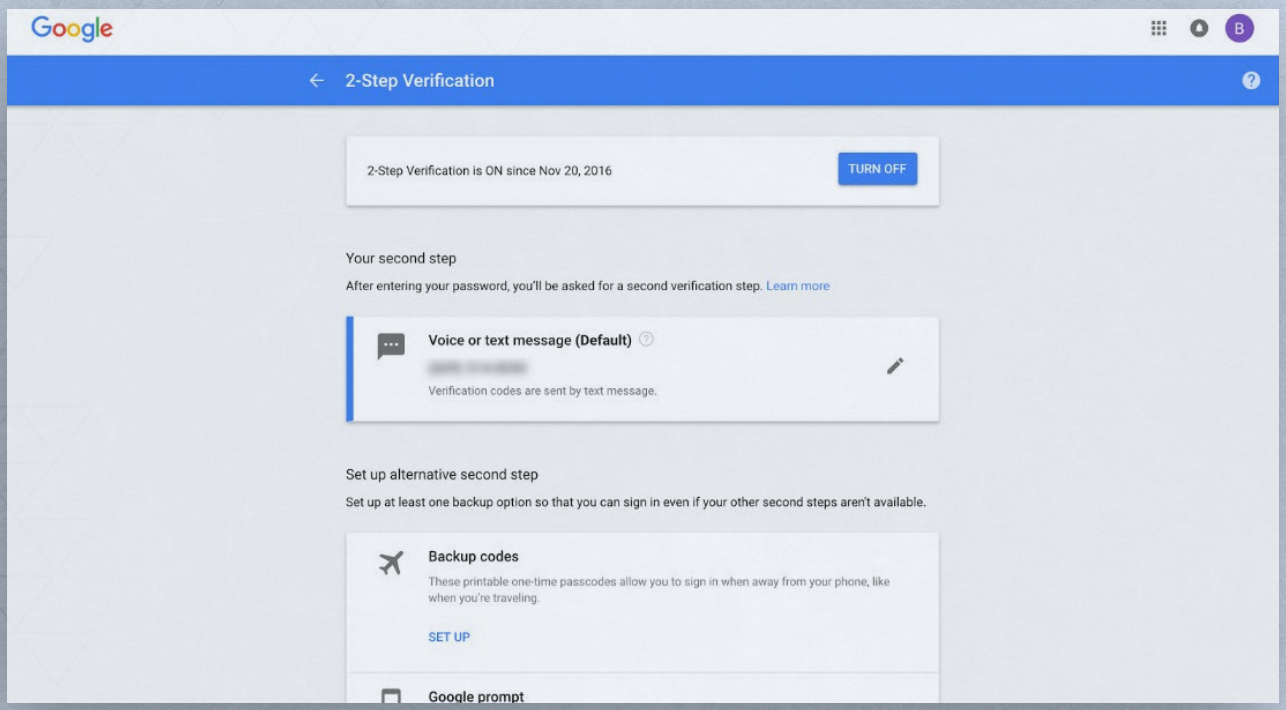


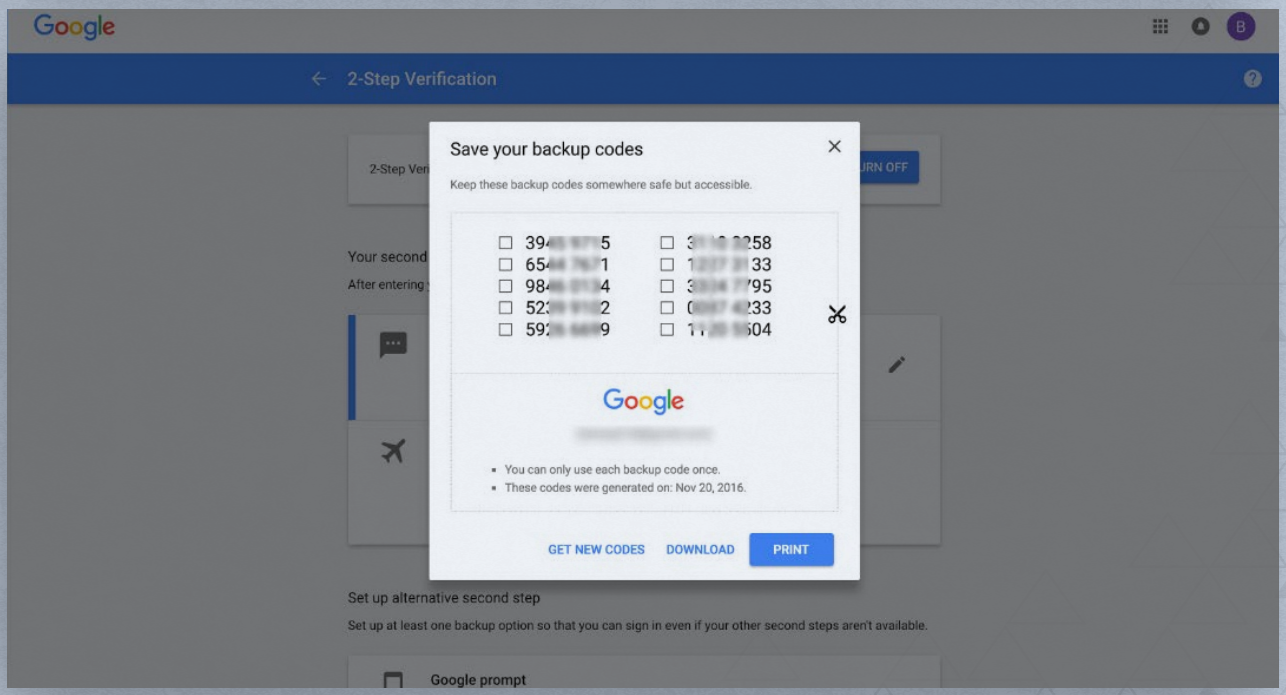
✔ In the page that follows, **enter the code** you received via text





- It's a good idea to set up backup codes to access your account when you don't have your phone at hand. When you click on backup codes, a list of codes comes up. Save these codes somewhere for future use.





That's it! Your 2FA has been set up!

If you set up 2-Step Verification using SMS text message or Voice call and also want to be able to generate codes using an Android, iPhone, or Blackberry, you can use the Google Authenticator app to receive codes even if you don't have an Internet connection or mobile service. Go to this link, to set it up.

WARNING: 2FA can really protect your account from being hacked or stolen but bear in mind that setting up 2FA requires that you provide personal information, like your phone number, other email addresses etc, that will make these accounts increasingly traceable to you. In addition, many users find 2FA cumbersome because every time they login, it's a 2-step process. All factors considered, it is up to you to make the best decision on 2FA based on your situation and your needs.

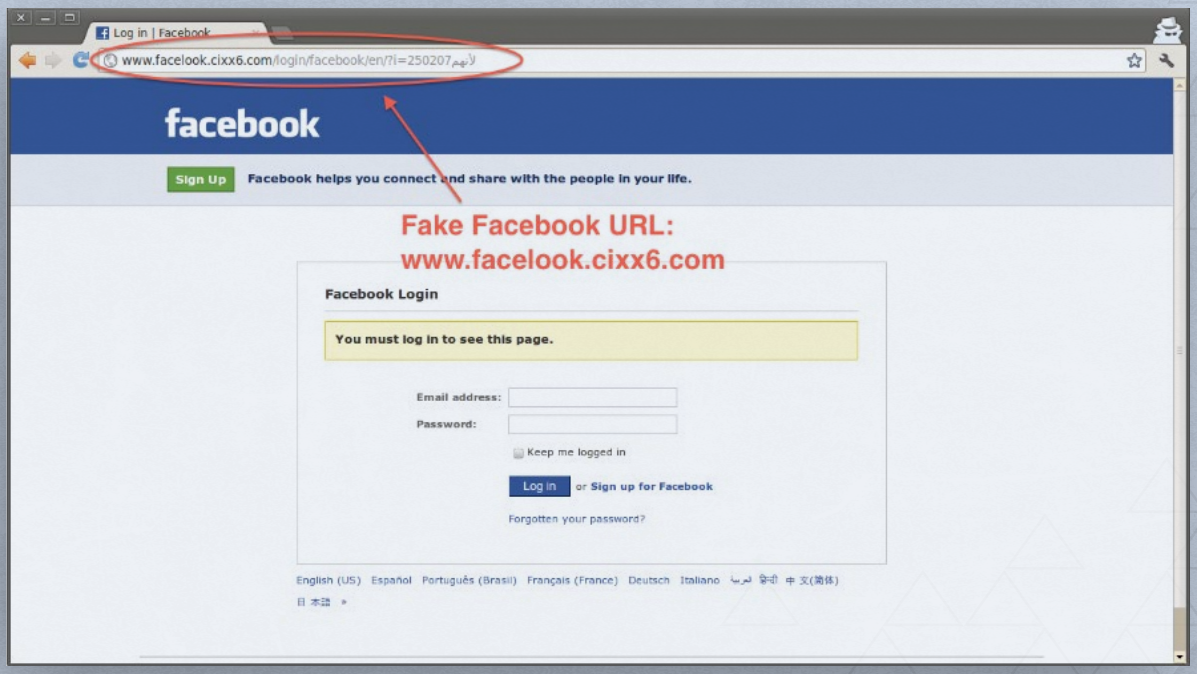
PROTECT YOURSELF FROM PHISHING

When an attacker sends an email or link that looks innocent, but is actually malicious, it's called **phishing**. Phishing attacks are a common way that users get infected with malware ("Malicious Software")—programs that hide on your computer and can be used to remotely control it, steal information, or spy on you.[25]

The vast majority of malware is criminal, aimed at obtaining banking information or login credentials for email or social media accounts. But malware is also used by state actors. State intelligence agencies use malware to carry out covert actions against other states' computer systems, such as Flame and Stuxnet. States and state-supporting actors also use malware to spy on activists, journalists, and dissidents.[26]

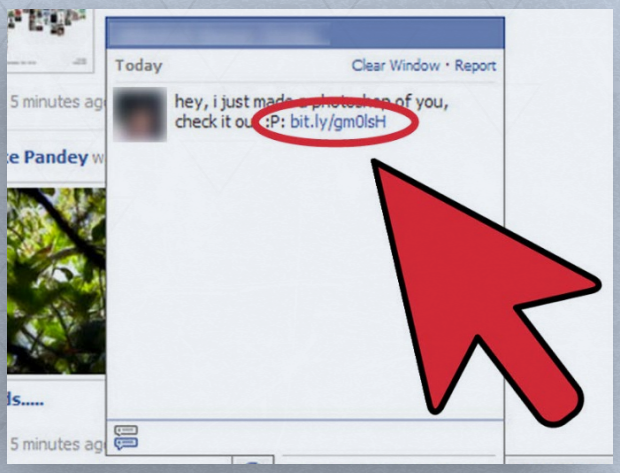
HOW CAN YOU IDENTIFY PHISHING SCHEMES?

The message contains a mismatched URL, or a misleading domain name.

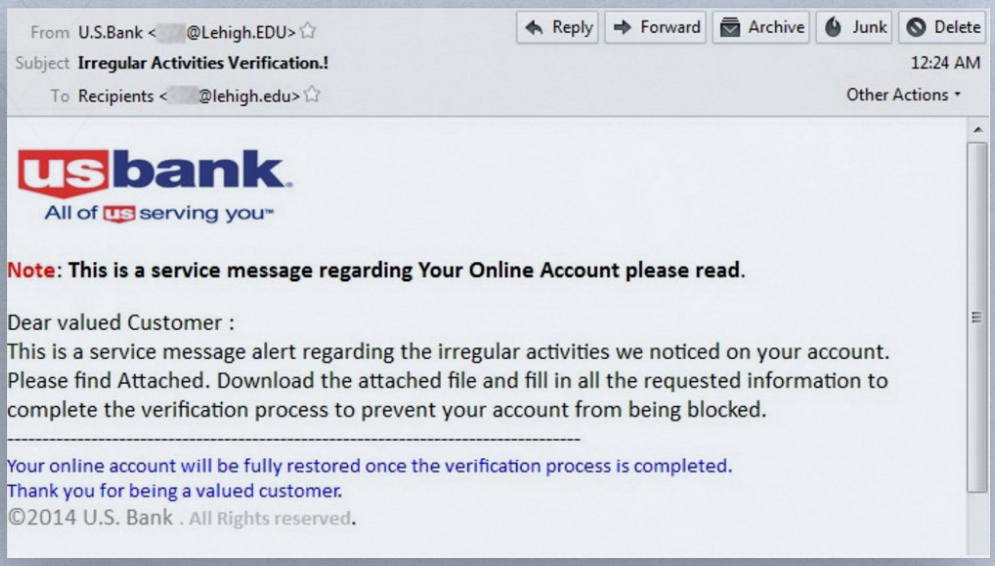


[25] https://ssd.eff.org/en/module/how-avoid-phishing-attacks
[26] https://www.eff.org/issues/state-sponsored-malware

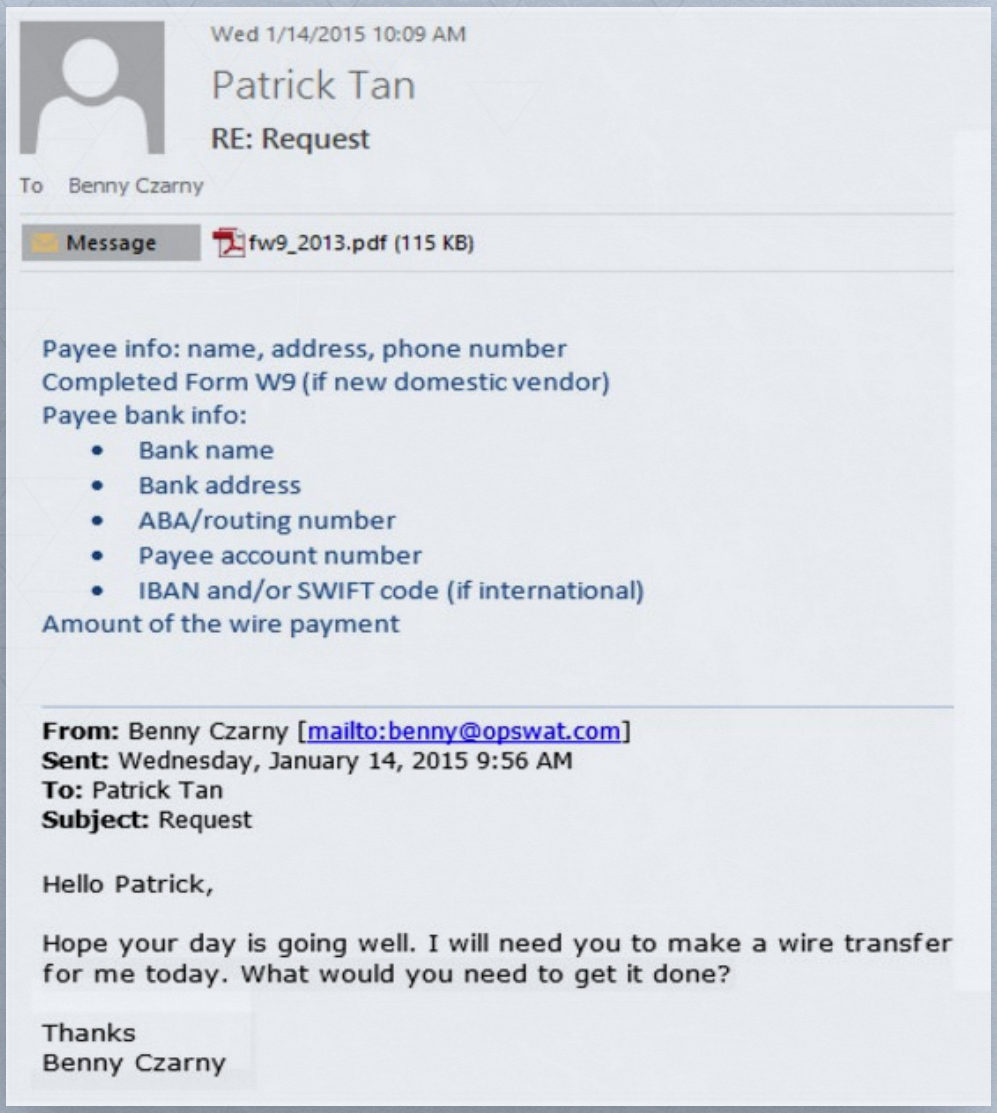
The message is coming from your friend, but doesn't sound like your friend



The message asks for personal information like banking information



You are asked to send money to cover expenses



Wed 1/14/2015 10:09 AM

Patrick Tan

RE: Request

To Benny Czarny

Message fw9_2013.pdf (115 KB)

Payee info: name, address, phone number
Completed Form W9 (if new domestic vendor)
Payee bank info:

- Bank name
- Bank address
- ABA/routing number
- Payee account number
- IBAN and/or SWIFT code (if international)

Amount of the wire payment

From: Benny Czarny [mailto:benny@opswat.com]
Sent: Wednesday, January 14, 2015 9:56 AM
To: Patrick Tan
Subject: Request

Hello Patrick,

Hope your day is going well. I will need you to make a wire transfer for me today. What would you need to get it done?

Thanks
Benny Czarny

DEALING WITH PHISHING

The best way to protect yourself from phishing attacks is to never click on any links or open any attachments sent to your email: this is unrealistic for most people. So here are some ways to deal.

Be alert. If something about a website doesn't feel right to you, it may not be:

- Check with the friend/family/bank/organization, over phone or another channel, to see if they actually did send you the files that were sent to you.
- If you have to frequently send and receive files for work consider sending the files through secure servers like Google Drive or Dropbox.

Antivirus software are programs that help protect your computer against most viruses, malware, worms, Trojan horses, and other unwanted invaders that can make your computer “sick” by performing malicious acts, such as deleting files, accessing personal data, or using your computer to attack other computers. We recommend that you use anti-virus software on your computer and on your messages. Note, installed software will not be useful if you do not update it regularly! Updates, keep the anti-virus on the lookout for the latest types of threats online.

We recommend Malwarebytes, Anti-Malware, Kaspersky labs and SOPHOS security, along with Windows Defender. These platforms are popular and used by many which keeps them efficient and more up-to-date than others.

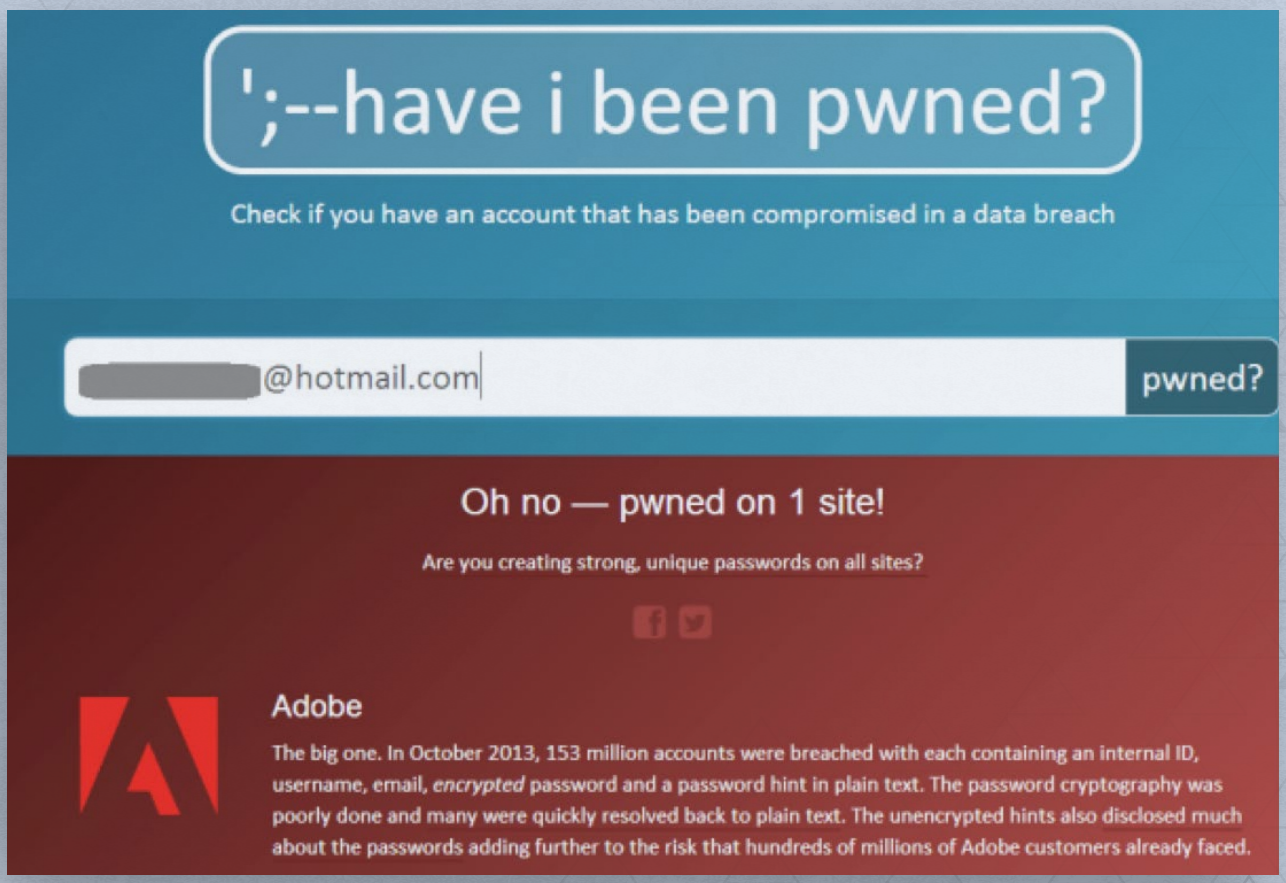
TIPS: Another tool that is useful to know of is VirusTotal is a free online service that analyzes files and URLs enabling the identification of viruses, games, and other kinds of malicious content detected by antivirus engines and website scanners. Any user can select a file from their PC or email using their browser and send it to VirusTotal. However, it is important to note that VirusTotal is not a substitute for any antivirus/security software installed since it only scans individual files/URLs on demand.

SO AGAIN NEVER OPEN ATTACHMENTS DIRECTLY ALWAYS OPEN IN GOOGLE DRIVE OR DOWNLOAD AND THEN SCAN IN VIRUS TOTAL

HAVE YOU BEEN COMPROMISED?

Everyday in the news, we hear about big corporations or websites getting hacked and being the bearers of bad news to their users informing them that their personal information has been stolen by hackers. These data breaches can include your name, passwords, government ID number, email address, date of birth, mother's maiden name, or any other piece of data you hand over to a website. Data from these breaches are posted on the internet for hackers of all types to see. These data leaks are often the source of bigger political hacks that can compromise movements.

One way to check to see when and where your data has been compromised is by using http://haveibeenpwned.com which is a service that catalogs data breaches as well as pastes (a type of publishing that is often used tech nerds and hackers). Be sure to change your passwords on these sites if you come up on a search.



COMBAT TROLLING BY FINDING YOUR DATA ONLINE

It is important to know where your personal data is online. By searching your information on the list of sites we have collected you can find and clear your presence on public data lists.

NOTE: While this is a painful and often shocking process for some, starting now can help reduce your footprint on the net.

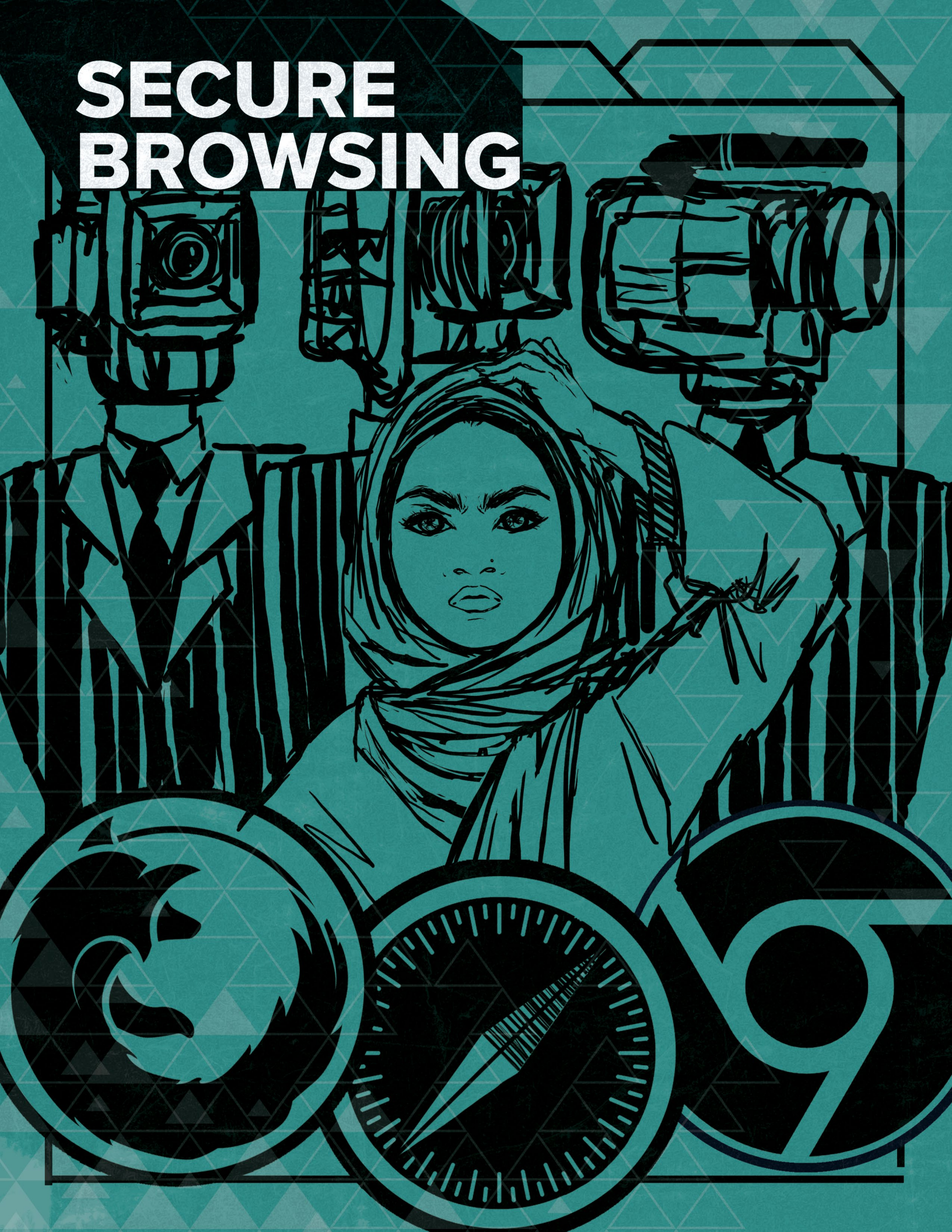
This can be crucial for when Trolls, stalkers, and worse try to bully our folks for speaking out, a common strategy they use is Doxxing. In Doxxing your personal information including addresses, phone numbers, work information and family members are exposed on public platforms so that it opens you up to physical harassment and intimidation offline.

We want to stop tactics that might open up you and your loved ones to attacks. Limiting data is a crucial harm reduction strategy in a time when we are increasingly being seen as the target.

Please check yourself out and begin your data reduction journey with a visit to these sites:

Spokeo (to remove listing: http://www.spokeo.com/opt_out/new)
Anywho.com (to remove listing: http://www.anywho.com/help/privacy)
INTELIUS (to remove listing: https://www.intelius.com/optout.php)
Whitepages (to remove listing: https://support.whitepages.com/hc/en-us/articles/203263794-Remove-my-listing-from-Whitepages-)
Finally, there is a more comprehensive list at Trollbusters at this link https://yoursosteam.wordpress.com/2015/08/30/remove-your-mailing-address-from-data-broker-sites/

SECURE BROWSING



NAVIGATING THE ONLINE: SEARCHING, BROWSING, AND EXTENSIONS

BROWSERS' BROWSER BROWSERS

A web browser is a software application used to browse, search, and display content on the World Wide Web. Today, some of the most popular web browsers, like Internet Explorer, Mozilla Firefox and Google Chrome are installed on most operating systems. And it is easy to notice the increasing threat coming from online criminals that try to take advantage of web browsers and their vulnerabilities. Some of the biggest networks, like Google, also have the ability to keep tracking you even when you're not signed in or on their page and follow you around the Internet to serve you with "relevant" advertising and content. Since almost everyone on the internet has some sort of account with a Google service, one can only imagine, the amount of data on civilians they hold.

So, securing our browser is one of the first steps we need to take in order to assure our online protection. Here are a few things you can do:

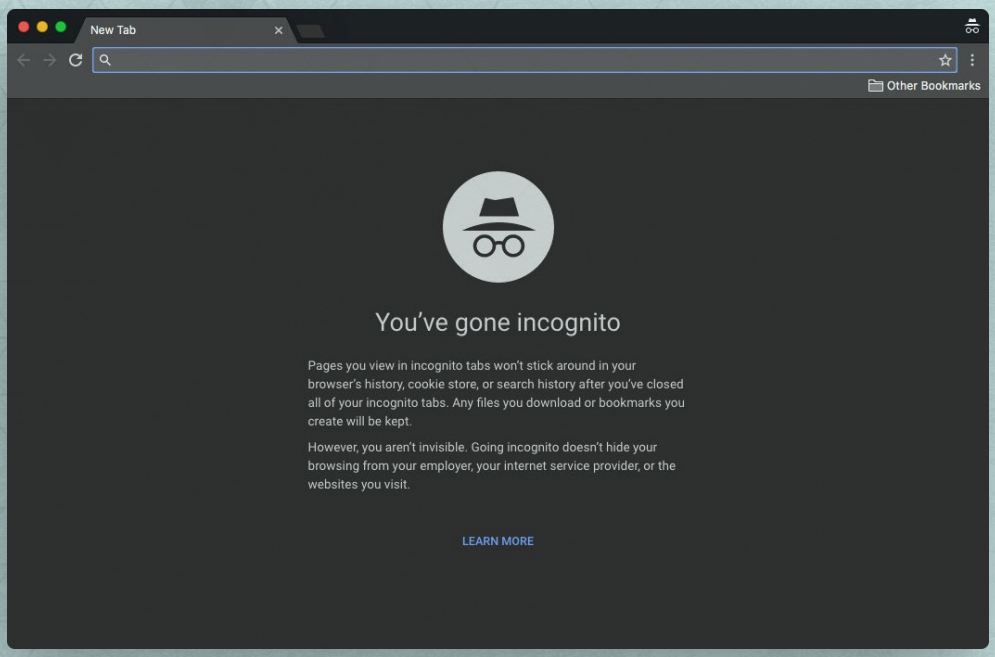
- Customize the settings on your browser for maximum security
- Add security extensions to your browser
- Use Alternative Search Engines

Changing your default browser settings will give you more control over who has access to your data.

GOOGLE CHROME

In recent years, the use of the Google Chrome web browser has significantly increased. As more and more people use it, there are a few actions we can take to also increase our online security.

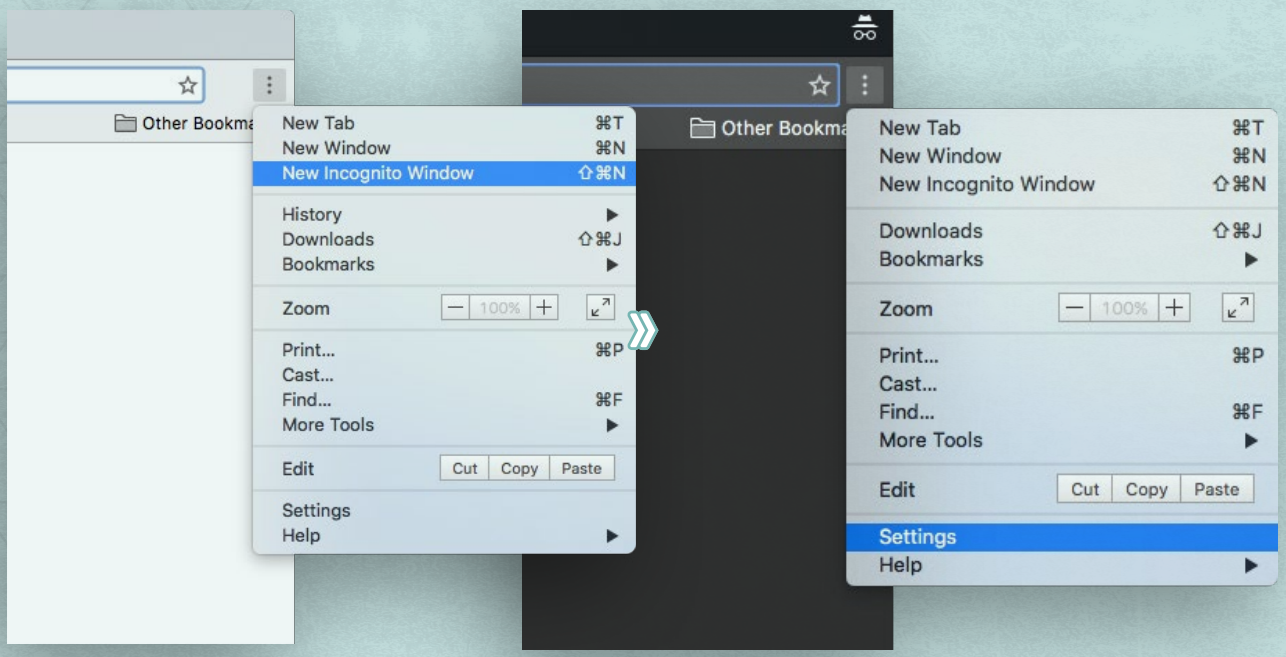
To start making the necessary modifications, we need to access the settings area. Please make the necessary changes in case you are using a different version of Google Chrome.

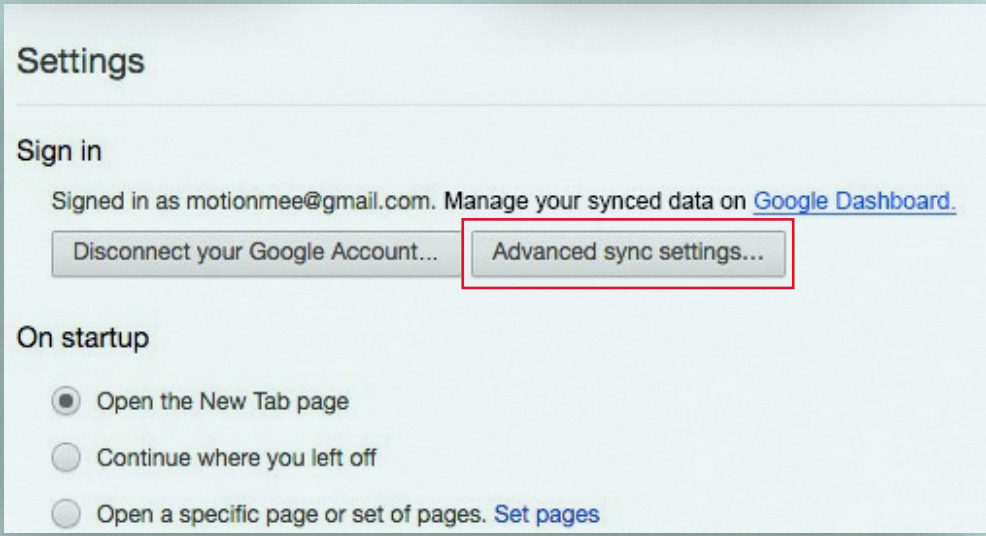


Chrome → ⋮ → Select "New Incognito Window"
Using Chrome's Incognito Mode means that when you close your browser, a number of traces created during the session are automatically cleared: your browser, search, web form and download histories, as well as cookies and temporary files.

- What is saved and deleted when you close the browser is already pre-defined—you can't customize 'private browsing mode' to suit your own needs.
- Only your browser history from this incognito session will be cleared. Your history from previous browsing sessions in 'normal mode' are unaffected.
- Trackers in the websites you visit can still collect data about you, including your browser history.
- Incognito mode does not give you anonymity on the internet.

- To access the settings area for Google Chrome, click the ⋮ button at the top right corner of the browser and select **Settings** from the drop-down menu.
- As soon as you access the Settings area, you will notice **Advanced Sync Settings** at the top, in the Sign-in section.

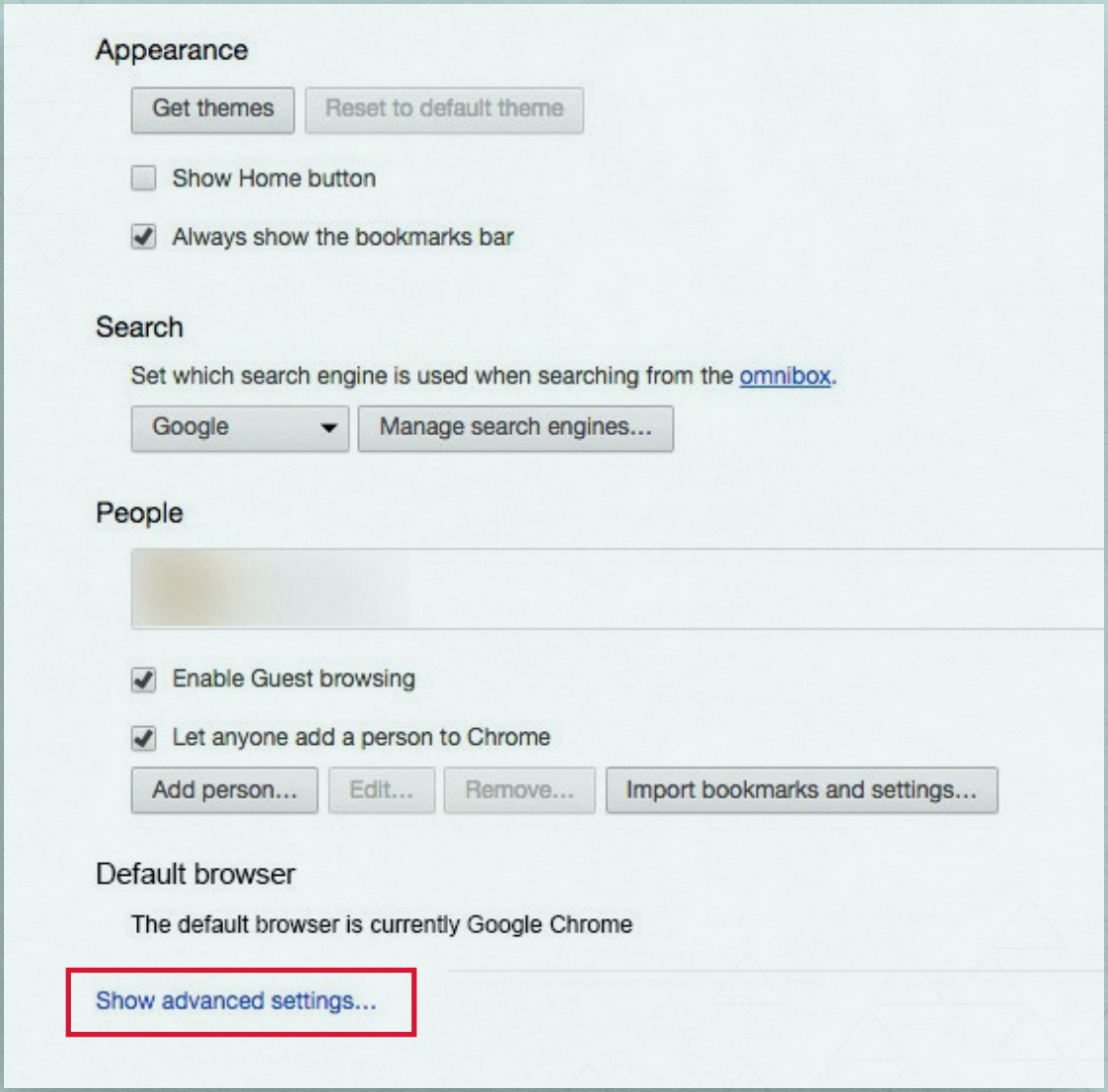




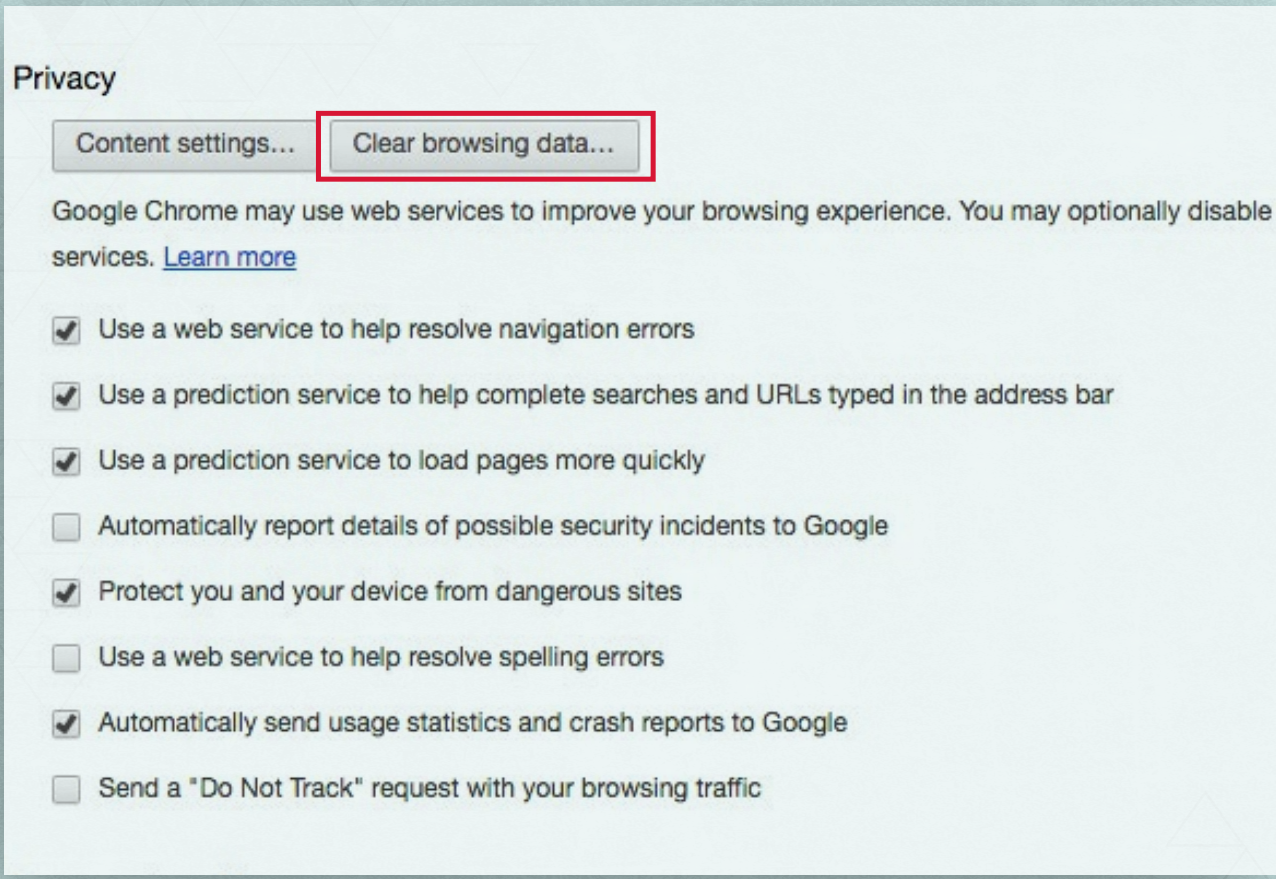
Google Chrome gives you the possibility to sync your settings and data with other systems or mobile devices where you signed-in with your Google account. This does create a vulnerability risk, since you are required by default to connect with your Google account on a device that also syncs with your other systems or devices.

To improve your security, you need to set a passphrase, which is an additional credential required to sync your devices.

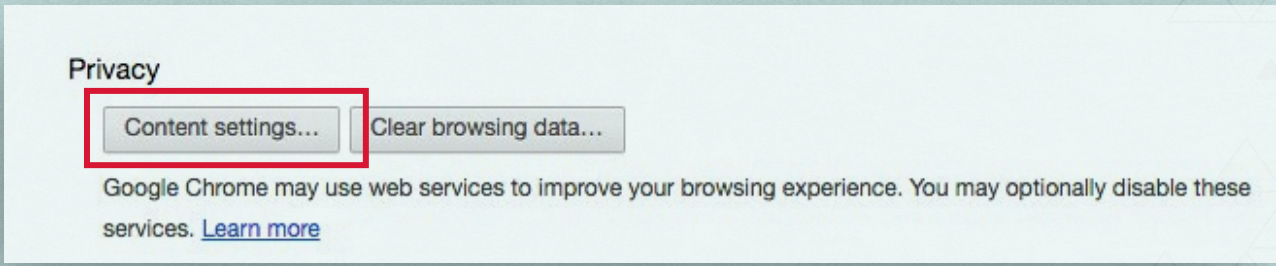
- If you scroll down at the bottom of the page, you will see a **Show Advanced Settings** option.
- Click the link in order to access the advanced settings available.
- The **Clear Browsing Data** option gives you the possibility to delete your browsing history, so don't forget to use that option if you are using a computer in a shared environment.



- The **Clear Browsing Data** option gives you the possibility to delete your browsing history, so don't forget to use that option if you are using a computer in a shared environment.

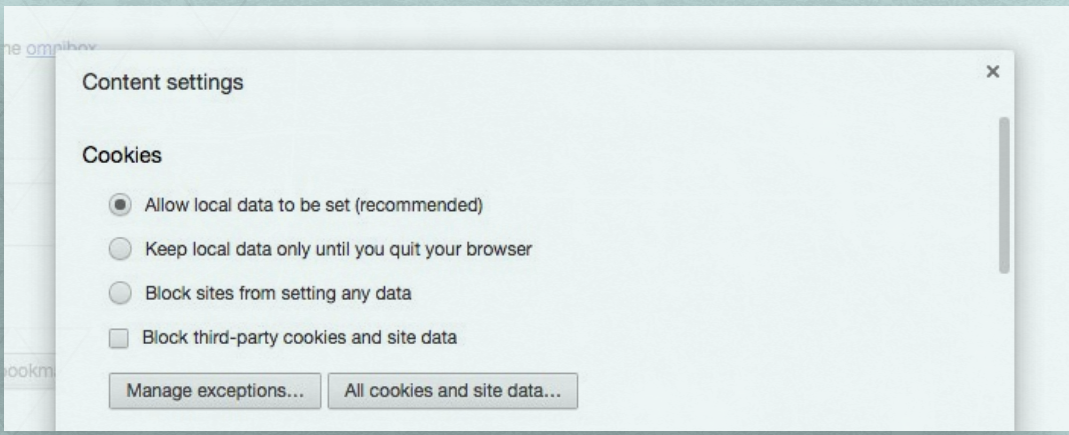


- The **Content Settings** option gives you more possibilities to address and improve your overall browsing security.

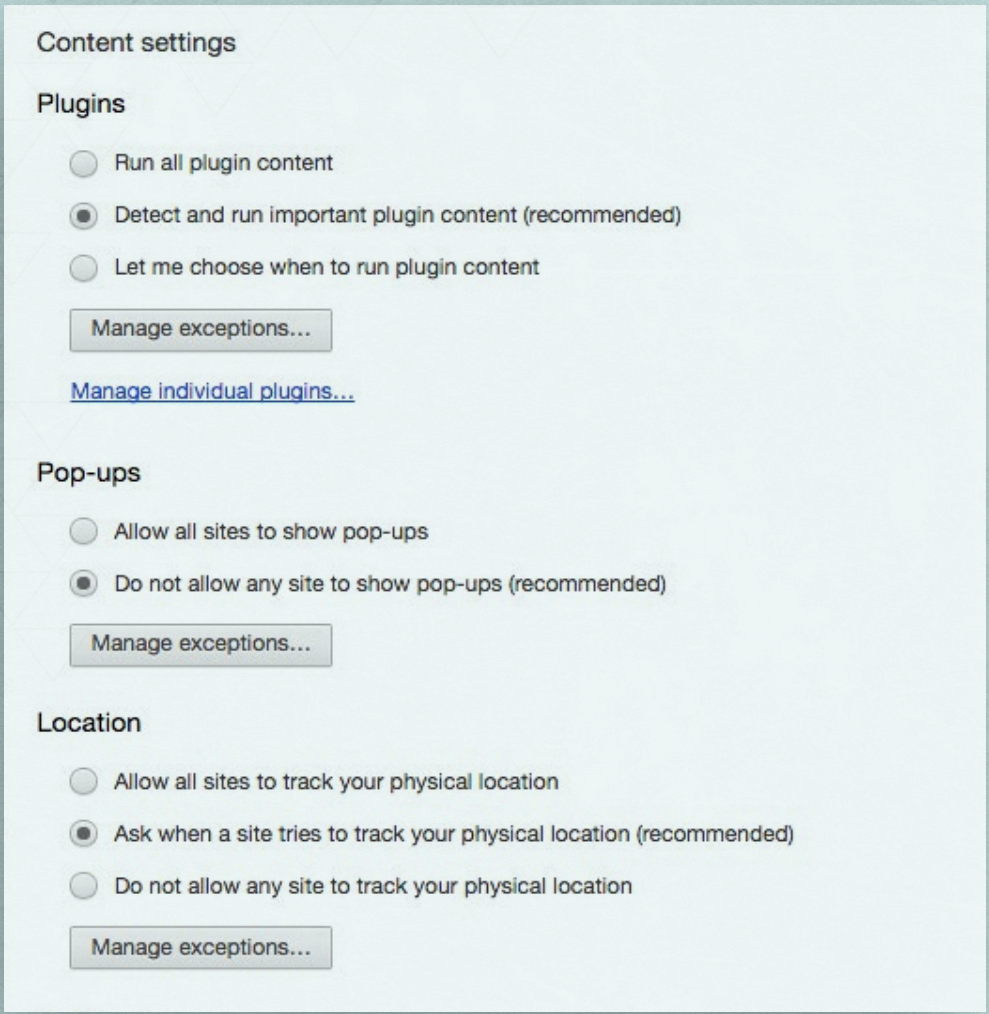


If you want to restrict cookies from being stored on your browser and using the collected information about your browsing habits, use the available options.

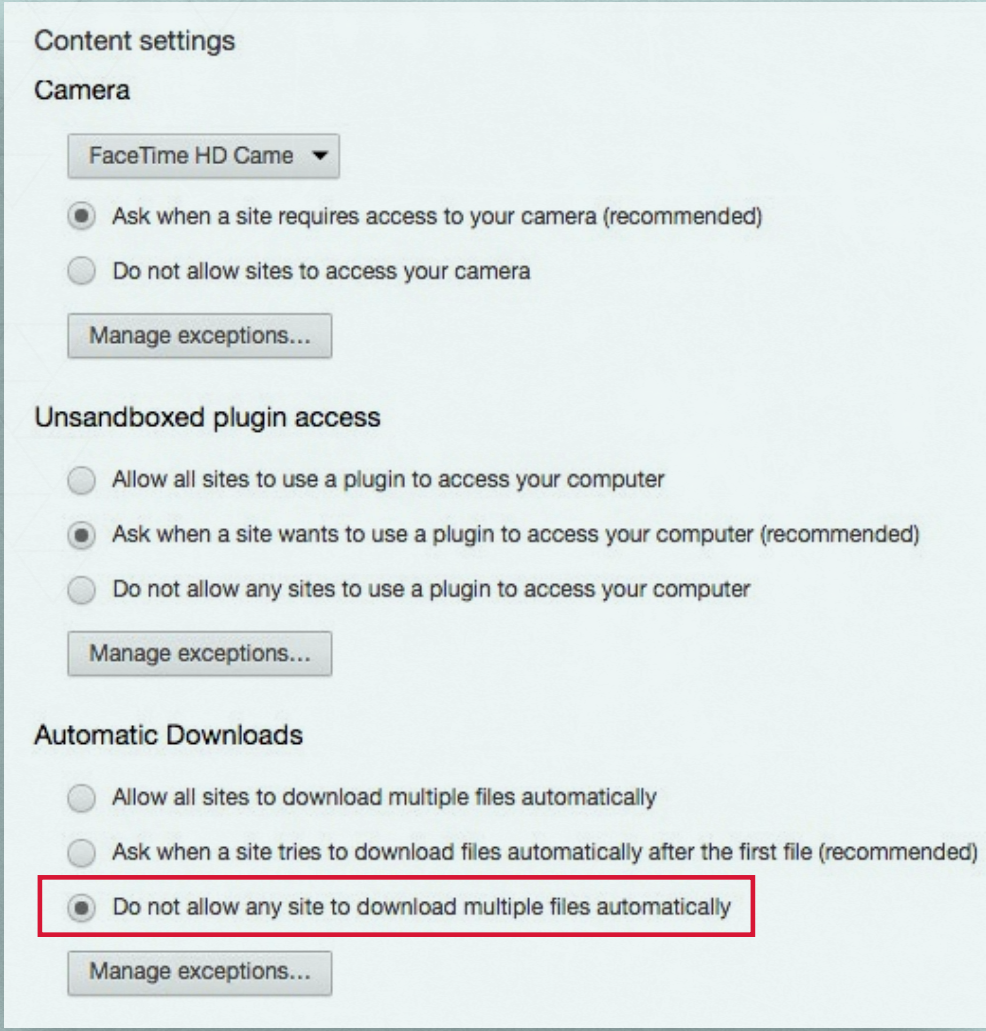
- To make the necessary changes in the **Content settings** window, you will need to scroll down in order to access the other options.



- Scrolling down, you find other options: You can control the behavior of your browser plug-ins, you can block pop-ups from disturbing your browsing session and you can stop a website from tracking your physical location.



- If you continue scrolling down to the bottom of the **Content settings** window, you will find the option to block websites from using a plugin to access your computer. There is also an option to block sites from downloading multiple files automatically on your computer, This can also further protect you from being exposed to sites that try to deposit security threats on to your device.



MOZILLA FIREFOX

Mozilla Firefox is another popular web browser and there are a few steps we can take to improve its security settings. To increase your protection against online threats in Mozilla Firefox (version 32.0.2), you need to access the settings area.

Private Browsing allows you to browse the Internet without Firefox saving any information in your browser history. You can set Private Browsing by default, or you can use it only occasionally.

Setting private browsing by default can be done in two ways:

✓ 1. Find **multiple →** ≡ **→ Preferences → Privacy → select Never remember history**

or

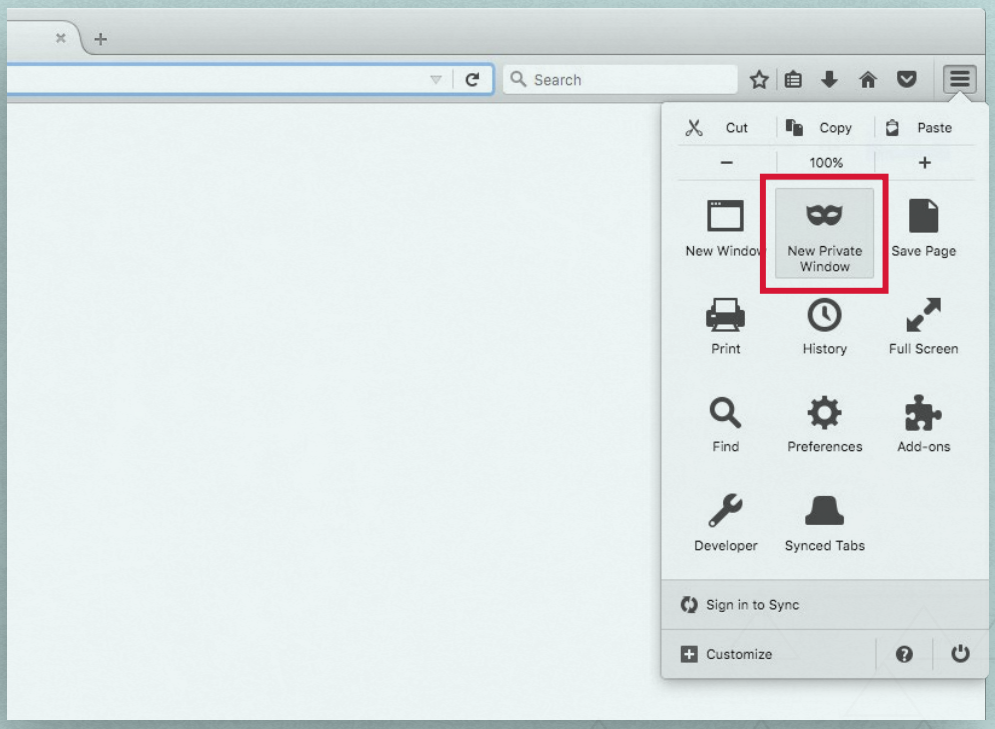
✓ 2. **Firefox →** ≡ **→ Preferences → Privacy → select use custom settings for history → check: Always use private browsing mode**

When you close Firefox, the following will be cleared: your browser, search, web form and download histories, as well as cookies and temporary files.

- What will be saved and what will be deleted is already predefined—you can't customize 'private browsing mode' to suit your own needs.
- Your history will only be cleared when you close the browser
- The trackers in the websites you visit can still collect data about you, including your browser history.
- Private browsing excludes the files you download and the pages you bookmark. These are saved.
- Private Browsing **does not make you anonymous on the internet**.

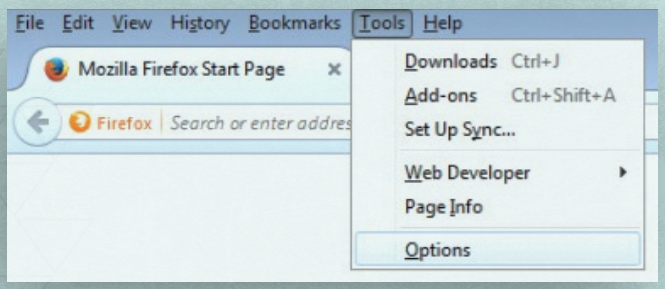
USING PRIVATE BROWSING OCCASIONALLY

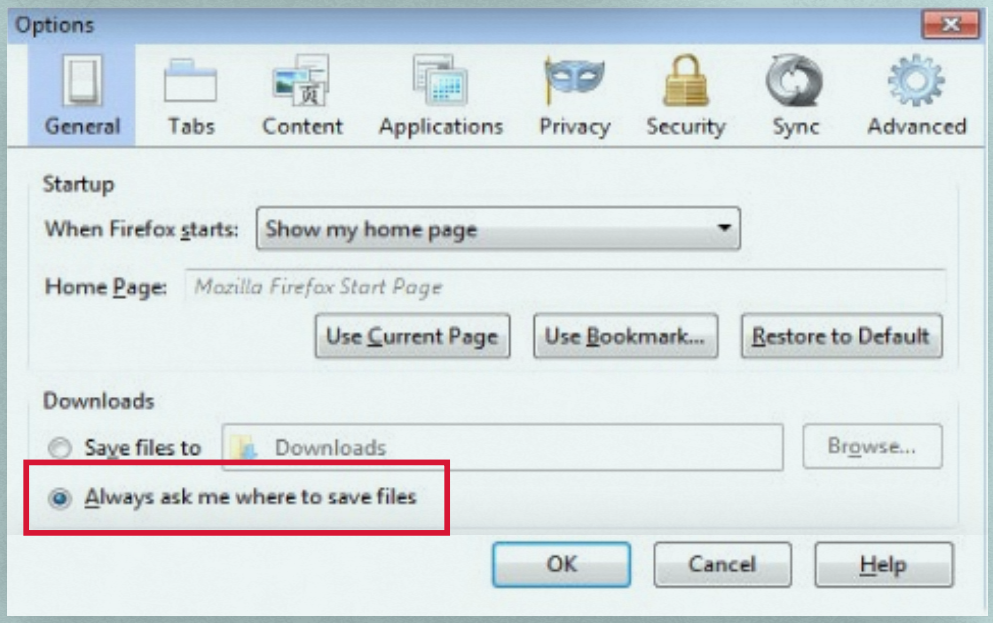
✓ Private Browsing' mode can also be used for a single window: **Open Firefox →** ≡ **→ New Private Window**



NOTE: Please make the necessary changes in case you are using a different version of Mozilla Firefox. To access the settings area, select **Tools and Options.**

- In the **Options** window, you need to access first the **General** category from the top menu.
- Under this section, you can select the option "**Always ask me where to save files**". This way, you won't have a web location trying to automatically save dangerous content to your computer. At the same time, you have the option to place suspicious content in a location where you can analyze it afterwards.

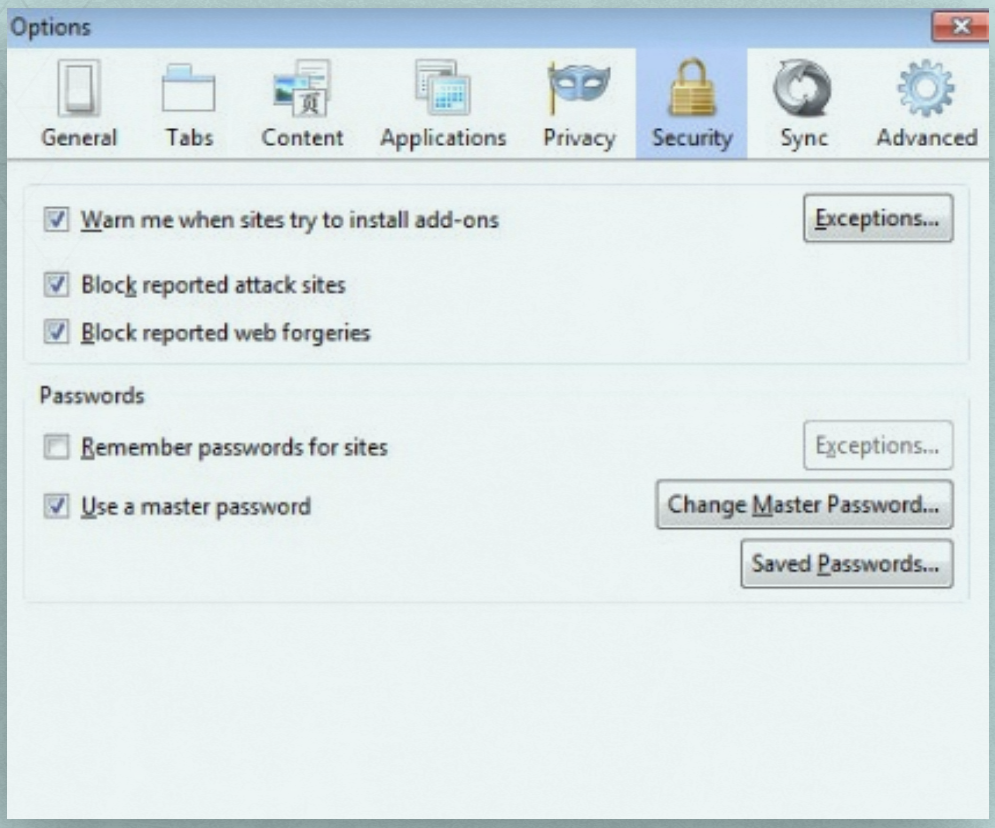




- In the Tracking section, check "**Tell sites that I do not want to be tracked**." Selecting this option informs a website that you would like to opt-out of third-party tracking for advertising purposes. In the "**History**" section, choose your browser **Never remember history**, especially if you are using a computer from a public location or you know that computer is used by more people.

- For a more detailed configuration of your **History** section, select from the drop-down menu Use custom settings for history.

You can choose for example, to **always use private browsing mode**, which we highly recommend if you find yourself in a shared environment. Selecting this option ensures that when you finish your Mozilla Firefox session, all browsing, search and download history, and all the cookies are removed. For a more detailed configuration of your online browsing settings, choose from the available options.



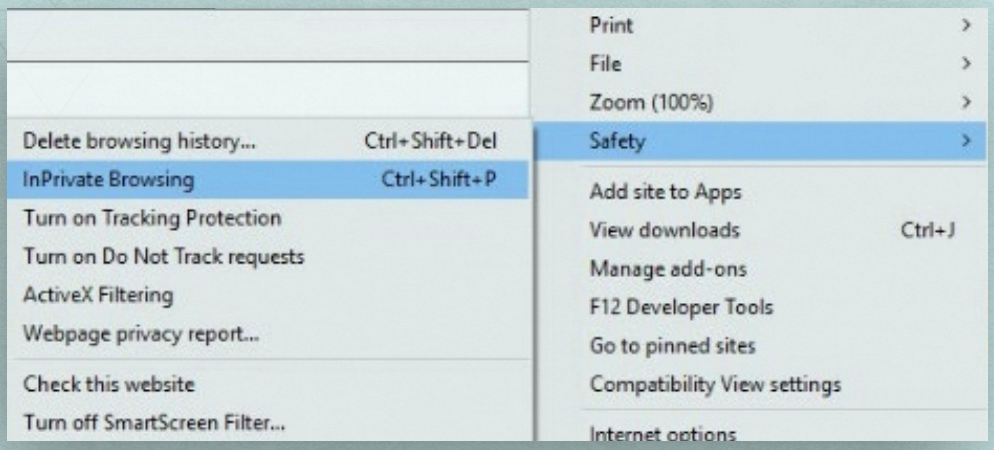
INTERNET EXPLORER

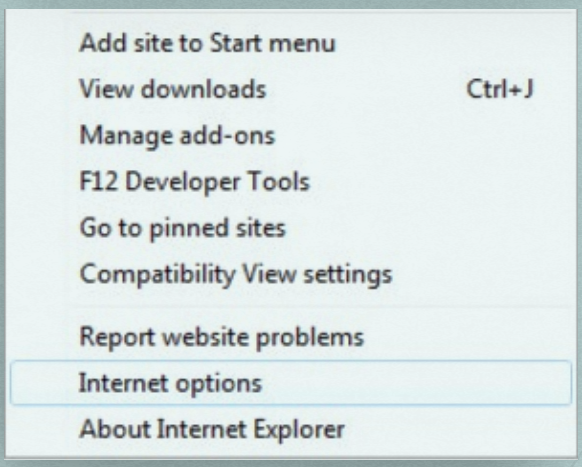
Microsoft Internet Explorer[27] is one of the most used web browsers in the world since it arrives pre-installed in our Windows operating systems. It supports Java and other active content, and it also implements ActiveX technology. While it is not the safest, and in fact, we do not recommend it at all, if you must use it, we recommend the following changes.

NOTE: To improve your overall security configuration in Windows 11, you need to access your browser settings area. Please make the necessary changes in case you are using a different version of Internet Explorer.

You can start a private browsing session in Internet Explorer (also called InPrivate Browsing).

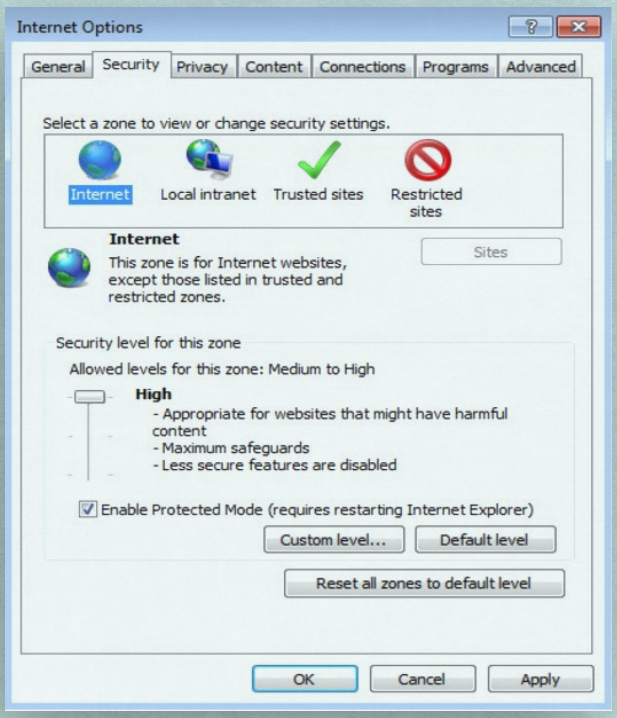
- Click on **Settings → Safety → InPrivate Browsing**. You can also use the keyboard shortcut Ctrl+Shift+P to launch it. Alternatively, you can right-click on the IE taskbar icon and select **Start InPrivate Browsing**.





[27] https://heimdalsecurity.com/blog/ultimate-guide-secure-online-browsing/

- To improve your Internet Explorer settings, access the **Internet Options** area.
- Go to the **Security** tab from the top menu.
- In this area you can locate: **Your trusted sites and security zones** for your computer. You also have the possibility to customize each security zone.



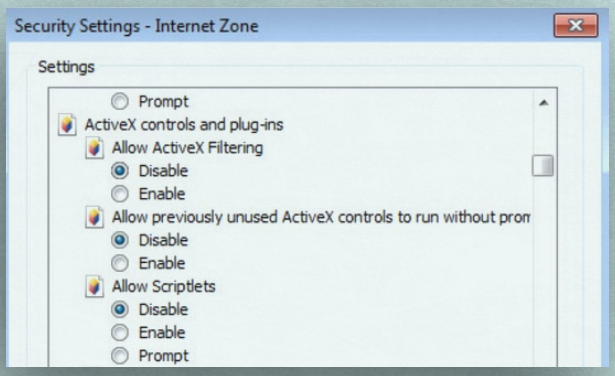
- For the Internet zone we recommend selecting the **High security level**. This selection will disable some browser features, such as ActiveX, Active scripting and Java, which can act as security breaches creating opening for threats to occur.

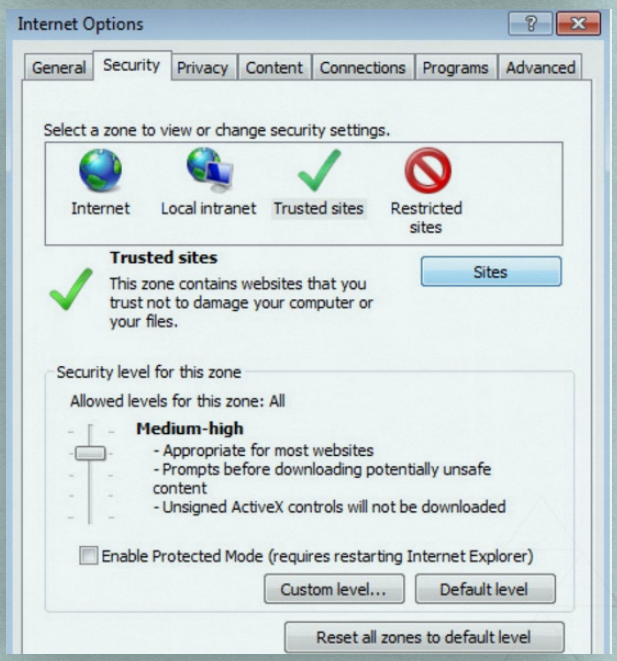
- To customize the security settings for a zone, choose the **Custom Level** option.

- In this area you can enable or disable specific security options for your selected Internet area. To return to the default levels for the selected Internet zone, simply click the “Reset” button.

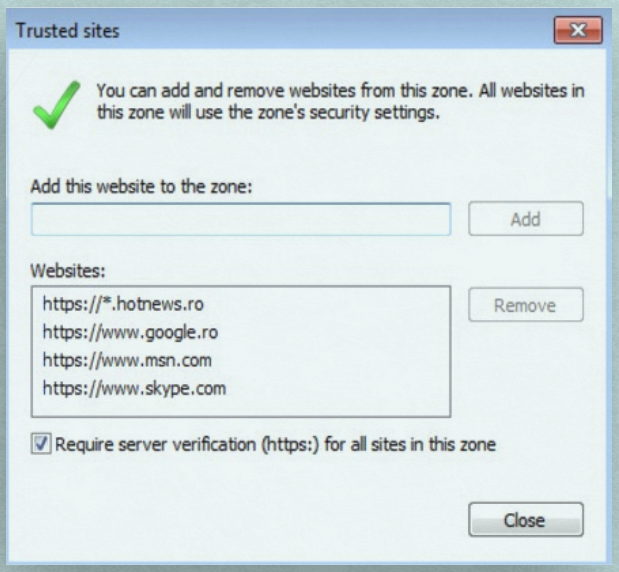
- If we return to the initial window and click the **Trusted sites** option, we find a security zone for sites which are safe to access.

- If you consider a particular website to be a safe online location that can be trusted, you can choose to add it to this area. To do this, click **Sites**.



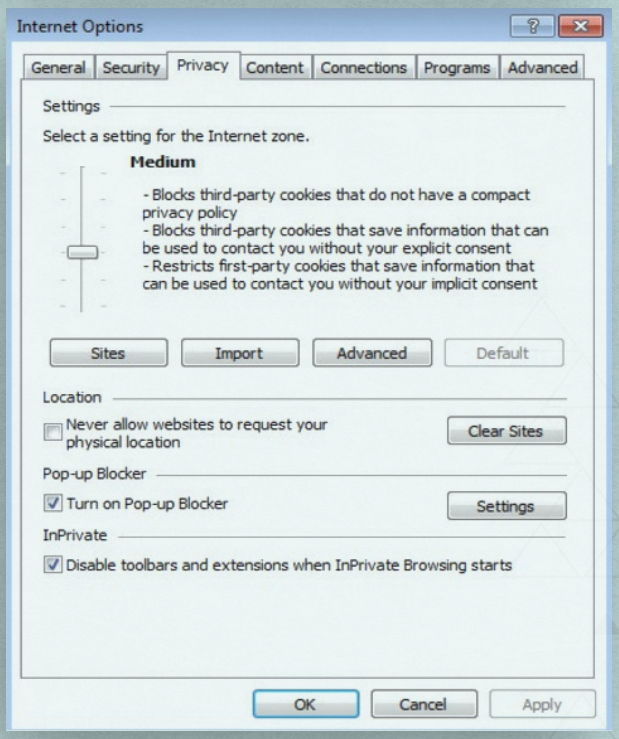


In this area, you can choose to add the website to a list of safe web locations. You can also choose to remove a site from the list.



The **Trusted sites** zone is useful if you chose the High security level for the Internet zone. Setting the High security level in the Internet zone causes browser features like ActiveX and Active scripting to stop functioning, and you may encounter some websites that don't function normally after that. To solve this, simply go to the Trusted sites zone and add the site that doesn't function as it should. Adding the site to the Trusted sites zone means that the website will work normally, by loading the browser features that are not allowed to function in the High security level.

The **Privacy** tab contains various settings for cookies in Internet Explorer.



Cookies are text files that are placed in your computer by websites you access. They contain data and information the sites store about your browsing habits or your preferences. In this space you can use the preset privacy rules available by using the slider and select one of the settings for your Internet zone. For example, choosing the High level will block cookies from most websites.

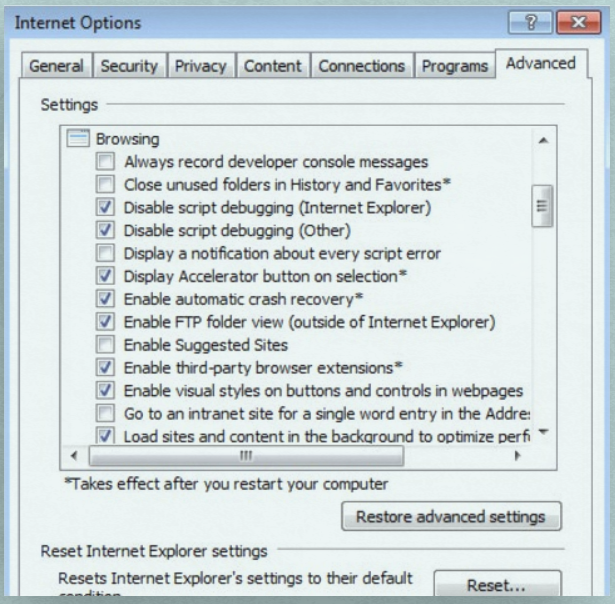
If you want to make modifications, you have other additional options.

To improve your security, select the **Advanced** button available.

This area contains settings that apply to all security zones.

- From this tab, we recommend you to **uncheck Enable third-party browser extensions** option.

If you leave it checked, different types of toolbars and addons are enabled on your system and this may affect your privacy. Many add-ons have proved to monitor your browsing habits or even attempt to collect private data from your browser.



EXTENSIONS FOR A SAFER ONLINE SESSION

Adjusting your browser settings will enhance its security to a certain degree, but for complete protection installing further security extensions will be needed.[28]

Browser extensions are small software programs that improve and personalize your online experience.

With so many extensions (or add-ons) out there, it is difficult to make the right choice. Some of them address your need for privacy, others, your need for protection and security while you access your online tax information or log into your banking account, for example.

When using a browser extension you have greater control over your browser behavior. You can block ads from some websites and pop-ups that may act like carriers for financial and data stealing malware. At the same time, you have the possibility to block others from breaching your privacy settings.

TIP: We want you to also be aware how these extensions work to provide security and also how to test these extensions

PRIVACY BADGER

EFF's Privacy Badger is a browser add-on that stops advertisers and other third-party trackers from secretly tracking where you go and what pages you look at.

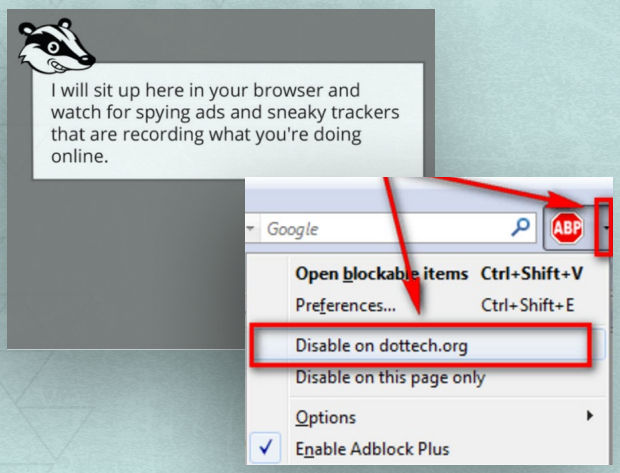
If an advertiser seems to be tracking you across multiple websites without your permission, Privacy badger automatically blocks that advertiser from loading any more content.

To the advertiser, it's like you suddenly disappeared. Privacy Badger was born out of the desire to be able to recommend a single extension that would automatically analyze and block any tracker or ad that violated the principle of user consent.

Although extensions like Disconnect, Adblock Plus, Ghostery work well, (in fact Privacy Badger is based on the ABP code!), all of them require some custom configuration to block non-consensual trackers and could have some conflict of interests in their business model.

[28] https://heimdalsecurity.com/blog/ultimate-guide-secure-online-browsing/

The internet freedom non-profit EFF developed Privacy Badger to be heuristic, which means it gets better at creating blacklists and blocking websites as time goes on, making it unique when compared to other blockers. Out of the box, Privacy Badger won't block nearly as many third-party requests as the commercial options but it does get better over time with frequent use. It will discover which hosts to block, it will also create a whitelist for important sites that are visited on a regular basis.

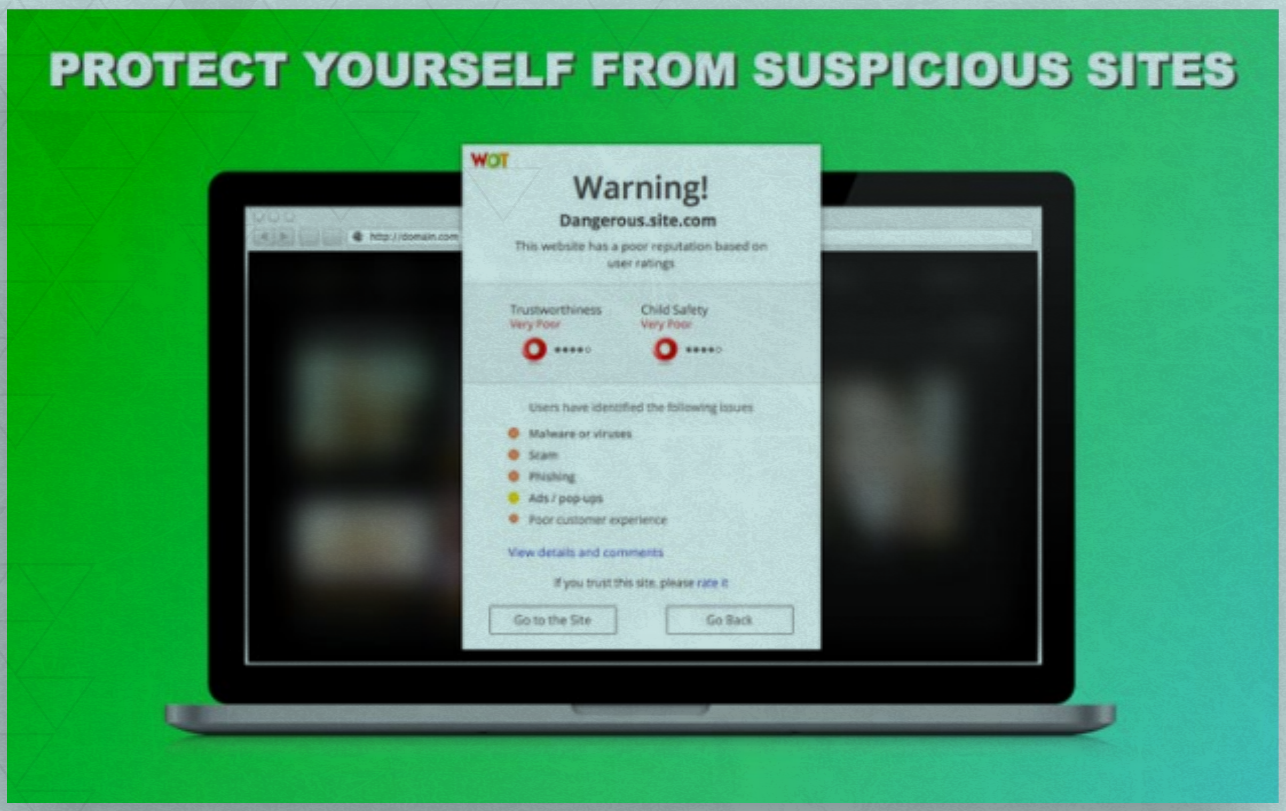


HTTPS EVERYWHERE

HTTPS Everywhere is an extension available for Mozilla Firefox and Google Chrome created by the Electronic Frontier Foundation.

WEB OF TRUST

Available for Mozilla Firefox, Google Chrome, and Internet Explorer, **Web Of Trust** ranks websites by reputation based on the amount of malware they host or tracking cookies they contain. Since it's an informational tool, it will not block ads, but its valuable information allows you to make an informed decision on your course of action.


PROTECT YOURSELF FROM SUSPICIOUS SITES
WOT
Warning!
Dangerous.site.com
This website has a poor reputation based on user ratings
Trustworthiness
Very Poor
Child Safety
Very Poor
Users have identified the following issues
Malware or viruses
Scam
Phishing
Ads / pop-ups
Poor customer experience
View details and comments
If you trust this site, please rate it
Go to the Site
Go Back

WHAT ABOUT SEARCH ENGINES?

Search Engines are big money for Google and Microsoft because what you search tells a lot about you and what your concerns are. Imagine if I search in one session about the cost of diapers, maternity centers, and child care, one could easily infer that I was thinking about children. Similarly if you are about to hold a protest and you search about non-violent direct action or the number for the lawyers guild, one could then infer you were thinking about a protest or some direct action. In essence who ever owns your search history owns you!

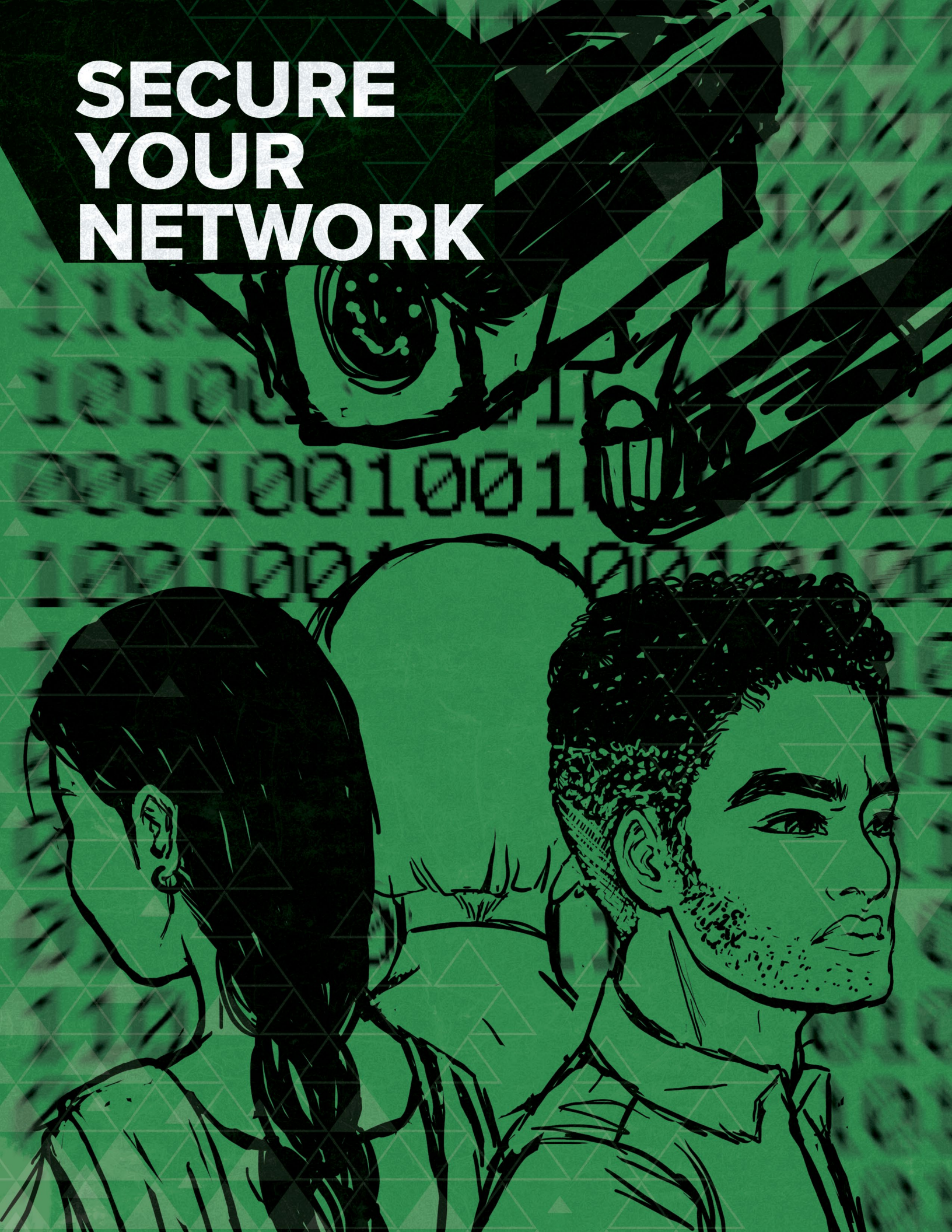
This is why choosing a search engine that does not track you is important. Currently all of your searches on engines like Google and Bing are used to help inform and create a very large Data shadow about you and your concerns. Imagine what that could reveal and how it could be used against you. The best option then is to use search engines that do not track you.

We recommend **DuckDuckGo**[29], but for folks who want to see a comparison the next page has some great options to explore. Try them and try them often. Once you find one that works switch!

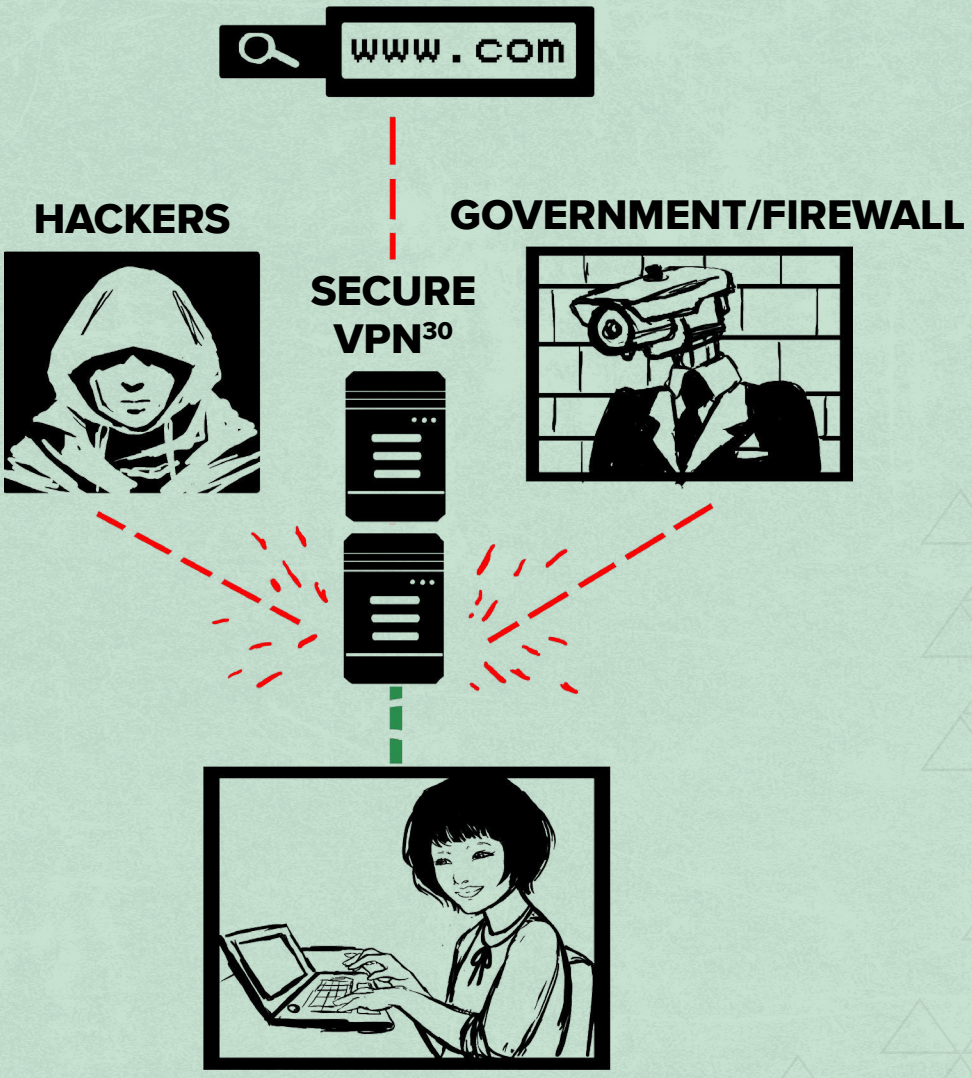
[29] https://duckduckgo.com

DuckDuckGo	searX	startpage
Cookies: Does not use cookies by default	**Cookies:** Does not use cookies by default	**Cookies:** Does not use identifying cookies
Tracking policy: Does not track and profile users	**Tracking policy:** Does not track and profile users	**Tracking policy:** Does not store its users' IP addresses
Personal information: Does not collect or store	**Personal information:** Does not collect or store	**Personal information:** does not collect or share personal data
Encryption: Yes, HTTPS	**Encryption?** Yes, HTTPS	**Encryption?** Yes, HTTPS
	Owned and managed by: La Quadrature du Net	**Extra:** Offers a free proxy service that allows for anonymous online browsing

SECURE YOUR NETWORK



CONNECTING TO THE INTERNET—HOW DOES IT ALL WORK?



The first step to connect to the Internet is typically made through an Internet Service Provider (ISP) at your home, office, cafe, library, or Internet cafe. Common ISP's in the US are Verizon Fios, Xfinity, and Time Warner Cable.

[30] https://securityinabox.org/en/lgbti-mena/anonymity-and-circumvention

The ISP then assigns your computer an IP address, which various Internet services can use to identify you and send you information, such as the emails and webpages you request.

Anyone who learns your IP address can figure out what city you are in. Certain organizations in the country, however, can use this information to determine your precise location.

Using your IP Address, your ISP will know which building you are in or which phone line you are using. Additionally, your internet and phone providers will know which device you were using at a given time, as well as which port or wireless access point you were connected to. Government agencies may know all of these details, as a result of their influence over the organizations above.

Your data funnels through ISP's which operate on the network infrastructure in your country. ISP's connect you to wesites that exist all over the world.

On the other end of your connection, the website or internet service you are accessing has gone through a similar process, having received its own IP addresses from an ISP in its own country.

This summary, even without all of the technical details, is super helpful when considering the various tools that allow you get around filters and remain anonymous on the internet. If you feel comfortable and now grasp this overview, read on to see how you can best protect your network access!

HOW WEBSITES ARE BLOCKED OR CENSORED

Essentially, when you go to view a webpage, you are showing the site's IP address to your ISP, and asking it to connect you with the webserver's ISP. And, if you have an unfiltered internet connection, it will do precisely that. If you are in a country that censors the internet, however, it will first consult a blacklist of forbidden websites and then decide whether to comply with your request.

In some cases, there may be a central organisation that handles filtering in place of the ISPs themselves. Often, a blacklist will contain domain names, such as www.jhalkaribai.com, rather than IP addresses. And, in some countries, filtering software monitors your connection, rather than trying to block specific Internet addresses. This type of software scans through the requests that you make and the pages that are returned to you, looking for sensitive key words and then deciding whether or not to let you see the results.[31]

To make matters worse, when a webpage is blocked you may not even know it. While some filters provide a 'block page' that explains why a particular page has been censored, others display misleading error messages. These messages may imply that the page cannot be found, for example, or that the address was misspelled.

In general, it is easiest to adopt a worst-case perspective toward internet censorship, rather than trying to research all of the particular strengths and weaknesses of the filtering technologies used in your country. In other words, you might as well assume that:

Your internet traffic is monitored for keywords.

- Filtering is implemented directly at the ISP level.
- Blocked sites are blacklisted by both their IP addresses and their domain names.
- You may be given an unclear or misleading reason to explain why a blocked site fails to load.

[31] https://www.eff.org/torchallenge/

BROWSE THE INTERNET ANONYMOUSLY AND BYPASS CENSORSHIP

TOR

Tor[32] is used by political activists, whistleblowers, journalists, domestic violence survivors, and average people around the world who need to shield their identities as they read and write online.

It helps you hide your **IP address** and prevent browser fingerprinting, making it more difficult for online trackers and even governments to surveil you.

In countries where huge swaths of the Internet are blocked, people use Tor to **access the open, uncensored web**. Tor is an effective censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content.

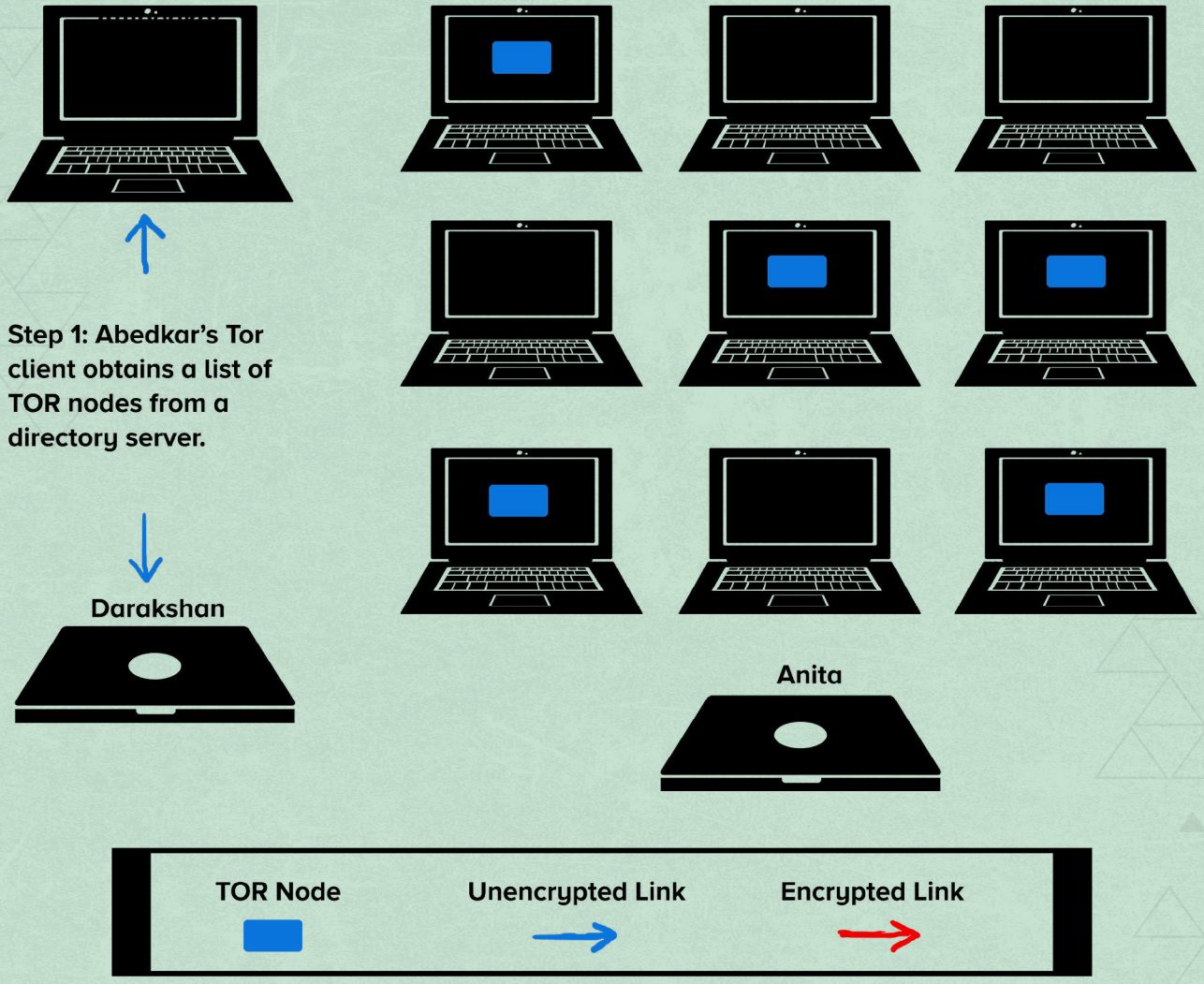
The range of people who use Tor are actually part of what makes it so secure. Tor hides you among the other users on the network, so the more populous and diverse the user base for Tor is, the more your anonymity will be protected.[33]

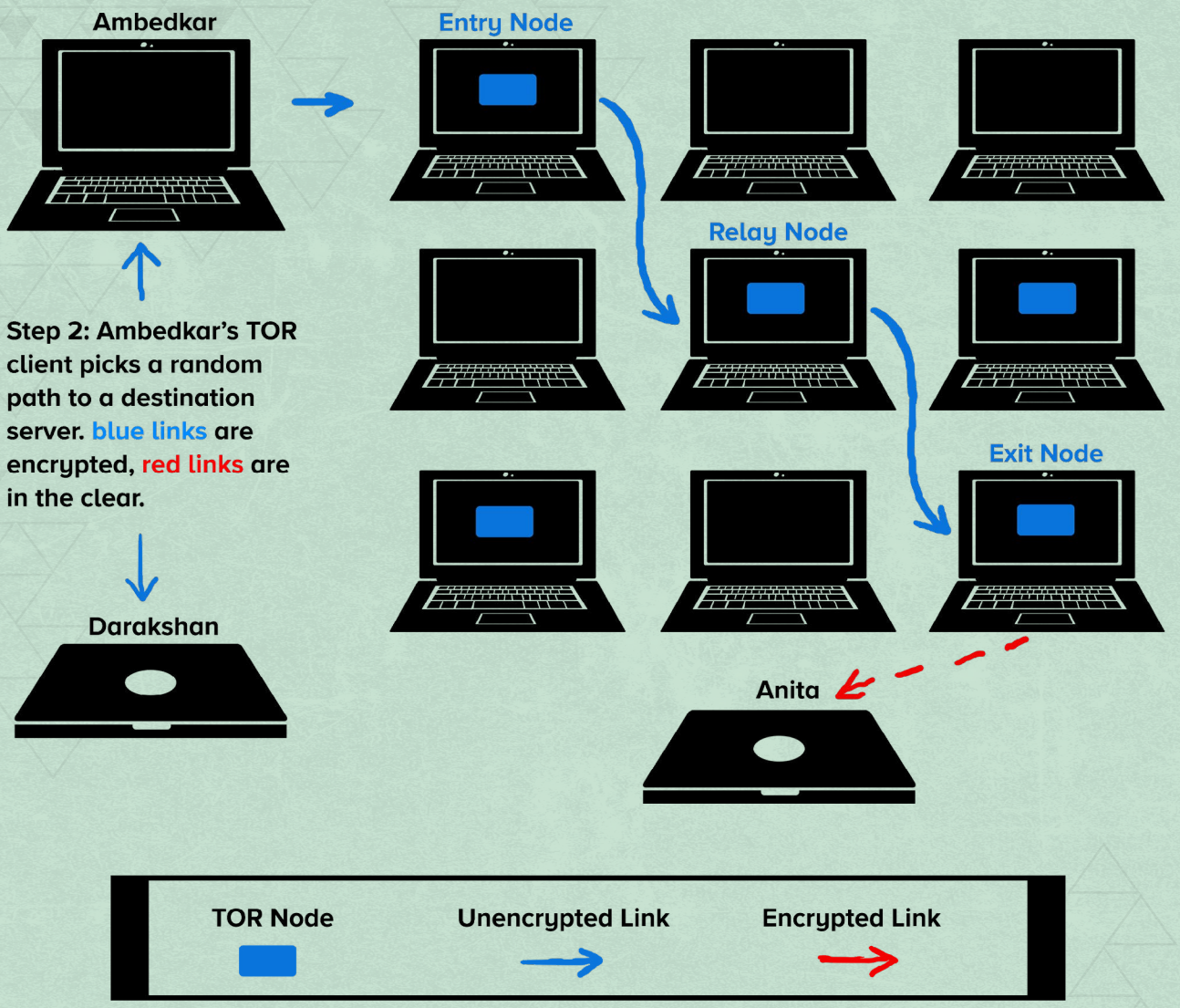
[32] https://www.eff.org/torchallenge/
[33] https://www.torproject.org/about/overview

There are lots of reasons you might want to use Tor. They can include:

- You have sensitive information and you don't want people to know that you are the person who sent it and where you are sending it from.
- You need to search politically sensitive content and you do not want to reveal your identity and geographic location when looking for such information.

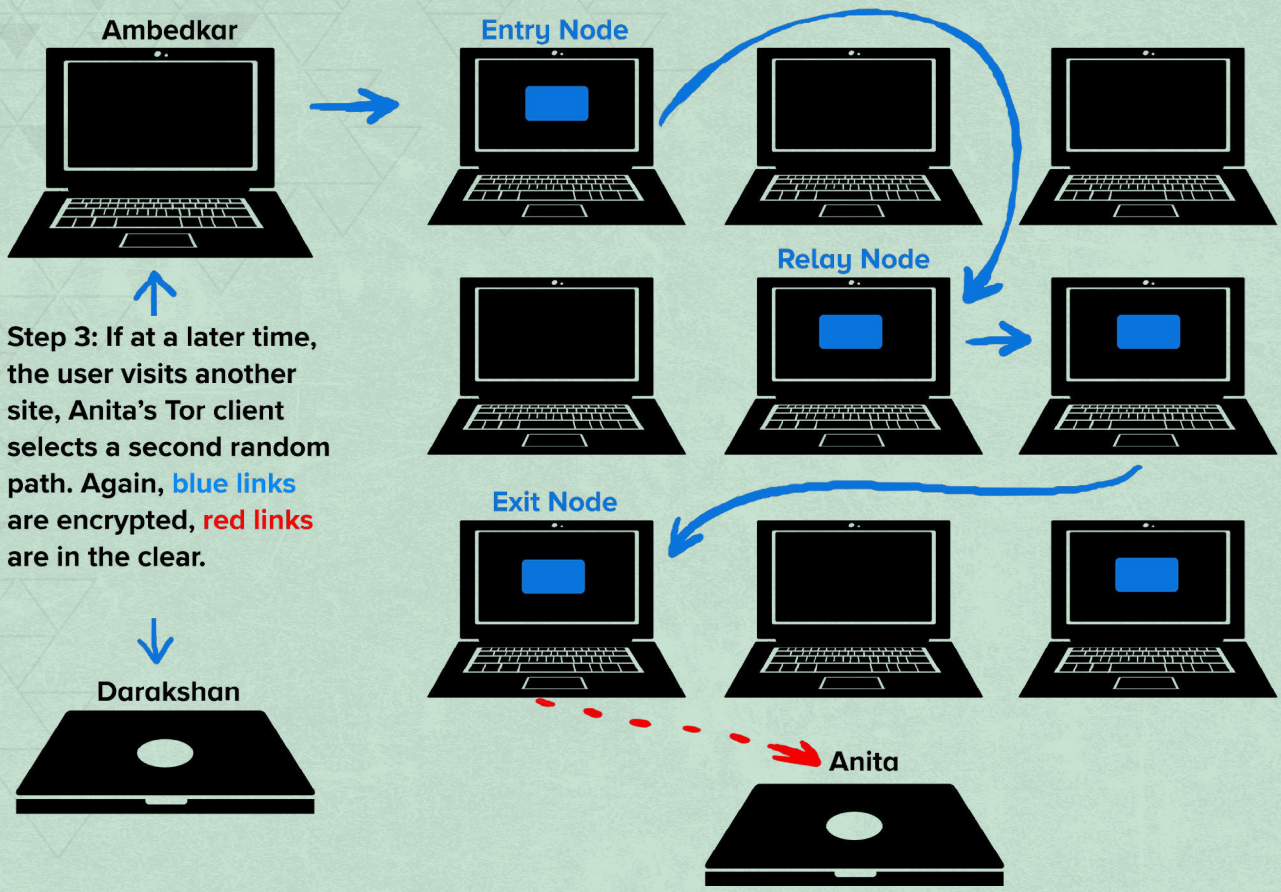
To better understand how Tor works below is a series of diagrams that wil help you understand the Tor process. In these diagrams our friend Ambedkar wants to send e-mails to his friend Anita.

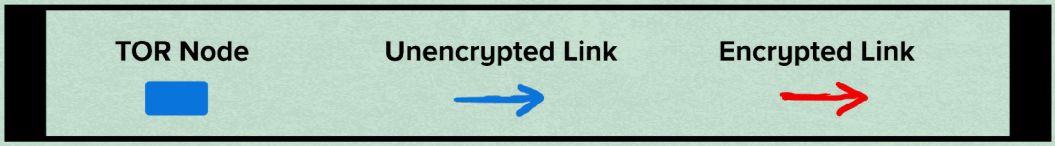




In this next step Ambedkar's client now picks a random path through multiple Tor servers across the world. The first computer is the entry node, and the second computer is the relay node, and the third computer is the exit node. That node is the IP address that is seen by the websites you visit, which recognize the country of origin where the exit node is located.

What is important to know is that the path between Anita and the exit node is UNENCRYPTED so please make sure you use the https protocol between sites.





WARNING: Tor is only protecting the network access. If your computer is communicating with a final destination site that is not using HTTPS then the content sent by the final node through the intermediate Internet route to the destination server will be UNENCRYPTED! YOU MUST USE HTTPS TO REMAIN PROTECTED. So check your URL's and use HTTPS EVERYWHERE as your browser extension.

Tor is only as good as the more diverse communities use it. If you want to learn more about Tor or even join the Tor community please visit www.torproject.org

VIRTUAL PRIVATE NETWORKS (VPN)

Another option for securely accessing the internet is a Virtual Private Networks or VPN. VPN's allow you to connect to the internet via a server run by a VPN provider. All data traveling between your computer, phone or tablet, and this "VPN server" is securely encrypted. As a result of this setup, VPNs:

- Provide privacy by hiding your internet activity from your ISP and the government.
- Allow you to evade censorship by school, work, your ISP, or the government.
- Allow you to "geo-spoof" your location in order to access services unfairly denied to you based on your geographical location(or when you are on holiday.
- Protect you against hackers when using a public WiFi hotspot.
- Allow you to Peer to Peer download in safety.
- Keep in mind a VPN protects one's right to privacy on the internet by creating anonymity. This anonymity is crucial to guaranteeing that none of your data will be divulged without your consent.

HOW DOES IT WORK ?

Normally, when you connect to the internet you first connect to your Internet Service Provider (ISP), which then connects you to websites (or other internet resources). All your internet traffic passes through your ISP's servers, and can be viewed by your ISP.

When using VPN you connect to a server run by your VPN provider (a "VPN server") via an encrypted connection (sometimes referred to as a "VPN tunnel"). This means that all data traveling between your computer and the VPN server is encrypted so that only you and the VPN server can "see" it.

This setup has a number of important consequences:

1. YOUR ISP CANNOT KNOW WHAT YOU ARE UP TO ON THE INTERNET

It cannot see your data because it is encrypted. It cannot know which websites (etc.) you visit because all internet activity is routed through the VPN server. Your ISP can only see that you are connected to the VPN server.

2. YOU APPEAR TO ACCESS THE INTERNET FROM THE IP ADDRESS OF THE VPN SERVER

If the VPN server is located in a different country to you, then as far as the internet is concerned you are located in that country (most VPN services run servers located in many different countries). Anyone monitoring your internet activity from the internet will only be able to trace it back to the VPN server, so unless the VPN provider hands over your details (more on this later), your real IP address is hidden. This means that websites etc. cannot see your true IP address (just that of the server).

3. IT IS SAFE TO USE PUBLIC WIFI HOTSPOTS

Because the internet connection between your device and the VPN server is encrypted. Even if a hacker somehow manages to intercept your data, for example by tricking you into connecting to

an “evil twin” hotspot or packetsniffing your WiFi data, the data is safe because it is encrypted.

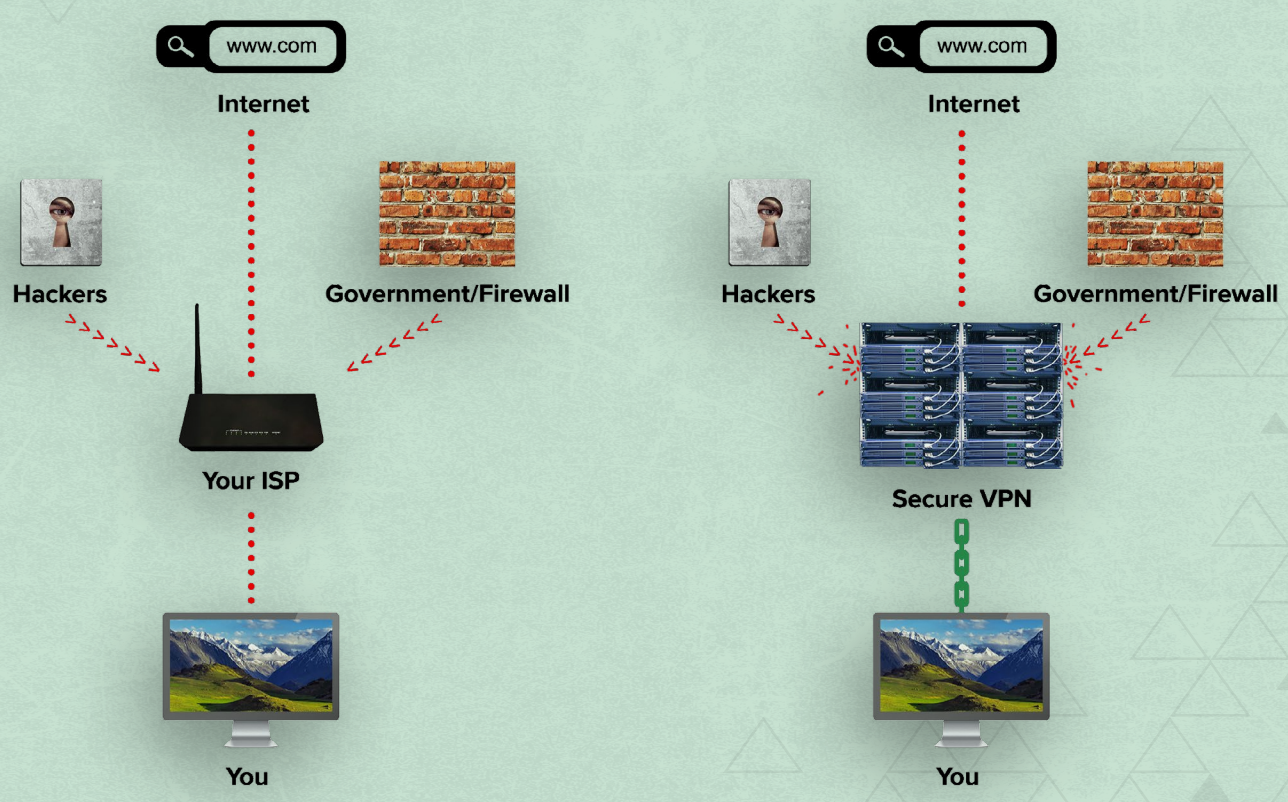
4. YOUR VPN PROVIDER CAN KNOW WHAT YOU ARE UP TO ON THE INTERNET

Your VPN protects your internet traffic from surveillance on the public network, but it does not protect your data from people on the private network you’re using.[34] This means whenever you are looking for a VPN, you want to see what their data sharing policies are and if they are dedicated to doing VPN’s or have only recently started. This can be an indicator to the expertise and seriousness of the service with regards to User privacy.

You are therefore shifting trust away from your ISP (which has no interest in, or commitment to, protecting your privacy) to your VPN provider who usually promises to protect your privacy. More privacy-minded VPN services mitigate this issue by employing various technical measures to know as little as they can about you. More on this later.

5. YOUR INTERNET WILL SLOW DOWN

Encrypting and decrypting data requires processing power. This also means that, technically, the stronger the encryption used, the slower your internet access. However, given the power of modern computers, this issue is relatively minor compared to the extra distance traveled by your data. Using VPN always introduces another leg to the journey that your data has to travel (i.e. to the VPN server), and thanks to the laws of physics, the further your data has to travel, the longer it takes.



[34] https://ssd.eff.org/en/module/choosing-vpn-thats-right-you

If you connect to the VPN server located geographically nearby in order to access a website that is also located nearby, expect a 10% decrease in internet speed. If you connect to a server half way across the planet, you should expect a much greater decrease in speed.

We encourage you to always look through the privacy policies of all VPNs that you work with. Some VPN's we recommend include VyprVPN by Golden Frog. Not all VPNs are transparent about what they share about you and where. Vypr currently has a minimal amount of data stored about you and your usage and they also hold all servers in house. The downside of Vypr is that it is a paid service. You can find it here: https://www.goldenfrog.com/vyprvpn

TOR VS VPN

There are subtle, but important differences between using Tor and a VPN:

	TOR	VPN
ORGANIZATION	Tor is a network run by global volunteers	A VPN is usually run by a private company unless you are using your own activist VPN
RESILIENCY	Tor nodes are distributed and harder to shutdown	A VPN company can be a target for legal requests to shut down or divulge data. You will have to trust your VPN partner to have good business practices
SPEED	Traffic through Tor is going through several parties and usually has a significant slowdown	Traffic is going only through your VPN and is much faster than Tor
EXIT NODE IP ADDRESS	You cannot guarantee the exit node IP Address will be the same between requests and sessions	You can choose a fixed IP Address from which your traffic will originate from
END-TO-END ENCRYPTION	Tor has encryption between all of the nodes, but does not have guaranteed end-to-end encryption	All traffic between you and the exit node is encrypted
LOGGING	Nodes are usually configured not to log traffic	A VPN company may log your traffic without your knowledge or consent

In short, Tor is slower but offers more privacy, and a VPN is necessary when dealing with sites that will not open in Tor. In either case, always check for HTTPS or you will be voiding your secure network access.

SECURE YOUR SOCIAL MEDIA

SOCIAL MEDIA: BEING SMART, STAYING SAFE!

Social media has been a powerful tool for all of our movements. Through social media we have been able to challenge the media blackout on many of our issues as well as rapidly mobilize collaborators across borders and issues. However, social media is not a neutral tool, social networks like Facebook, Twitter, and Instagram may operate like civic public spaces, but in fact these are private self-surveilling corporate platforms with various degrees of collaboration with government surveillance systems.

As a result, many of us are vulnerable because we are unaware how our posts, tweets, and pictures are being used to create an enormous data portfolio for these corporations to use, sell, and share with other corporations and governments. **This is why these platforms are not really free, because we pay for them with our data**.

The question of visibility is something we all have to make our own risk assessments by doing a thorough analysis of the areas of your life that may contain risks if exposed. Many of us began by creating personal accounts on social media, later realizing the political, professional, and personal implications such visibility could have on our lives. A few common sense safeguards will go a long way in avoiding unwanted leaks of personal information or embarrassing reveals that can affect you and the worlds that you may be a part of.

All actions online must be well considered. Filling out a "Profile" or "About me" may seem relatively harmless, it is in fact a moment where you have to decide what information you want to make available, and how that relates to, or affects the work you do. Say for instance, you reveal the city you live in, the broad unknown online public will have information they can use to figure out your physical location. If security settings on your account are not set tightly, you may have made yourself vulnerable. We recommend you make decisions with careful consideration based on what you feel most comfortable with.

Questions to ask yourself:

- Who can access the information I am putting online?
- Who controls and owns the information I put into a social networking site?
- What information about me are my contacts passing on to other people?
- Will my contacts mind if I share information about them with other people?
- Do I trust everyone with whom I am connected?

COMPARTMENTALISATION: PERSONAL VS PROFESSIONAL ACCOUNTS

A piece of sound advice is to maintain two accounts if you feel vulnerable. It's perfectly acceptable to develop separate accounts for personal and professional uses. Many folks open two accounts within the same social media site, one for each purpose. However, be aware that your colleagues could be connected to you via a professional account only but there is still a chance they could find and view your personal account.

Many activists today already maintain a professional and personal Facebook account. This helps the individual to express harder political points of view on Facebook, Instagram, and other platforms without worrying about how their views will affect their job searches and employment. So the first part of this section will speak to this compartmentalization.

PROFESSIONAL

- Links and Resources
- Positions on Academic/Industry Focus
- No Explicit political position

PERSONAL

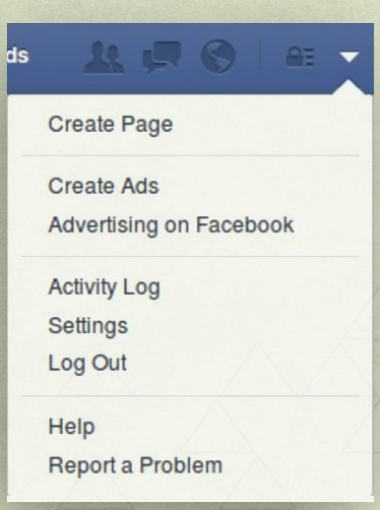
- More political
- More personal
- Understanding these are thoughts in process

FACEBOOK

Here are some ways we can assign settings that make our experiences on Facebook as private and safe as possible.

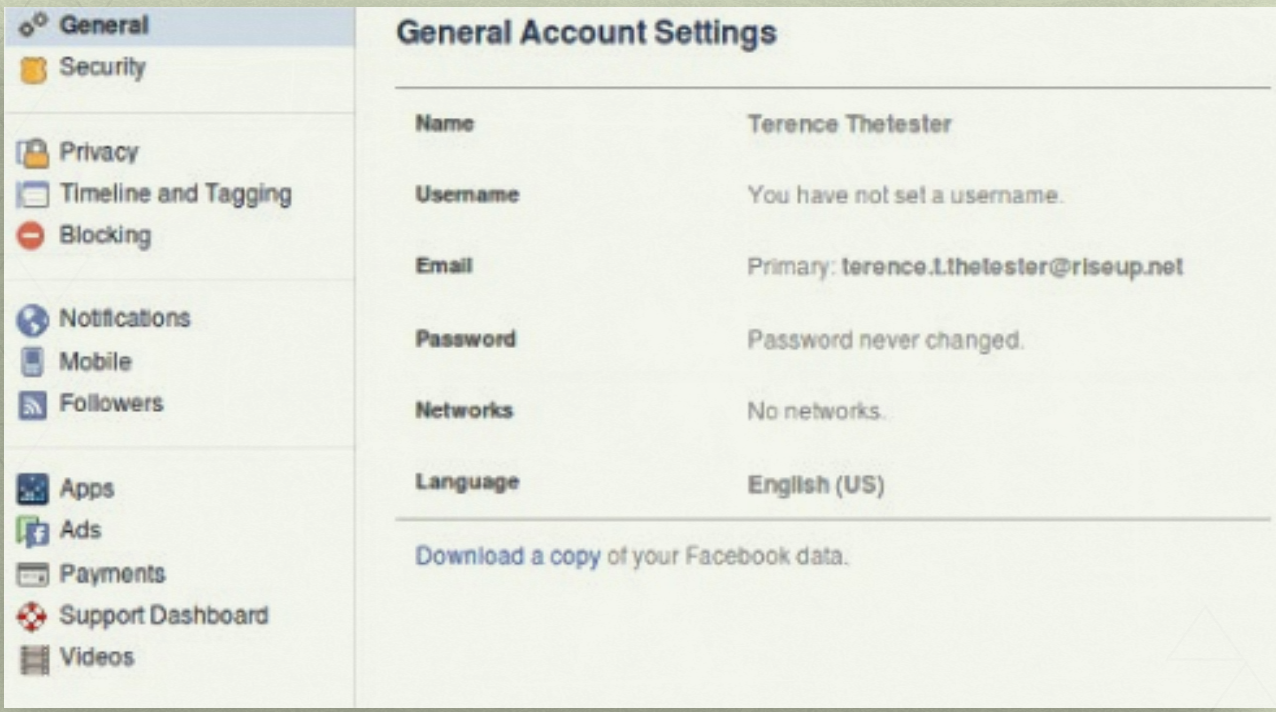
GENERAL SETTINGS AND TOOLS

From your Facebook Home page, click on the small arrow beside Home in the top right-hand corner and select **Settings**.



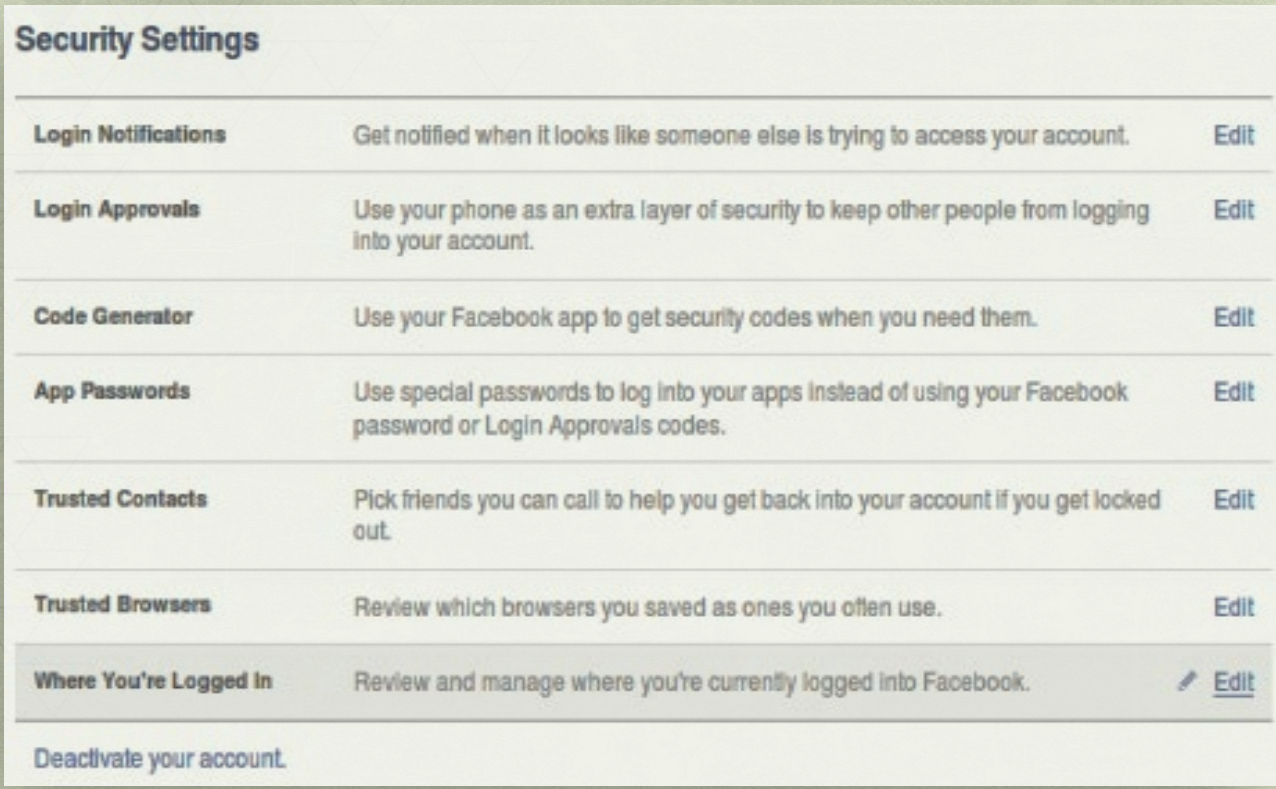
This will take you to the Settings menu. On the left-hand side, you can choose different categories of settings. The first tab is **General Account Settings**, where you can edit information about your name, username, email, password, networks, and language.

You should update your password regularly, preferably at least once every three months. Remember, it is extremely important that you choose a strong password to protect your account and your information.



SECURITY SETTINGS

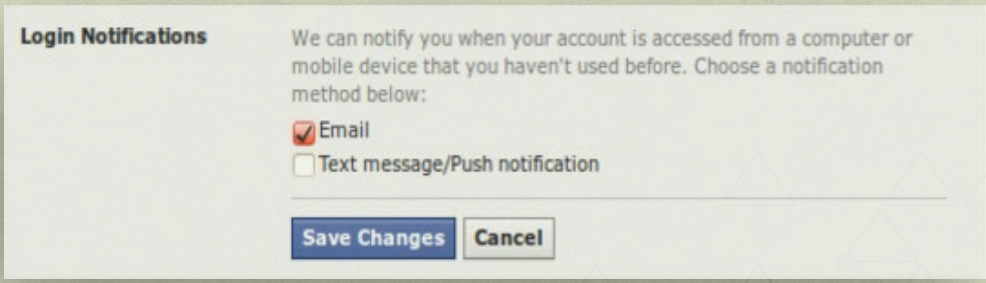
Click on Security in the menu on the left hand side. This will open the Security Settings page.



LOGIN APPROVALS

Click on **Login Notifications**. Here, you can choose to be notified if an attempt is made to log in to your Facebook page from a device which you have not used before. Choose whether to receive by **Email** or Text **Message/Push Notification**.

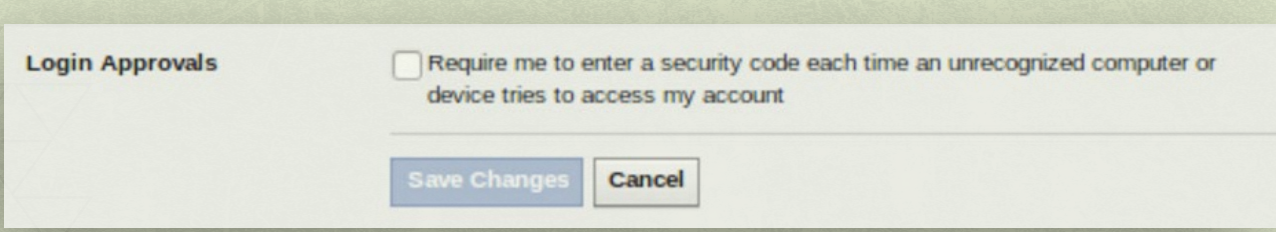
WARNING: If you choose to receive alerts via Text Message, this means you will link your mobile phone number to your Facebook account, making your activities on the site more easily identifiable.



LOGIN APPROVALS (TWO-FACTOR AUTHENTICATION)

For added security, you can choose to enter a security code every time your account is accessed from a computer or device **Facebook** does not recognise. The security code will be sent as SMS to your mobile phone.

NOTE: Enabling this option will make it more difficult for someone else to access your account unless they also have access to your mobile phone. However, as mentioned above, it also involves associating your mobile phone number with your **Facebook** account. You should consider the pros and cons of this for your own situation and make the choice that you consider more secure for you.

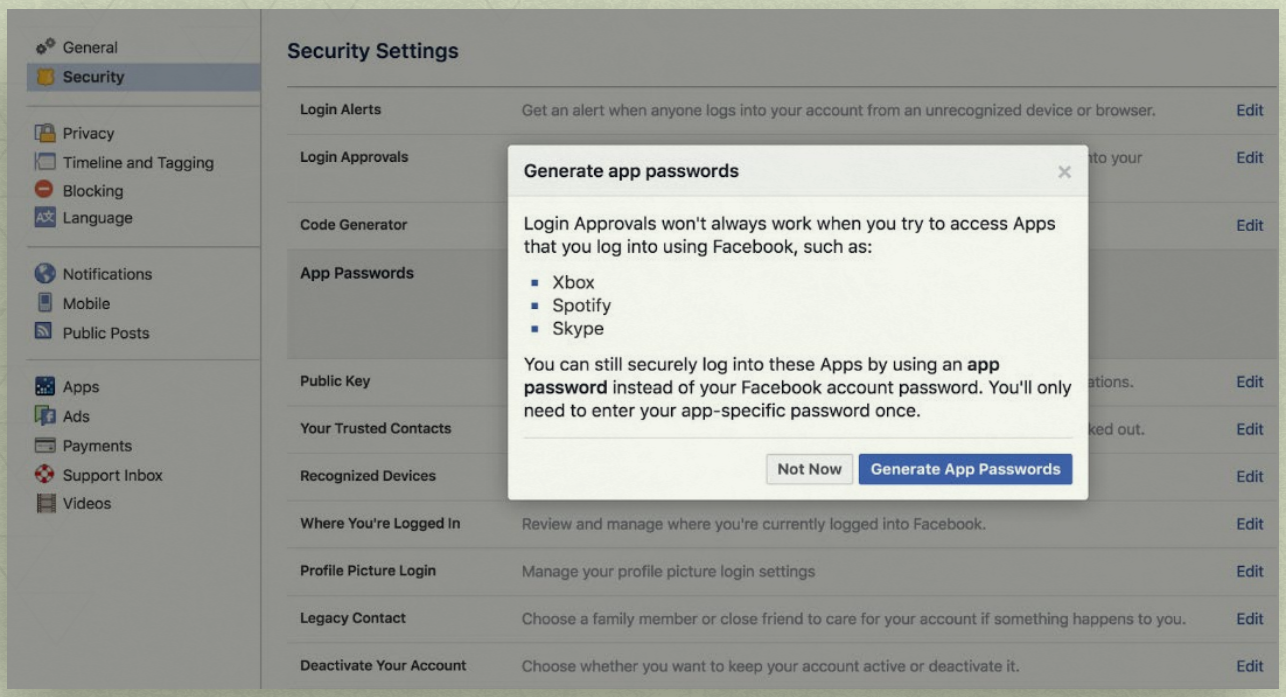


CODE GENERATOR

This setting allows you to use the **Facebook** mobile app on your smartphone in order to generate login codes or new passwords.

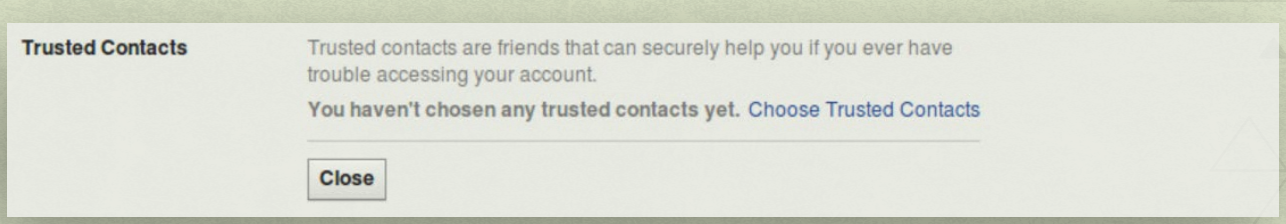
APPLICATION PASSWORDS

If you use applications on **Facebook**, this option allows you to generate individual passwords for them. Unless you have a specific need to do so. However, we recommend avoiding Facebook applications.



TRUSTED CONTACTS

This option allows you to select certain contacts from your **Facebook** friends who can help you to log-in to your account if for some reason you are otherwise unable to. This is done through sharing a secret code with your contact. If you decide to use this option, be sure to choose your trusted contacts carefully and establish a secure means of communication for sharing the code.



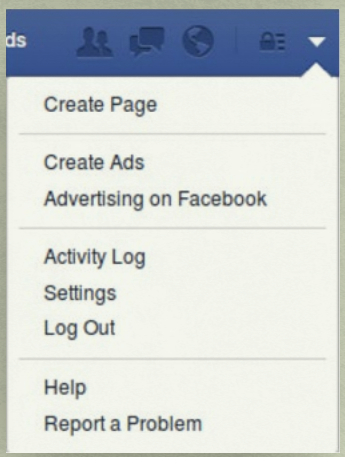
TRUSTED BROWSERS

Here you can review the browsers most frequently used to access your Facebook account.

ACTIVE SESSIONS

This shows details of any Facebook session that you may have forgotten to logout of—for example in an internet café, or a friend's computer—and therefore is still active. The location is determined by the IP address.

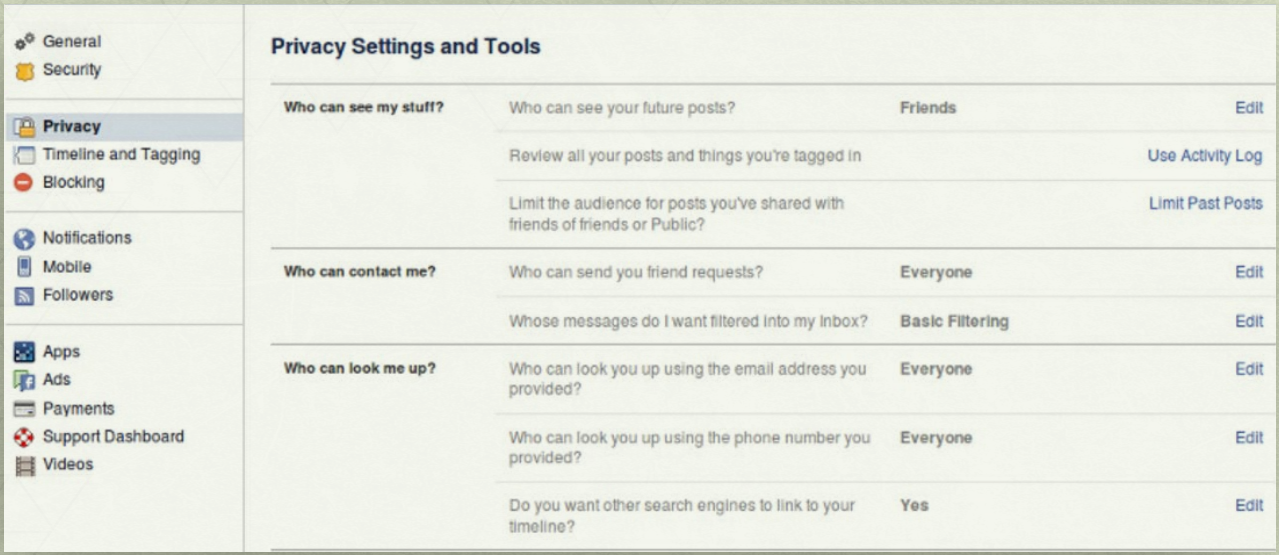
It is very important to close these sessions in order to prevent anyone else accessing your Facebook account, especially if you note any devices in the list which are not yours or you do not recognisze.



SPECIFIC PRIVACY SETTINGS AND TOOLS

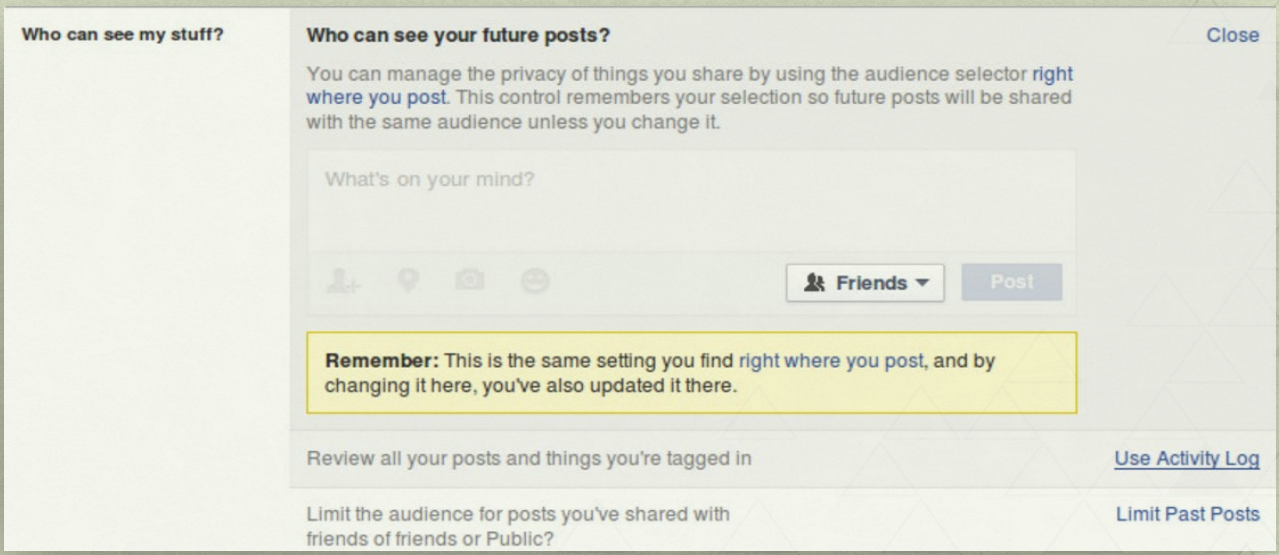
To edit your **Facebook** Privacy Settings, **click** on the small arrow beside Home in the top right-hand corner and select Settings.

- This will take you to the Settings menu. On the left-hand side, **choose Privacy**.

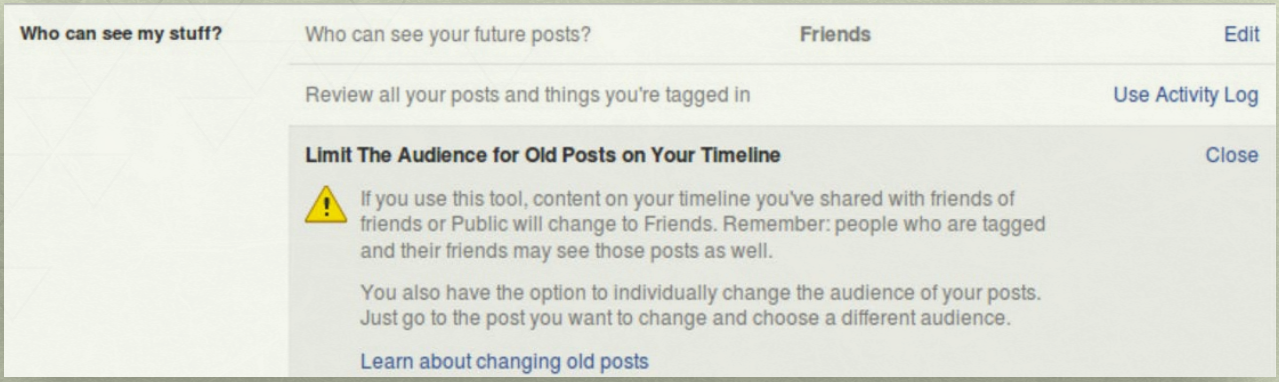


- **WHO CAN SEE MY STUFF?**
  The first option here creates a default rule for your future status updates: Who can see your future posts? Here, you can **choose** between making them available to the entire public, your **Facebook** friends, yourself only, or a custom group which you can determine. Note that you can also change this for individual status updates, so that you can decide which ones are public, which ones are for friends or which ones are for a specific group. It's also worth noting, though, **that everything you post is recorded by Facebook (including when you select Only Me) and can be handed over by them to third parties**.

- The second option allows you to **review** the posts which other **Facebook** users have tagged you in. To see this, **click** on Use **Activity Log**.



- The third option allows you to **restrict** access to previous status updates of yours which may have been public.

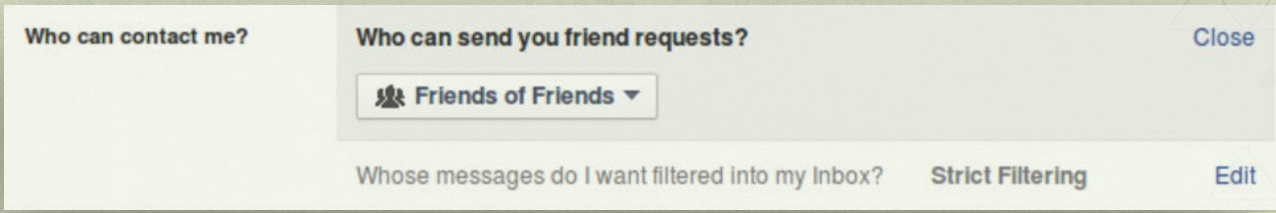


NOTE: However, the limitation that individuals you tagged and their friends will still be able to see this content.

WHO CAN CONTACT ME?

In this section, you can decide who is able to send you a friend request. This is not particularly important in terms of information security, since in the end, it is still you who decides who to accept as a friend, and you should always exercise caution and **avoid adding people who are unknown or untrusted**. If you want to change this setting, **click** Edit.

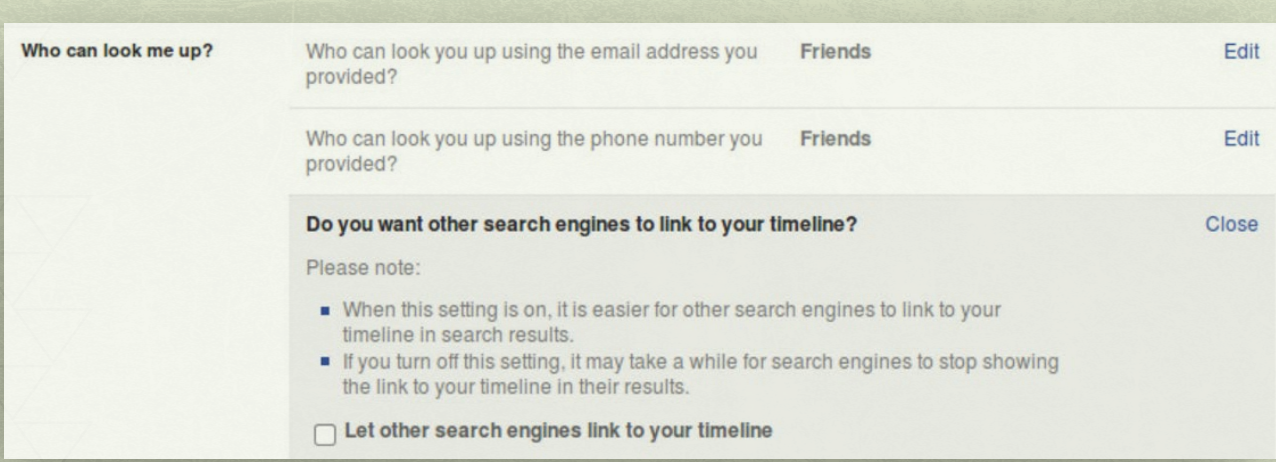
Whose messages do I want filtered into my inbox?: **Facebook** allows you to filter the messages you receive into two folders: **Inbox** and **Other**. Here you can **choose** between **Basic Filtering**, which is more permissive of messages from people who are not on your friend list, and **Strict Filtering**, which is less permissive.



WHO CAN LOOK ME UP?

Here, you can limit the ease with which people can look you up by knowing your phone number or e-mail address (although this is still technically possible), as well as limiting people's ability to find your **Facebook** page via search engines. FB's default settings make it as easy for individuals to find you this way, including possible adversaries.

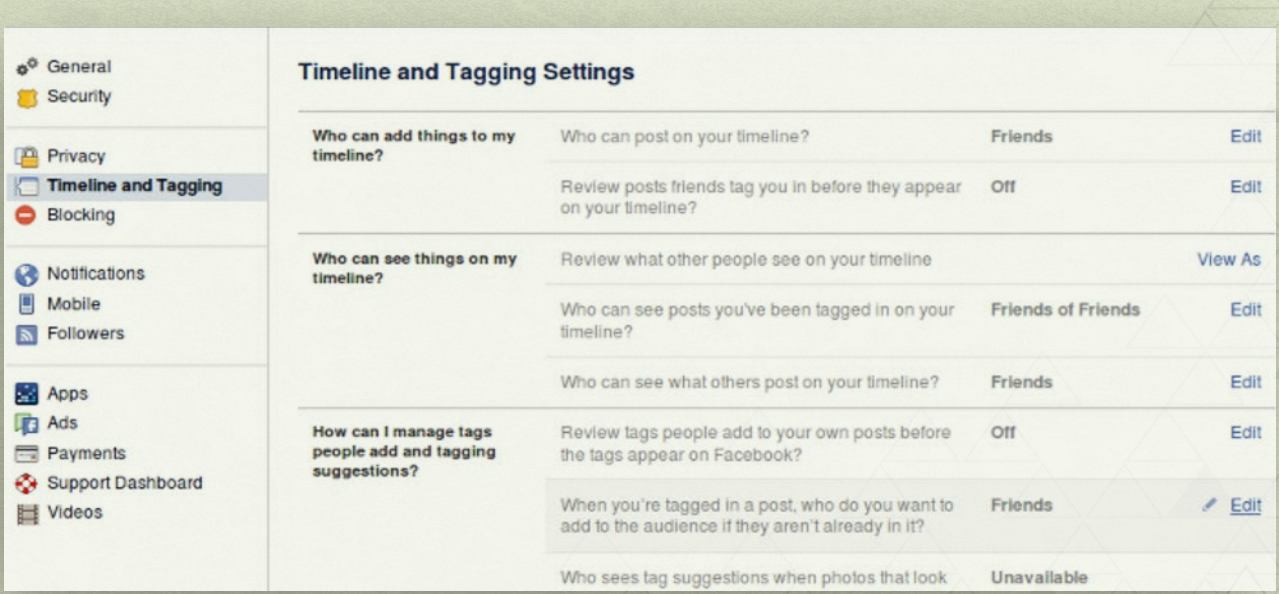
- ✓ Click Edit on the first two options and ensure that only Friends can search for you by your email address and phone number. For the third option, **click Edit** and **uncheck** the box which says Let other search engines link to your timeline.



TIMELINE AND TAGGING

As we have mentioned before, your information security on **Facebook** has a lot to do with the behavior of your friends. In the **Timeline and Tagging** menu, you can determine what happens when friends tag you or your posts and what happens when they post on your timeline.

- ✓ In the left-hand sidebar, **click** on the Timeline and Tagging menu.



If you want your timeline to be truly yours, it's advisable to **disallow** posts on your timeline from anyone but yourself. To do this, click edit beside **Who can post on your timeline** and select **Only Me**.

Here, you can decide what happens when other friends tag you in their posts and photographs.

- It is advisable that you **click edit** and **enable** the **Review posts that friends tag you in** option so that you can prevent any irresponsible tagging appearing on your timeline. However, this will not prevent their posts (including your tag) from being visible to their friends, or perhaps even the public, depending on their settings.

Who can add things to my timeline?	Who can post on your timeline?	**Only Me**	Edit
	Review posts friends tag you in before they appear on your timeline?	**On**	Edit

Who can see things on my timeline? This item is associated with the previous options. Previously, we've decided who gets to publish material to your timeline, and here, you get to decide who can read them.

- If you **click Edit**, you can change these settings so that either everyone, friends of friends, a custom group of people, or only yourself can see posts you've been tagged in, or things others post on your timeline.

The first option, **View As**, is an interesting way to see what certain individuals can see on your timeline.

Who can see things on my timeline?	Review what other people see on your timeline		View As
	Who can see posts you've been tagged in on your timeline?	**Only Me**	Edit
	Who can see what others post on your timeline?	**Only Me**	Edit

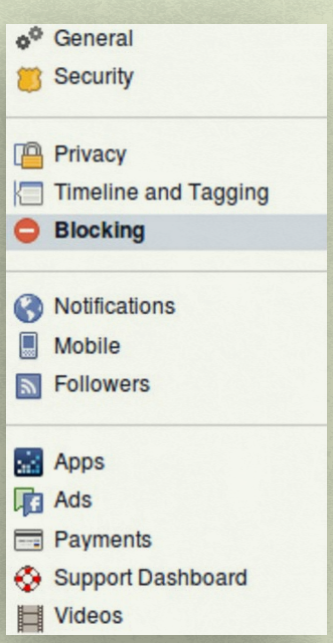
WARNING: When you see the warning sign, take note. These are important side notes that are meant to stress to avoid actions that could make you vulnerable or include actions that could keep you safer.

How can I manage tags people add and tagging suggestions? This refers to tags of you by other users of **Facebook**. It's best if you **switch on** the Review tags people add to your own posts before the tags appear on Facebook option, and limit the audience for the second option to Only Me. **Facebook** has begun using a form of **facial recognition** technology which allows it to identify

photographs that look like you among your friends and contacts photos. Facebook will even notify them to tag you. Naturally, for rights advocates, this could be particularly sensitive.

- It's strongly recommended that you **deactivate** this option if it is available to you.

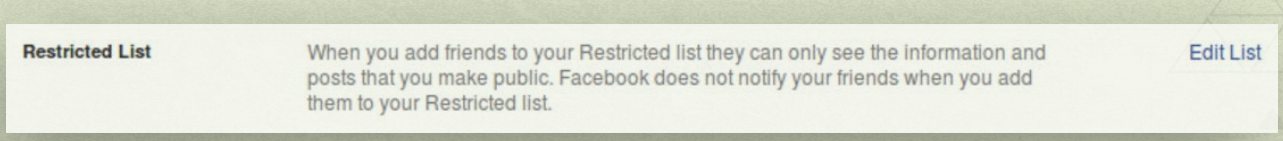
- **BLOCKING USERS AND APPS**
  In the menu on the left, **select Blocking**. Here, **Facebook** offers ample opportunities for blocking unwanted, intrusive, and sometimes potentially dangerous information.



RESTRICTED LIST

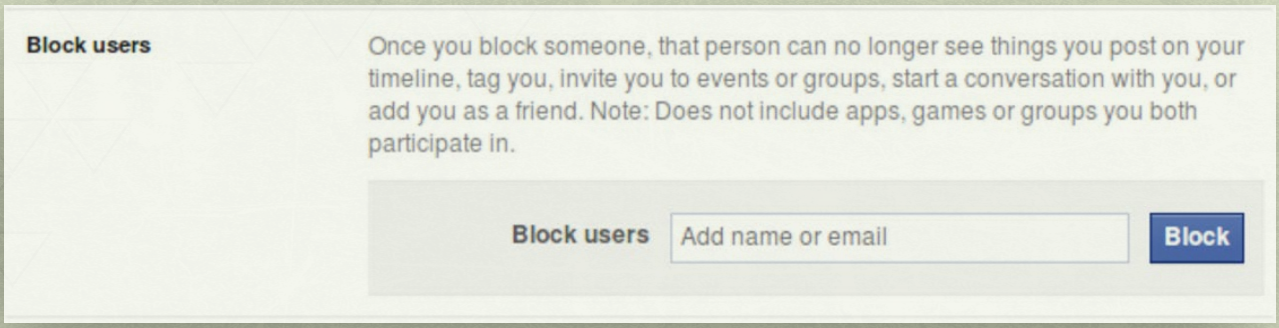
Here, you can discreetly add **Facebook** friends to a list which will limit them to only being able to view information you share publicly on your timeline (per the settings we explored above). To add friends to the list,

- **click Edit List**.



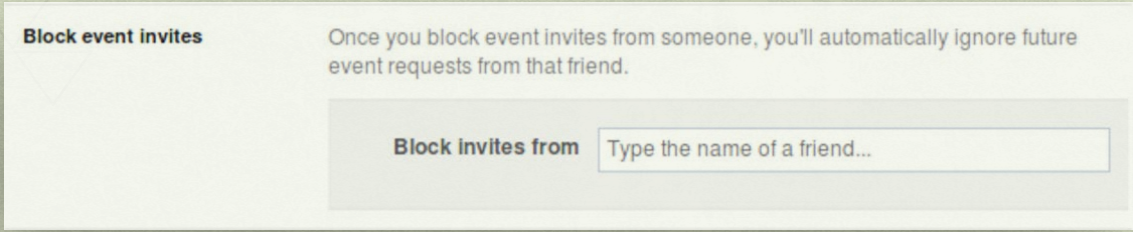
BLOCK USERS

Here you can block a user from accessing your **Facebook** page, any of your content, or adding you as a friend.



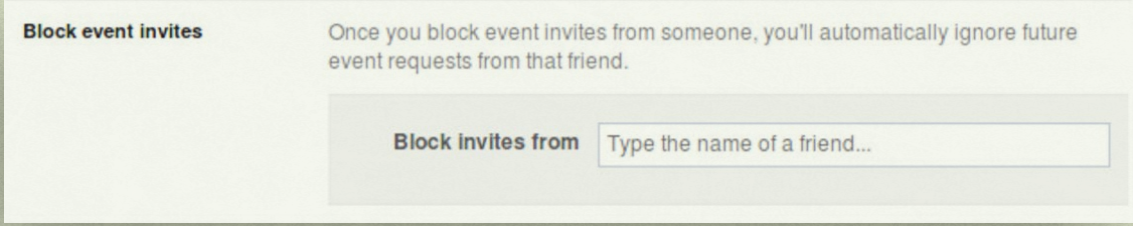
BLOCK APP INVITES

Often, we will have **Facebook** friends who are enthusiastic about a particular application, often a game, and they will continuously send us invites to join this game. Here, you can block application invites from such friends.



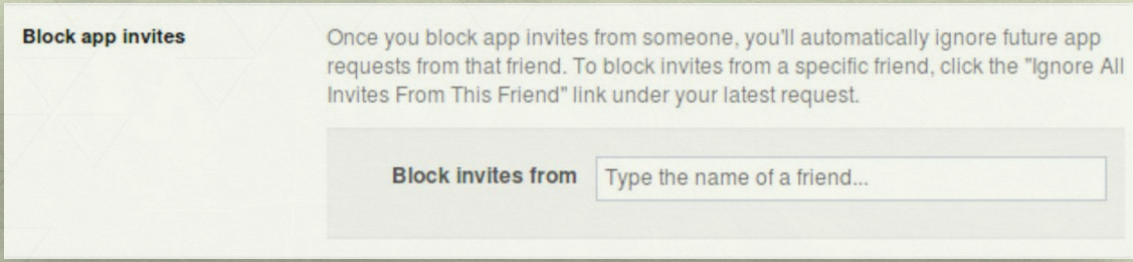
BLOCK EVENT INVITES

Similarly, here you can block invitations to events from certain **Facebook** friends.



BLOCK APPLICATION

As the name suggests, here you can prevent an application from accessing all but your public information.



FOLLOWERS

Facebook gives you the option of allowing people to subscribe to your news feed, without being friends. Be aware however, that if you allow others to subscribe to your news feed, then some of your data is available for them and others in their network to see. The safest option is not to allow people to subscribe to your news feed.

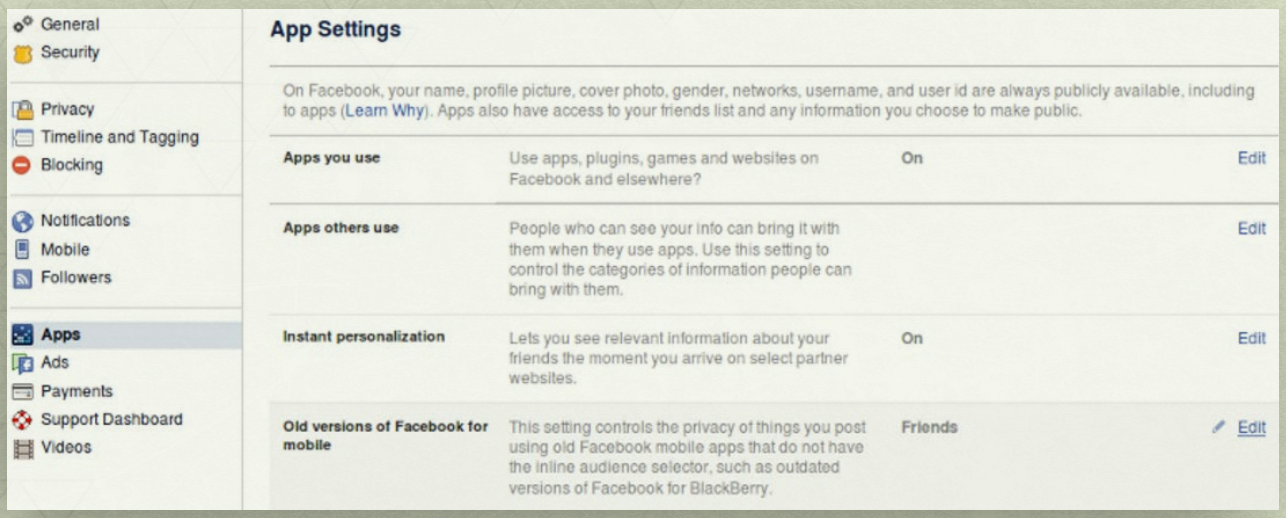
Click on Followers from the menu on the left. Ensure that Friends is **selected**.

FOLLOWER SETTINGS

Applications

Many Facebook users love and actively add third party applications in order to play games, enhance communications, and more. But keep in mind each application is associated with your Facebook account, and the basic data of your Facebook account will be available to any application (such as your name, gender, public pictures and network). Also, when installing a new application, it may ask for your permission to have access to information about you and your friends. This includes a variety of data, such as age, place of residence, education, circle of friends and contacts. Thus, the application can gather and share information such as what country you come from and where you currently are, information you may consider sensitive. Therefore, for safety reasons, we recommend not to use Facebook applications unless you really need to.

- Click on **Apps** in the menu on the left.

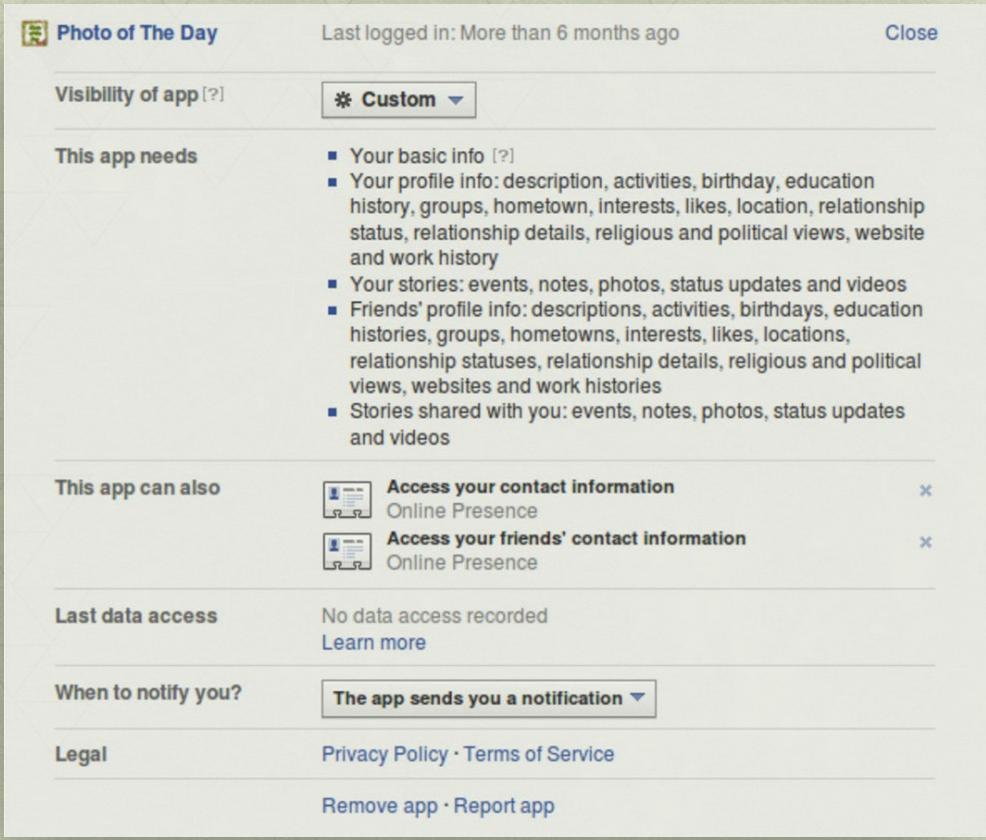


APPS YOU USE

Here, you can enable or disable the so-called "Facebook Platform" which allows you to quickly register and sign in on other sites using your **Facebook** account. This option is enabled by default. On the one hand, it's convenient: no need to spend time on registration forms, filling in fields. On the other hand, comments on news storys, or signed petitions can link to your **Facebook** account, where it's recorded and possibly shared.

- If using Apps is not important to you or your work, we recommended that you **click Turn Off Platform** in order to better protect your privacy. If you do decide to leave the option enabled, then pay attention to the list of applications already installed at this point. Do you really need them all?

- By **clicking** on an app you can see what information it has access to.

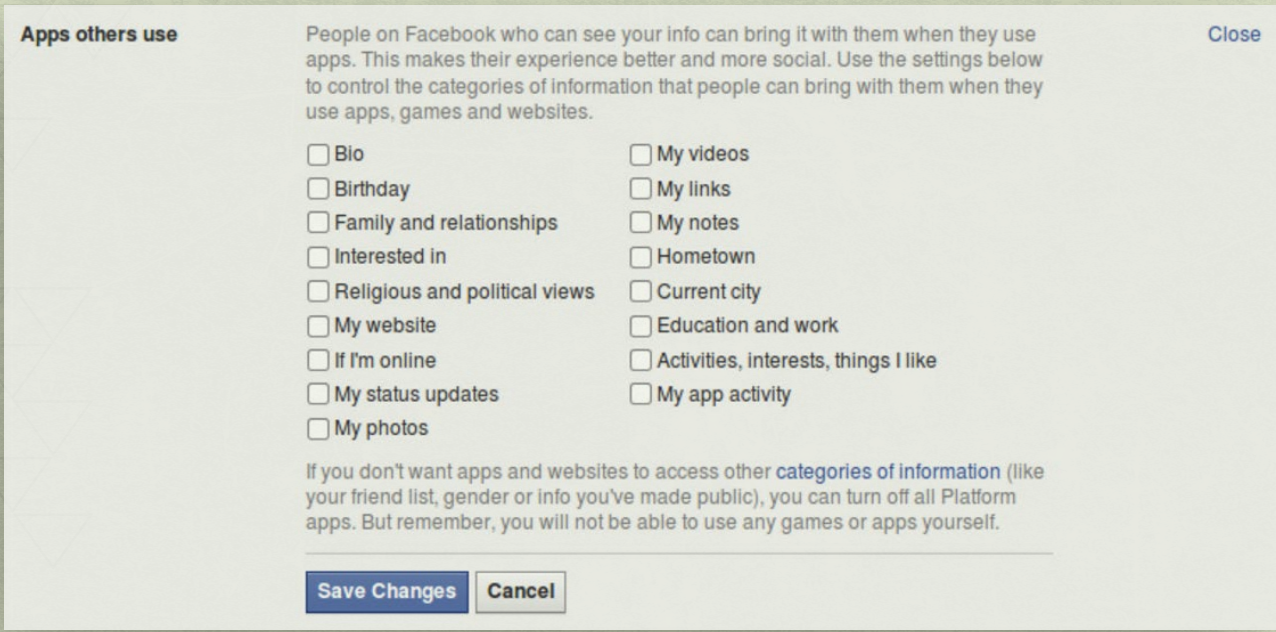


- To remove an application, **click on the 'x'** beside the app in the list, and then **click Remove** in the warning window which pops up.

APPS OTHERS USE

We also have to consider that some of our Facebook friends bring our information into the apps that they use.

- By clicking on **Apps others use**, you can uncheck the boxes beside categories of your information which you do not want to share with your friend's applications.



ADVERTISING SETTINGS

Advertising is fundamentally important to social networking companies because it's how they make their money. There will always be advertisements on social networking sites such as Facebook, though we can make them less personal, which is the right move in terms of information security and privacy.

- In the column on the left, select Ads.

Facebook currently promises not to associate your name or picture with third-party advertisements, although they leave space for this to be possible in the future. It's a good idea to change these settings so that your details still remain private in case advertising rules change in the future.

✔ Click Edit beside Third Party Sites. Select No-one and select Save Changes.

Third Party Sites

Facebook does not give third party applications or ad networks the right to use your name or picture in ads. If we allow this in the future, the setting you choose will determine how your information is used.

You may see social context on third party sites, including in ads, through Facebook social plugins. Although social plugins enable you to have a social experience on a third party site, Facebook does not share your information with the third party sites hosting the social plugins. Learn more about social plugins.

If we allow this in the future, show my information to

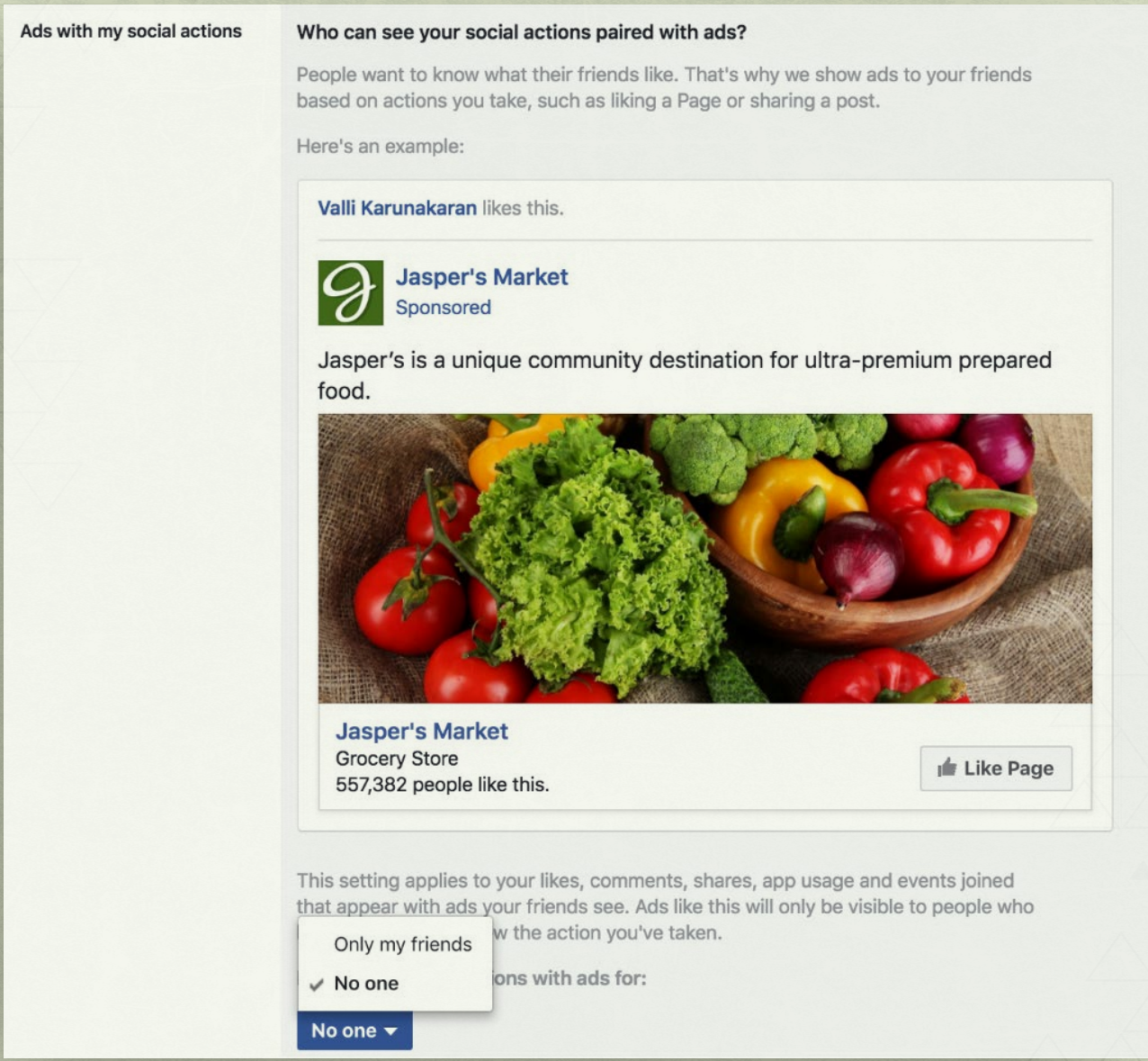
No one

Save Changes | Cancel

SOCIAL ADS

Here, **Facebook** encourages users to become ambassadors for products or pages they have 'liked'. This means that you could be used to advertise a page or product to your friends. If this makes you uncomfortable, it's recommended that you disable it.

✔ Under Ads and friends, **click Edit** and **select No-One** from the drop-down menu.



By default **Facebook** tries to display targeted advertising on your tastes and interests.

✔ To get rid of this, you need to **click** on the **Opt Out** link in this paragraph.

Website and Mobile App Custom Audiences

One of the ways that a company can reach you is to ask Facebook to show you ads that are customized based on what you do on that company's websites and apps off Facebook. For example, Facebook may show you ads, on and off Facebook, announcing the release of a new album by your favorite band after you visit that band's website.

When you use Facebook from a web browser, you can find out why you saw an ad and how you can control it by choosing "About this ad" from the menu that shows with the ad (usually found by clicking on the "✕" or "⌄" in the upper right corner of the ad).

- Learn more about how Facebook uses cookies and similar technology for advertising
- Opt out of ads that are selected for you by Facebook based on what you do on a particular company's websites and apps off Facebook
- Learn more about how other companies do this on and off Facebook and how you can control ads through the Digital Advertising Alliance (DAA): Canada, Europe, or other locations

This will open a page titled **Custom Audiences** from your **Website and Mobile App**, where Facebook gives more information about its advertising policy.

✔ In the middle of the text is the Opt Out button for you to confirm.

WARNING: Changes made to this setting are not recorded by Facebook, but rather are stored in your browser. Unfortunately, you must repeat this process for every contact, call, and device you use to connect to Facebook.

How can I stop seeing these ads?

If you don't want Facebook to show you ads based on your activity on an advertiser's websites or apps, opt-out below:

Opt out

After a request for confirmation, you will see the result:

✔ You have successfully opted out.

Opt in

TWITTER

Twitter[35] has become a valuable platform where activists around the world break their stories and ideas. It's become a place for, real on the ground news updates on movements and protest, where the oppressd have a voice and are able to connect with people in a real and powerful way.

Twitter states in its terms of service: "*This license is you authorizing us to make your Tweets available to the rest of the world and to let others do the same. But what's yours is yours—you own your content.*" While this may be the case, Twitter reserves the right to hand over your information to governments should a request be made.

Keep in mind, **Twitter is actively monitored by numerous governments**, including the United States. Moreover, Twitter's Terms of Service state that they **will share your information in response to legal requests including governmental investigations**. For more information, see Twitter's Privacy Policy and its Transparency Report.

Although it's a website, many people interact with and manage Twitter via desktop and smartphone applications that are known as Twitter clients. If you use a client you should make sure it is connecting to the site securely, over an encrypted connection.

Like Facebook, many people use Twitter in conjunction with numerous other websites and applications in order to share status updates, photos, locations, links, and so forth. Using these applications pose many potential additional security vulnerabilities, and it is very important that the privacy settings on all other applications are made as secure as possible.

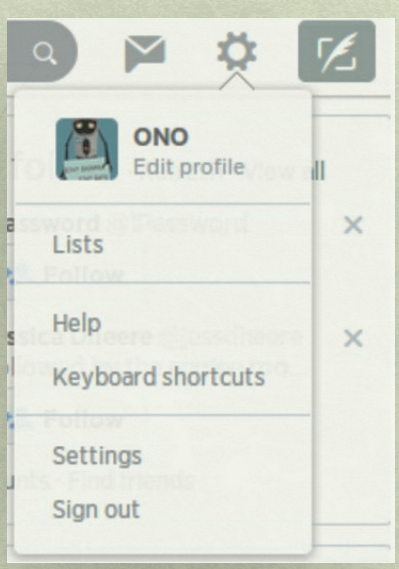
Read on to understand how better to secure your Twitter!

BASIC ACCOUNT SETTINGS ON TWITTER

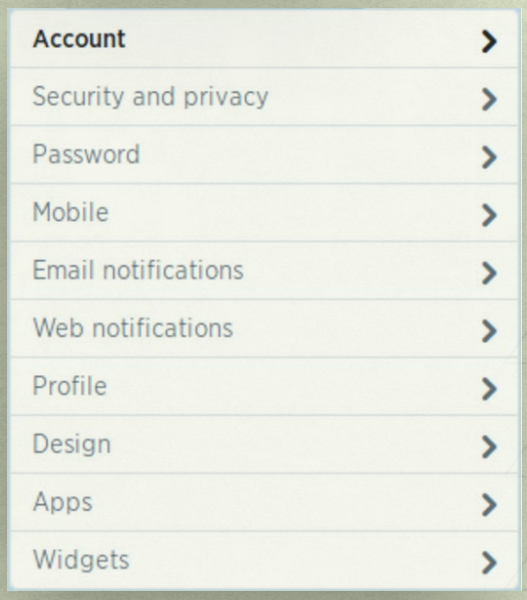
Twitter's Basic Account Settings allow you to control how people can find your profile, what information you share and the level of security your account requires when you are using the web-browser based version of **Twitter** (that is to say, not a client, smartphone app, or GSM phone).

[35] https://securityinabox.org/ru/twitter_main

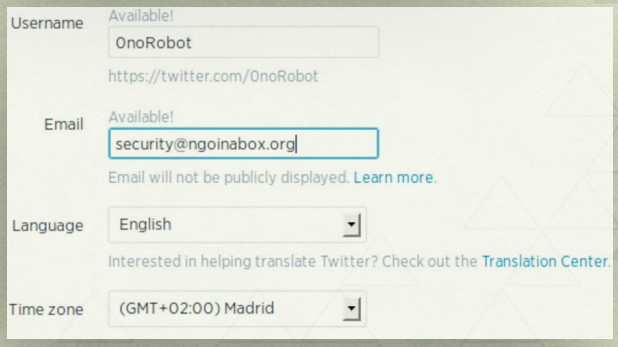
- In order to access your account settings, log in to your account using your browser and click on the icon at the top right of the screen to open the **Options** menu



- In the drop-down menu, choose **Settings**. This will open the settings page. You will find a list of pages on the left-hand side where you can click between various categories of settings.



- At the top of the Account Settings list, you will find the username and e-mail settings. **Choose carefully whether you want to use your real name or a pseudonym as your username**, and which email address you wish to associate with your profile. It may be best to set up a new e-mail address using the Tor Browser and connect to **Twitter** only using **Tor** if you wish to protect your **identity**.



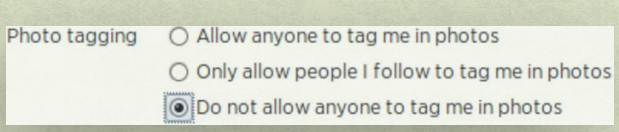
SECURITY AND PRIVACY SETTINGS ON TWITTER

Click on **Security and privacy** in the left-hand sidebar in order to access the Security and Privacy settings page.

Twitter gives you the option of sending a message to your mobile phone or smartphone any time your account is accessed. This is recommendable if you are also using the Twitter application on your smartphone. In this case, choose the **Send login verifications to the Twitter app** option.

WARNING: While this may be useful in alerting you to an unauthorized attempt to access your account, associating your mobile phone to your Twitter account makes your account more easily identifiable and is not advisable if you want to use Twitter anonymously or with a pseudonym.

In the photo-tagging section, Twitter allows you to control who, if anyone, can tag you in photos they upload. Since there is no option to approve or disapprove tagging in photos, it's advised that you choose the option **Do not allow anyone to tag me in photos. This is particularly important in cases where you may be photographed during protests, for example, which could later be used as evidence.**



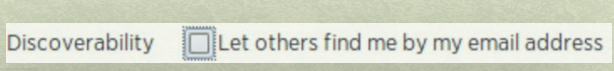
Twitter allows you to control who can see your tweets: the public in general, or only individuals who you allow to follow you.

Go to **Tweet Privacy settings**. Choose the **Protect My Tweets** option.

WARNING: Even if you choose the **Protect my Tweets** option, they are still accessible to Twitter and therefore can still be recorded and handed over to third parties.

Twitter also gives you the option of adding a location to your tweets under the **Tweet Location** option. This option is disabled by default. If sharing your location widely is appropriate in order to stay safe, then this option may be useful. However, it is generally **recommended that you leave this feature disabled** as your location information can also be very useful to your adversaries.

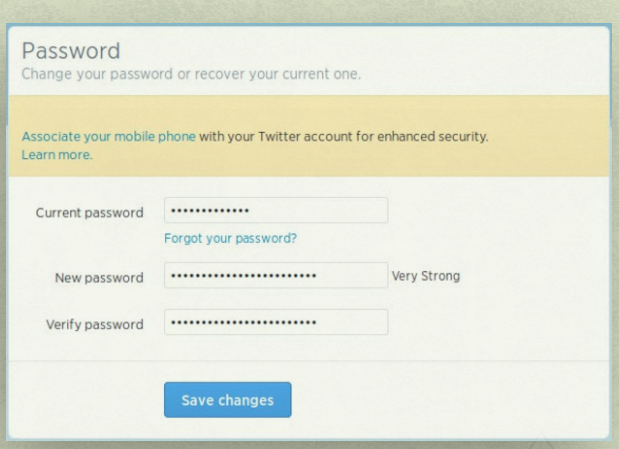
Discoverability gives you the option of allowing people to find your Twitter account if they already have your e-mail address. If you wish to maintain more privacy for your Twitter account, it's recommended that you disable this option.



In the **Personalization and Promotion** section, Twitter gives you the option of allowing them to monitor your behavior on their site and other websites. This allows them to tailor the content and ads they show you, which are selected based on you interests. It also helps them know which third parties might be interested in buying information related to your consumer behaviors and hobbies. It is recommended that you uncheck these boxes for more privacy.

PASSWORD SETTINGS ON TWITTER

Here, Twitter allows you to change your password. It's recommended that you select a strong, memorable password and update it regularly. For more, see section on "How to create and maintain strong passwords." Page 71



NOTE: The pencil sign denotes important details that often will provide important background to comprehending the section at hand.

MOBILE SETTINGS ON TWITTER

You can open Twitter's mobile settings by clicking on Mobile in the menu on the left-hand side. Here, Twitter encourages you to download the smartphone app and also gives you the option of activating Twitter text messaging, which allows you to tweet directly from your mobile phone. **As noted above, it is not advisable to associate your Twitter account to your mobile phone if you wish to maintain a degree of privacy or anonymity while tweeting.** Also, remember that **text messages sent over the GSM network are not encrypted and are easily interceptable and traceable to their authors.**

GENERAL GUIDELINES ON CLIENTS AND APPS

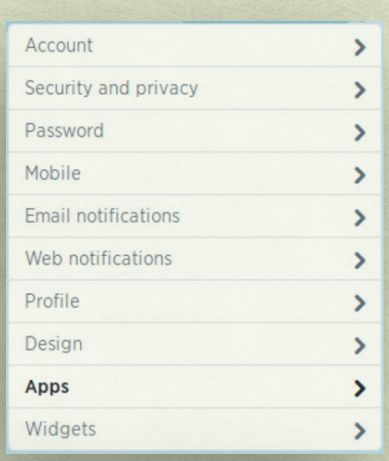
Twitter users can allow various third-party applications, including other social networking and photo-sharing sites to interact with their **Twitter** accounts, for example in order to share photos uploaded via websites such as **Instagram**, or **TwitPic.**[36] However, data when using social networking sites you must be careful when integrating your profiles on different social networking

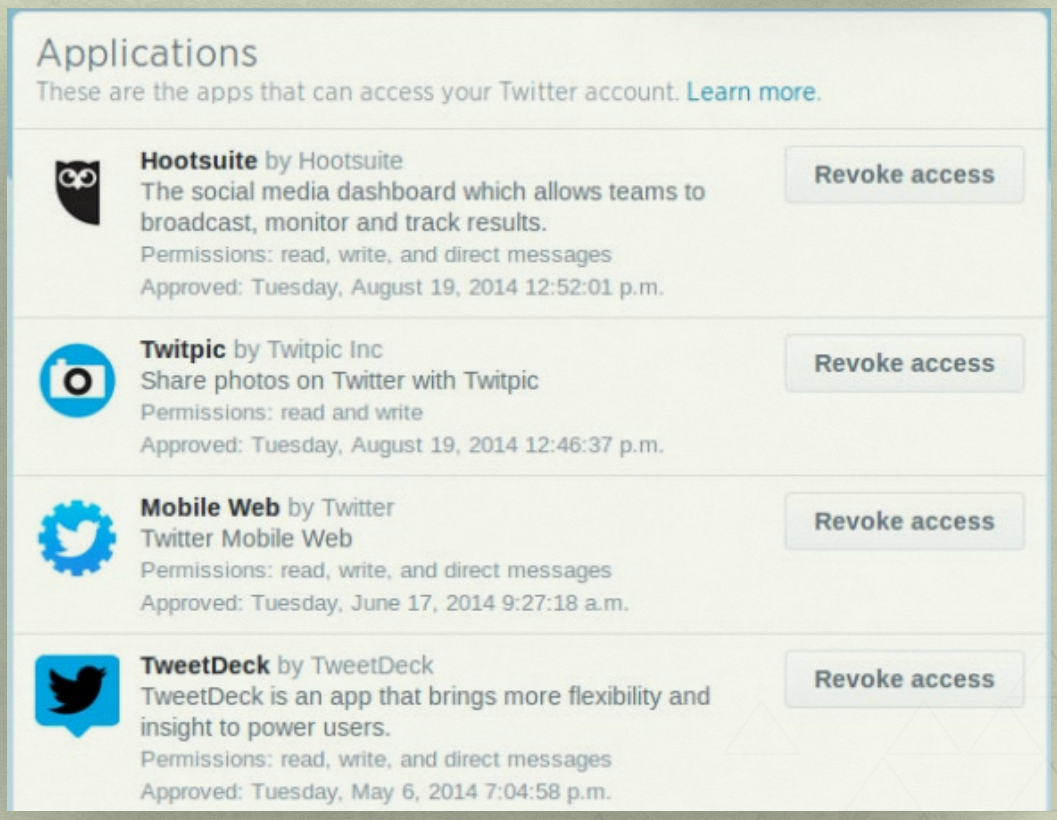
[36] https://securityinabox.org/ru/twitter_clients#2.0

sites. These third-party sites have their own terms of use, privacy policies and privacy settings which are not necessarily the same as Twitter's. Even if your **Twitter** account is relatively secure, your profiles on a third-party app/website may be completely exposed. Using the same username for multiple sites and accounts can make it easier for you to be tracked, using different names decreases that risk. The number of third-party sites and apps are vast, and only a few are explored in this guide. However, it is vital that you research and update your security settings on all third-party apps linked to your **Twitter** page. If you do not consider them secure enough, delete your profile and revoke its access to your **Twitter** account.

- Should you wish to revoke the access of an application to your Twitter profile, go to **Settings** of your account and click the **Apps** tab on the left-hand side.

  Having opened the list of apps connected to your Twitter account, select the app to which you wish to revoke access, click Revoke access





INSTAGRAM

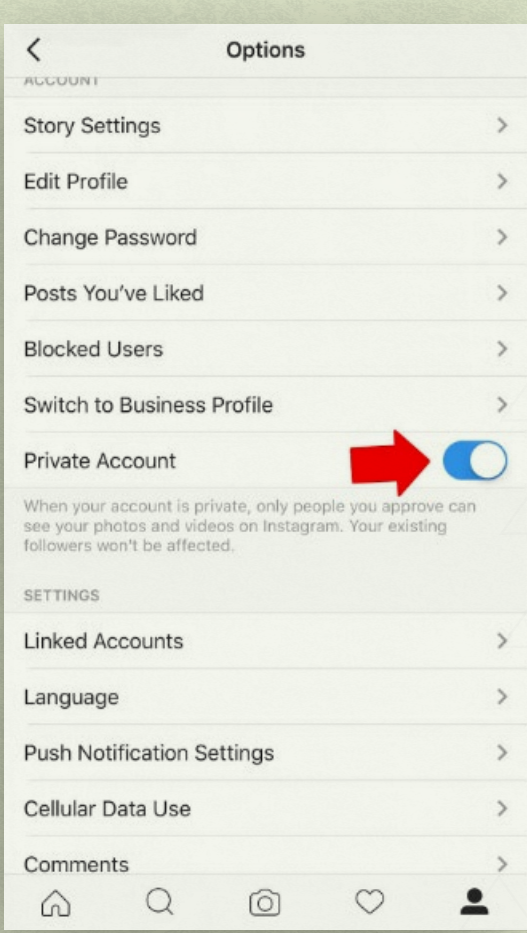
Instagram[37] is a popular image-sharing smartphone application which belongs to **Facebook** and is often used in conjunction with **Twitter**. Since it is primarily a mobile application that is also owned by Facebook, using Instagram with Twitter and Facebook associates your account to your mobile device, which can mean a lot of information and metadata on your phone can be shared between these platforms all of whom can then share them with the state. It is not recommended that you use Instagram if you are concerned about sharing your location and other personal details.

By default, anyone can view your profile and posts on Instagram, you can make both private which grands access to followers that you have approved or that were following you before you made your accout private. If your posts are set to private, only your approved followers will be able to see them in the Photos tab of **Search & Explore** or on hashtag or location pages.

To set your posts to private from the Instagram app:

IPHONE OR WINDOWS PHONE

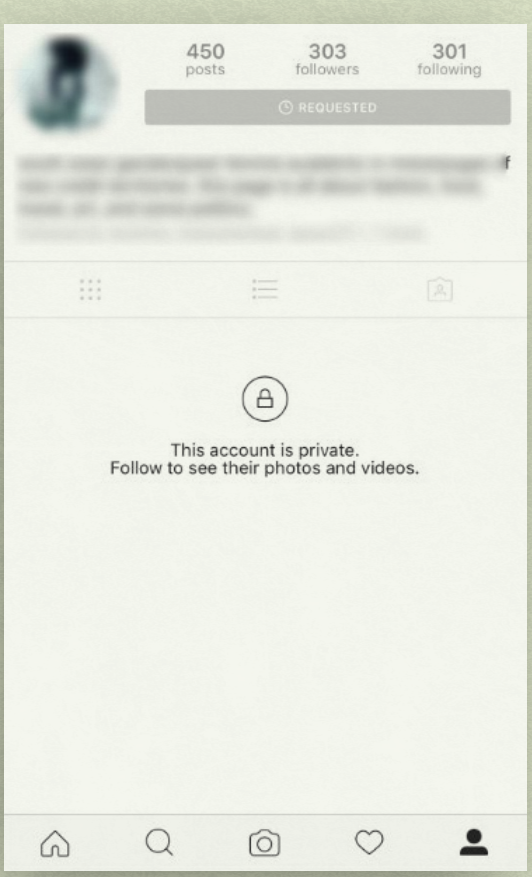
Go to your profile by tapping
Tap
Turn on the **Private Account** setting



[37] https://help.instagram.com/116024195217477/

ANDROID

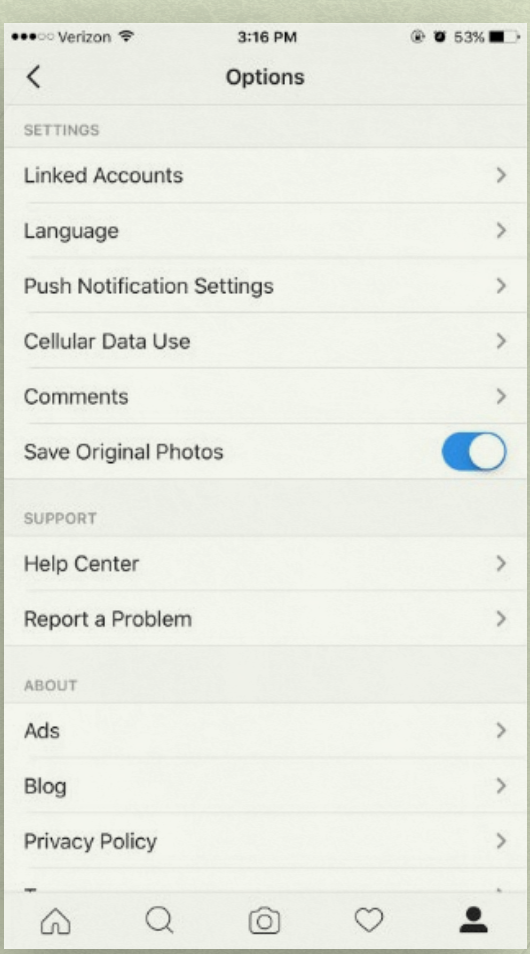
Go to your profile by tapping
Tap ⋮
Turn on the **Private Account** setting



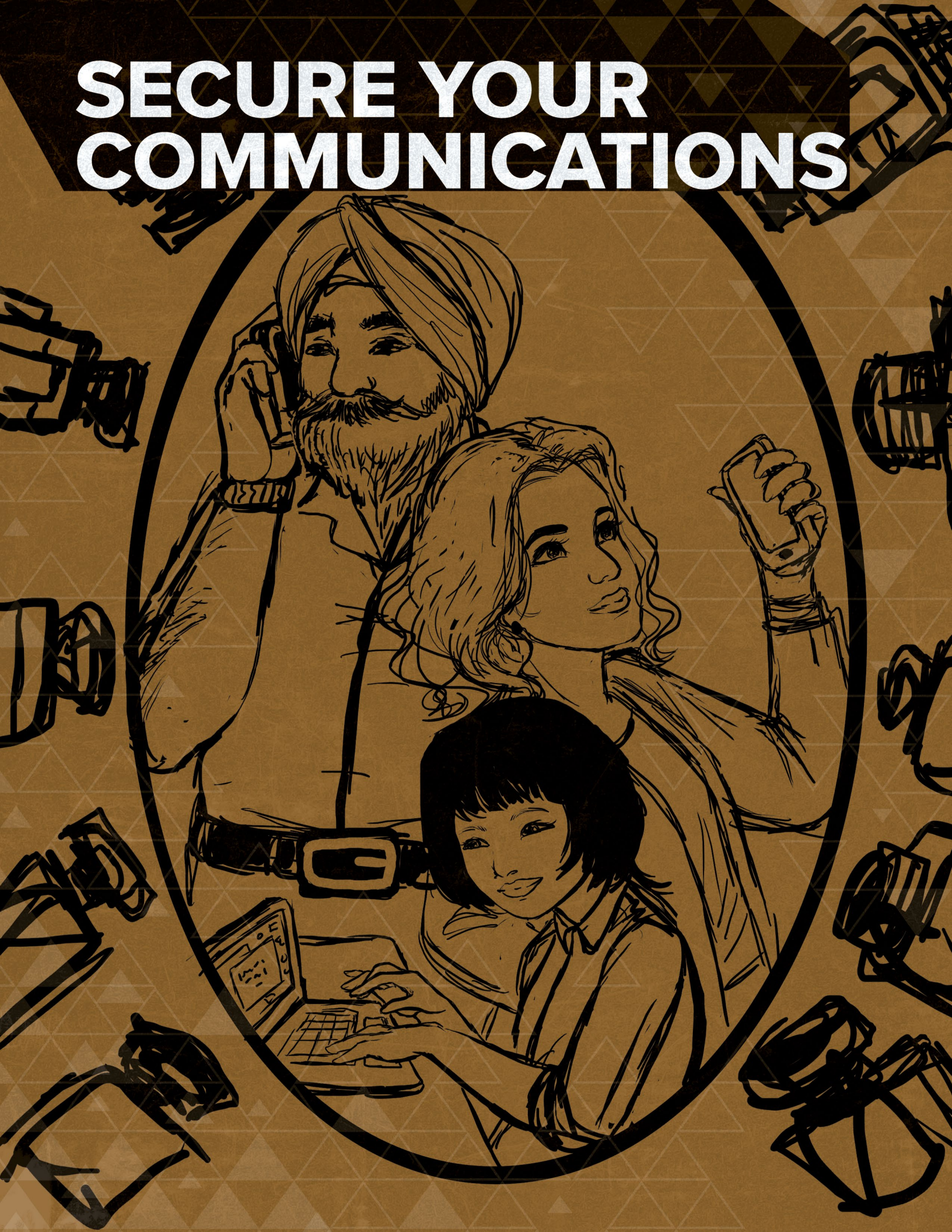
Things to keep in mind about private posts:

- Private posts you share to social networks may be visible to the public depending on your privacy settings for those networks. For example, a post you share to Twitter that was set to private on Instagram may be visible to the people who can see your Twitter posts.
- Once you make your posts private, people will have to send you a follow request if they want to see your posts, your followers list or your following list. Follow requests then appear in **Activity**, where you can approve or ignore them.
- If someone was already following before you set your posts to private and you do not want them to see your posts, you can block them.
- People can send a photo or video directly to you even if they're not following you.

- Under settings in instagram, go to **Linked Accounts** and de-link any other accounts associated.



SECURE YOUR COMMUNICATIONS



ENCRYPTION: THE PATH TO SECURE COMMUNICATION

Digital communications is the backbone for all of our organizing work. Whether it's phone, text, whatsapp or facebook messenger we are constantly in communication with each other, our families, and our movements.

The problem is that almost all of these forms of communications are easily surveilled. We must maintain habits that safeguard the data shared when collaborating or working with other communities, activists, and each other. Encrypted communication protects our right to privacy when the laws and corporate platforms do not.

That is where **End-to-End Encryption Messaging (E2EE)** comes in! E2EE is designed to keep eavesdroppers out of the conversation. Think of it as putting a seal on the users' messages, especially as they travel across the social web, and only the sender and recipient have the tool to break open this seal. Even companies that own the messaging platform would not have the means to decrypt the files.

While many apps say they offer E2EE, we give Signal our highest recommendation because they store the least amount of data and was developed by progressive developers to explicitly protect the right to privacy.

WhatsApp, Facebook, and Apple Imessage all offer some form of E2EE but these corporations still monitor and share the content of your data while not being transparent about what

they would share with a government agency if you are targeted.

Sometimes these platforms may be the only way to reach people. Implement Signal where possible but if you must use these other tools only do so when necessary. We highly recommend you practice resk reduction by enabling encryption and verifying contacts.

Finally, we want to emphasize that digital communications still comes second to face to face meetings. However, we do realize this may not be possible for many collaborations. So, ultimately, we emphasize that the best security is **discretion**. If you have things you want confidential then do not say them on communication platforms. Say only what you feel comfortable having a government official knowing because you do not know when your communications might be compromised.

SO PLEASE BE SAFE AND BE STRATEGIC IN WHAT YOU SAY, WHOM YOU SAY IT TO AND WHEN.

Now let's explore then how to send End-to-End Encryption Messages on each of these platforms.

SIGNAL

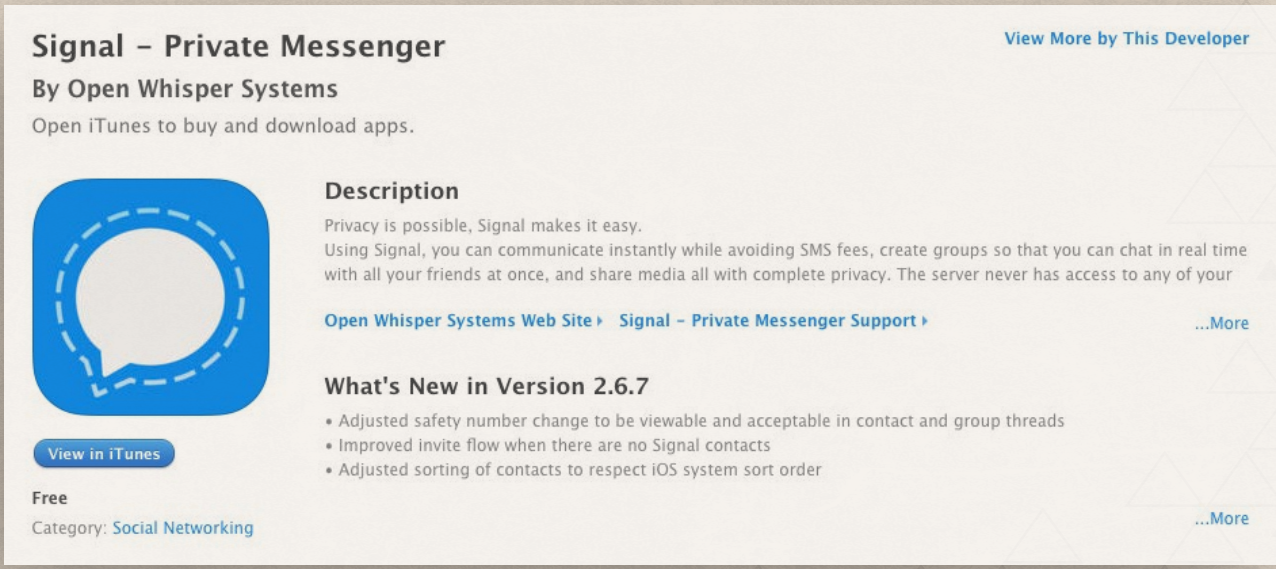
Signal[38] is a free and open source communication app for Android and iOS that employs end-to-end encryption, allowing users to have encrypted conversations with other Signal users and send end-to-end encrypted texts, group texts, photos, and video messages. Signal uses your data connection, so all parties in a Signal communication must have internet access on their mobile devices. **Signal users don't incur SMS and MMS fees**.

You can download Signal as an app on your phone or use it as a browser extension on your computer.

SIGNAL FOR ANDROIDS AND IPHONES

When you search for the app on your mobile device, make sure to select the version developed by Open Whisper Systems. Download the app, then click Install. You'll see a list of functions, such as TK, that Signal needs to access in order to work properly.

- ✓ Click **Accept**. After Signal has finished downloading, click **Open** to launch the app.

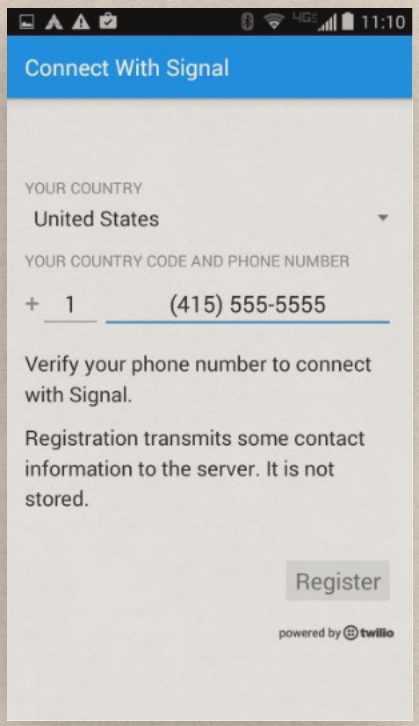


[38] https://ssd.eff.org/en/module/how-use-signal-android

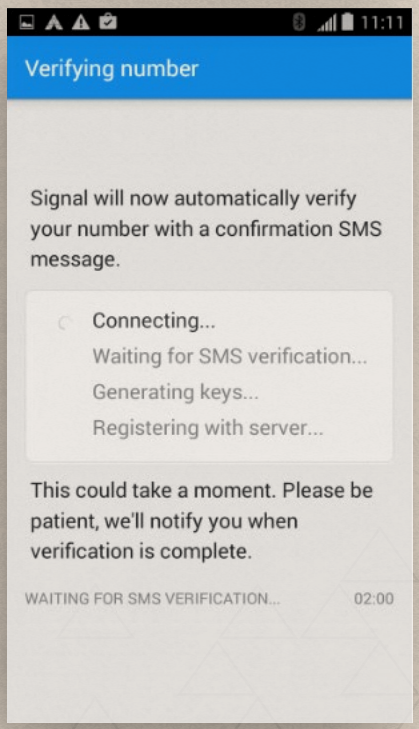
NOTE: The guiding screenshots here are from an Android phone but the procedure is similar for iPhones.

INSTALLING SIGNAL AND REGISTERING YOUR NUMBER

Register and verify your phone number. You will see a screen that looks like this:

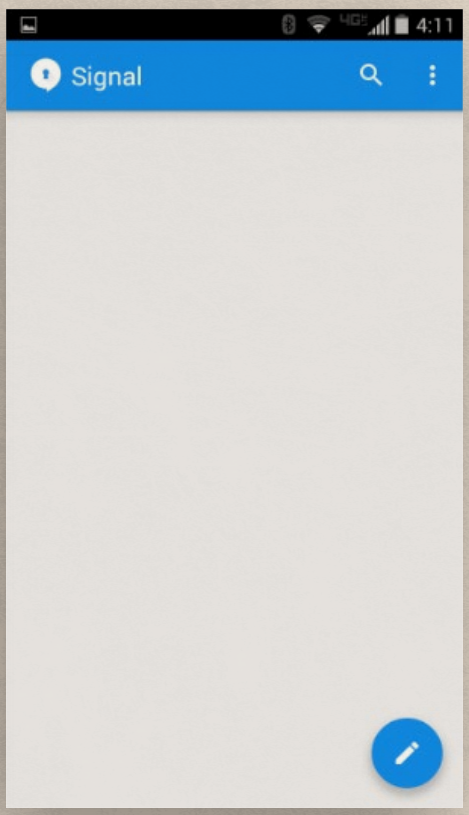


Enter your mobile phone number and click **Register**. In order to verify your number, you will be sent an SMS text with a six-digit code. Since Signal can access your SMS text messages, it will automatically recognize when you've received the code and complete your registration.

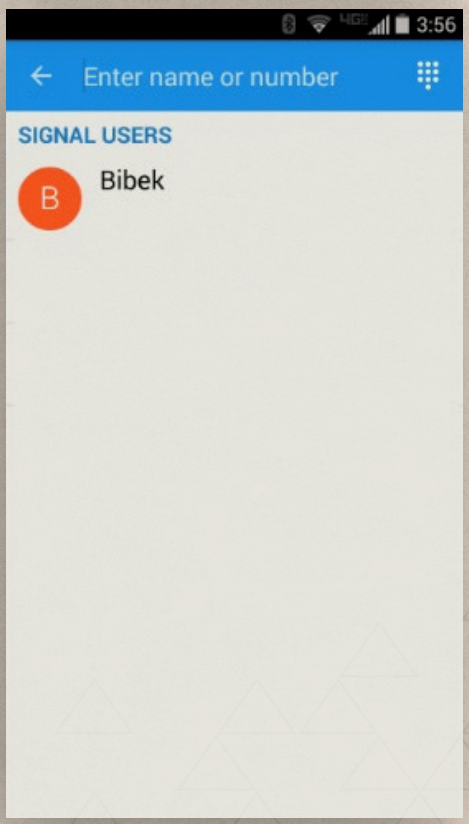


MAKING PHONE CALLS USING SIGNAL

In order to use Signal, the person you are contacting must also have Signal for Android or iOS installed. If you use Signal to send a message to someone who does not use the app, it will send a standard, non-encrypted text message. If you try to call the person, it will place a standard phone call. To get started, click the pencil icon in the lower-right corner of the screen.

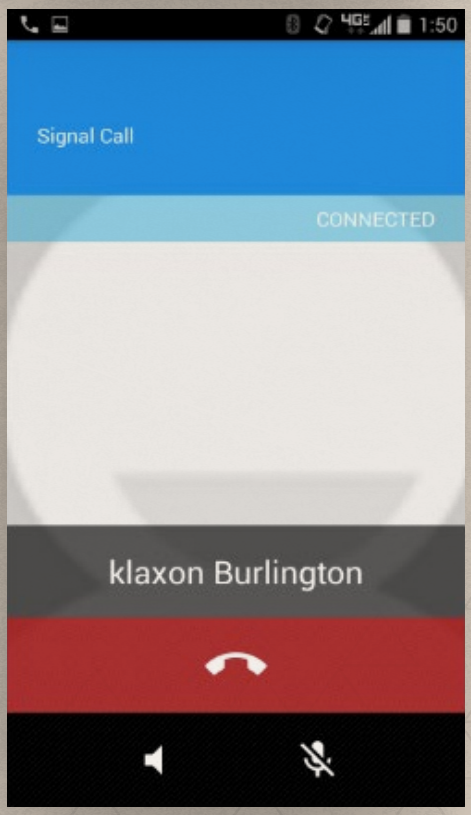


You will see a list of all the registered Signal users in your contacts. You can also enter the phone number of a Signal user who isn't in your contacts. When they are selected, you can choose to either call them or send them a message.



- To initiate an encrypted call to a contact, first check to see that the person can accept Signal calls. Select the contact from your list, then look for a small padlock icon next to the phone icon. Click the phone icon to initiate a call.

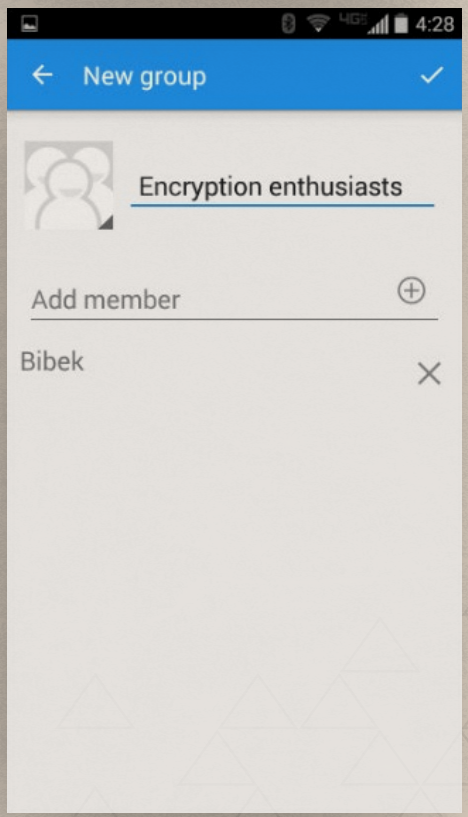
- The most trustworthy way to verify a caller's identity is to use out-of-band verification ⓘ to verify the **word pair**. You can also read the words aloud if you recognize the caller's voice, although very sophisticated attackers might be able to defeat this. The word pair must be identical on both users' phones for you to be sure your message is not being intercepted.



SENDING ENCRYPTED TEXTS

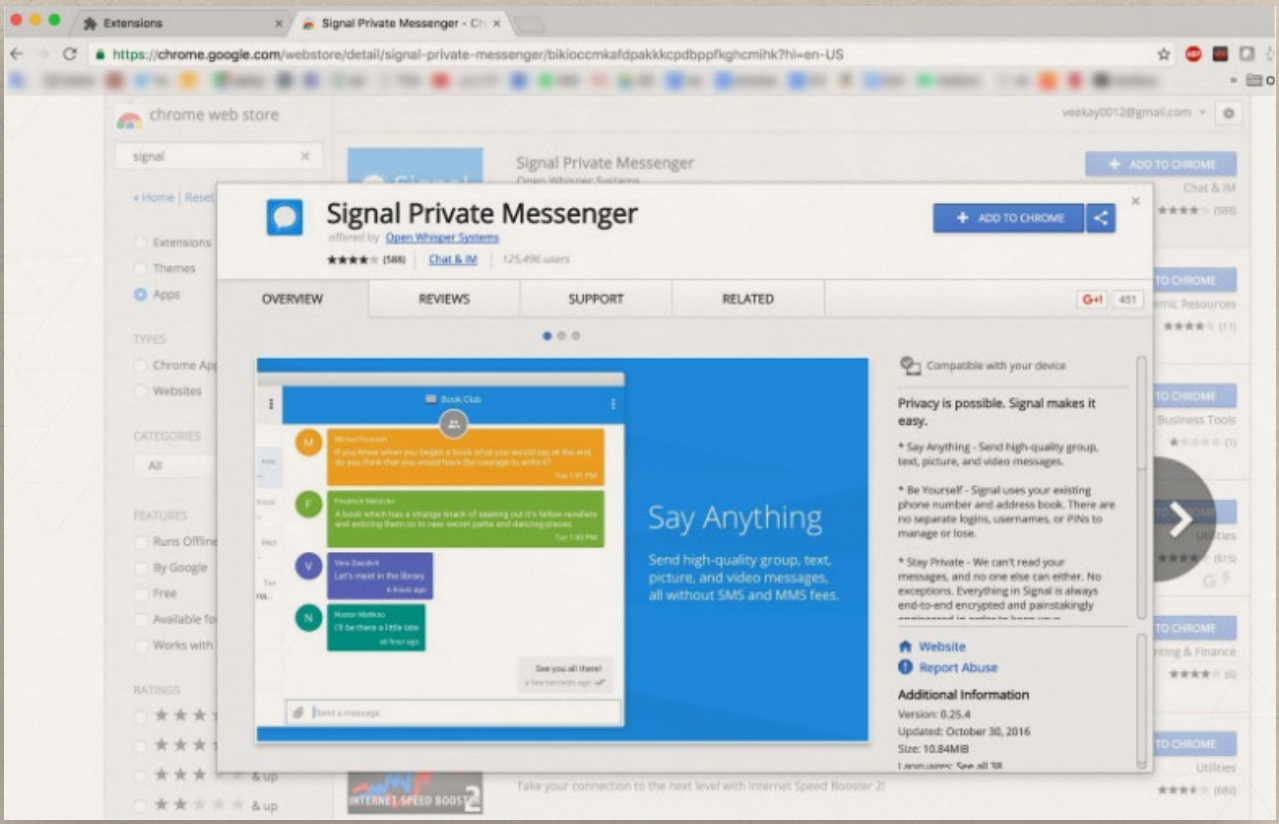
In order to send an end-to-end encrypted text, picture, or video message, navigate to your contact list, click on the contact's name, and send your message.

You can send an **encrypted group message** by clicking the overflow icon (the three dots in the upper-right corner of the screen) and selecting "**New group**".

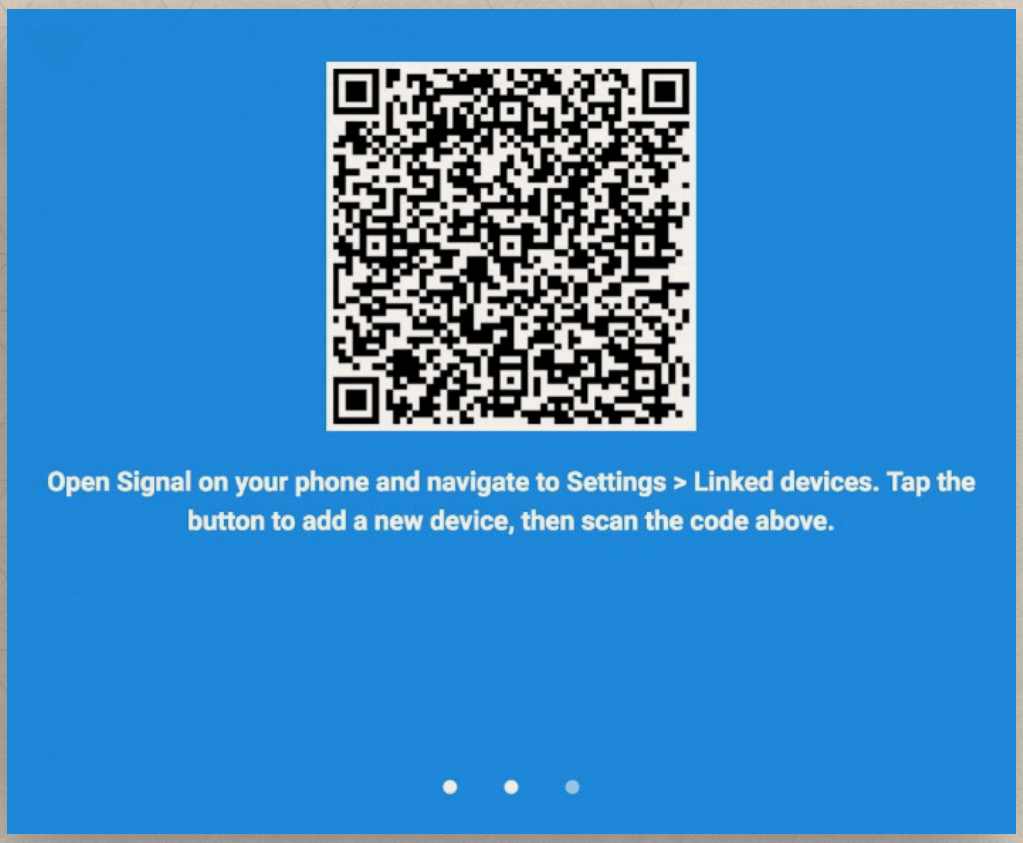


SIGNAL FOR COMPUTER—CHROME EXTENSION

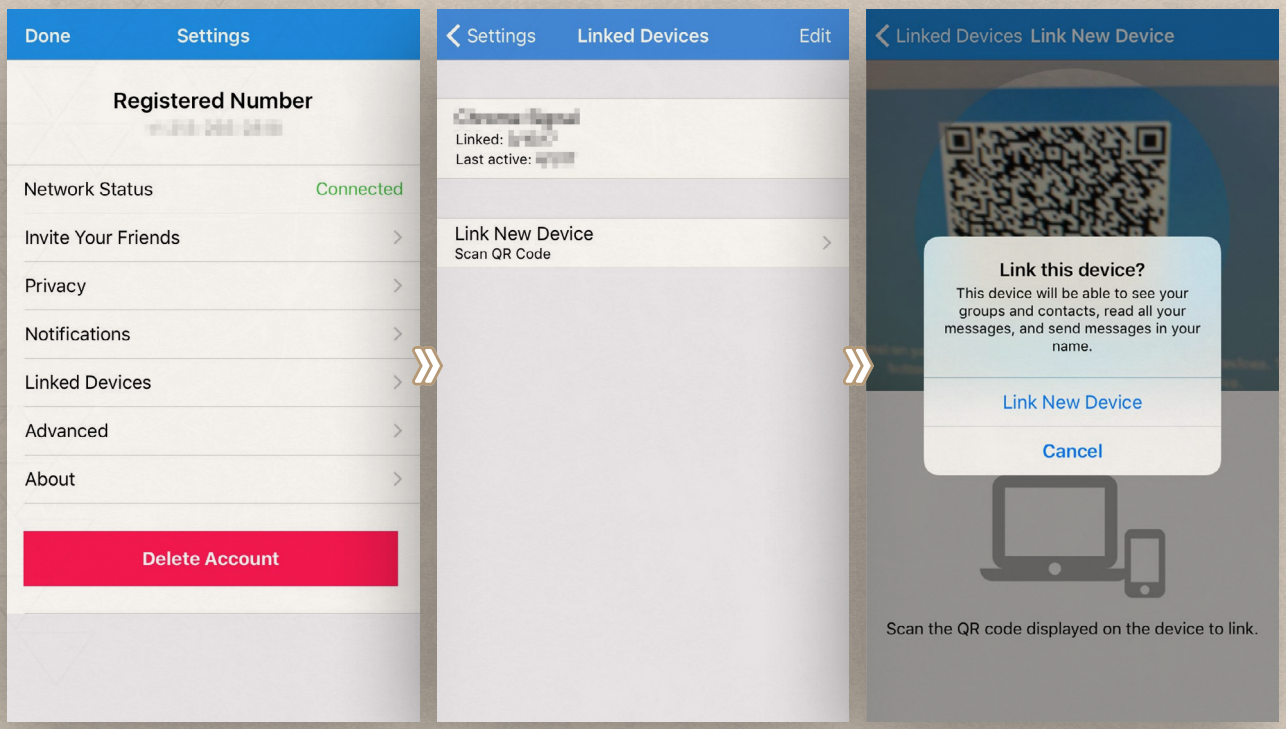
Signal's Google Chrome extension allows you to seamlessly continue text conversations on both your mobile device and computer. All your communications will remain encrypted throughout the process. Signal Private Messenger is a Chrome app that links to your phone, so all incoming and outgoing messages are displayed consistently on all your devices. You can comfortably chat using your full desktop or laptop keyboard.



- Click on Add to Chrome. You will see a scan code, as below.



- Open the Signal app on your phone. Go to **Settings → Linked Devices → Link New Device**. This selection will activate your camera and allow you to scan the code on your computer screen. When prompted, click on **Link New Device**.



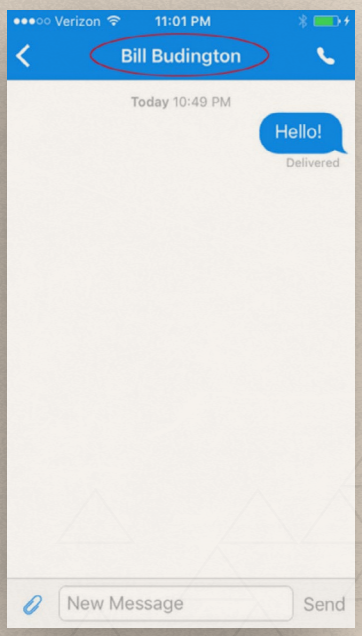
Signal automatically syncs your contacts and messages, so you are good to go.

SAFETY NUMBERS ON—SIGNAL

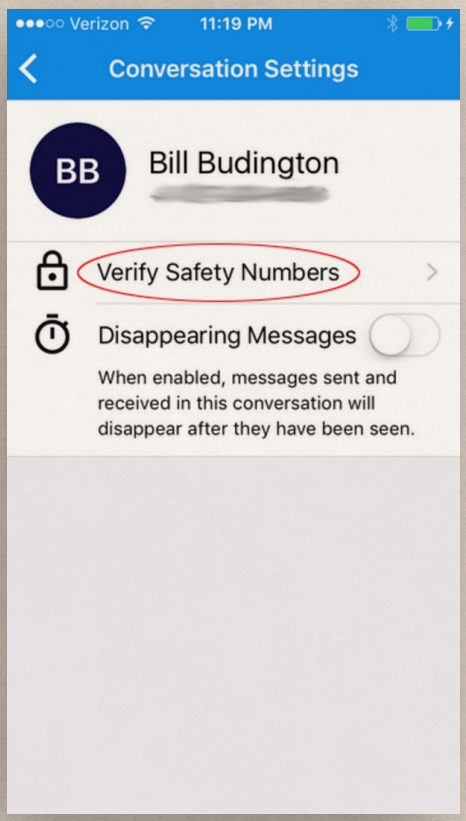
Safety numbers allow Signal users to verify the privacy of their communication with a contact, either by comparing a number or by scanning a single QR code.

- To set this up, open the screen where you are able to message your contact, as described above. From this screen, tap the name of your contact at the top of the screen.

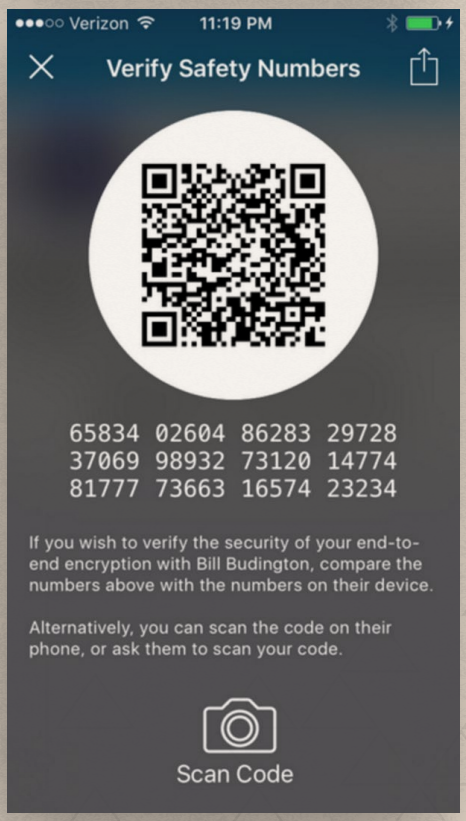
  On the following screen, tap **Verify Safety Numbers**.



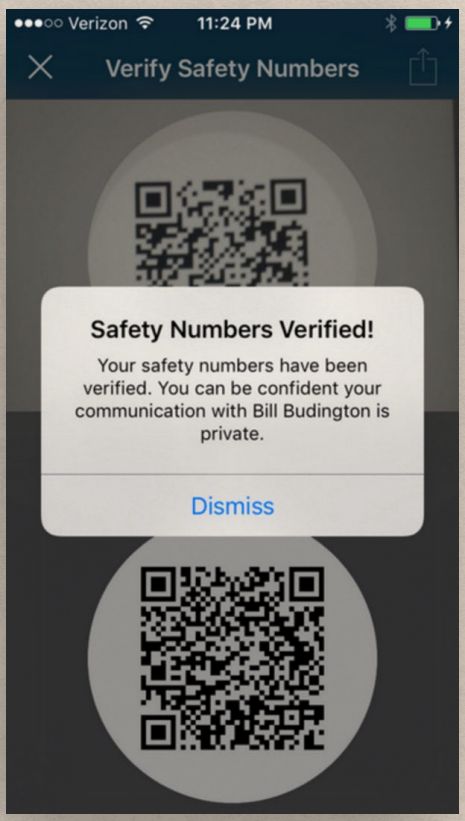
- This will take you to a screen with a QR code and a list of "safety numbers." This code will be unique for every contact. Have your contact navigate to the corresponding screen for their conversation with you, so they have a QR code displayed on their screen as well.



- Tap **Scan Code**. At this point, Signal may ask for permission to access the camera. Tap OK.

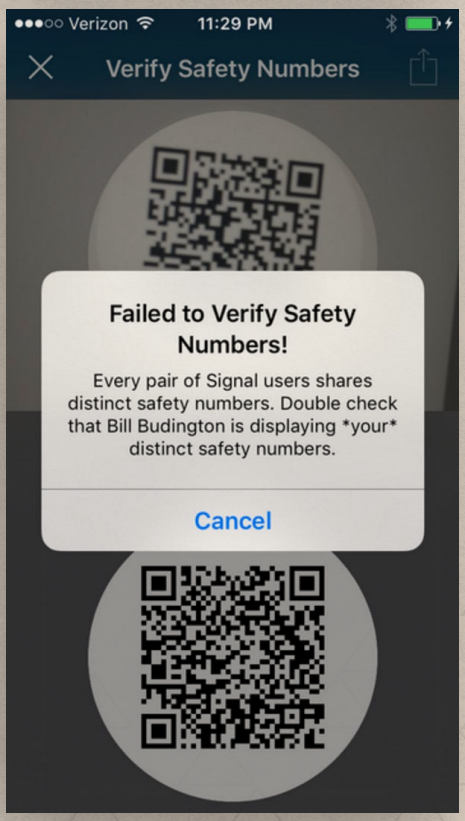


- If verification didn't work, you'll see a notification that says "Failed to Verify Safety Numbers!"



- You may want to avoid **discussing sensitive topics with anyone until you have verified keys with them**.

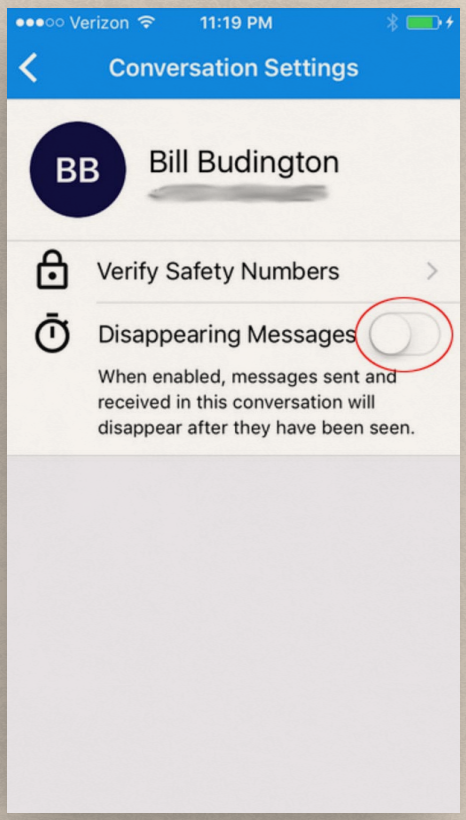
NOTE: Power users the screen displaying your QR code also has an icon to share your safety numbers in the top-right corner. It's best to verify contacts in person when possible, but you may have already authenticated your contact using another secure application, such as PGP. Since you've already verified your contact, you can verify safety numbers within Signal without having to be with your contact in person. In this case, you can share your safety numbers with that application by tapping the "share" icon, and send your contact your safety numbers.



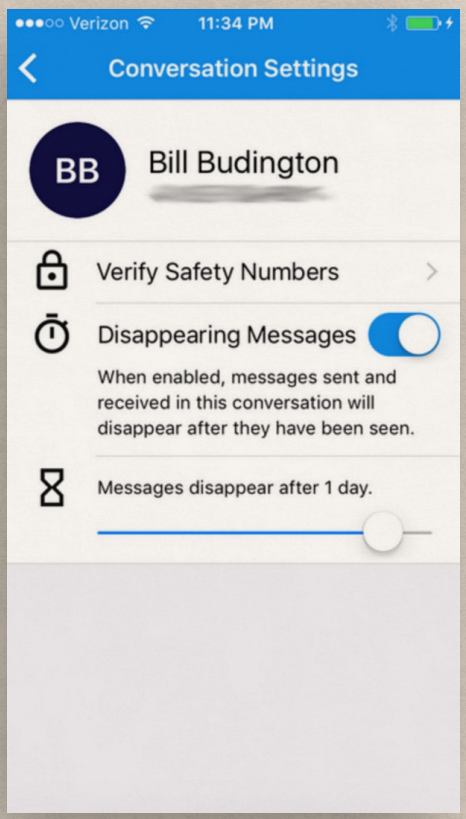
DISAPPEARING MESSAGES ON—SIGNAL

Signal has a feature called “disappearing messages” that automatically removes messages from you and your contact's devices after a chosen period of time after they’ve been seen. To enable disappearing messages for a conversation, open the screen where you message your contact. From here, tap the name of the contact at the top of the screen, then tap the slider next to **Disappearing Messages**.

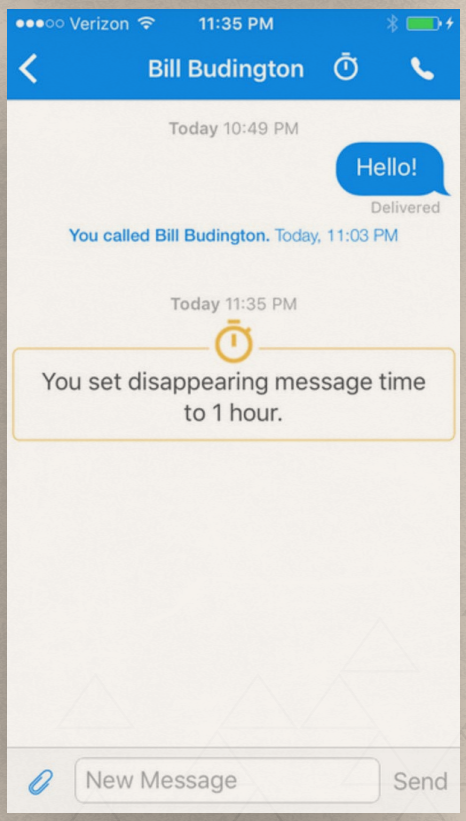
- You'll then see a slider that allows you to choose how quickly messages will disappear.



- After you select an option, tap the < icon at the top-left corner of the screen. You should see a notification indicating that disappearing messages has been enabled.



- You can now send messages with the assurance that they will be erased after the chosen amount of time.

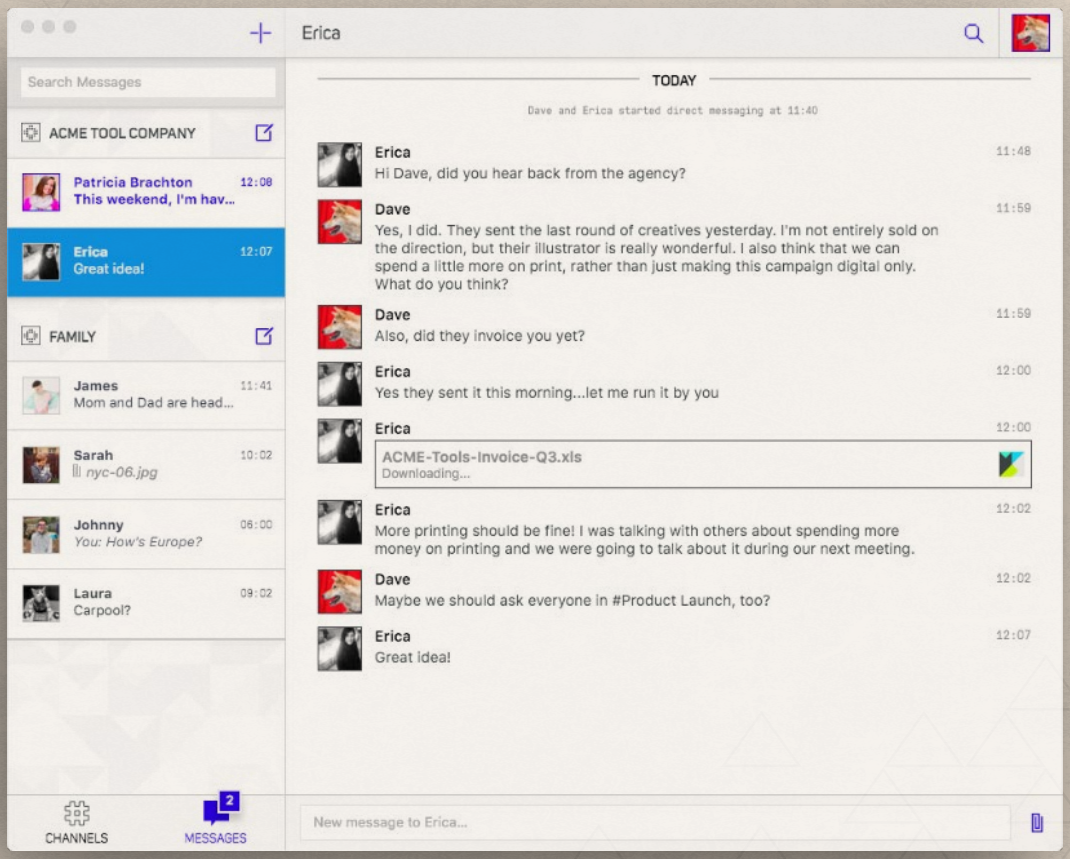


SEMAPHOR

SpiderOak has been a trusted company in the backup space for almost a decade, known for their Zero Knowledge privacy practices. They have been endorsed by Edward Snowden in general and specifically as an alternative to Dropbox in October of 2014.

Semaphor[39] is a real-time team collaboration application created by SpiderOak intended to provide an experience comparable to products like HipChat, Slack, or IRC. Because they are Zero Knowledge, it means that they know nothing about the encrypted data you store on their servers. Their unique design means nothing leaves your computer until after it is encrypted and is never decrypted until it is unlocked with your password on your computer.

Each conversation is cryptographically compartmentalized meaning only the participants in any given conversation have access to that data or the encryption keys; however members who join the conversation later can see content created before their entry into the conversation.



[39] https://spideroak.com/solutions/semaphor

Here is how Semaphor lines up with other similar services in terms of security provisions.

Semaphor is user-friendly and easy to navigate. You can get it both on your phone and your computer. Overall, it gives you the ability to communicate safely and robustly with your colleagues and co-organizers. The downside is that it is a paid service but we do recommend the investment.

	Semaphor	Slack	Hipchat	Microsoft Teams	Skype for Business
Reviewable source code	✓	✗	✗	✗	✗
Zero knowledge end-to-end encryption	✓	✗	✗	✗	✗
Visitor data not shared with third parties	✓	✗	✗	✗	✗
Protects content from blind subpoena risks	✓	✗	✗	✗	✗
Man-in-the-middle SSL attack protection	✓	✗	✗	✗	✗
Vendor admin can't see user data	✓	✗	✗	✗	✗
End-to-end encrypted message content	✓	✗	✗	✗	✗
End-to-end encrypted channel metadata	✓	✗	✗	✗	✗
End-to-end encrypted file sharing	✓	✗	✗	✗	✗
Invulnerable to password-based attacks	✓	✗	✗	✗	✗
Secure key exchange	✓	✗	✗	✗	✗
Contact verification	✓	✗	✗	✗	✗
Message and content verification	✓	✗	✗	✗	✗

WHATSAPP

WhatsApp messenger (**now a subsidiary of Facebook**) is used all around the world, it was one of the first corporate messaging apps to provide end-to-end encryption by default for all users.

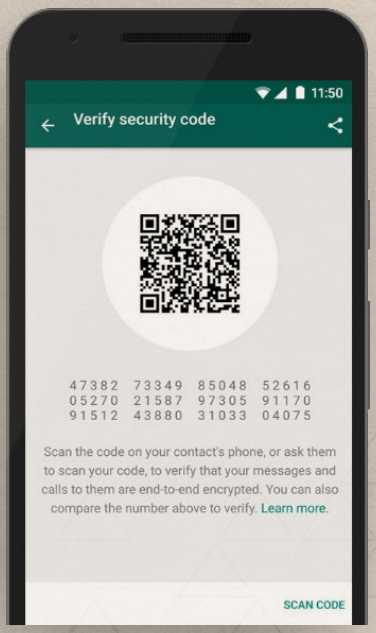
This makes WhatsApp far safer than other platforms. But keep in mind WhatsApp still retains the metadata of your chat logs, which reveal who you were talking with and when. **Additionally, content in WhatsApp helps to inform your Facebook algorithm and contributes to your Facebook profile**.

So use WhatsApp carefully. First and foremost, make sure all of your contacts are using the most recent version of WhatsApp, to make sure encryption is enabled.

Then, it is good practice to authenticate the person you're talking to in order to make sure it's really them. Each of your chats has its own security code used to verify that your calls and messages are end-to-end encrypted.

NOTE: The verification process is optional and is used only to confirm that the messages you send are end-to-end encrypted.

This code can be found in the contact info screen, both as a QR code and a 60-digit number. These codes are unique to each chat and can be compared between chat participants to verify that the messages you send are end-to-end encrypted. Security codes are visible versions of the special key shared between you. Don't worry, the codes don't represent the actual key itself; the key is always kept secret.



To verify that a chat is end-to-end encrypted

- ✔ Open the chat, tap on your contact's name to open their info screen.
- ✔ Tap **Encryption** to view the QR code and the 60-digit number.

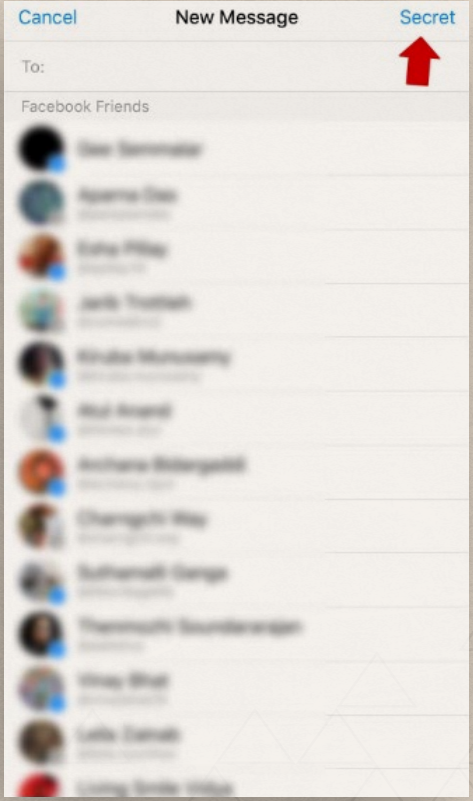
If you and your contact are physically next to each other, one of you can scan the other's QR code or visually compare the 60-digit number. If you scan the QR code and it is indeed the same, a green checkmark will appear. Since they match, you can be sure no one is intercepting your messages or calls.

FACEBOOK MESSENGER

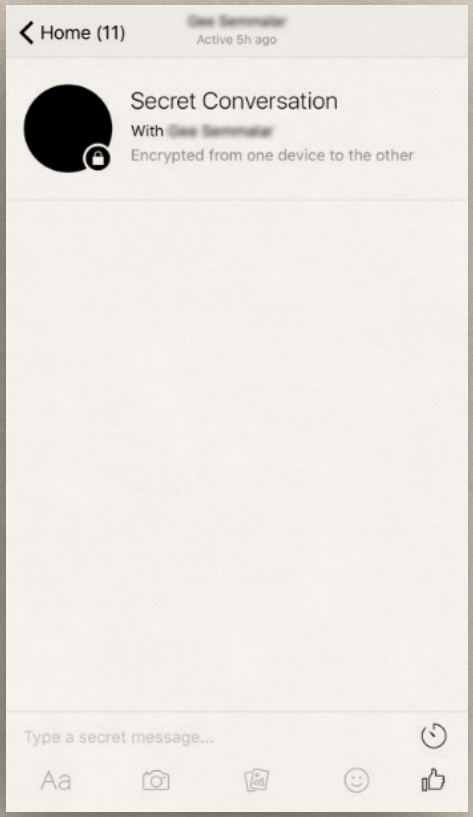
Facebook Messenger has recently introduced the option to send encrypted private messages. Since many of us use Messenger to organize protests and meetings, it is important that we know how to securely use this line of communication.

WARNING: Again, please keep in mind that by turning on Facebook's encrypted messaging you are practicing harm reduction—**not guaranteeing your complete privacy**. Facebook's privacy policies leaves much to be desired by activists since they are willing to hand over personal information to authorities. Be safe and practice risk assessment to gauge your level of safety on this platform.

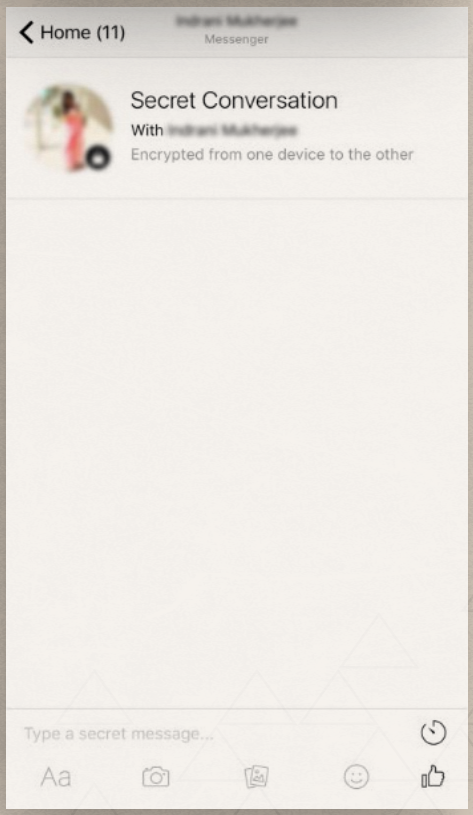
To start a new encrypted conversation:
Tap the new conversation icon at the top right, then tap **Secret** in the top-right corner.



Choose your recipient and begin messaging.



Tap **Secret Conversation** to switch it over.



SENDING SECURE EMAIL USING ENCRYPTION

WHAT IS ENCRYPTION?

Encryption[40] as we've explained, is when data is scrambled in such a way that only someone with the secret password or key can read it. The scrambling relies on mathematical techniques. These techniques are powerful enough that even major governments cannot unscramble the data you choose to encrypt.

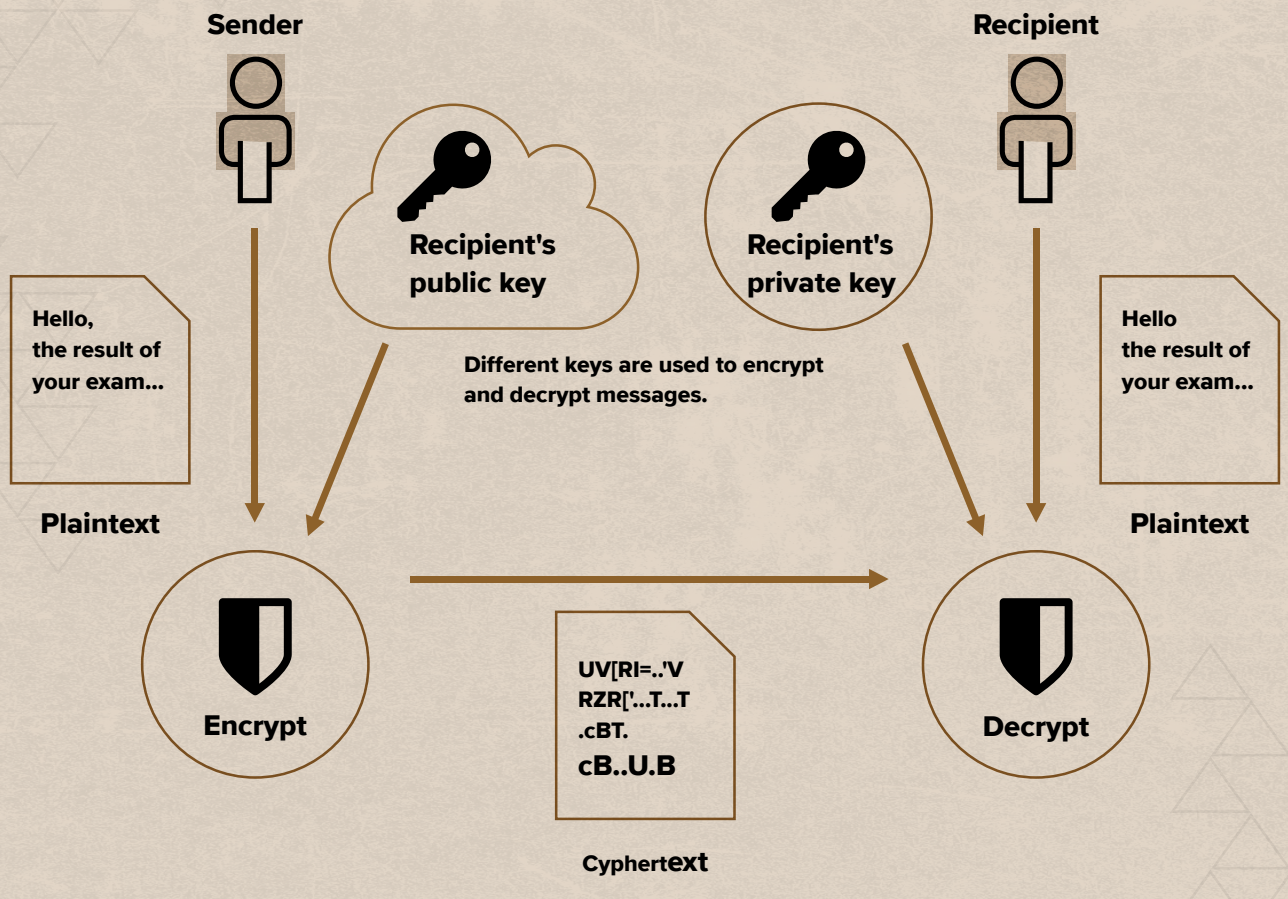
ENCRYPTION FOR PERSONAL USE

When you encrypt data on your computer, it will require a password—also known as a **private key**—that only you know. This process is called private key encryption, and it's good for protecting your data on physical objects that you carry with you such as a USB drive, phone, or laptop hard drive.

[40] https://www.virtru.com/blog/encryption-basics-quick-guide/

ENCRYPTION TO COMMUNICATE BETWEEN PEOPLE

There is a dilemma if you want to have secure and private email or communication between you and your collaborators, and you're the only one using private key encryption. You can encrypt your data and send it to your friend, but then you'd need to tell your friend the password so they can unscramble it. This can be a problem if the government, an ISP, or a hacker has access to your communications and can overhear or capture this password/private key.



To address this problem, we use public key encryption. To understand how this process works, consider the following example:

- You want to communicate securely to your friend. Instead of sending them a private key, you ask your friend to send you a lock that only they have the key to. The lock your friend sends is called a public key.
- You receive your friend's lock, then put your message in a box and lock it with that lock.
- You send the locked box to your friend.
- Your friend uses their private (secret) key, is paired to the lock to unlock it and securely read the message.[41]

You may be thinking, "What if a government or hacker hires a locksmith to pick the lock?" In this scenario, a **weak encryption technique** (low-bit encryption algorithm) would represent an easy-

[41] https://help.gnome.org/users/seahorse/stable/about-diff-private-public.html.en

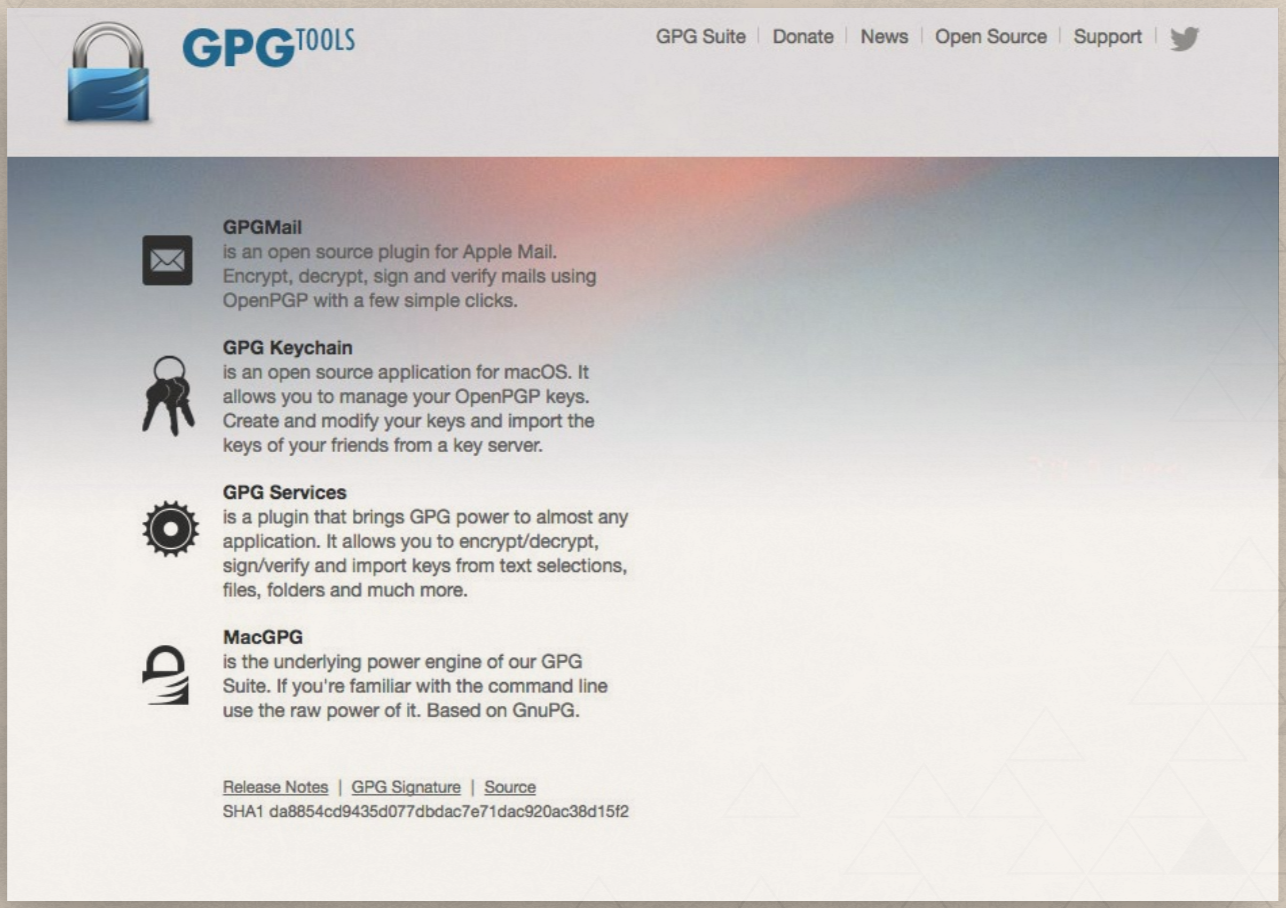
to-pick lock that would only take a few minutes to break. A **strong encryption algorithm** (known as an RSA, which is used in the GPG software package you'll read about on the next page), would take a locksmith hundreds of years to pick.

Using a technique like this, you can communicate over an insecure network and still have security. The set of mathematical techniques that allow this to happen electronically is called **public key encryption**. This encryption techniques is the basis for all secure communication on the internet, whether it's HTTPS, GPG, Signal, Tor, or VPNs.[42]

NOTE: To begin using encryption, we recommend **GPGTools for Mac** and **GNU Privacy Assistant for PC**. You will learn about both in the following pages.

USING GPGTOOLS FOR MAC

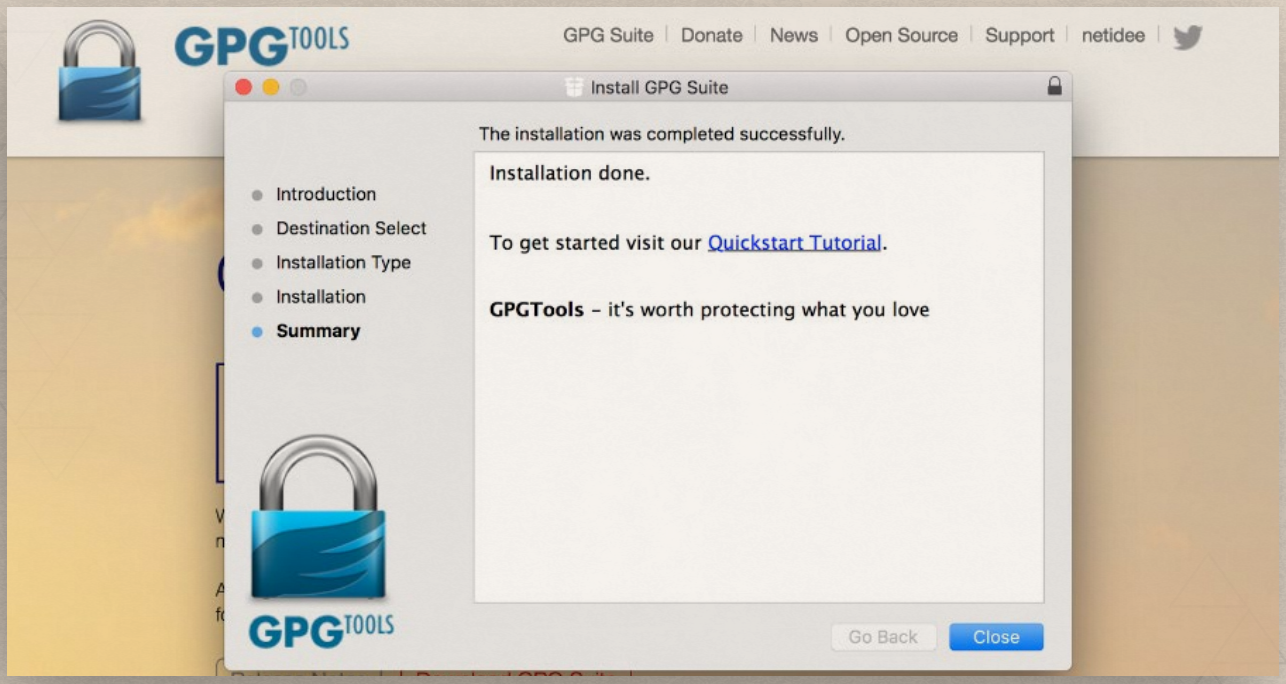
GPGTools is a free open-source software package that allows you to use public key encryption in your communications, primarily over email. You and your collaborator will both need to have a copy of GPG installed on your device.



[42] https://wordtothewise.com/2014/09/cryptography-alice-bob/

How to send encrypted email

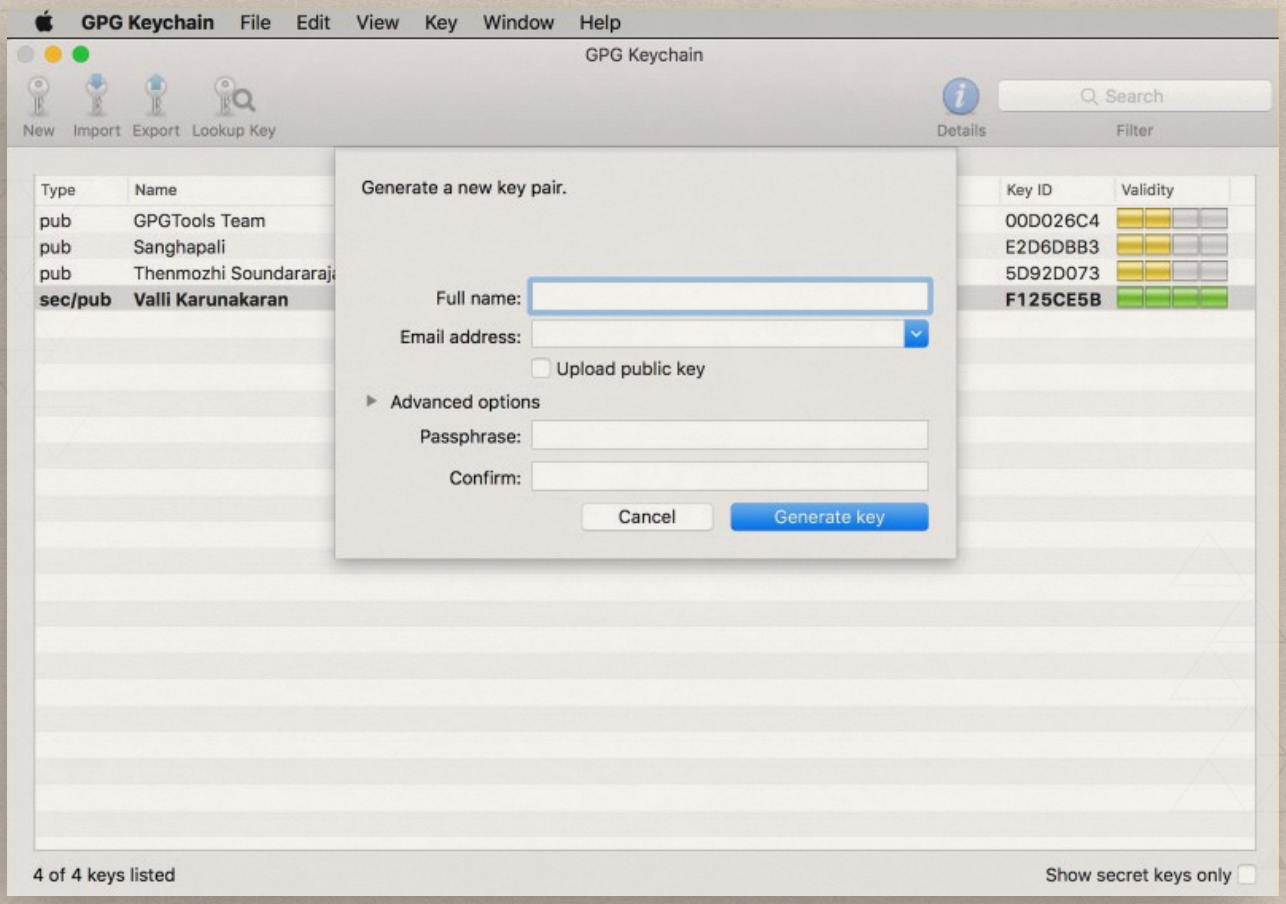
- Download and install the GPG suite from here
- Create a private and public key pair for your use (in other words, generate both your lock and your key). You only need to do this once.
- On the GPG Keychain program window, click **File → New Key → Enter your name**, your email address and your passphrase.



PASSPHRASE RULES

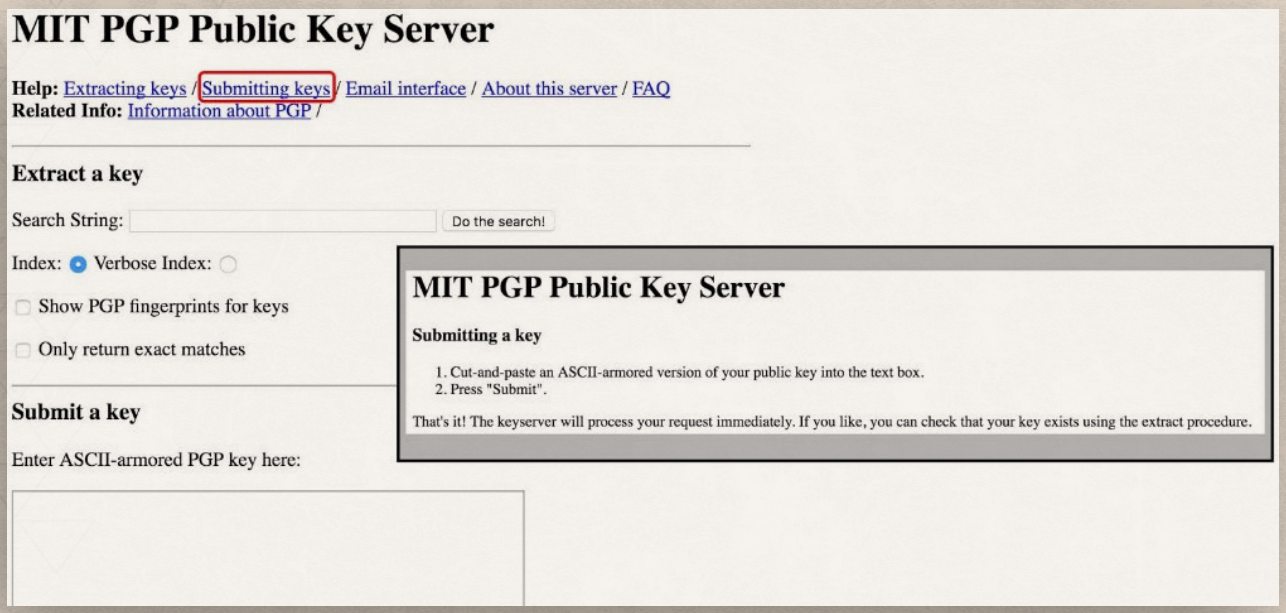
Make sure your passphrase is one you haven't used elsewhere, contains at least one capital letter, one number, and one special character. **MOST IMPORTANTLY: MAKE SURE YOU REMEMBER THE PASSPHRASE**.

WARNING: For initial convenience, jot down your passphrase on a piece of paper. We strongly recommend that you memorize your passphrase, then destroy the paper.



Next, if you are frequently communicating with new contacts add your key to the MIT PGP Public Key Server. This is like making sure you're listed in the yellow pages of the PGP community. Depending on the extent to which this key is tied to your personal identity, you may instead choose to share it directly with people you wish to correspond with, as opposed to sharing it publicly.

- To add your key to the server, first you must export it by clicking on **Export** in the GPG keychain. Open that file on your desktop and copy it. Then, go to pgp.mit.edu and enter your key into the text box under "**Submit a key**" and click "**Submit this key to the keyserver**! Here you can also look for other users by searching for names, emails, or specific key IDs in the "**Search String**" field. Finally, you can also use the file of your exported key to send your public key to a collaborator via email.

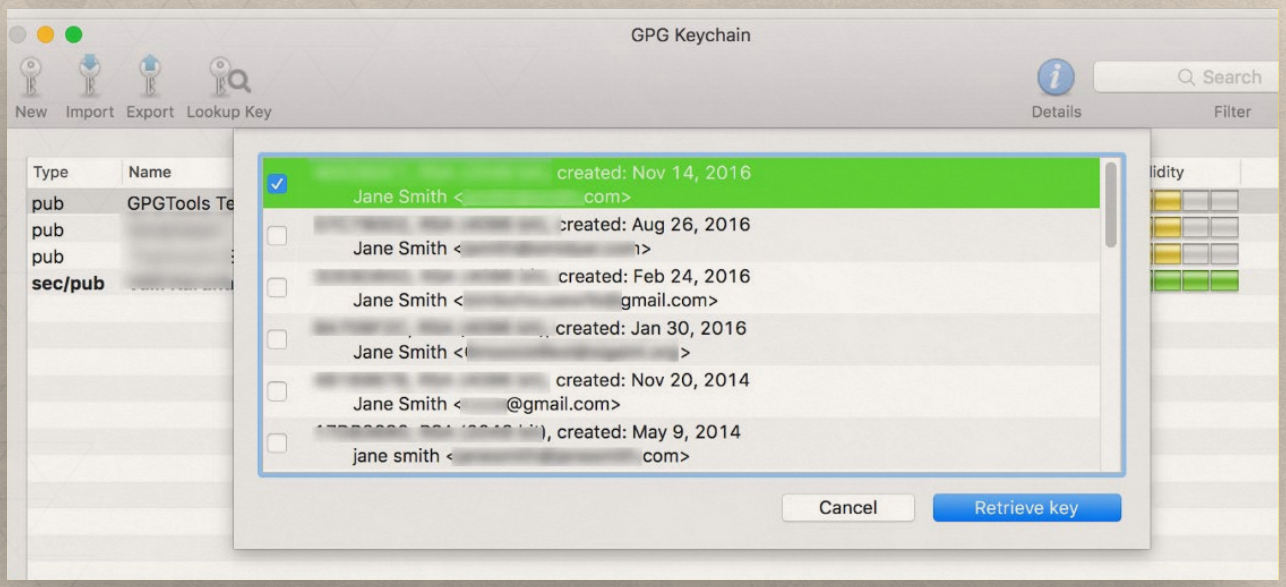


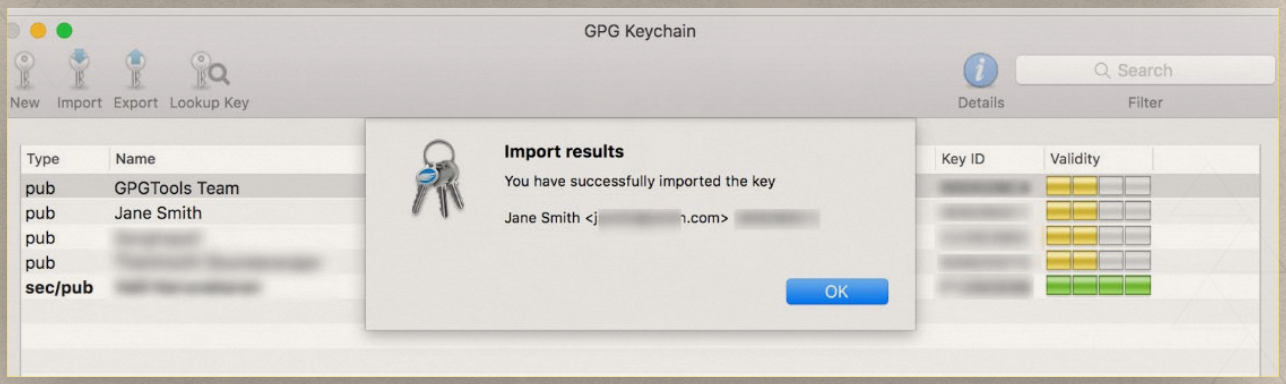
SENDING AN ENCRYPTED EMAIL

First, find your recipient's key on the PGP key server.

- You can do so by going to **Key → Look up key on server**. In the search box, enter the email address of the person you are looking for.

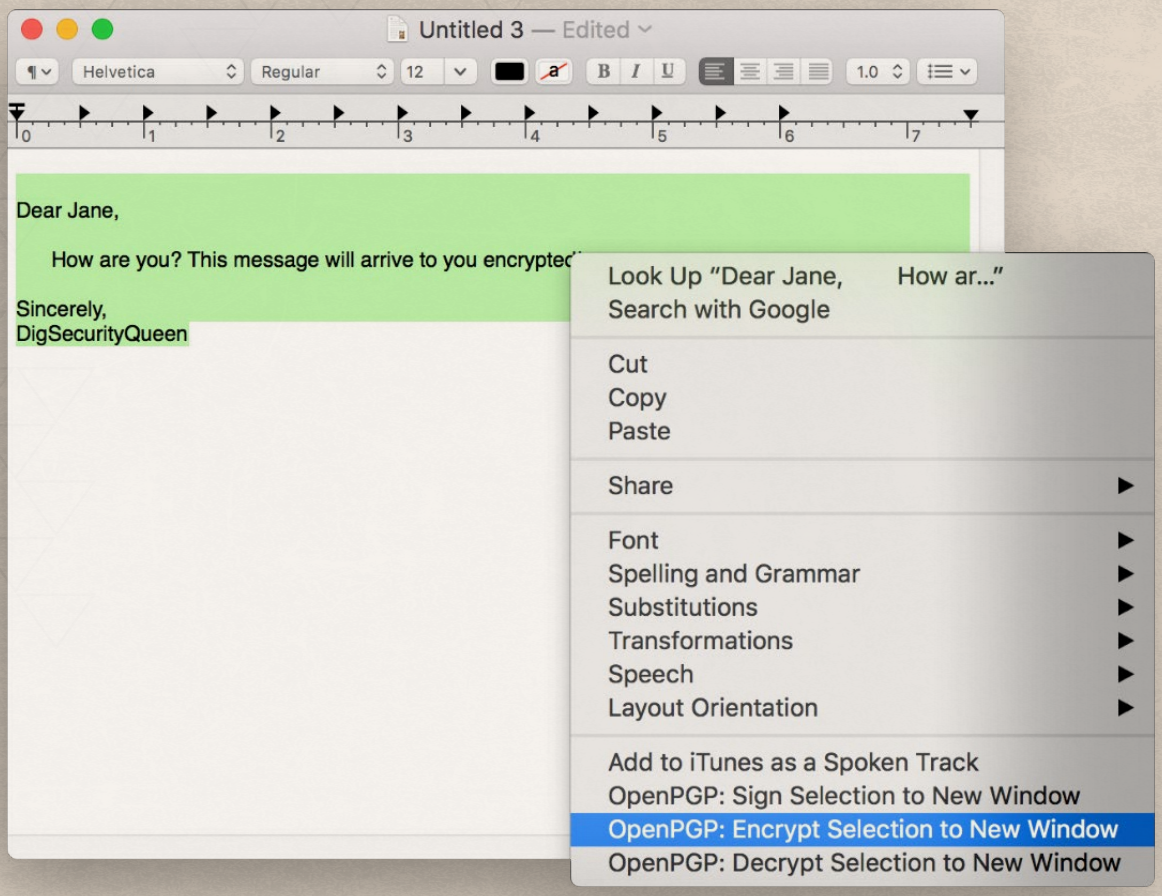
- Find the person you wish to communicate with in the search results. Click on their name, then click **Retrieve Key**.



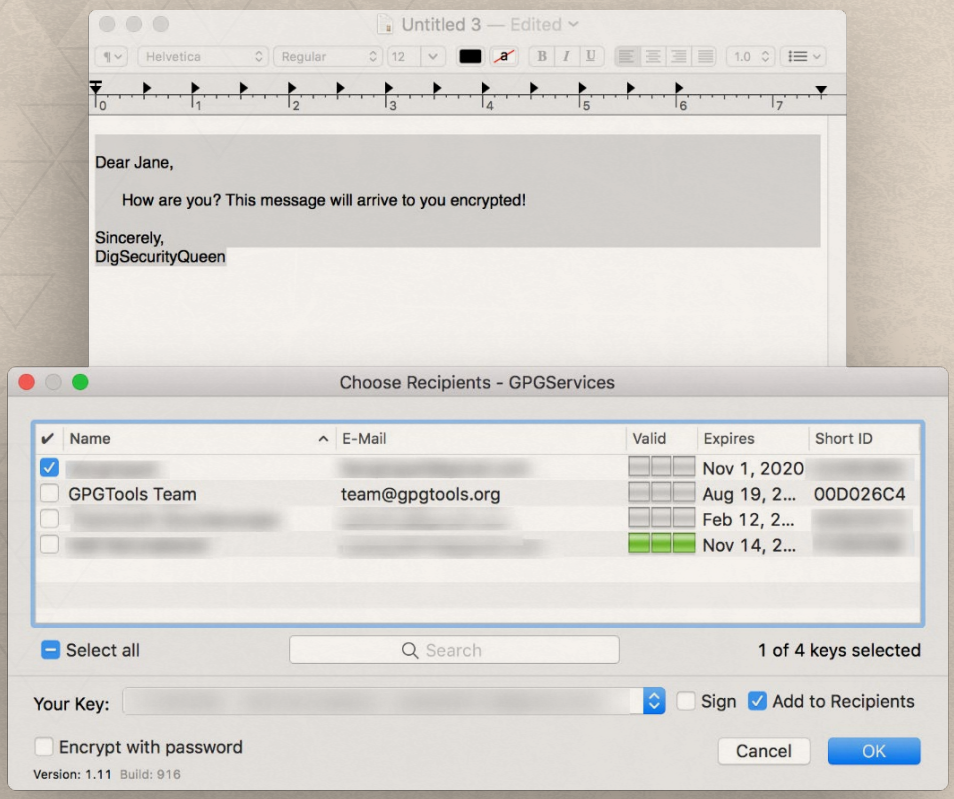


Once you have their key, you are ready to send an encrypted message.

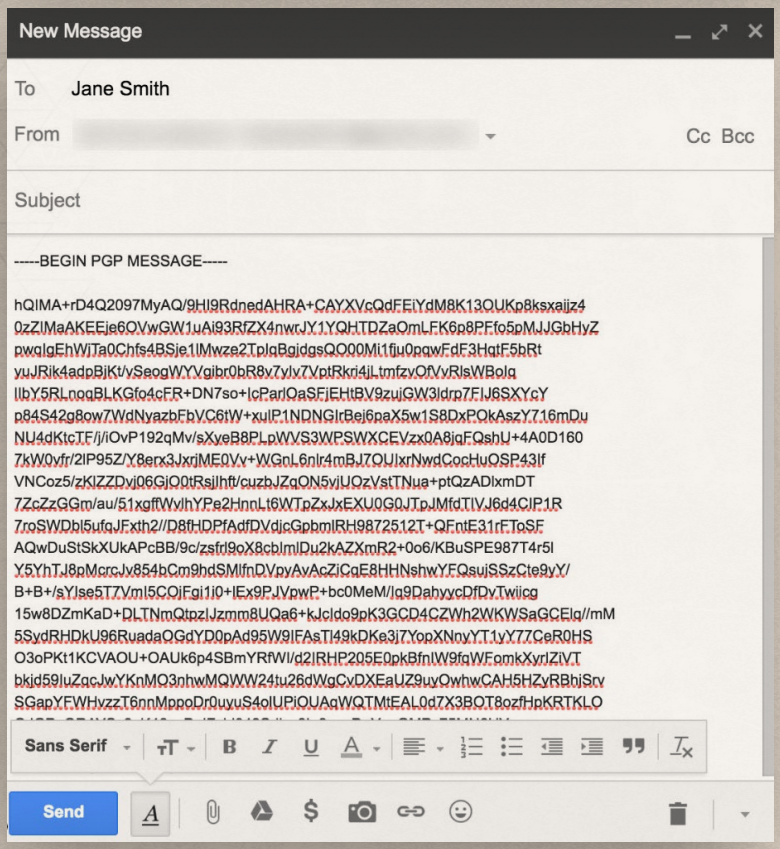
- Open TextEdit on your computer. Type your email message, highlight all of the text, and **right-click (or Control + click)**. Click on the option "**Open PGP: Encrypt Selection to a New Window**."



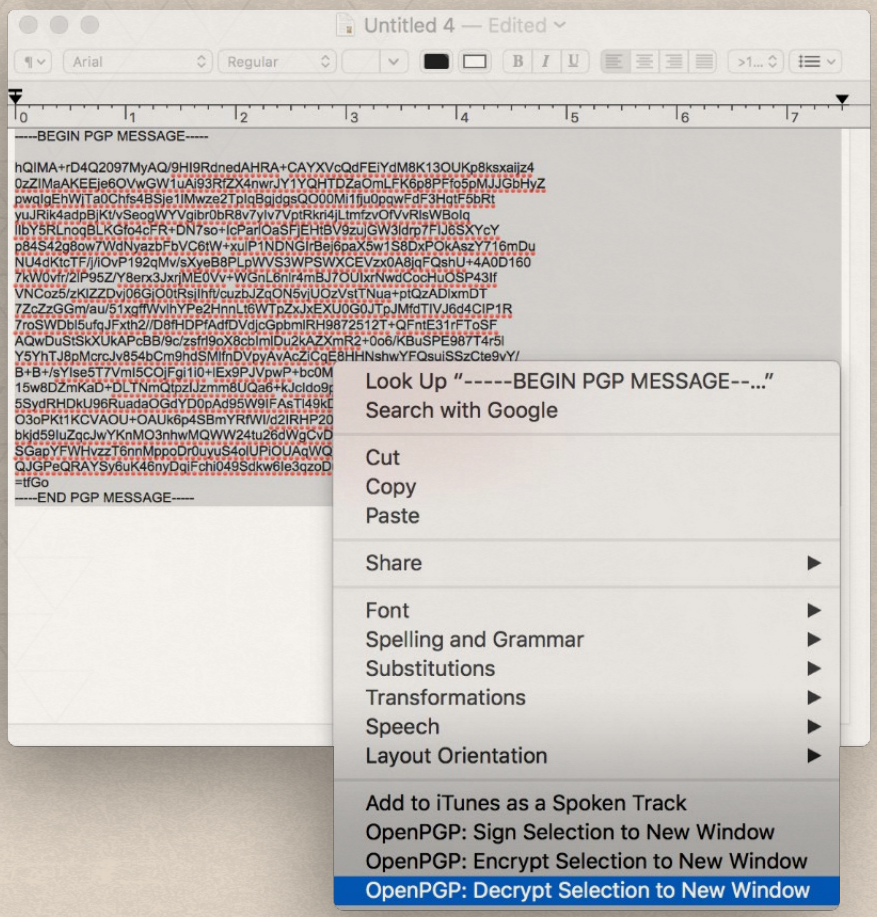
- A window will pop up asking you to select the recipients with keys on your list. Select one or more recipients to whom you would like to send the message.



✔ Copy the body of this message and email it to your collaborator.



- Once they receive the email, they will select use their passphrase to decrypt the message and read it in plain text.



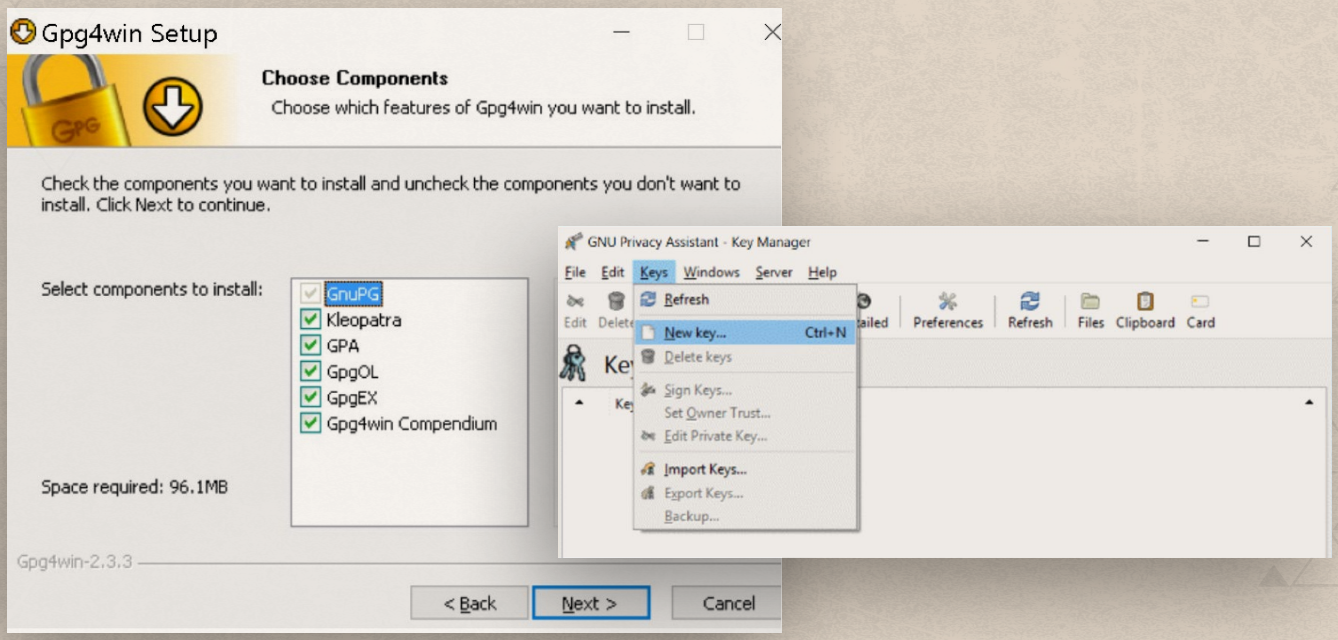
GPG FOR WINDOWS USING GNU PRIVACY ASSISTANT

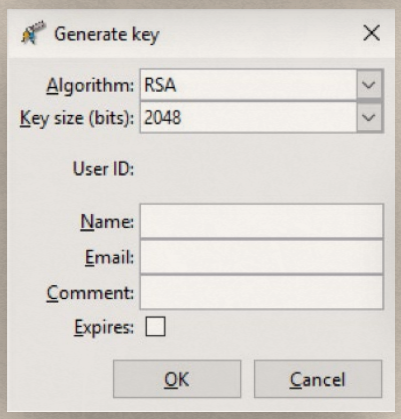
GNU Privacy Assistant is a useful application that's comes bundled with Gpg4win. You can download Gpg4win at https://www.gpg4win.org/download.html

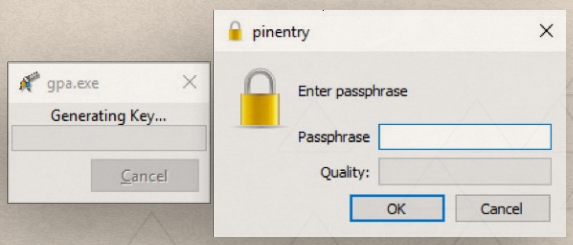
NOTE: When installing Gpg4win, check the "GPA" box to activate it, as it is not turned on by default.

CREATE AND PUBLISH A KEY

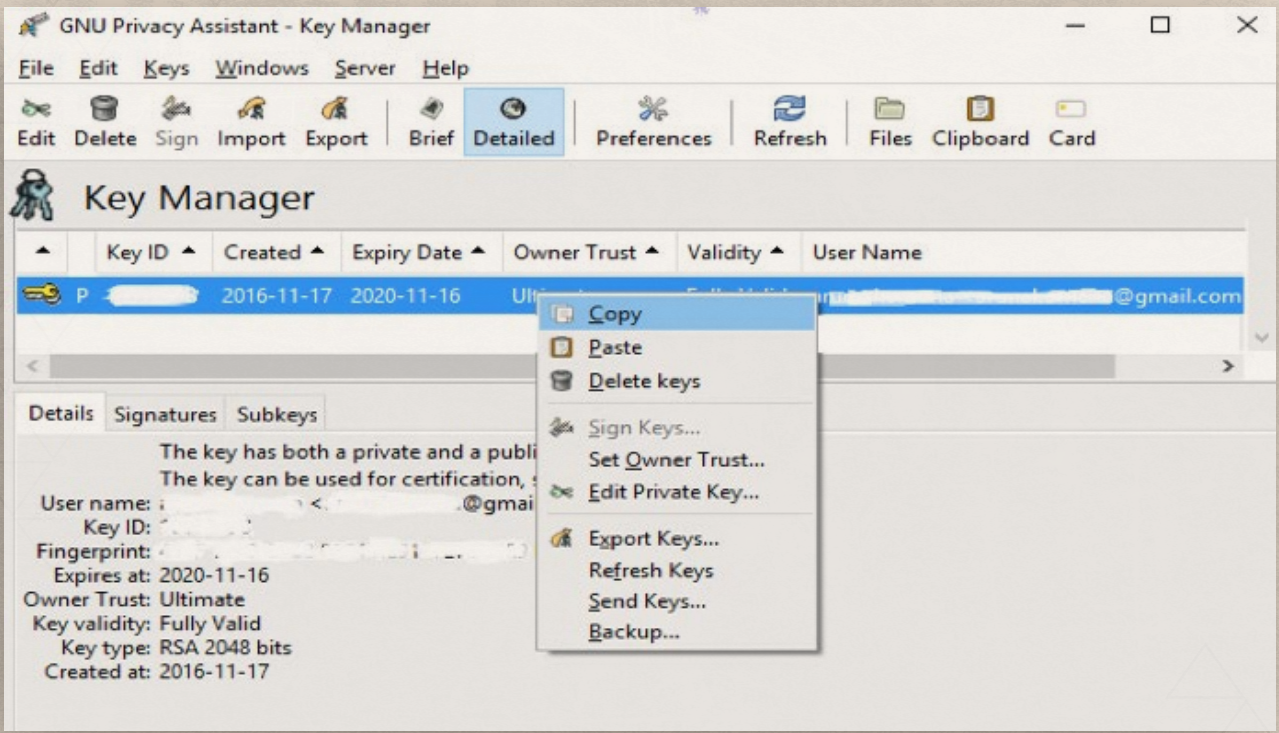
Create a public/private key pair for yourself by going to **Keys → New key**. You will be asked to give a name and email address for this key. The private key will be for your use only and kept secret at all times. Others will use your public key to encrypt messages to you. You can also use your public key to "digitally sign" your communications.







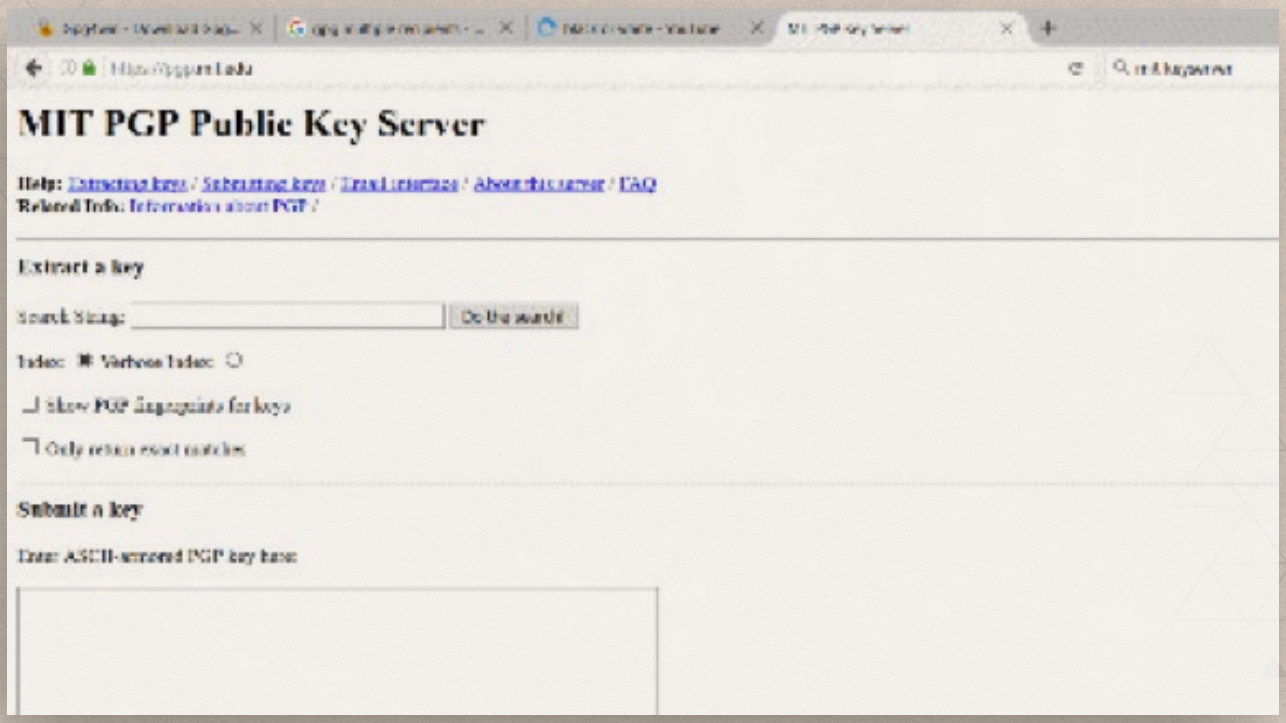
- Once the private/public key pair is created, you will want to publish your public key on the internet to a keyserver, so that people who wish to communicate with you can search for you and find your keys. You can publish your public key at https://pgp.mit.edu/. This is like making sure you are listed in the yellow pages of the PGP community. Depending on how tied this key is to your personal identity, you may choose instead to share it directly with people you wish to correspond with, as opposed to sharing it publicly.



- To do so, you'll first export your key by right-clicking on the new key that appears in the **Key Manager**. Then, select Key. You will see a notification that says, "**The keys have been copied to the clipboard**."

TIP: There is so much to learn with GPG encryption. If you would like to read more, check out this handy kit from the folks at Riseup https://riseup.net/en/security/message-security/openpgp/best-practices

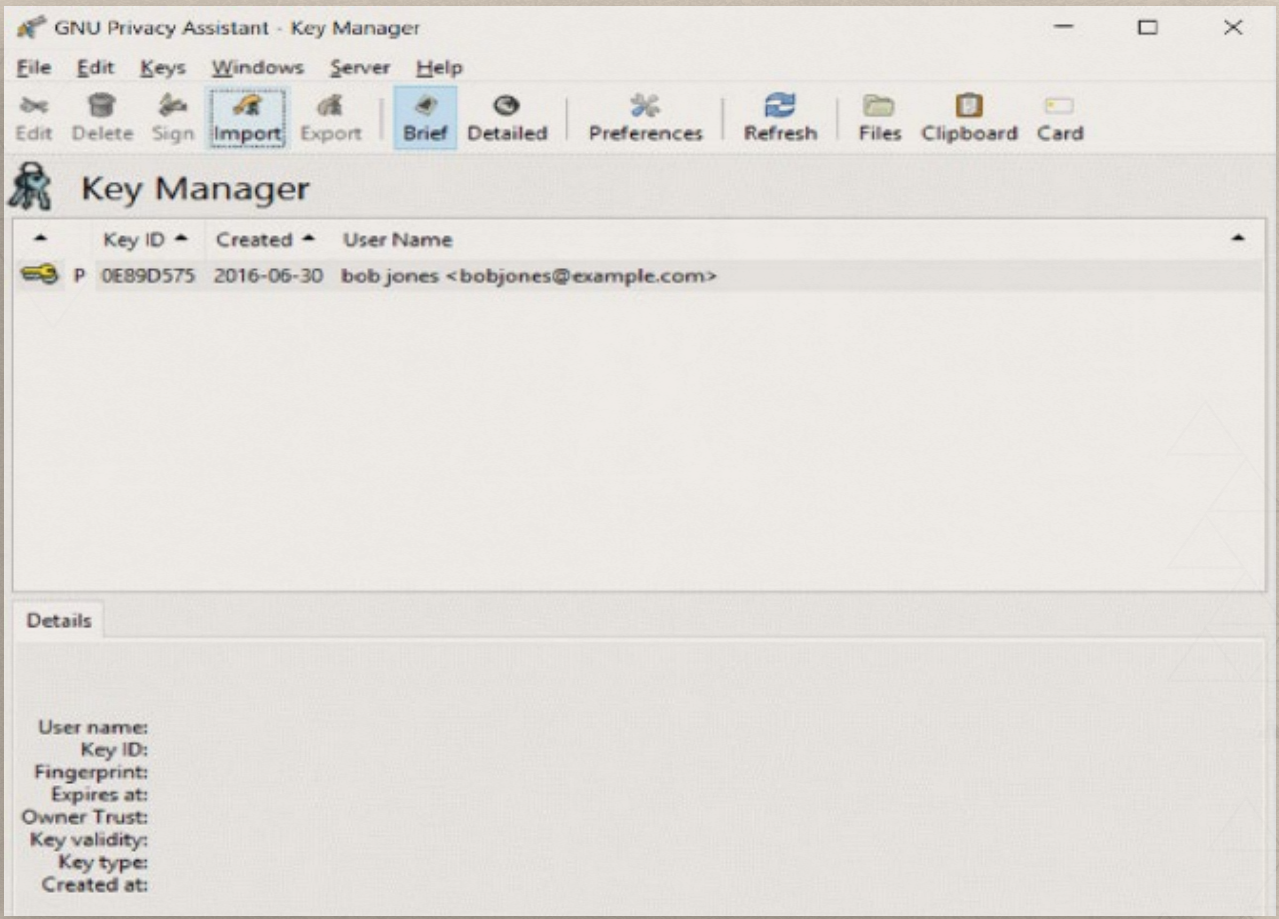
- Go to pgp.mit.edu. There, you can upload your key by copy-pasting from the clipboard. You can also look for other users by searching for names, emails, or specific key IDs (as can anyone!). Finally, you can also use the file of your exported key to send your public key to collaborator (over email).



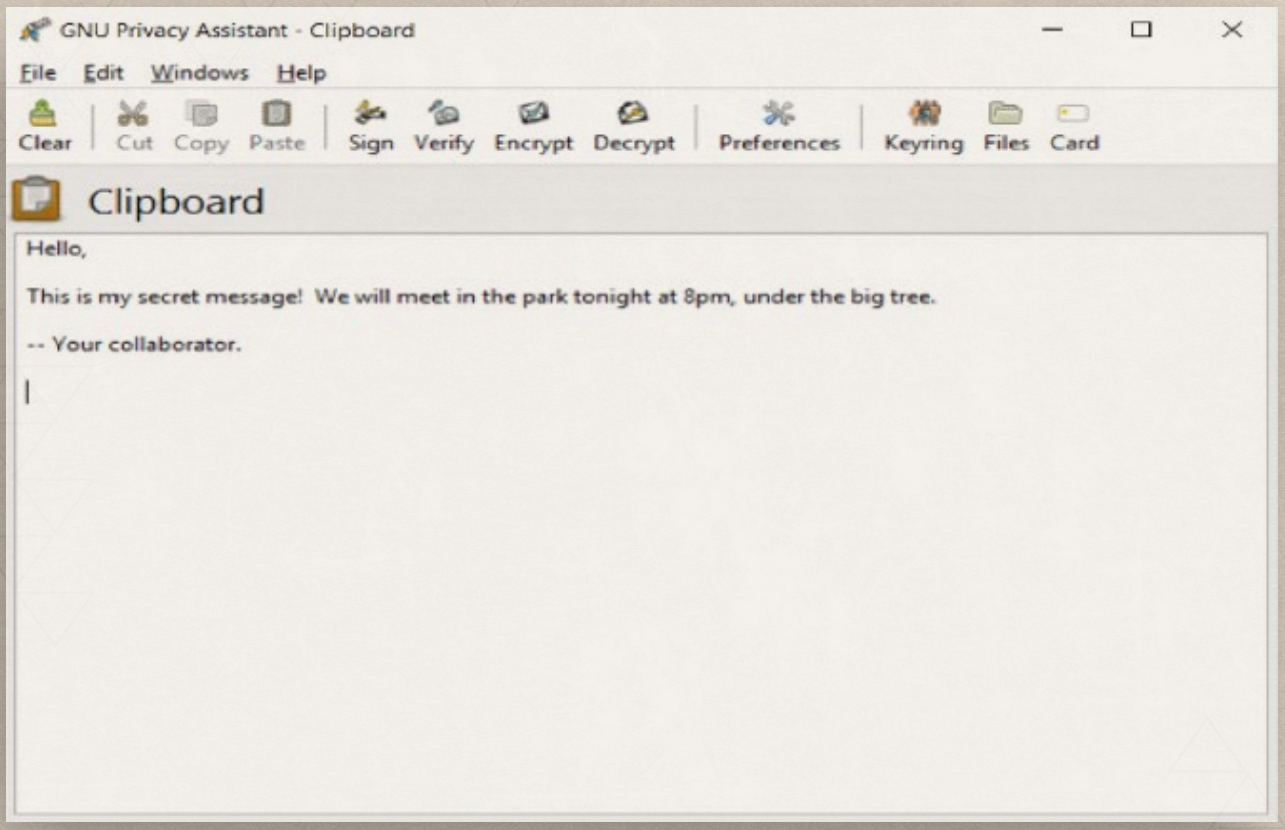
ENCRYPT A MESSAGE

- In order to encrypt a message, you will need to obtain your collaborator's public key. You will use their public key to encrypt your message, which they will later decrypt using their private key. You can use the MIT PGP Public Key Server to look up your collaborator's public key, if it's published there.

  The keyserver will associate an ID with the key that looks something like "0x5db78.7" You can make note of this ID and ensure that it is the correct (authentic) with your collaborator via phone or email. This step will add an additional layer of security, similar to the two-factor authentication used in WhatsApp or Gmail. Once you confirm the key, go ahead and copy it into your clipboard, starting with the line that begins with "-----**BEGIN PGP PUBLIC KEY BLOCK**-----."

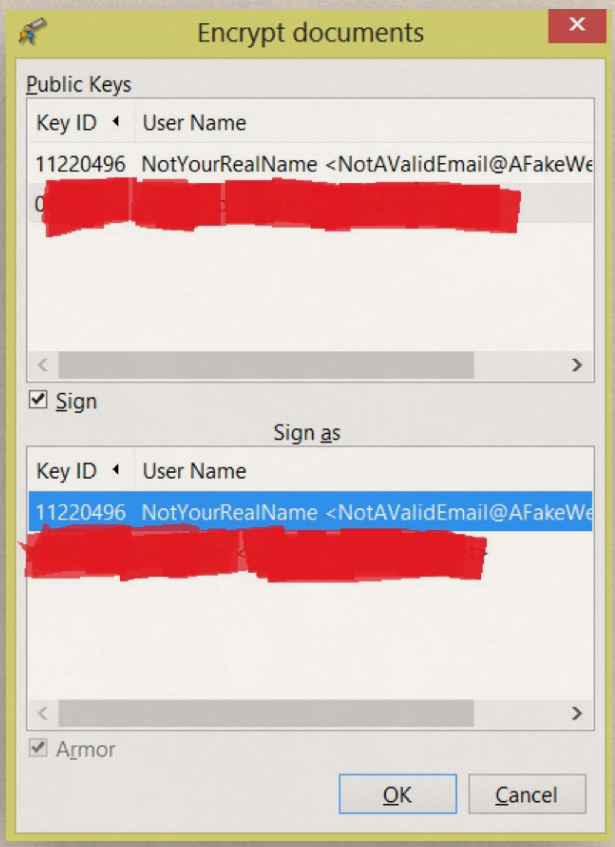


- Once you've copied the key, you can import your collaborator's public key by clicking "**Import**."
- After you've imported the public key, you are ready to encrypt a message. To do so, click on "**Clipboard**" and enter your message.



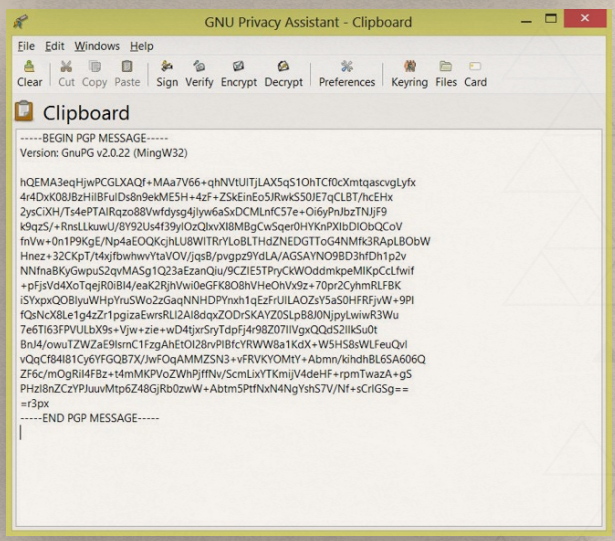
- In the clipboard window click on “**encrypt**” and use your collaborators public key to encrypt. If you check the “**sign**” box, your message will be “**signed**” using your key. This way, your collaborator can verify that the message that is sent is really coming from you. Your text in the clipboard should transform into an encrypted block.

- You are now ready to send your encrypted email. Copy and paste the encrypted block into an email or SMS, and send it to your collaborator.



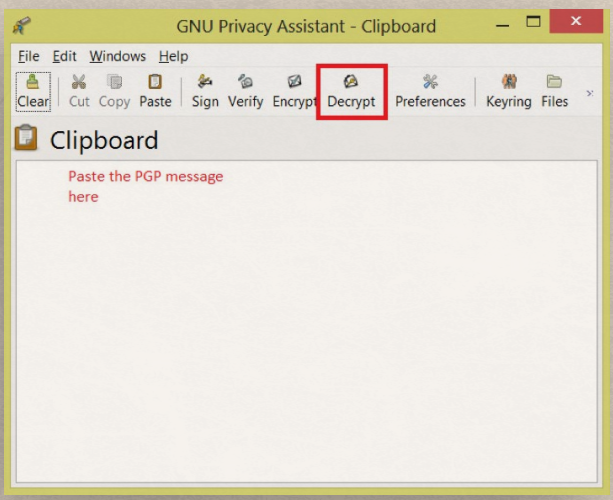
DECRYPT A MESSAGE

- When you receive an encrypted message that was sent using your public key, you can copy that message into the clipboard, hit the **Decrypt** button, and enter private key and password.



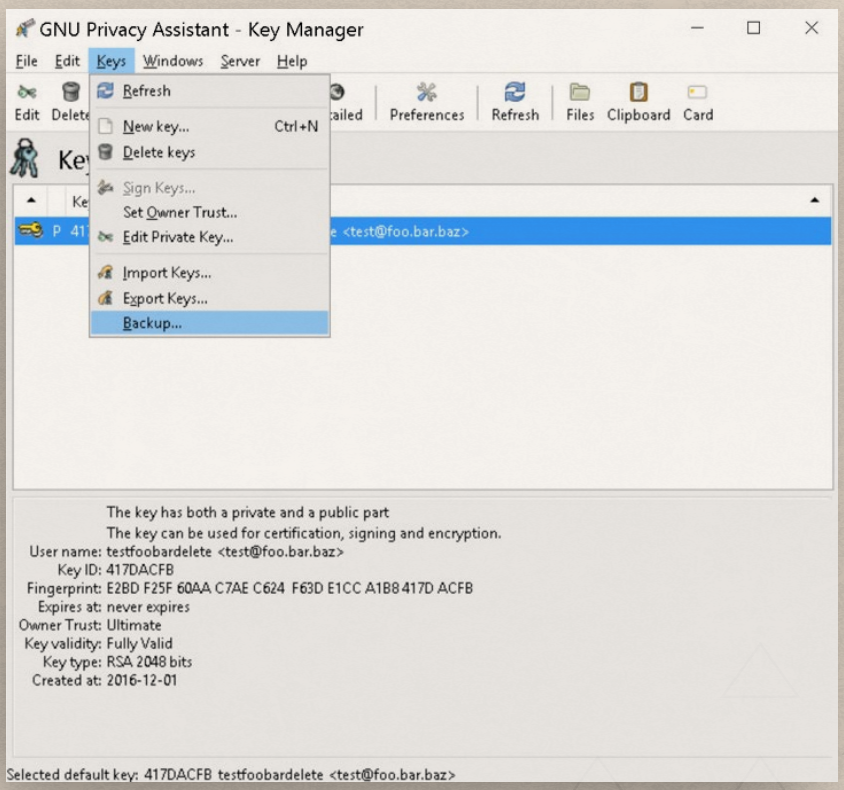
BACKING UP YOUR KEY

You may want to store a copy of your encryption key on a USB stick for carrying around. Or, you can back up your private key by going to **Keys → Backup**. Your key will be saved to the appropriate location.



USING GPG IN YOUR BROWSER

With some caveats based on browser security, there are plugins for Chrome and Firefox to enable OpenPGP encryption for webmail. Mailvelope (https://www.mailvelope.com/) provides a relatively simple option for users who are new to encryption and unable to easily switch to a different desktop email application. Mailvelope is open source, audited in 2014, and compatible with most webmail providers, such as TK or TK. Mailvelope works by adding a button in the "**compose**" window to open a pop-up window in which you can write an email. You can then encrypt the message and send only the encrypted text to the webmail system you primarily use.



TIP: Mailvelope is working to improve its support for email attachments, so stay tuned!

SAFER ONLINE ACTIVISM 101: SETTING UP SOCIAL MEDIA ACCOUNTS THAT CAN'T BE TRACKED

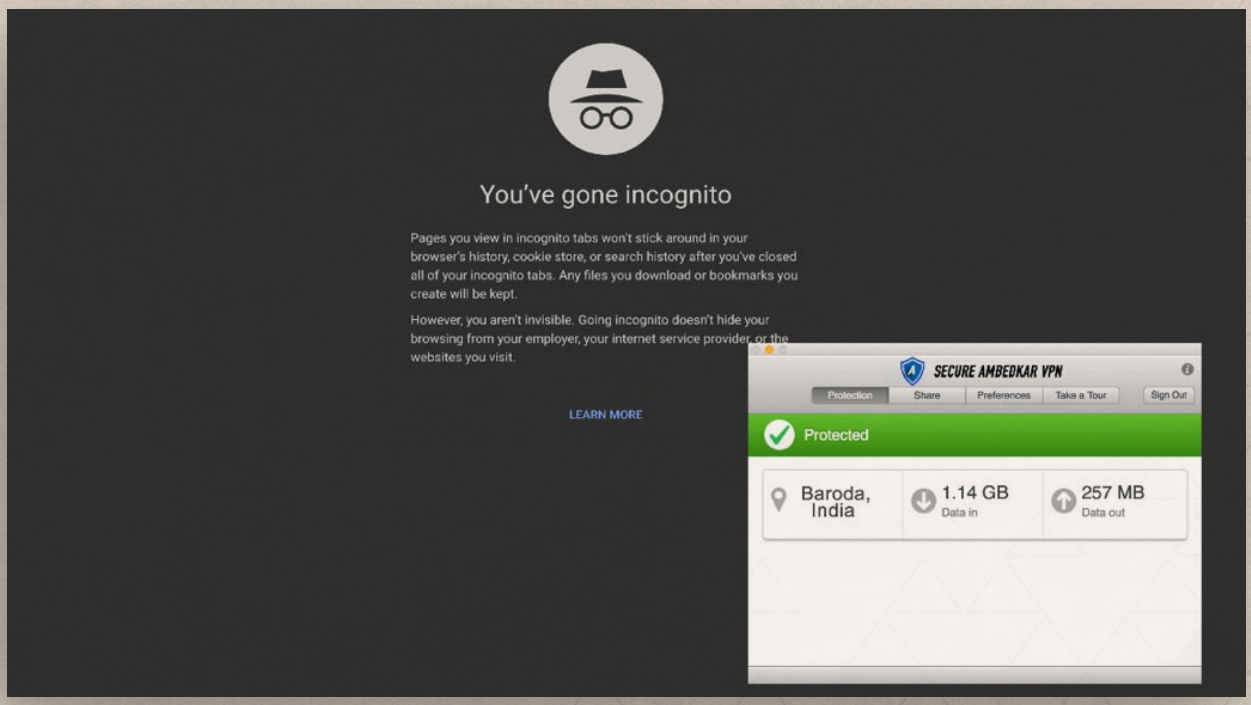
Online activism can leave you vulnerable to trolls and other more malicious actors who can threaten your online and physical safety because they disagree with your politics or activism. In the past year, many activists have shut down online. This means that, sometimes, you have to position yourself as an anonymous entity in order to TK.

This section will cover how to make accounts that can easily be traced back to your physical self. In order to create anonymous social media accounts, you will need services that can generate temporary and anonymous email addresses, or temporary phone numbers and a secure VPN network.

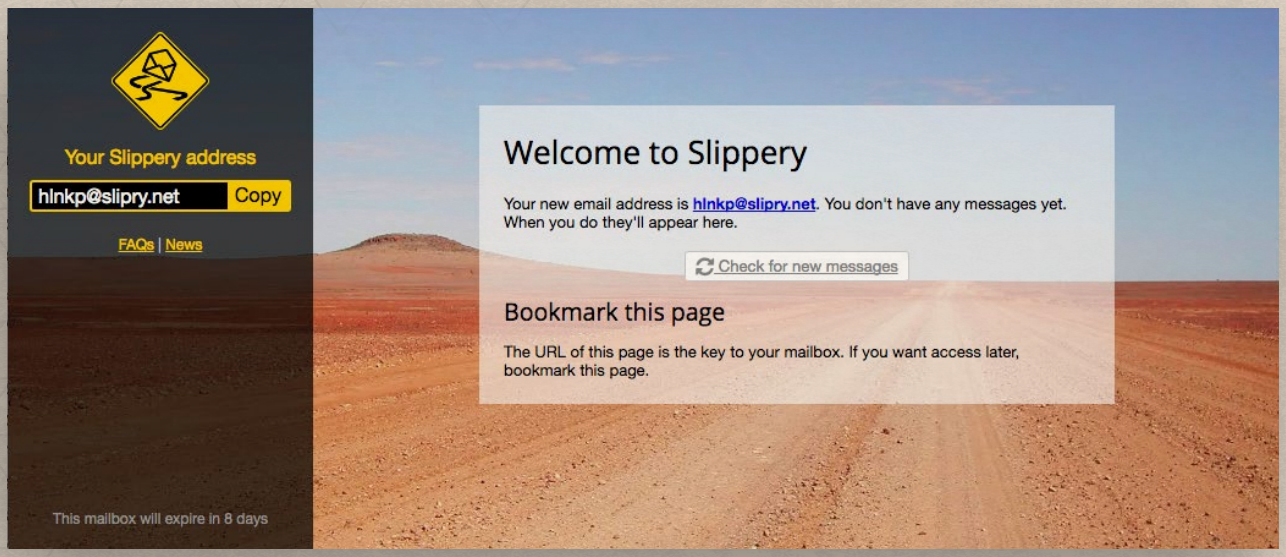
First, sign out of all your accounts, close your browser, and restart your computer. Make sure you are logged in to Tor and/or a secure VPN network and are using private browsing.

You can then use the following services to generate temporary emails

- Riseup: https://user.riseup.net/forms/new_user/first
- Slippery: https://slippery.email
- Guerrilla Mail: https://www.guerrillamail.com



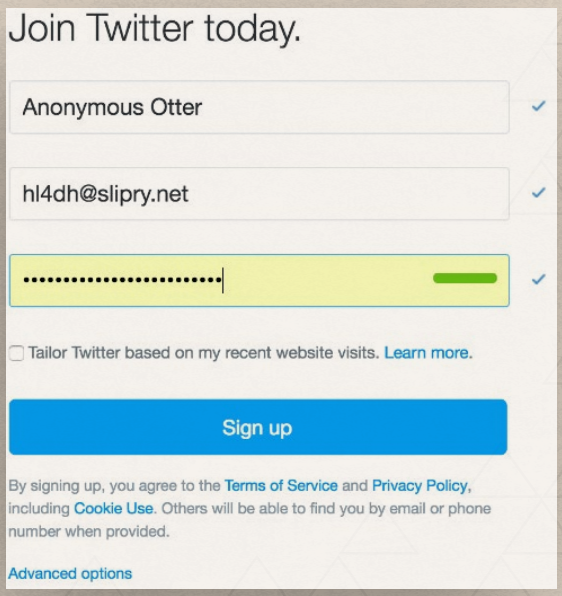
NOTE: It is crucial that you use Tor use only HTTPS sites and are signed out of all other accounts every time you access an anonymous account you have created.



These emails self-destruct within a period of days or weeks, which reduces the chance that accounts created with these emails can be traced back to you.

Using your new temporary email address, register your anonymous social media account.

NOTE: It is crucial that you use Tor use only HTTPS sites and are signed out of all other accounts every time you access an anonymous account you have created.



IN CONCLUSION

Alright, Fam, are you overwhelmed? Guess what? So are we! But the good news is we have one another. And, fundamentally, this is the most important lesson of this curriculum. Digital security is not a destination. It is a journey. By taking it together, we travel as a community toward safety and resilience.

Our hope is that this curriculum acts as a guide you can return to again and again. Use it to inspire your networks and fellow techies to ask hard questions and create collective solutions.

We believe our liberation lies with one another. As this curriculum demonstrates, a commitment to collective safety goes a long way in protecting us, our beliefs, and our movements.

As we enter this new era, we ask you to apply the same ingenuity we use to resist in the streets to resist injustice in the digital sphere. By staying safe—and encouraging others to stay safe—we help ensure the longevity of our ideologies and movements in domains that are crucial to our survival as cultures, peoples, and resistances.

As we say goodbye, we would like to say:

HOLD FAST! COURAGE IS THE ABILITY TO FACE THE DREAD AND NOT LET IT DEFEAT YOU. WE HAVE LOVE, WE HAVE RESILIENCE, AND WE HAVE ONE ANOTHER!

Love,
Equality Labs

APPENDIX: MORE INFORMATION AND RESOURCES

- Security in a Box: https://securityinabox.org
- Heimdal Security: https://heimdalsecurity.com
- Electronic Frontier Foundation (EFF): https://www.eff.org
- Encrypt Your iPhone tutorial (EFF) https://ssd.eff.org/en/module/how-encrypt-your-iphone
- Apple privacy and location services for iOS 8 and later (Apple support) https://support.apple.com/en-us/HT203033
- Using guided access on iPhone and iPad (iMore) http://www.imore.com/how-use-guided-access-iphone-and-ipad
- Security tips for Macs (Intego) https://www.intego.com/mac-security-blog/15-mac-hardening-security-tips-to-protect-your-privacy/
- Choosing a VPN (EFF) https://ssd.eff.org/en/module/choosing-vpn-thats-right-you
- https://www.WhatsApp.com/faq/en/general/28030015 https://videotron.tmtx.ca/en/topic/google_nexus6p/hiding_your_phone_number.html
- How to set a SIM lock on iPhone (PC Advisor) http://www.pcadvisor.co.uk/how-to/mobile-phone/how-to-set-up-a-sim-lock-on-an-apple-iphone-3304041/
- Encryption basics (Virtru) https://www.virtru.com/blog/encryption-basics-quick-guide/
- Cryptography with Alice and Bob (Word to the Wise) https://wordtothewise.com/2014/09/cryptography-alice-bob/
- "Civil Liberties and Law in the Era of Surveillance" (Stanford Lawyer) https://law.stanford.edu/stanford-lawyer/articles/civil-liberties-and-law-in-the-era-of-surveillance/
- Surveillance Under the Patriot Act (ACLU) https://www.aclu.org/infographic/surveillance-under-patriot-act
- The Security Auditing Framework and Evaluation Template for Advocacy Groups (SAFETAG) https://safetag.org
- Agents of Repression: The FBI's Secret Wars Against the Black Panther Party and the American Indian Movement by Ward Churchill
- The Soft Cage: Surveillance in America From Slavery to the War on Terror by Christian Parenti.
- https://safetag.org

GLOSSARY OF TERMS

ACTIVEX
An ActiveX control is a component program object that can be re-used by many application programs within a computer or among computers in a network. The technology for creating ActiveX controls is part of Microsoft's overall ActiveX set of technologies, chief of which is the Component Object Model (COM). An ActiveX control is roughly equivalent in concept and implementation to the Java applet.

ADWARE/MALWARE
Also referred to as malware, sneakware, or spyware, adware is a program installed without a user's consent or knowledge during the installation of another program. Much like spyware, adware tracks an individual’s Iinternet activity and habits to help companies advertise more effectively. Adware is usually installed on a computer with free programs, as the developers are often paid if they include it with their program. Like spyware, adware can be located and removed from a computer using software utilities available on the internet.

ANTIVIRUS PROGRAM
An antivirus program—also known as antivirus software, AVS, antivir, or just AV—is a software utility designed to protect your computer or network against computer viruses. If and when a virus is detected, the computer gives you the option to remove or ignore the infected file, or move it to the vault.

APPLICATION
A web browser, or simply "browser," is an application used to access and view websites. Common web browsers include Google Chrome, Mozilla Firefox, Microsoft Internet Explorer, and Apple Safari.

BROWSER
A web browser, or simply "browser," is an application used to access and view websites. Common web browsers include Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, and Apple Safari.

COOKIES
Cookies are TK that may store information such as a session identifier, user ID, pricing information, user preferences, and more on your web browser. By changing the value of one of these parameters, an attacker can obtain additional information from the server, such as a user's personal or financial information.

DECRYPTION
Decryption is the process of converting encoded or encrypted text or data into text that you or a computer can read and understand. This can be done manually or with the proper codes or keys.

DIGITAL SECURITY

Encrypted data is data that's purposely rendered unreadable by other humans or computers to prevent access to its contents. It's generated using an encryption program such as PGP or a simple encryption key, and it appears as garbage until it is decrypted. Only those who have the correct password or decryption key can make the data readable again.

ENCRYPTED DATA

The process of making data unreadable by other humans or computers for the purpose of preventing others from gaining access to its contents. Encrypted data is generated using an encryption program such as PGP, encryption machine, or a simple encryption key and appears as garbage until it is decrypted. To read or use the data, it must be decrypted, and only those who have the correct password or decryption key can make the data readable again.

FIREWALL

A firewall is a software utility or hardware device that limits outside network access to a computer or local network by blocking or restricting network ports. Firewalls help prevent unauthorized access to a company or home network.

BROWSING HISTORY

Web browsing history refers to the list of web pages a user has visited recently—along with associated data such as page title and time of visit—which is recorded by web browser software for a certain period of time. Web browser software does this to provide the user with a back button and a history list they can use to return to pages they've visited. It also as well as displaysing visited links so the user doesn't have to remember where they've been on the web. In addition to the web browser software itself, third-party services can also record a user's complete or partial web browsing history. For example, in Google's web History, registered users clicks are recorded and stored in individual user histories, each of which are browsable and searchable by that user.

INCOGNITO MODE

Also referred to as Private Browsing, InPrivate Browsing, or Private Window, Incognito mode is a setting that prevents internet history from being stored. This means that when you visit any web page, your computer will not store any text, pictures, cookies, searches, or forms during your sessions.

IP ADDRESS

An Internet Protocol (IP) address is an identifier for a computer or device on a network. It is a 32-bit numeric address written as four sets of numbers separated by periods.

ISP

An internet service provider (ISP) is a company that provides customers with internet access. Data may be transmitted using several technologies, including dial-up, DSL, cable modem, wireless, or dedicated high-speed interconnects. ISPs also frequently give their customers email accounts, and offer services including telephone and television.

JAVA

Java is a programming language expressly designed for use on the Internet. It was designed to have the "look and feel" of the C++ language, but it is simpler to use than C++ and enforces an object-oriented programming model. Java can be used to create complete applications that may run on a single computer or be distributed among servers and clients in a network. It can also be used to build a small application module or applet for use as part of a Web page. Applets make it possible for a Web page user to interact with the page.

METADATA

Metadata is is data that serves to provide context or additional information about other data. For example, a document's metadata could include information about the file's title, subject, author, typeface, enhancements, and size. It may also describe the conditions under which the data stored in a database was acquired, its accuracy, date, time, method of compilation and processing, etc. For example, the government may have the authority to collect metadata about our phone calls. This means they cannot collect the actual content of the call, but can collect metadata like the call's duration, location it was made from and to, the time of the call, and so on.

MODEM

A modem is an electronic device that helps transmit data to or from a computer via telephone or other communication lines.

SOCIAL MEDIA

Social media is a collection of internet-based communities that allow users to interact with one another online. This includes web forums, wikis, and user-generated content (UGC) websites. However, the term is most often used to describe popular social networking websites like Facebook, Twitter, Instagram, and Tumblr.