ALA American Library Association

PRIVACY AND SECURITY ONLINE

BEST PRACTICES FOR CYBERSECURITY

Nicole Hennig

Library Technology Reports
Expert Guides to Library Systems and Services

APRIL 2018
Vol. 54 / No. 3
ISSN 0024-2586

Library Technology
REPORTS
Expert Guides to Library Systems and Services

Privacy and Security Online: Best Practices for Cybersecurity

Nicole Hennig

ALA TechSource
alatechsource.org

American Library Association

Library Technology
REPORTS

ALA TechSource purchases fund advocacy, awareness, and accreditation programs for library professionals worldwide.

Volume 54, Number 3

**Privacy and Security Online:
Best Practices for Cybersecurity**

ISBN: 978-0-8389-1612-4

American Library Association

50 East Huron St.
Chicago, IL 60611-2795 USA
alatechsource.org
800-545-2433, ext. 4299
312-944-6780
312-280-5275 (fax)

Advertising Representative

Samantha Imburgia
simburgia@ala.org
312-280-3244

Editor

Samantha Imburgia
simburgia@ala.org
312-280-3244

Copy Editor

Judith Lauber

Production

Tim Clifford

Editorial Assistant

Colton Ursiny

Cover Design

Alejandra Diaz

Library Technology Reports (ISSN 0024-2586) is published eight times a year (January, March, April, June, July, September, October, and December) by American Library Association, 50 E. Huron St., Chicago, IL 60611. It is managed by ALA TechSource, a unit of the publishing department of ALA. Periodical postage paid at Chicago, Illinois, and at additional mailing offices. POSTMASTER: Send address changes to Library Technology Reports, 50 E. Huron St., Chicago, IL 60611.

About the Author

Nicole Hennig is an expert in mobile technologies for libraries. In her fourteen years of experience at the MIT Libraries, first as web manager, then as head of user experience, she won awards for innovation and worked to keep academics up-to-date with the best mobile technologies. In 2013, she left to start her own business helping librarians stay current with new technologies. She is the author of several books, including *Keeping Up with Emerging Technologies: Best Practices for Information Professionals*. Her newsletter, *Mobile Apps News*, helps librarians stay current with mobile technologies. For more information, visit her website http://nicolehennig.com.

Abstract

It seems that every day there is news of a security breach or invasion of privacy. From ransomware to widespread breaches of private data, the news is full of scare stories. Luckily, there are strategies you can implement and actions you can take to reduce your risk. You can learn to see beyond the hype of media scare stories and better understand what's worth paying attention to by following certain best practices. Using advice from security experts, this issue of *Library Technology Reports* (vol. 54, no. 3), "Privacy and Security Online: Best Practices for Cybersecurity," discusses the difference between possible threats and likely risks. Hennig discusses security best practices for password managers, backing up data, using public Wi-Fi, mobile devices, mobile payment systems, private browsing, social media, and more. The report provides advice on how to make your own security plan and concludes with ideas for sharing this information with library users and a bibliography of resources.

Subscriptions

alatechsource.org/subscribe

Contents

Chapter 1

Assessing Your Security and Privacy Needs

It seems that every day there is news of a security breach or invasion of privacy. From ransomware to widespread breaches of private data, the news is full of scare stories. Sometimes it feels like there is nothing that you as an ordinary citizen can do to protect your data—except to renounce all modern technologies and head to the hills!

Luckily, when it comes to the security of your personal and professional data, there are things you can do to reduce your risk. That's what this report is about. You can learn to see beyond the hype of media scare stories and learn what's worth paying attention to with advice from security experts.

In this report, we'll discuss answers to these questions:

- What are the best ways to back up your data?
- What's the best thing to do if your device is lost or stolen?
- How do intruders get access to your data?
- Can criminals hold your data captive and ask for ransom?
- Is your laptop's or smartphone's traffic being harvested when on public Wi-Fi?
- Should you trust a password manager?
- Is it advisable to use Touch ID or Face ID on iPhones?
- Is it a good idea to use mobile payment systems in retail stores?
- How can you make theft of your identity less likely?
- Are you giving away information for targeted advertising?
- How easy is it for anyone to see all of your search engine history?
- How can you browse the web privately and anonymously?
- What can be learned from your location history?
- How can you protect your privacy on Facebook?
- Should you use encrypted messaging and email? How?
- Is your laptop camera or microphone recording without you knowing it?
- How can you control your privacy if you use smart home devices like Amazon Alexa or Google Home?

For each question, we'll look at what security experts recommend for protecting your data. We'll also discuss the difference between threats (all the bad things that can happen) and risks (the likelihood that each threat might happen). Understanding your risks will help you create an individualized security plan for the different types of data you work with every day since not all data needs the same level of protection. I'll offer information on how to create such a plan for both your personal and your work-related data.

And finally, we'll discuss why it's important for everyone to practice good online security since what you do affects others. I'll recommend a few simple steps for getting started since it can be overwhelming to consider all of this at once. I'll end with some ideas for sharing this information with library users, along with a bibliography of resources to further your learning.

Which Advice to Trust

When reading about security threats, you'll often come across scary headlines from blogs and news sites. It's disheartening to see so many of these stories

about security threats, especially when you are busy and don't have time to learn about each risk and how it might affect you.

How do you know which advice to trust? When evaluating any security tool (such as a password manager app), I recommend looking at two sources: documentation from the vendor about its own security practices and reviews from independent security experts.

Here are some things to look for in the documentation provided with software that is designed to protect your data:

- Is it easy to move to another service if you want to leave this one? (Does it offer easy data exports, for example?)
- Does it use open standards that can be verified by independent security experts?
- Does it regularly audit its own systems for vulnerabilities?
- Does it encrypt data on your computers and mobile devices and also while the data is in transit over the internet?
- Does it keep highly sensitive data in a secure place on your own device rather than transmit it over the internet?
- Are you a paying customer of the service, or are you the data? (When the Equifax breach happened,[1] people soon remembered that our individual information was the data that was being purchased by banks and lenders. In that scenario, we are the data, not the customers.)
- Does it sell your data to others?

As for independent security experts, here are a few individuals and organizations worth following. They often write about the latest security and privacy issues on their blogs and for major media outlets:

- **Bruce Schneier** covers security issues in his blog, *Schneier on Security*. He's the chief technology officer of IBM Resilient, a fellow at Harvard's Berkman Center, and a board member of the Electronic Frontier Foundation. He's an internationally recognized expert on security and the author of many books and academic papers on security topics.
- **Brian Krebs** maintains his blog, *Krebs on Security*. He's a journalist and investigative reporter known for his coverage of cybercriminals.
- **EFF** (Electronic Frontier Foundation), a nonprofit that defends digital privacy, free speech, and innovation.
- **EPIC** (Electronic Privacy Information Center), a public interest research center in Washington, DC, that works to bring public attention to privacy and civil liberties issues.

Schneier on Security
https://www.schneier.com

Krebs on Security
https://krebsonsecurity.com

EFF
https://eff.org

EPIC
https://epic.org

When you see a scary headline about the latest security breach, it's a good idea to look for commentary about it on the blogs of these experts. They will often bring a balanced view of what has happened and offer recommendations on what to do about it. Of course, there are other experts, but these are the ones I have found to be most consistently useful and trustworthy.

Building Your Threat Model

One piece of advice from the EFF that I have found very helpful is to build your own "threat model."[2] This is a plan you can create that helps you decide what level of security you will need for each different type of data you work with.

When working with data, EFF recommends you ask yourself the following questions:

1. What do I want to protect?
2. Who do I want to protect it from?
3. How bad are the consequences if I fail?
4. How likely is it that I will need to protect it?
5. How much trouble am I willing to go through to try to prevent potential consequences?[2]

Threats are any potential harm to the security and privacy of your data. A risk, on the other hand, is the likelihood that a potential threat will happen. You'll start to realize that for some of your data, the likelihood of something bad happening is small or the outcome of the worst-case scenario is not important to you. Since each kind of protection that you implement has a cost in lost time, money, or inconvenience, it's a good idea to be selective about which of your collections of data need strong locks and which don't. You already do the same in the physical world when deciding where to put locks or alarms and where not to.

- **When it comes to question 1, "What do I want to protect?"** make a list of the data you keep, where you store it, who has access to it, and what you already do to keep it safe.

- **For question 2, "Who do I want to protect it from?"** make a list of who might want to get access to each type of information you deal with. This could include individuals or groups, criminals or not, who may benefit in some way from accessing your data.
- **For question 3, "How bad are the consequences if I fail?"** write down what your adversaries might do with your private data. This could be anything from your internet provider selling your browsing history, to advertisers, to a criminal hacker using your credit card to make purchases.
- **For question 4, "How likely is it that I will need to protect it?"** for each threat, write down whether it's worth putting a lot of effort into protecting the data or not. This is somewhat subjective because everyone has different tolerances for risk. But it's usually fairly obvious which items are extremely unlikely to happen or which outcomes would not be so serious if they did happen.
- **For question 5, "How much trouble am I willing to go through to try to prevent potential consequences?"** write down which options you have available to help protect against each threat. If you don't have an answer, mark these threats with a question mark for now. After reading this report, you can come back to them and choose which security or privacy tool fits each need. Sometimes financial, technical, or social reasons (such as budgetary limitations) make it difficult to implement certain choices. It's a good idea to make note of those too.

As your situation changes over time, these risks and threats may also change. It's a good idea to create a new threat model each calendar year.[3]

Notes

1. Allen St. John, "Equifax Data Breach: What Consumers Need to Know," Consumer Reports, September 21, 2017, https://www.consumerreports.org/privacy/what-consumers-need-to-know-about-the-equifax-data-breach/.
2. For complete details, see the Electronic Frontier Foundation, "Assessing Your Risks," Surveillance Self-Defense, last reviewed September 7, 2017, https://ssd.eff.org/en/module/assessing-your-risks.
3. Ibid.

Chapter 2

Security

Backups

The Importance of Local and Cloud Backups

One of the most important things you can do to protect your data is to make sure it's safely backed up on a regular basis. If you're like many people, you either don't have backups at all, don't have recent backups, or don't have all of your devices and data backed up. It's a good idea to back up all of your computers and all of your mobile devices. Having both local backups and cloud backups will protect against the loss of data in many different situations. If your house is destroyed in a fire and you had backups only on local hard drives, you might lose both the computers and the drives.

Many people wonder about the security of backing up your data to cloud services. These days, most security experts recommend doing so, and when you learn more about the security practices of the best services, you can feel more confident about using them.

Cloud Synchronization vs. Cloud Backup

Cloud services can be grouped into several different types. Here we'll look at two types: cloud sync services and cloud backup services.

Some examples of cloud sync services are Google Drive, Dropbox, Microsoft's OneDrive, and Box. These services are used to keep particular folders or directories of documents in sync across multiple devices. For example, when you add or change a file in your Dropbox folder on your computer, it also appears in the same folder in the app on your mobile phone. Change it on one device, and the change happens on all of your connected devices. In this way, they stay in sync. Sync services often have free versions for a limited amount of data and offer tiered pricing for syncing larger amounts of data. Most of these services also have special pricing for non-profits and educational institutions.

Google Drive
https://www.google.com/drive

Dropbox
https://www.dropbox.com

OneDrive
https://onedrive.live.com/about/en-us

Box
https://www.box.com/home

Some examples of cloud backup services are Backblaze, iDrive, Carbonite, and SpiderOak ONE. These services are designed to automatically back up all the files on your computer on a regular basis to an encrypted remote location, with easy ways to restore your files in case your computer is lost, stolen, has a virus, or is otherwise destroyed. They usually provide a way to "set it and forget it," with an app that you set up once and runs silently in the background, keeping your files safely backed up. These services usually have a reasonable monthly or yearly fee and often have special pricing for educational institutions and non-profits.[1]

Backblaze
https://www.backblaze.com

iDrive
https://www.idrive.com

Carbonite
https://www.carbonite.com

SpiderOak ONE
https://spideroak.com/one

Even if you keep most of your important files in a service like Dropbox, it's still a good idea to have a dedicated backup service like Backblaze that will handle complete backups of all of your files and make it easy to get up and running quickly if your computer is stolen. Most of these services have an option for sending your files to you on a portable hard drive so that you can get your files back quickly without having to download them all over the internet.

These services encrypt your files before they leave your computer, so the files can't be accessed while in transit or on the company's servers (except via a warrant, subpoena, or court order). Some services let you add an encryption key known only to you, so even the employees of the remote service can't access your data under court order. The best services offer unlimited storage at a fixed price so that no matter how much your data needs grow, your files will be backed up.

You might wonder why it's not enough to use sync services like Dropbox or OneDrive for this purpose. They are wonderful services for what they do, but they don't usually offer the option of a private encryption key for your most sensitive files, like many cloud backup services. They also require you to add files to a certain location on your computer in order for them to be synchronized, and they don't keep previous versions of your files.

To learn more about all the features of these services, with a recommendation of the best one for your needs, see "The Best Online Cloud Backup Service" by Joe Kissell.[2]

Local Backups

It's a good idea to back up regularly to local hard drives as well. If you need a quick way to restore files that you've accidentally deleted, or to get files that were on a lost or broken device, getting them from a local drive is usually the quickest way. The cost of portable USB drives is very reasonable these days. An article on Wirecutter recommends the 2B Seagate Buckup Plus Slim.[3] This information will of course change over time, so look to Wirecutter as an excellent site for reviews of the best hardware and software by experts.

The Wirecutter
https://thewirecutter.com

Backing Up Your Mobile Devices

IOS DEVICES

If you have an iPhone or iPad, it's good to use iCloud (for cloud backups) and also to make local backups of your mobile devices to your computer using iTunes.[4] When you have backups on your computer, and your computer in turn is being backed up by a cloud service like those mentioned above, your device backups will get copied and encrypted there as well. This gives you several options for restoring all of your data should your iPhone or iPad get lost or go missing.

If you want an alternative to iTunes for backing up your iOS devices to a Mac or PC, try iMazing. It's very user-friendly and is great for backing up everything from your iOS devices.[5] In my opinion, it's much better than iTunes and worth the price of forty dollars for a single-user license. They offer enterprise accounts for organizations as well. It's available for Windows as well as Mac, so if you have an iPhone, iPad, or iPod Touch, you might prefer this to iTunes. You can use it to manage the copying of apps, photos, music, videos, call logs, notes, and voice memos (in either direction, computer to iOS device or vice versa). It also makes it easy to transfer e-books and PDF documents to iBooks.

iMazing
https://imazing.com

ANDROID DEVICES

Google automatically backs up your calendars, contacts, and Gmail, but what about all of your apps, documents, and media files? There are several good backup apps recommended by experts, and they range in price from free to thirty dollars (most being less than five dollars).[6] These days so much important data is stored on our phones, and your mobile devices are often more likely to get lost, damaged, or stolen than your home computer. That's why it's especially important to have good backups of these.

Back Up Your Mobile Photos

When it comes to your photos (most of us have many thousands of these), it's useful to use more than one cloud backup solution. I use Google Photos, Amazon

Photos, and Dropbox to automatically back up all the photos on my iPhone whenever I'm on Wi-Fi.[7] Google Photos is one of my favorites of these services—it automatically backs up photos to the cloud, keeps your photos private unless you choose to share some of them, and offers some useful ways to search everything using Google's artificial intelligence. (Find every photo that contains dogs, for example).[8] Since so many of these services have free options, and since it's easy to turn on auto-backup, why not have redundant backups of your precious photos?

Lost or Stolen Devices

There is a simple action that's worth doing to increase the chances of getting a lost or stolen device returned to you. Even more importantly, it's a way to remotely wipe the data on your device if it's been stolen. It's called Find My iPhone, and you can activate it for all of your Apple devices—iPhone, iPad, Mac, Apple Watch, or iPod Touch. For Android phones, you can use Google's Find My Device.[9]

Let's use Apple's system as an example. When you get a new Apple device, go to your settings, and turn it on. Follow the instructions from Apple: "Set Up Find My iPhone on All of Your Devices."

Apple—Set Up Find My iPhone on All of Your Devices
https://support.apple.com/en-us/HT205362

After you've activated this feature, you can use the Find My iPhone app or log in to iCloud.com from any web browser, to do the following: see your missing device on a map, play a sound to help you find it (perhaps it's lost in your house), or remotely erase your data. You can set a new passcode and create a special message that will appear on your lock screen. You can customize the message with contact information of a friend or family member so that someone who finds your phone can contact you.

Sometimes your data is more important than the device itself, depending on what you have on it. So being able to remotely wipe the device can be extremely useful. This feature is easy to use on both iOS and Android devices and is one of the best reasons to turn it on.

How Intruders Get In

Phishing Attacks and Malware

Now let's look at one of the primary ways that intruders can access your data: *phishing attacks*. You've probably heard of them. These are attempts by criminals to capture your private information or install malware on your device by sending messages that appear legitimate but are actually links to fake sites.

These messages arrive most often by email but can also appear in social media or text messages. They usually take advantage of human psychology by making it appear that you need to act quickly—claiming that your bank account will be frozen or some other bad thing will happen unless you click the link and enter your information immediately. Sometimes they say that you've won a prize or a lottery and that you need to enter your personal information in order to claim it.

When you look at the "From" email address in one of these messages, it will usually be very similar to one that looks legitimate. For example, in a recent phishing attack, messages were sent from lloydsbacs.co.uk, instead of the real address, lloydbank.co.uk. That domain was hosted by a Dutch IP address and was a known source of spam.[10] Some attacks are aimed at workers within a specific company, appearing to be from a CEO or other person in power. Sometimes they look as if they are from a contractor or business partner and ask you to open an attachment that ends up installing malware on your computer.

These scams are called "phishing" as a slang form of the word *fishing*. The attacker is fishing for private information to exploit. Recent statistics show that, on average, about 1.4 million new phishing sites are created every month.[11] These fake pages look like the company they are pretending to be, such as Google, Chase Bank, PayPal, Dropbox, or Facebook. Criminals are getting more sophisticated by building websites that last for only four to eight hours and then moving to a different site, so it's less likely that their site will be marked as malicious by automated tools.

Not only individuals, but also companies and universities, are victims of these attacks. Thousands of companies are hit every year.[12] One high-profile attack hit MacEwan University in Edmonton, Alberta, Canada, in 2017. According to a statement from the university, "A series of fraudulent emails convinced university staff to change electronic banking information for one of the university's major vendors. The fraud resulted in the transfer of $11.8 million to a bank account that staff believed belonged to the vendor."[13] As you can imagine, that was a terrible event for everyone involved.

To learn more about the growing impact of phishing scams, read the report from Webroot *Quarterly Threat Trends: Phishing Attacks Growing in Scale and Sophistication*. The report concludes that "attacks are becoming much more sophisticated, hiding behind benign domains, obfuscating true URLs, carrying more malignant payloads, and fooling even security-savvy users with realistic impersonated websites."[14]

How to Avoid Being Phished

Most of us feel that we are too savvy to fall for one of these attacks. Perhaps your non-tech-savvy relative would, but not you. It turns out that even people with current knowledge of technologies and how phishing works have fallen for one of these scams.

Here are some things to look for when deciding whether a message is real:

- **Spelling errors and bad grammar.** The most obvious one is spelling errors and poor grammar. It's common for criminals to use services like Google Translate to convert their messages to English from their own first language. This doesn't always work accurately, and often you'll see weird grammar, spelling errors, or unusual sentence structure.
- **Incorrect, but similar URLs.** Another thing to look for is the use of shortened URLs from services like TinyURL or Bit.ly. These are legitimate services for creating short links for email messages, so use of shortened URLs alone is not evidence of a scam, but you should always hover your mouse over these links to see where they actually point. If a message doesn't use a link shortener, it's still a good idea to examine the link carefully because often just one letter is different, and it's hard to spot a fake link. Remember also that in HTML email, it's possible to see a correct URL as the visible link, but clicking it sends you to a different link (which you can see by hovering your mouse over the link). One good practice is to not click on the embedded link, but instead start fresh in your web browser, typing in the address that you know is your bank or other official site that the message claims to be from. Another option is to use a service that shows where short URLs point to, like https://www.checkshorturl.com.

TinyURL
https://tinyurl.com

Bitly
https://bit.ly

Check Short URL
https://www.checkshorturl.com

- **Strange email address.** The next thing to look for is a strange address in the "From" field of the email. Sometimes scammers, hoping you won't check, use a long string that is clearly not who it claims to be from. Other times they create a domain name that looks almost exactly the same as an official one. It's even possible to get these messages from the exact correct email of someone you know if that person's account has been hacked.
- **Too good to be true.** If the message is about winning a contest, getting free tickets, or some other perk, and you're asked to enter your information to get your prize, be wary.

Here are some additional precautions to take:

- **Don't click on an attachment (without checking that a person you know sent it to you).** Attachments are a prime way of spreading malware to your computer, so be wary. Don't click on attachments unless you have communicated with the person who sent it to you, hopefully before you received it. If you get an attachment from a colleague that you're not expecting, check with that person in another way to make sure he or she actually sent it.
- **Disable macros in Microsoft Office software.** Most current versions of Office apps come with the macros turned off by default, but some older versions might have macros turned on. Viruses can be spread by attached documents that autorun macros when you click on them, so it's a good idea to keep macros turned off until you need to use them in your own documents.[15]
- **Keep your software up-to-date.** Attackers often rely on bugs in software to get malicious software (malware) onto your computer. When particular bugs become known, the software developer will usually release a security update to fix them. This can be an operating system update to Windows or Mac computers, or a particular software or plug-in update. It's a good idea to keep up with these updates in order to reduce your risk.

Learning More

For an entertaining and informative podcast episode on this topic, listen to Phia Bennin, "What Kind of Idiot Gets Phished?"—episode 97 of *Reply All*.[16] In this episode, she conducts an experiment to see if she can fool her tech-savvy coworkers into being phished.

For more details about different types of phishing scams, read this article by Danny Palmer: "What Is Phishing? Everything You Need to Know to Protect Yourself from Scam Emails and More," published on ZDNet.[17] And for a good overview document that you can recommend to others, see "How to: Avoid Phishing Attacks" from the Electronic Frontier Foundation.[18]

Ransomware

You've probably heard about the problem known as "ransomware." It made the headlines in 2017 with an attack known as WannaCry.[19] In that attack, many

people around the world were faced with a lock screen when they tried to use their computer. The screen explained that the entire computer was locked down with encryption and that to get the code to unlock it, the user needed to pay a ransom of approximately $350 using a payment system known as Bitcoin.

The attack affected computers of businesses and organizations around the world (mostly not individuals on their home computers). Some of the targets included the National Health Service in the UK and FedEx in the United States. Ransomware attackers aim to target those who need immediate access to their computers at all times and therefore are most motivated to pay the ransom—such as banks, law enforcement agencies, and hotels.

Of course, this incident highlights the importance of having good backups from which you can restore quickly. Those who do have good backups can erase their computers and install everything from those backups, wiping out the ransomware. Even if you do pay the ransom, there is no guarantee that the attackers will provide you with the unlock key (though often they do).

The primary way that ransomware spreads is through phishing attacks (with attachments containing the code). Windows PCs that don't have the latest security patches are usually the most vulnerable, and sometimes companies and organizations don't have good plans for keeping all of their software updated. So this is not only an individual problem, but an organization-wide problem for businesses, universities, libraries, and other organizations.

The best advice for avoiding this kind of attack is to keep your systems updated with security patches and to avoid being phished (as described in earlier in this chapter). And of course, if you do get ransomware, having good backups is the solution—erase the entire computer and install from your backups. Even organizations that do have good backups sometimes pay the ransom anyway because the amount of time it takes to restore everything means so much lost business that paying the ransom seems worth it.

To learn more about the details of ransomware, how it spreads, and how to protect against it, see the *Wired* article "4 Ways to Protect against the Very Real Threat of Ransomware" by Kim Zetter.[20]

Using Public Wi-Fi

Man-in-the-Middle Attack

One thing that most people don't think about when they use public Wi-Fi hotspots is how easy it is for their internet traffic to be viewed by hackers. For example, if you are in a coffee shop or airport with free Wi-Fi, it's possible for someone to set up technology that grabs your traffic and analyzes it without your knowledge. One thing they look for is usernames and passwords for services they would benefit from accessing (like your bank).

This is often called a "man-in-the-middle" attack, meaning that hackers can intercept your communication by inserting themselves in the middle, between your computer and the internet. Sometimes attackers set up a rogue Wi-Fi hotspot, with a name that is similar to the location that you're in—"Free Airport Wi-Fi," for example. So when you connect, your traffic is going through their computer first and then sent on to the destination—with a copy of all of your data being grabbed for analysis.[21]

If the website you are connecting to uses `https` at the beginning of the URL, then your connection is encrypted, which can prevent this type of spying. That's why you see it being used these days on most login pages, especially at shopping destinations, banks, and services like PayPal. However, many of these sites use `https` only for the login, and then switch back to unencrypted pages for the rest of the session (`http`). And there are still websites that don't use this type of encryption at all. Google Chrome and some other browsers will usually label a site as insecure if it doesn't use `https`.

Using a VPN to Protect Your Data

One useful tool that can protect you is a browser extension called HTTPS Everywhere. You can install it in Chrome, Firefox, and Opera browsers, and it will force the use of `https` on all pages where it can be used. Websites have to enable that use, and not every website does, so this isn't a complete solution.

HTTPS Everywhere
https://www.eff.org/https-everywhere

An even better solution is to use a VPN when on public Wi-Fi. VPN stands for "virtual private network." It's software that encrypts the connection between your computer and the internet, using something called a "secure tunnel." All of your traffic flows through that tunnel and can't be accessed by eavesdroppers.

There are many VPN services these days, some free and some paid. It's worth using a paid solution to get a quality product that works well and doesn't slow down your computer. Luckily, the prices are reasonable. My favorite VPN service is ExpressVPN, which costs $12.95 per month, or $99.95 per year (which brings it down to $8.32 per month).[22]

It's available for many platforms—Mac, Windows, iOS, Android, many different routers, and every major web browser. With one click, you can turn it on

and leave it running in the background. You can let it choose a server near you, or you can choose from its list of servers around the world (useful when you want to make your computer appear as if it's located in a specific country when connecting). It doesn't slow down your connection as some of the free VPNs do. It uses very strong encryption, and it doesn't keep logs of which sites you visit.

Normally your internet service provider (ISP) keeps logs of every site you visit. So does your employer or university network. Individual websites also keep logs of computers visiting them (by IP address) so they can view and analyze their usage statistics. But when you use a VPN, your ISP can no longer see which sites you are visiting. You might care about this especially because of a law that was passed in the US in 2017. This law eliminated privacy regulations that would have made it illegal for ISPs to sell your browsing history to advertisers without your consent.[23] When you use a VPN on your home internet connection, your ISP can't collect your data in this way. Many paid VPN services work well, and most experts suggest avoiding free VPNs.[24]

Passwords and Authentication

Managing Your Passwords

If you're like most people, you probably have an overwhelming number of passwords to keep track of for various online services. Most people solve this either by using the same password everywhere or a few variations of the same password. Some people keep a list of passwords, perhaps in a Word document on their computer or in a paper notebook.

Using the same password everywhere (or in a few of the same places) is a bad idea. That's because your password is only as secure as the least secure site where you use it. If a particular site gets breached and hackers steal all the usernames and passwords, the first thing they will do is attempt to use those same credentials on other sites, like banks, Amazon, PayPal, or other sites where they can benefit financially.

A common tactic known to those who hack for personal gain is to automate the creation of lists of possible passwords that include many variants of the same words or phrases. In order to save processing time when trying to hack a system, they usually begin with lists of the most common passwords that people use. They can deal with many different roots with different appendages (a suffix or prefix). The roots can be a word, or just something pronounceable, since that's what people tend to use. They use different dictionaries to create these lists, including English and other languages, proper names, and so on. The appendages can be numbers, letters, or parts of words. They run through words with common substitutions, such as a dollar sign in place of the letter *s*. In this way, they can break a great many passwords and crack many systems.[25]

USING A PASSWORD MANAGER

These days, security experts recommend the use of a password manager. An example is 1Password, by AgileBits. Its slogan is, "Go ahead. Forget your passwords." A password manager like this is an encrypted database (in the form of a mobile app and desktop software) that securely stores all of your passwords. You need to remember only one master password to unlock the app. Typically password managers can generate secure, hard-to-crack passwords for you, according to the criteria of the sites you are signing up for. They also provide browser plug-ins that will autotype the password into login pages for you. So you never need to see or remember these passwords.

1Password
https://1password.com

1Password, like many of these tools, synchronizes your database of passwords between your desktop or laptop and your mobile devices. So you always have all of your passwords with you on all devices. You can also use a password manager to store other data, such as different shipping addresses, answers to security questions, your credit card data, passport number, and much more. All of it is securely encrypted and easy to find when you search for it in the app.

THE SECURITY OF PASSWORD MANAGERS

The first questions that most people ask about these tools are, "How secure are they? What if the password manager gets cracked?" These are reasonable questions, and I've seen that most people no longer worry so much about that after they learn how these tools work.

Of course, no tool is 100 percent perfect, but the use of a password manager is many times more secure than what most people do currently (such as saving passwords in a document on their computer). When evaluating the security of a tool like this, I look at two kinds of information: what the vendor says in its own documentation about its security practices, and what independent security experts say after evaluating the service.

Let's use 1Password as an example. Here are some things to know about it.

- Your master password is never transmitted from your computer or mobile device. It works entirely locally, on the device—so you can stop imagining it being hacked from a remote database on the internet.

- You never tell 1Password what your master password is. You are the only person in possession of it. So be sure to store it safely, perhaps on paper in a place where you store other important documents, like birth certificates. Remember, you can always reset your password on any website if, in the worst case, you lose access to your list of passwords.
- 1Password uses very high-level encryption for the database of your passwords. Learn more about it on the Security page on its website (https://1password.com/security).[26]
- 1Password uses open standards for its encryption tools, so the safety of these tools can be verified by independent experts around the world.
- You are never locked in to its system. 1Password makes it easy to export your data if you wish to switch to another password manager at any point.

Independent security experts, like Bruce Schneier, recommend the use of a password manager rather than keeping track in other ways.[27] The Electronic Frontier Foundation also recommends using a password manager.[28] Additionally, 1Password has received many positive reviews.[29]

There are quite a few options when it comes to choosing a password manager. A review from Wirecutter recommends LastPass (a free option) as its first choice.[30] It also recommends 1Password as an excellent choice if you are willing to pay for a tool like this (currently about thirty-six dollars per year for an individual account). It's worth reading the entire review to learn more about the criteria used and about several services and how they compare.

THE FUTURE OF AUTHENTICATION: MOVING BEYOND PASSWORDS

When you think about how easy it is for passwords to be cracked and how inconvenient it is for all of us to have to manage so many passwords, you probably think, "There must be a better way!" There are some additional forms of authentication that we will discuss in this report, such as two-factor authentication and biometric security.

One of the best essays I've seen about this problem is by Bruce Schneier: "Stop Trying to Fix the User."[31] It's written for security experts, and it chastises them for feeling superior to people who fall for phishing attacks or use the same password on many sites. I agree with what he says here: "The problem isn't the users: it's that we've designed our computer systems' security so badly that we demand the user do all of these counterintuitive things. Why can't users choose easy-to-remember passwords? Why can't they click on links in emails with wild abandon? Why can't they plug a USB stick into a computer without facing a myriad of viruses? Why are we trying to fix the user instead of solving the underlying security problem?"[32] His main point is this: "Usable security doesn't mean getting people to do what we want. It means creating security that works, given (or despite) what people do."[33]

I hope that security systems will improve over time and become more user-friendly, based on real-world behavior. In the meantime, read on for information about some current means of authentication that work together with passwords, and in some cases replace them.

Two-Factor Authentication

Two-factor authentication is the practice of asking users for a second piece of identifying information in addition to a password. If your username and password have been compromised, an attacker still won't be able to access your sites without this second factor.

This second factor is usually a numeric code, sent to you by text message, by email, or by use of an authenticator app that generates the code. It's a one-time use code, so there is no need to store it anywhere. You get a new code each time.

It's a good idea to turn this feature on where it's available because it makes it more difficult for your accounts to be compromised.[34] Many popular services, like Google, Dropbox, Twitter, Apple, Facebook, Instagram, PayPal, and Evernote, offer this feature.

At first, the idea of one more thing you need to do when logging on sounds inconvenient, so some people resist activating this feature. But remember that most sites and apps keep you logged on all the time (unless you choose to log out), so you need to enter this extra code only when installing an app for the first time on a new computer or device or when using an unfamiliar device that you haven't used to log on before.

Since most people have their mobile phone with them all the time, it's usually convenient to get your code via text message. But sometimes it's useful to use a special app, such as Authy, to generate your codes. This app is more convenient than apps that are dedicated to a particular service (like Google Authenticator) because you can use it from any of your devices and with many different accounts, including multiple Gmail accounts. It's available for multiple platforms, both desktop and mobile. Learn more about its features on the Features page of the Authy website.

Authy
https://authy.com

Authy: Features
https://authy.com/features

Some sites, like Google, also offer backup codes that you can print and keep in your wallet.[35] You could use these codes if you want to log on to a public computer and you don't have your phone with you. These are eight-digit codes that you can use only once, so you cross off each one as you use it. When you've used all the codes, you can generate a new list from Google's site.

One more thing to be aware of, especially if you are a well-known person or someone likely to be targeted by hackers (an activist, perhaps), is that it is possible for someone to hijack your SIM card and take over your mobile phone account. This is called a "SIM swap scam" and involves social engineering. Someone impersonating you calls your provider, such as Verizon, and convinces them to issue a replacement SIM encoded with your phone number. This enables the hacker to receive two-factor codes sent by text message and take over your account, even if you've added two-factor authentication.

In 2016, this happened to a Black Lives Matter activist; his Twitter account was compromised in exactly this way.[36] To protect against this, most mobile providers offer an extra (optional) security step that you can turn on, such as an account PIN. Call your mobile phone provider (or visit its website) to activate this feature.

Mobile Payments in Retail Stores

If you've wondered about the security of using mobile payment systems in retail stores—know that they can be *more* secure than using your credit card. This section will explain why.

By mobile payments, I mean Apple Pay, Google Pay, Samsung Pay, and the like. With these systems, you add your credit or debit cards to the app in advance and then swipe your phone or smartwatch at payment terminals in retail stores.

Apple Pay
https://www.apple.com/apple-pay

Google Pay
https://pay.google.com/about/

Samsung Pay
https://www.samsung.com/us/samsung-pay

The reason these services are more secure than swiping your credit card is that they make use of a random number (or token) that stands in for your credit card number and is useless if stolen. If your retail store gets hacked, your token will be on the list instead of your credit card number. This is called "tokenization" and is a way to keep your information secret from the retailer that uses it. Basically, when you enter your card information into the app, it gets encrypted and sent to your phone manufacturer's servers. The manufacturer decrypts it to identify the payment network and re-encrypts it with a key that only the card issuer and authorized providers can unlock. It sends that information to the bank, which generates a Device Account Number and sends it back to the phone manufacturer. The manufacturer doesn't decrypt that number; instead, it stores the number securely on your phone.

If you should lose your phone, you can remotely wipe your device, as described earlier in this chapter. Then you can deregister your cards from the mobile payment system and register them again on another device.

To make this system more secure, you also add to your device a passcode, fingerprint ID, or Face ID that you use to confirm your identity when using mobile payments. We'll discuss the security of biometric identification (such as Touch ID or Face ID) in the next section.

If you're interested in learning more details about how mobile payments work, see this article on Bluefin: "The Security of 'Traditional' Payments vs. Alternatives: Mobile Wallets."[37] For details about Apple Pay, see "Apple Pay Security and Privacy Overview" in the Apple support pages.[38]

Biometric Security

Biometric security involves the use of a person's physical characteristics to authenticate access. Some examples of this are fingerprint scanners, eye scanners, and facial recognition.

Let's look at two examples of these methods that are in widespread use today on Apple's iPhones: Touch ID (fingerprints) and Face ID (recognizing your face).[39]

APPLE'S TOUCH ID

Many people imagine that Apple has a central database somewhere with the fingerprints or face photos of its users. Luckily, that isn't true. As you can imagine, that would be something that cybercriminals would love to crack.

Instead, Apple stores your biometric data on your phone itself; it is never transmitted to Apple. When you set up Touch ID on an iPhone, you are asked to hold any of your fingers or your thumb over the home button a few times at different angles. You can set up any finger or thumb you like, or multiple fingers. Apple stores a mathematical representation of your fingerprint using security software called Secure Enclave on your iPhone. This is not an image of your fingerprint, but a mathematical representation of it.

This data is stored in an encrypted state inside of the Secure Enclave. Security experts say that the expertise needed to break into the Secure Enclave is far beyond the scope of the average cybercriminal.[40] Of course it is possible that someday, someone could steal your phone and crack this, but it's very, very unlikely.

One of the main advantages of Touch ID on iPhones is that it causes more people to lock their phones since it's so convenient to open it each time with your fingerprint. Before Touch ID was available, many people left their phone unlocked. Another thing to know is that your fingerprint works together with your passcode. When you restart your phone, or reset your password, you still need to enter the passcode as an additional security measure.

Touch ID can be used for unlocking your phone, authenticating Apple Pay, and authenticating your purchases on the iTunes store. You can choose to use it for any or all of these tasks. Many apps also use Touch ID to offer a convenient way to unlock individual apps. For example, 1Password (the password manager discussed earlier in this chapter) offers a way to unlock the app with Touch ID. So if you share an iPad with your family members, you can let them use it for games and movies without their being able to open your password manager.

Android phones with fingerprint ID work in a similar way. They use a secure part of the processor called Trusted Execution Environment (TEE). As on Apple's devices, the data is stored in an encrypted state on your phone. For both Apple and Android, when you erase your phone (as you would do when selling it to someone), your fingerprint data is wiped completely from the device, along with everything else.

APPLE'S FACE ID

With the release of the iPhone X in November 2017, Apple introduced Face ID—a facial recognition system for unlocking your iPhone. It replaced Touch ID on the iPhone X, which doesn't have a home button.

Of course, when this was announced, there were many questions about its security—from the public, from journalists, and from security experts. Let's look at how it works in order to understand the security situation.

The iPhone X has some special features in its front-facing camera. When you look at your phone, over 30,000 invisible dots are projected onto your face, which are read by an infrared camera. From there, the shape and structure of your face are sent to the A11 Bionic chip in your iPhone, where they get transformed into a mathematical model. This model is stored and used for comparison each time you look at your phone to unlock it.

If you choose to set up Face ID on your iPhone, you are brought to a setup screen where you are asked to turn your head around in a circle so that the camera can take the first reading. The data gets stored in the Secure Enclave chip on your phone. Your phone stores only a mathematical representation of your face, not a photograph. This data is encrypted and never leaves your device. In addition, it is not backed up in iCloud when you back up your phone.

Third-party apps that offer Face ID don't get access to the raw data model of your face. Instead, Face ID tells the app whether your face matched or not. The data is still safe in the Secure Enclave. This makes it easy to use Face ID to open apps that you have locked down individually, such as password managers or banking apps.

Face ID works in the dark and in low light because it uses an infrared camera. It also works when you are wearing a hat or glasses (and most, but not all sunglasses), or if you grow a beard or change your hairstyle. It learns over time what your appearance is since it updates the data each time you use Face ID.

Like Touch ID, Face ID doesn't entirely replace your passcode. It just reduces the number of times you need to use it. You still need to enter your passcode in certain situations, like when you restart your phone, when it hasn't been unlocked for more than forty-eight hours, or after you've made five unsuccessful attempts to use Face ID. You also need to enter your password if you remotely lock your iPhone with Find My iPhone (described earlier in this chapter). As you can see, these are important features that increase the security of your phone.

There is also a way to disable Face ID temporarily. To do that, hold down either volume button at the same time as the power button for about two seconds. (This is easy to do by squeezing your phone, since the buttons are on opposite sides. You could do this while it's in your pocket.) When the Power Off screen shows up, hit the Cancel button. You'll need to re-enter your passcode the next time to turn Face ID back on. This works the same way if you choose the Emergency SOS slider that also shows on that screen (for calling 911 or other emergency services).

Experts are recommending that you turn off Face ID (or never use it to begin with) if you are worried about law enforcement having access to your phone if you get arrested. In that situation, it is wise to turn off Face ID right away (as described above) so that your phone will be locked by a passcode instead. Courts have ruled that police can force you to use fingerprints to unlock your phone (and Face ID would presumably fall into the same category), but they can't force you to give them your passcode. According to the ACLU, it's a Fifth Amendment issue. Giving over your passcode is considered an act of testimony against yourself, but biometric data is considered an act of identification rather than an act of testimony.[41]

DECIDING WHETHER TO USE BIOMETRIC SECURITY

As with every security measure, nothing is completely secure all the time and will eventually be cracked. When new technologies like Touch ID and Face ID are announced, many people try to crack them, putting them through all kinds of extreme measures as a way of stress-testing them. The first few times someone cracks a new technology it gets a lot of media attention, with dramatic headlines. If you happen to see those headlines, you may come to feel that nothing is secure and no new technology is worth the risk.

Here's an example that came out soon after Face ID was available: "Hackers Say They've Broken Face ID a Week after iPhone X Release," by Andy Greenberg, senior writer for WIRED.[42] Greenberg makes some good points. Since this break required detailed measurements or a digital scan of the owner's face, taking about five minutes, this would be likely to happen in only a few situations—perhaps highly targeted espionage and kidnapping, not the type of hacking most iPhone owners would face.

When you are deciding whether to use Face ID or Touch ID, consider the likelihood that one of these risks will occur and the consequences to you if some of your data gets exposed. Also consider the convenience factor, since higher amounts of security are usually less convenient. The chances of a dishonest person grabbing an iPhone that you left behind somewhere with neither a passcode nor biometric security are pretty high. It would be very easy to erase the phone and sell it on eBay. So if using Touch ID or Face ID makes it convenient enough for you to implement, you are much better off.[43]

LEARNING MORE

To learn more about how biometric security works, along with the ways it could possibly be hacked, see "Biometric Authentication Overview, Advantages and Disadvantages," by Paul Cucu and available on Heimdal Security's blog.[44] And to learn about other types of biometrics, such as facial recognition of people in public places, see "Face Recognition" on EFF's website.[45]

Data Breaches and Identity Theft

Data Breaches

Data breaches are becoming more common these days.[46] This happens when criminals gain access to private information such as usernames, passwords, phone numbers, addresses, or social security numbers by hacking into sites like retail stores, email providers, and credit bureaus.

Some of the most publicized breaches in recent years include those of LinkedIn, Yahoo, and Equifax.[47] These breaches very likely made the private data of large numbers of users available on the black market to be used by cybercriminals at any point in the future.

A good way to find out if your personal data has been breached is to use the website Have I Been Pwned? This site keeps track of known data breaches. You can search by any username or email address that you use for logging in to websites. It will show you if that username has been released and which breaches contained it. My own personal email address came up in ten breaches, including LinkedIn, Adobe, and Tumblr. For each one, it will tell you when the breach happened, which data was released (usually passwords, but sometimes other data), and other details about the breach.

Have I Been Pwned?
https://haveibeenpwned.com

The site also has a Notify Me service where it will email you with news of any new breaches that contain your usernames. Have I Been Pwned? was created by Troy Hunt, a security expert, for the benefit of the general public.[48]

If you find your data in the lists, make sure to change your password on those sites and any other sites where you use the same credentials. It's common for criminals to use the same lists to try to break into many other sites, especially sites where they can spend your money, like online retailers. They know that most people use the same passwords on many sites.

Luckily, I've been using the password manager 1Password for several years, so I was using a unique password for each site and had to update passwords only for the sites that were breached. Of course I had to remember to never use those passwords for other services in the future.

To find interesting statistics on data breaches, see the "Data Breaches" at the Privacy Rights Clearinghouse.[49] It maintains a chronology of breaches from 2005 to the present in order to assist with research on breaches. It's not an exhaustive list, since many organizations are not aware they've been breached and also because laws vary by region on whether organizations are required to report breaches.

The Privacy Rights Clearinghouse also has a useful page called "What to Do When You Receive a Data Breach Notice."[50] It gives good advice and is a good page to recommend to your library users whose data has been breached.

Remember that even if your data was breached, you won't know if it was used until you are the victim of some type of fraud. The next section discusses identity theft, looks at how common it is, and talks about how to reduce the likelihood of it happening.

Protecting Your Identity

HOW COMMON IS IDENTITY THEFT?

Stories about identity theft are frequently seen in the news. But how common is it actually? When you look into the statistics, you see large numbers, but it's important to know what's behind the statistics.

Identity theft is often used as an umbrella term for several different types of fraud: credit card fraud, existing account takeover, new account creation, and identity creation.[51] Credit card fraud is easily solved by calling your bank, and often the banks notice fraudulent charges before you do and issue you a new card.[52] Full-blown identity theft, where someone takes out loans in your name, is true identity theft and is more difficult to recover from.

All of these types of fraud are often lumped together in statistics, making it hard to see how common full-blown identity theft actually is. A good source for looking at these statistics in the United States is the Bureau of Justice Statistics. It compiles statistics every couple of years and breaks them down in useful ways. From its 2014 report (the most recent available at the time of this writing) you can learn that about 7 percent of US residents (age sixteen or older) were victims of some kind of identity theft in 2014.[53] The numbers were similar in 2012. However, the majority of those cases (86 percent) were of credit card or bank account fraud.[54] According to the same report, less than 1 percent experienced the misuse of personal information to open a new account or for other fraud. There are a few other types of fraud broken down in the report, with many other interesting details and statistics.[55]

So when you see stories like this one—"Identity Fraud Hits Record Number of Americans in 2016," by Herb Weisbaum—notice that it uses statistics from a study by Javelin Research that was paid for by LifeLock, a company that sells identity theft protection.[56] This study groups credit card fraud together with full-fledged identity theft. It focuses on how much money was lost (by banks, not individual consumers) and the growth rate from previous years. For example, it states, "Fraud leaps to a record high incidence—In 2016, 6.15 percent of consumers became victims of identity fraud, an increase by more than 2 million victims from the previous year."[57]

So while identity theft is an increasing problem, the majority of cases involve fraudulent use of credit cards, which is something that is easy to recover from quickly by contacting your bank. Luckily, we have good consumer protection laws in the US, which means that the most you can be held liable for in the case of a stolen card is fifty dollars.[58] Most banks will waive this fee and pay any losses. And if you haven't lost the actual card but someone used your number, you aren't liable at all.

While it's true that the number of victims of full-blown identity theft is not a large percentage of the population, it does happen, and you need to know what to do if it does. For that, see the FTC's IdentityTheft.gov site, which offers useful advice.

IdentityTheft.gov
https://www.identitytheft.gov

BEST TYPES OF PROTECTION

According to *Consumer Reports*, it's not worth paying for identity protection services.[59] All these services do is notify you when someone uses your identity. They do nothing to prevent it. An easier (and free) way to find this out is to set up alerts from your banks and other accounts (credit cards, retirement accounts, etc.). Every bank these days has an option to notify you by email or text message when certain events occur—such as withdrawals that are over an amount that you would usually take out (you choose the amount). *Consumer Reports* recommends monitoring your accounts on a regular basis so that you can notify your banks right away if you see fraudulent activity.[60]

Security experts also recommend getting your annual free copy of your credit report and reviewing it to see if there is any false information that needs to be corrected. You can do this easily at the website AnnualCreditReport.com (https://www.annualcreditreport.com).

If you find out that your information has been compromised in a data breach, use the Federal Trade Commission's IdentityTheft.gov site. It will give you advice on what to do, depending on the circumstances, such as changing your password on the breached site and other sites where you've used the same login credentials.

Another thing you can do to protect your data is to put a freeze on your credit bureau accounts. (The top three bureaus in the US are Equifax, Experian, and TransUnion). A freeze will keep a lender from drawing your record. If you are planning to take out a car loan, get a new credit card, or apply for any type of loan, you can find out which bureau your lender is going to use and temporarily unfreeze the account so the lender can get your information. There is a fee associated with this action that ranges from five to twenty dollars, depending on which state you live in.[61] You pay the fee separately for each bureau and for each time you freeze or unfreeze your records. Experts recommend that if you don't foresee applying for any loans in the near future (or ever, especially if you are elderly), you go ahead and freeze your records.

None of these measures is 100 percent foolproof, but they can make it more difficult for your

information to be used for identity theft. And remember that in recent years, 7 percent of people in the US have been victims of ID theft that includes credit card fraud, and only 1 percent have been victims of full-fledged identity theft. So when you see news stories with dramatic headlines, keep these numbers in mind.

Notes

1. Backblaze charges five dollars per month or fifty dollars per year, for example (Backblaze "Buy" page, accessed January 3, 2018, https://secure.backblaze.com/buy.htm).
2. Joe Kissell, "The Best Online Cloud Backup Service," last updated October 3, 2017, Wirecutter, now owned by the *New York Times*, https://thewirecutter.com/reviews/best-online-backup-service/#our-pick-backblaze.
3. Justin Krajeski and Kimber Streams, "The Best Portable Hard Drive," Wirecutter, last updated October 24, 2017, https://thewirecutter.com/reviews/best-portable-hard-drive.
4. See "How to Back Up Your iPhone and iPad," by Brad Ward, January 4, 2017, on TechRadar, www.techradar.com/how-to/software/how-to-backup-iphone-ipad-1299014, for some useful instructions.
5. See "iMazing 2.2 Review: A Better Way to Use Your Mac to Manage Your iPhone and iPad," by J. R. Bookwalter, in Macworld, May 16, 2017, https://www.macworld.com/article/3196571/software/imazing-2-2-review-a-better-way-to-use-your-mac-to-manage-your-iphone-and-ipad.html, for a detailed review of all it can do.
6. For a good comparison review, see "Best Android Backup Apps," by John Corpuz, on Tom's Guide, June 27, 2017, https://www.tomsguide.com/us/pictures-story/633-best-android-backup-apps.html.
7. For a useful comparison review of these services for photo backups, see "iCloud Photo Library: The Best Cloud Photo Management Solution," by Bradley Chambers, on The Sweet Setup, October 16, 2017, https://thesweetsetup.com/apps/best-photo-management-solution.
8. Sally Wiener Grotta, "Google Photos Review: The Best Photo/Video Backup App," Tom's Guide, May 24, 2017, https://www.tomsguide.com/us/google-photos-ios-android,review-4395.html.
9. See Ed Rhee and Alina Bradford, "Find Your Lost Android Device with Google's Find My Device," CNET, May 17, 2017, https://www.cnet.com/how-to/find-your-lost-android-device-with-android-device-manager.
10. Please note Lloydbank.co.uk is now found at https://www.lloydsbank.com; Danny Palmer, "New Trojan Malware Campaign Sends Users to Fake Banking Site That Looks Just Like the Real Thing," ZDNet, August 14, 2017, www.zdnet.com/article/new-trojan-sends-users-to-fake-banking-site-that-looks-just-like-the-real-thing.
11. Danny Palmer, "1.4 Million Phishing Websites Are Created Every Month: Here's Who the Scammers Are Pretending to Be," ZDNet, September 22, 2017, www.zdnet.com/article/1-4-million-phishing-websites-are-created-every-month-heres-who-the-scammers-are-pretending-to-be.
12. Danny Palmer, "What Is Phishing? Everything You Need to Know to Protect Yourself from Scam Emails and More," ZDNet, September 6, 2017, www.zdnet.com/article/what-is-phishing-how-to-protect-yourself-from-scam-emails-and-more.
13. MacEwan University, "University Discovers Online Fraud: IT Systems Not Compromised by Incident," MacEwan News, August 31, 2017, https://www.macewan.ca/wcm/MacEwanNews/PHISHING_ATTACK.
14. Webroot, *Quarterly Threat Trends: Phishing Attacks Growing in Scale and Sophistication*, September 2017, 12, https://www.webroot.com/us/en/business/resources/threat-trends/sept-2017.
15. Julie Foote, "Beware—New Kind of Virus Embedded in a Word or Excel Document," MVTV Wireless, January 12, 2016, https://www.mvtvwireless.com/beware-new-kind-of-virus-embedded-in-a-word-or-excel-document.
16. Phia Bennin, "What Kind of Idiot Gets Phished?" episode 97 of *Reply All*, Gimlet Media, May 18, 2017, https://gimletmedia.com/episode/97-what-kind-of-idiot-gets-phished.
17. Danny Palmer, "What Is Phishing? Everything You Need to Know to Protect Yourself from Scam Emails and More," ZDNet, September 6, 2017, www.zdnet.com/article/what-is-phishing-how-to-protect-yourself-from-scam-emails-and-more.
18. "How to: Avoid Phishing Attacks," Electronic Frontier Foundation, Surveillance Self-Defense, last reviewed September 6, 2017, https://ssd.eff.org/en/module/how-avoid-phishing-attacks.
19. Andrew Tarantola, "'WannaCry' Ransomware Attack Spreads Worldwide," Engadget, May 12, 2017, updated May 13, 2017, https://www.engadget.com/2017/05/12/12-countries-hit-in-massive-cyber-heist.
20. *Kim Zetter,* "4 Ways to Protect against the Very Real Threat of Ransomware," *Wired*, May 13, 2016, https://www.wired.com/2016/05/4-ways-protect-ransomware-youre-target.
21. To learn more about how this works and how freely available this how-to information is, see Gary Sims, "How Easy Is It to Capture Data on Public Free Wi-Fi—Gary Explains," Android Authority, November 14, 2016, https://www.androidauthority.com/capture-data-open-wi-fi-726356.
22. For a detailed review of this service, see Brad Smith, "Express VPN Review," TheBestVPN, last updated September 16, 2017, https://thebestvpn.com/reviews/expressvpn.
23. Jon Brodkin, "How ISPs Can Sell Your Web History—and How to Stop Them," Ars Technica, March 24, 2017,https://arstechnica.com/information-technology/2017/03/how-isps-can-sell-your-web-history-and-how-to-stop-them.
24. To learn what to look for when choosing a VPN service, see "Choosing the VPN That's Right for You," from the Electronic Frontier Foundation, Surveillance Self-Defense, last reviewed June 9, 2016, https://ssd.eff.org/en/module/choosing-vpn-thats-right-you.
25. Bruce Schneier, "Choosing Secure Passwords," *Schneier on Security* (blog), March 3, 2014, https://

www.schneier.com/blog/archives/2014/03/choosing_secure_1.html.
26. You can learn more about the details of 1Password's security practices in its white paper *1Password Security Design*, https://1password.com/files/1Password%20for%20Teams%20White%20Paper.pdf.
27. Schneier, "Choosing Secure Passwords."
28. Electronic Frontier Foundation, "Want a Security Starter Pack?" under 5. Creating Strong Passwords, Surveillance Self-Defense, last reviewed October 16, 2017, https://ssd.eff.org/en/playlist/want-security-starter-pack.
29. Robert McGinley Myers, "1Password: The Best Password App and Manager (and Why You Need One)," The SweetSetup, August 8, 2017, https://thesweetsetup.com/apps/best-password-manager-and-why-you-need-one.
30. Joe Kissel, "The Best Password Managers," Wirecutter, August 3, 2017, last updated December 8, 2017, https://thewirecutter.com/reviews/best-password-managers.
31. Bruce Schneier, "Stop Trying to Fix the User," *IEEE Security and Privacy* 14, no. 5 (September–October 2016): 96, http://ieeexplore.ieee.org/document/7676198 (requires login).
32. Schneier, "Stop Trying to Fix the User."
33. Ibid.
34. For a list of sites that support two-factor authentication, see the website Two Factor Auth (2FA), accessed January 4, 2018, https://twofactorauth.org.
35. See the Google Account Help page "Sign In Using Backup Codes," accessed January 4, 2018, https://support.google.com/accounts/answer/1187538?hl=en.
36. Lisa Vaas, "DeRay Mckesson's Twitter Account Hacked with Just His Name and Four Digits," Naked Security, June 14, 2016, https://nakedsecurity.sophos.com/2016/06/14/deray-mckessons-twitter-account-hacked-with-just-his-name-and-four-digits.
37. "The Security of 'Traditional' Payments vs. Alternatives: Mobile Wallets," Bluefin, May 12, 2016, https://www.bluefin.com/bluefin-news/security-traditional-payment-methods-vs-alternatives-spotlight-mobile-wallets.
38. "Apple Pay Security and Privacy Overview," Apple support pages, September 21, 2017, https://support.apple.com/en-us/HT203027.
39. "Use Touch ID on iPhone and iPad," Apple Support pages, November 7, 2017, https://support.apple.com/en-us/HT201371; "About Face ID Advanced Technology," Apple Support pages, December 20, 2017, https://support.apple.com/en-us/HT208108.
40. Paul Cucu, "Biometric Authentication Overview, Advantages and Disadvantages," Heimdal Security, last updated July 28, 2017, https://heimdalsecurity.com/blog/biometric-authentication.
41. To learn more about this issue, see "Will Apple's FaceID Affect Your Rights?" by Brett Max Kaufman, Staff Attorney, ACLU Center for Democracy, September 22, 2017, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/will-apples-faceid-affect-your-rights.
42. Andy Greenberg, "Hackers Say They've Broken Face ID a Week after iPhone X Release," *Wired*, November 12, 2017, https://www.wired.com/story/hackers-say-broke-face-id-security.
43. Bruce Schneier says, "I don't think this is cause for alarm, though. Authentication will always be a trade-off between security and convenience. FaceID is another biometric option, and a good one. I wouldn't be less likely to use it because of this." (Bruce Schneier, "Apple FaceID Hacked," *Schneier on Security* [blog], November 15, 2017, https://www.schneier.com/blog/archives/2017/11/apple_faceid_ha.html).
44. Paul Cucu, "Biometric Authentication Overview, Advantages and Disadvantages," Heimdal Security's blog, last updated July 28, 2017, https://heimdalsecurity.com/blog/biometric-authentication.
45. "Face Recognition," EFF, Street-Level Surveillance, accessed January 4, 2018, https://www.eff.org/pages/face-recognition.
46. Olga Kharif, "2016 Was a Record Year for Data Breaches," Bloomberg Technology, January 19, 2017, https://www.bloomberg.com/news/articles/2017-01-19/data-breaches-hit-record-in-2016-as-dnc-wendy-s-co-hacked; "2017 Data Breaches," Identity Theft Resource Center, accessed December 12, 2017, www.idtheftcenter.org/Data-Breaches/data-breaches.
47. Robert Hackett, "LinkedIn Lost 167 Million Account Credentials in Data Breach," *Fortune*, May 18, 2016, http://fortune.com/2016/05/18/linkedin-data-breach-email-password; Selena Larson, "Every Single Yahoo Account Was Hacked—3 Billion in All," CNN Tech, October 4, 2017, http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html; Seena Gressin, "The Equifax Data Breach: What to Do," FTC Consumer Information, September 8, 2017, https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.
48. Troy Hunt, "Who, What & Why," Have I Been Pwned? accessed January 4, 2018, https://haveibeenpwned.com/About.
49. "Data Breaches," The Privacy Rights Clearinghouse, accessed January 4, 2018, https://www.privacyrights.org/data-breaches.
50. "What to Do When You Receive a Data Breach Notice," The Privacy Rights Clearinghouse, February 1, 2006, revised November 2, 2017, https://www.privacyrights.org/consumer-guides/what-do-when-you-receive-data-breach-notice.
51. This article does a good job of explaining the different types of fraud that are counted under the term *identity theft*: Bob Sullivan, "Just How Common Is ID Theft?" NBC News, last updated June 20, 2005, www.nbcnews.com/id/8409283/ns/technology_and_science-security/t/just-how-common-id-theft.
52. "Among victims who experienced the unauthorized use of an existing account, 48% discovered the incident when a financial institution contacted them about suspicious activity on their account." (US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, "Victims of Identity Theft, 2014," NCJ 248991 (September 2015, revised November 13, 2017): 5, https://www.bjs.gov/content/pub/pdf/vit14.pdf.)
53. Bureau of Justice Statistics, "Victims of Identity Theft, 2014." Depending on when you are reading this, you

may want to look for a more recent report from the Bureau of Justice Statistics on its Identity Theft page (https://www.bjs.gov/index.cfm?ty=tp&tid=42).

54. Bureau of Justice Statistics, "Victims of Identity Theft, 2014."
55. Ibid.
56. Herb Weisbaum, "Identity Fraud Hits Record Number of Americans in 2016," NBC News, February 2, 2017, https://www.nbcnews.com/business/consumer/identity-fraud-hits-record-number-americans-2016-n715756; "Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study," news release, Javelin, February 1, 2017, https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new; LifeLock homepage, accessed January 4, 2018, https://www.lifelock.com.
57. Ibid.
58. "Am I Responsible for Unauthorized Charges if My Credit Cards Are Lost or Stolen?" Consumer Financial Protection Bureau, July 11, 2017, https://www.consumerfinance.gov/ask-cfpb/am-i-responsible-for-unauthorized-charges-if-my-credit-cards-are-lost-or-stolen-en-29.
59. "Don't Get Taken Guarding Your ID: Do-It-Yourself Safeguards Are Just as Effective as Paid Services," *Consumer Reports*, January 2013, updated September 8, 2014, https://www.consumerreports.org/cro/magazine/2013/01/don-t-get-taken-guarding-your-id/index.htm.
60. Ibid.
61. Katherine Ross, "How Much It Costs in Every State to Freeze Your Credit Report," ValuePenguin, September 2017, https://www.valuepenguin.com/states-where-freezing-your-credit-will-cost-you-most.

Chapter 3

Privacy

Is Privacy Dead?

With so many news headlines recently about privacy invasions, it may seem as if privacy is dead. Some people say, well, all my data is out there already, and I have nothing to hide, so I don't care. I'm a needle in a haystack. Others fear using websites and tools used by most people (like Facebook) because they've heard scare stories about what these sites know about us.

It's true that in many ways our data is no longer private, but it's also true that we can take steps to make our data more private. That's what this section is about. You can learn to use tools like ad blockers, private browsing, private search engines, anonymous browsers, encrypted messaging, and more. I'll define these tools, explain how to get them, and discuss under what circumstances you might want to use them.

Private Browsing and Searching

Targeted Advertising

Have you ever noticed that ads appearing on Facebook or other websites are showing you products that you recently looked at elsewhere? This can feel quite eerie, and some people fear that Facebook is spying on them. There are even those who fear that Facebook is listening to their conversations through the microphone on their phone.[1]

What's actually happening is something called "targeted advertising." It works like this: there are ad networks whose goal is to show you relevant ads, based on your web browsing behavior. They use a bit of code called a "third-party cookie" to do this. Cookies have been in use by websites for a long time. They are bits of text that are stored in your browser for the purpose of saving your preferences for a particular site—preferences like your username, your zip code (for weather sites), your game scores, and the like. Cookies set by the site you are currently on are called "first-party cookies." They save your information in order to make it easier for you the next time you visit. Third-party cookies are used by ad networks, and they are shared by all the members of an ad network. So if you are browsing for new shoes on one site, the next day you might see ads for similar shoes on other sites or on Facebook. Some people don't mind this because they are seeing ads that are relevant for things they are interested in. Others don't like it and feel it to be an invasion of privacy.

If it bothers you, there are ways you can opt out. One of the easiest ways is to install an ad blocker extension in your web browser. One of the most popular ad blockers is Adblock Plus. It's a free, open-source tool that you can install in browsers like Chrome, Safari, Firefox, and more. It can hide ads and disable tracking with those third-party cookies described above. You can get mobile app versions for iOS and Android as well. For a good list of recommended privacy tools like this, see the article "Best Ad Blockers and Privacy Extensions," by John Corpuz, on Tom's Guide.[2] Most of these tools have the ability to whitelist particular sites. You may want to allow ads on certain sites you want to support since they rely on advertising dollars. It's just a quick click of a button in your browser to allow ads on a particular site.

Adblock Plus
https://adblockplus.org

Adblock Plus for iOS
https://itunes.apple.com/us/app/adblock-plus-abp-remove-ads-browse-faster-without-tracking/id1028871868?mt=8

Adblock Plus for Android
https://adblockplus.org/android-install

To turn off targeted advertising in Facebook, go to your Settings, Ads, Ad Settings, then "Ads based on your use of websites and apps." You can choose to turn it off or leave it on. Facebook reminds you that you will still see ads, just not those based on what you do on other websites. Facebook calls these "interest-based ads."

This type of targeted advertising is so common and on so many sites that it almost seems creepy—you look at something, and suddenly it appears on all the other sites you visit.[3]

Your Search Engine History

If you wonder how easy it is for others to see your search history, the answer is, *very* easy. If you share your computer with others and have a snoopy friend or family member, all they have to do is visit the History menu of your browser. The History menu was designed to be a convenient way to go back to sites you've visited in the past, especially when you can't remember what they were called. Just browse through your history until you find the site you're looking for. But sometimes people use this feature to see what sites others have been visiting.

Also, Google tracks your search history when you are logged into any Google services, such as Gmail, YouTube, Google Voice, Google Contacts, and so on. You can log out of Google before you do a search, but it's possible that not being logged in will decrease the relevancy of your Google results. Google uses your previous searches to "personalize" your results. It is possible to delete your search history by visiting your My Activity page. From there you can delete individual searches or delete your entire history. If you've never looked at your My Activity page, it's worth taking a look at. You might be surprised how much data is there.

Google—My Activity
https://myactivity.google.com

To keep your searches private from people who share your computer, you can use private browsing (known as Incognito Mode in Chrome). This allows you to open a new private window where your search and browsing history won't be tracked. This feature is found in the File menu of your browser; look for New Incognito Window or New Private Window. You can do this in your mobile browsers also. In Safari on an iPhone, tap the squares to open a new tab, then tap Private. You'll get a window that looks different and reminds you that you are in Private mode. To turn it off, tap Private again—it's a toggle.

Websites and Apps for Privacy

Another solution for private browsing is to use special apps or search engines. Two of the best are Firefox Focus (a mobile app for iOS and Android) and DuckDuckGo (a private search engine website and mobile app).[4] Firefox Focus is set up for automatic private browsing. It doesn't track you or let ad networks track you. You type into a search box and browse from there. You can hit the Erase button when you're finished to erase everything you've done in that session. It's handy for an occasional private search on your mobile device. It's not convenient to use it as your primary browser because it doesn't have features we've come to expect, like tabs and bookmarking. But it's great as a supplement to your primary browser.

DuckDuckGo is a search engine that is focused on protecting your privacy. It doesn't track your searches ever. You can find it on the web or use the DuckDuckGo mobile app for Android or iOS.

DuckDuckGo
https://duckduckgo.com

Using Private Mode or these special privacy apps will hide your searches from those who share your computer, but certain parties can still see what you've searched—your internet service provider, your employer (if you are on a company network), and the individual sites that you visit (since they keep logs of the IP addresses of visitors). And in early 2017, the US Senate voted not to implement privacy regulations that would have required ISPs to get your consent before selling your web browsing data to advertisers.[5]

So if you don't want your ISP to have your browsing data, there are some other useful tools. The first is a VPN (virtual private network), discussed in the last chapter. A VPN will encrypt your entire session so that even your ISP can't see which sites you are visiting.

If you also want to be anonymous, there is a useful tool called Tor (The Onion Router). It consists of software and a global network of servers that make

it difficult to trace web traffic back to its source.[6] It works by sending your traffic through a relay of different servers, each with a layer of encryption that is peeled back at each relay in order to find out where to send it to next. This makes it very difficult to find out which computers are visiting which sites. Tor has a desktop web browser and mobile apps for many different platforms. You can download the browser the website and find the mobile apps in the iTunes store or Google Play. There are several different apps, and two of the most highly recommended ones are Onion Browser (iOS), and Orbot (Android).

Tor
https://www.torproject.org

Onion Browser
https://mike.tig.as/onionbrowser

Orbot
https://guardianproject.info/apps/orbot

If you need anonymity, Tor is a good option. It can be slow, however, since it's sending your traffic through so many relays, so it's not practical to use for everything. Who uses Tor? It's used by criminals on the dark web, journalists who need to protect their sources (and themselves), people in countries with restricted internet, and everyday users who value privacy. Even though criminals sometimes use it, it also has many positive uses for activists, whistleblowers, law enforcement, IT professionals, and people researching sensitive topics.[7]

Your Location History

Many mobile apps use location tracking features to provide useful information, like directions and traffic reports or weather for your current location. Often the location tracking continues even when you're done using the app.

If you've never checked the location settings for the apps on your mobile devices, it can be surprising to see how completely your movements can be tracked. For an example, take a look at your location history on a map in Google's Timeline. You'll see all the places where Google has tracked you, going back in time. Most of this data is from the location services on your mobile phone. Android users have this data collected routinely, and Apple users have it collected if you use Google Maps or Google search on your iPhone or iPad. Your location data is tracked from cell towers, Wi-Fi, and GPS satellites. If you don't want to be tracked this way, you can turn off your location history in Google on the Help page. You can pause tracking temporarily or turn it off permanently. You can also delete all of your past location history.

Google—Timeline
https://www.google.com/maps/timeline

Google Support—Manage or Delete Your Location History
https://support.google.com/accounts/answer/3118687

It's also a good idea to check the location settings for individual apps. On Apple devices (iOS 11), you can do this by going to Settings, Privacy, Location Services. On that screen, you can see a list of all your apps that use location data. You can turn off Location Tracking entirely for all apps, but if you do that, you won't be able to use many important features of your phone, such as navigation in Google Maps. So instead, look at the list of apps, and for each one, select Never, While Using the App, or Always. I set most of my apps to While Using the App, but for Google Maps, I keep it on Always because it's needed for navigation, real-time traffic and transit updates, and seeing places near me. I use these features often, so I feel the trade-off is worth it. When you are on the screen for each app, be sure to read the notes about how the app uses your location. For example, I have a travel app called App in the Air. The note says, "App in the Air will use your location information to identify nearby airports and enable in-airport navigation." These notes make it easy to know what features you will lose if you set it to Never.

At the bottom of the iOS Location Services screen, after the list of apps, is a choice called System Services. Here you can turn location on or off for features like Compass Calibration, Emergency SOS, Find My iPhone, Location-Based Apple Ads, and so on. For detailed advice on which settings to choose, see Christian Zibreg's blog post "How to Stop iPhone from Tracking Your Location," *iDownload Blog*.[8] For instructions on how to manage your location settings on Android, see Brittany McGhee's article "How to Stop Android Apps Accessing Your Location."[9]

If you would like to learn more about what your location history can show about you, along with the privacy implications, read "Location Tracking" on the privacy website Me and My Shadow.[10] As you can see, there is a trade-off between the convenience of location services and the privacy implications. Luckily, most modern mobile devices have fine-grained settings, as described above, that you can use in ways that make sense for you.

Facebook Privacy Settings

If you use Facebook, you'll find it useful to check your privacy settings and ad settings. From the Facebook Settings screen, start by looking at the section called Privacy. Here you can make choices under "Who can see my stuff?" "Who can contact me?" and "Who can look me up?" For each item, such as Future Posts, you can select from choices like Public, Friends, Friends Except..., Specific Friends, Only Me, and Custom. Using these options, you can make lists of groups of friends and fine-tune who sees your posts. You can also choose who can send you friend requests and who can look you up by your email address or phone number.

Another section of Facebook settings that's worth looking at is the Ads section. You may want to begin with the subsection called Ad Settings. Here you can say Yes or No to "Ads based on your use of websites and apps." This is the targeted advertising that we discussed earlier in the chapter. Facebook calls this "online interest-based advertising" and reminds you that if you say No, you'll still see ads; they just won't be based on your interests and therefore probably less relevant.

If you don't want all of your friends to see everything that you like on Facebook, you can turn that off in the subsection called "Ads with your social actions." The two choices for this are No One or Only My Friends.

Another part of the Ads section that is worth looking at and adjusting is the subsection called Your Interests. Here you'll see many specific topics related to things you've clicked on or liked on Facebook. It's worth looking through these and deselecting the topics that are not of interest to you. Some of these are very broad, like Air Travel, and others are specific, like Human Rights Watch. For each of these, Facebook tells you that "you have this preference because you liked a page related to [fill in the topic]." If you care about the type of ads you see on Facebook, this could help make the ads more relevant to you.

Facebook has a page that describes how it collects information about you for targeted advertising. It's worth reading to understand how this works.[11] M.J. Kelly, a blogger for Mozilla, also recommends checking your app settings to see what Facebook apps you're sharing information with. To learn more about Facebook privacy, see M. J. Kelly's blog post "Facebook Privacy Tips: How to Share without Oversharing."[12]

More Privacy with Encryption

Encrypted Messaging

An excellent way to keep your messaging private is to use an app that encrypts all of your messages by default. This means that even if your network traffic is being monitored, no one can read the contents of your text messages, not even those who run the app's servers. One of the best apps for this is called Signal, from Open Whisper Systems. It's recommended by security experts like Bruce Schneier and also by Edward Snowden.

Signal
https://signal.org

Signal is available for desktop and mobile platforms and is very easy to use. See its website for links to the apps for various platforms, including iPhone, Android, Mac, Windows, and Linux. The Electronic Frontier Foundation has some useful guides to using Signal,[13] but it's so easy, you likely won't need a guide. You can also make secure video calls or voice calls with Signal. Signal is free and open-source, and Open Whisper Systems doesn't do any kind of ad tracking.[14] It's a nonprofit, supported by grants and donations.

Of course, if you want encrypted communication, you'll need to convince those you communicate with to use Signal. Signal is very good for situations where you need the most secure and private communication. If you back up your phone to a cloud service, your Signal messages are not included. They stay safely encrypted on your device. When you share your contact list with the app, so you can find other users, Signal encrypts the list before it goes to the server. It's used only to match you with people in your contacts list who also have Signal.

When would you need this level of privacy? You might use Signal if you are worried about snooping from your government, law enforcement, employers, or criminal groups. You might be an activist, a journalist protecting sources, or just someone who cares a lot about privacy. News sources like the *New York Times* recommend that people use Signal and similar apps to send them confidential tips.[15] This is a good app to recommend to someone you know who is in a situation that requires very strong privacy.

To learn more about how Signal compares to other secure messaging apps, read Michah Lee's article "Battle of the Secure Messaging Apps: How Signal Beats WhatsApp" in the *Intercept*.[16] Signal is worth using for keeping your messages and phone calls completely private.

Encrypted Email

If you want to communicate securely by email, there are some useful tools that will enable that. Most email providers have a web version, and you should always look to see if the address bar contains `https` at the beginning of the URL (instead of `http`). This is known

as transport-layer encryption and is often used by retail websites and banks.

This is good, but even with https, your email provider still gets an unencrypted copy of your messages. If you are worried about government or law enforcement contacting your email provider with a warrant to read your messages, this won't give you privacy. For example, let's say you are working for a company and learn of wrongdoing that you would like to report to the media by email. Even if your company email uses `https`, the company will still be able to read your messages, so it's not a good idea to use its system if you are a whistle-blower.

This is when a fully encrypted email app becomes useful. One of the best and easiest ones to use is a webmail app called ProtonMail. It's a secure email system, based in Switzerland. It stores all of your email fully encrypted, so even ProtonMail itself can't read your messages. If a warrant was issued for your messages, they would have nothing to turn over. It has a web version and mobile apps for iOS and Android.

ProtonMail
https://protonmail.com

Learn more about ProtonMail in Melanie Pinola's article "ProtonMail Is the Easiest Way to Send and Receive Encrypted Emails," in Lifehacker.[17]

Another encryption tool you might want to try is Mailvelope. It's a browser extension for Chrome and Firefox that you can use to encrypt messages in various webmail providers, like Outlook.com, Yahoo Mail, or Gmail. Learn more in Andy Wolber's article "Simple Security: How Gmail, Mailvelope, and Virtru Make Encrypted Email Easier," in TechRepublic.[18] You may also want to check the Mailvelope installation guide, which describes the basics of how it works.

Mailvelope
https://www.mailvelope.com

Mailvelope Installation Guide
https://www.mailvelope.com/en/help

Metadata: What It Reveals

End-to-end encryption is very useful, but it protects only the contents of your communication, not the fact that you communicated with someone. Metadata is associated with your communications, and this can be mined to learn things about you.

For example, someone who has access to your phone call metadata could find out that you called a suicide prevention service, or an HIV testing service, or your gynecologist and then Planned Parenthood, and so on. They don't know what was said, but they might conclude things about you. If you are calling from your cell phone, then your location can be tracked as well. Metadata that can be found (if you use encryption without a VPN) include which websites you visit, what phone numbers you call or message, and your IP address (which tells the location of your computer).

If you want to protect your metadata, security experts recommend using Tor, a VPN, or both at the same time as full encryption. (Tor and VPNs were discussed earlier in this report). This will make you anonymous (or nearly so, for all practical purposes).[19] To learn more details about Tor, what it's used for, who uses it, and why, see Will Nicol's article "A Beginner's Guide to Tor: How to Navigate through the Underground Internet," in Digital Trends.[20]

Webcam Privacy and Internet of Things

Remote Camera Hacking

Have you ever thought about covering your laptop or desktop computer's camera? Does that seem too paranoid? If you search Google for "laptop camera hacked," you'll see many stories of people who were spied on. It turns out that this kind of spying is something that's fairly easy to do, and there have been many instances of spying on random people through their webcams.[21]

Security experts recommend that you cover your laptop camera, because even on Macs (which are usually less vulnerable to malware), the indicator light for your camera can be turned off as part of a hack.[22] So you have no idea that your camera is recording.[23]

According to former hacker (now security expert) Kevin Mitnick, even your cell phone camera can be hacked by those willing to pay the cost of the software to do it. For someone who has physical access to your phone and knows your passcode, there is software that anyone can buy online to enable this kind of spying, for example, Flexispy. Remember, someone has to have access to your phone to do this, so it's usually done by someone who knows you, such as a significant other who suspects you of cheating.

Flexispy
https://www.flexispy.com

Cell phone cameras can be hacked remotely, but that is very, very expensive, so it's usually done by only nation states or government agencies like the FBI, law enforcement, or the NSA. There are software

exploits that can be purchased for more than a million dollars that will let someone remotely spy on an individual's iPhone without being easily detected.[24] Android exploits are a bit cheaper, since Android devices are easier to hack.

Experts recommend the simple solution of covering your computer's webcam. You can search online for "webcam cover" for commercial solutions, or try one of the simple DIY approaches from Jacob Brogan's blog post, "What's the Best Way to Cover Your Webcam?" from *Slate*.[25] I use his suggestion of Japanese washi tape, since it's easy to remove without leaving a residue.

It's also recommended that you keep your operating systems up-to-date on your computers and mobile devices. Whenever software vulnerabilities are found (such as those that could enable remote camera hacking), vendors rush to release updated versions that fix the problem. So it's a good idea to install updates soon after they are released.

Smart Home Devices

Smart speakers like Amazon Echo and Google Home have some people worried. Do we really want a device that is always listening in our homes? Luckily, it's not as awful as it seems.

The way these devices work is that they listen for the assigned "wake word," such as "Alexa," or "Hey Google." Then they record what you ask them, stopping the recording when they begin to answer a few seconds later. So even though the microphones need to be on in order to hear your wake word, they aren't recording except after each wake word and before each answer.

These devices send your questions to the cloud in order to pull the information they need from the internet. So your questions are stored on Amazon's or Google's servers. You can choose to go online and delete particular recordings, or all of your recordings if you like. For Amazon, go to your Alexa mobile app and look under Settings, History. From there you can see and hear all of your saved recordings and delete them one by one. If you want to delete all of them at once, you can do that from your computer's web browser on the Amazon site, under Manage Your Content and Devices, Your Devices, Amazon Echo, Manage Voice Recordings. From there you can delete all of the saved recordings. Google has the same features on its My Activity page. Look for Assistant, choose that and see each recording, which you can delete one by one. To delete a whole batch of recordings (or all of them), look for the three dots on the top menu bar of My Activity. In that menu, select Delete Activity By, then choose Assistant as the product, and enter a date range. From there you can delete a batch of recordings.

Google—My Activity
https://myactivity.google.com

It's also good to know that you can turn off the microphones anytime you like on these devices (if you aren't going to use them for a while). This is handy when you are listening to a podcast or TV show that mentions your wake word frequently. The off button for an Echo is on the top, and for Google Home is on the back.

Other privacy features are available as well, such as setting a PIN code for voice purchasing on the Echo (so you can order products by voice only if you know the PIN). Google Home has a way to train it to recognize different people in your household and connect each person only to their own calendar so that others can't access your appointments. Amazon's Alexa service has also added the feature of recognizing individual voices after you train it. You can also choose to turn off personal results (calendar, upcoming flights, etc.) in the settings for Google Home.[26]

For more details on controlling your privacy on these devices, see David Nield's Field Guide article "How to Lock Down Your Privacy on the Amazon Echo and Google Home."[27] And for some interesting thoughts about the future of internet-connected devices, see "The Internet of Things Connectivity Binge: What Are the Implications?" by Lee Rainie and Janna Anderson, Pew Research Center.[28] This article consists of interviews with several experts and concludes with this thought: "Despite wide concern about cyberattacks, outages and privacy violations, most experts believe the Internet of Things will continue to expand successfully the next few years, tying machines to machines and linking people to valuable resources, services and opportunities."[29]

Notes

1. Emma Hinchliffe, "Why Everyone Is So Convinced Facebook Is Spying on Their Conversations," Mashable, October 7, 2017, http://mashable.com/2017/10/07/why-it-feels-like-facebook-is-spying/#It3XCCGa8aqZ; Antonio Garcia Martinez, "Facebook's Not Listening through Your Phone. It Doesn't Have To," *Wired*, November 10, 2017, https://www.wired.com/story/facebooks-listening-smartphone-microphone.
2. John Corpuz, "Best Ad Blockers and Privacy Extensions," Tom's Guide, July 6, 2017, https://www.tomsguide.com/us/pictures-story/565-best-adblockers-privacy-extensions.html.
3. For a good story that explains the details of targeted advertising, see the article "Facebook's Not Listening through Your Phone. It Doesn't Have To," by Antonio Garcia Martinez, in *Wired*, November 10, 2017, https://www.wired.com/story

/facebooks-listening-smartphone-microphone.
4. Nick Nguyen, "Introducing Firefox Focus—A Free, Fast Private Browser for iPhone," *Mozilla Blog*, November 17, 2016, https://blog.mozilla.org/blog/2016/11/17/introducing-firefox-focus-a-free-fast-and-easy-to-use-private-browser-for-ios; DuckDuckGo homepage, accessed January 5, 2018, https://duckduckgo.com.
5. Jon Brodkin, "Senate Votes to Let ISPs Sell Your Web Browsing History to Advertisers," Ars Technica, March 23, 2017, https://arstechnica.com/tech-policy/2017/03/senate-votes-to-let-isps-sell-your-web-browsing-history-to-advertisers.
6. Lee Mathews, "What Tor Is, and Why You Should Use It to Protect Your Privacy," *Forbes*, January 27, 2017, https://www.forbes.com/sites/leemathews/2017/01/27/what-is-tor-and-why-do-people-use-it/#41e4fbb97d75.
7. Learn more about use cases for Tor on the "About Tor" page from the project website (https://www.torproject.org/about/torusers.html.en).
8. Christian Zibreg, "How to Stop iPhone from Tracking Your Location," *iDownload Blog, April 28, 2016,* www.idownloadblog.com/2016/04/28/how-to-stop-phone-location-tracking.
9. Brittany McGhee, "How to Stop Android Apps Accessing Your Location," AndroidPIT, February 7, 2017, https://www.androidpit.com/how-to-stop-android-apps-accessing-your-location.
10. "Location Tracking," Me and My Shadow, last updated February 15, 2017, https://myshadow.org/location-tracking.
11. See the page "About Facebook Ads," Facebook, https://www.facebook.com/ads/about.
12. See M. J. Kelly's blog post "Facebook Privacy Tips: How to Share without Oversharing," *Mozilla Blog, January 25, 2017,* https://blog.mozilla.org/internetcitizen/2017/01/25/facebook-privacy-tips.
13. Electronic Frontier Foundation, "How to: Use Signal on iOS," Surveillance Self-Defense, last reviewed March 17, 2017, https://ssd.eff.org/en/module/how-use-signal-ios; Electronic Frontier Foundation, "How to: Use Signal for Android," Surveillance Self-Defense, last reviewed March 17, 2017, https://ssd.eff.org/en/module/how-use-signal-android.
14. Read the Privacy Policy (https://signal.org/signal/privacy) for more information.
15. "Got a Confidential News Tip?" *New York Times* website, accessed January 5, 2018, https://www.nytimes.com/newsgraphics/2016/news-tips.
16. Michah Lee, "Battle of the Secure Messaging Apps: How Signal Beats WhatsApp," The Intercept, June 22, 2016, https://theintercept.com/2016/06/22/battle-of-the-secure-messaging-apps-how-signal-beats-whatsapp.
17. Melanie Pinola, "ProtonMail Is the Easiest Way to Send and Receive Encrypted Emails," Lifehacker, March 17, 2016, https://lifehacker.com/protonmail-is-the-easiest-way-to-send-and-receive-encry-1765491376.
18. Andy Wolber, "Simple Security: How Gmail, Mailvelope, and Virtru Make Encrypted Email Easier," TechRepublic, July 13, 2016, https://www.techrepublic.com/article/simple-security-how-gmail-mailvelope-and-virtru-make-encrypted-email-easier.
19. Glenn Fleishman, "Anonymous Browsing with Tor Reduces Exposure but Still Has Risks," Macworld, January 17, 2017, https://www.macworld.com/article/3152823/security/anonymous-browsing-with-tor-reduces-exposure-but-still-has-risks.html.
20. Will Nicol, "A Beginner's Guide to Tor: How to Navigate through the Underground Internet," Digital Trends, January 29, 2016, https://www.digitaltrends.com/computing/a-beginners-guide-to-tor-how-to-navigate-through-the-underground-internet.
21. Mark Yates, "Time to Tape Over the Camera on Your Laptop," AVG, September 26, 2016, https://www.avg.com/en/signal/why-you-should-cover-the-camera-on-your-laptop-or-tablet; Charlie Osborn, "Shodan: The IoT Search Engine for Watching Sleeping Kids and Bedroom Antics," ZDNet, January 26, 2016, www.zdnet.com/article/shodan-the-iot-search-engine-which-shows-us-sleeping-kids-and-how-we-throw-away-our-privacy.
22. Bruce Snell, "IoT and Privacy: Keeping Secrets from Your Webcam," McAfee, February 10, 2016, https://securingtomorrow.mcafee.com/consumer/family-safety/iot-and-privacy-keeping-secrets-from-your-webcam.
23. Ashkan Soltani and Timothy B. Lee, "Research Shows How MacBook Webcams Can Spy on Their Users without Warning," *Washington Post*, December 18, 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/12/18/research-shows-how-macbook-webcams-can-spy-on-their-users-without-warning/?utm_term=.58f6603424b6.
24. Chris Synder, "Hackers and Governments Can See You through Your Phone's Camera—Here's How to Protect Yourself," Business Insider, March 7, 2017, www.businessinsider.com/hackers-governments-smartphone-iphone-camera-wikileaks-2017-3.
25. Jacob Brogan, "What's the Best Way to Cover Your Webcam?" from *Slate*, September 15, 2016, www.slate.com/blogs/future_tense/2016/09/15/the_best_ways_to_cover_a_webcam.html.
26. See the Google Home help page "Data Security & Privacy on Google Home," accessed January 5, 2018, https://support.google.com/googlehome/answer/7072285?hl=en.
27. David Nield, "How to Lock Down Your Privacy on the Amazon Echo and Google Home," April 27, 2017, https://fieldguide.gizmodo.com/how-to-lock-down-your-privacy-on-the-amazon-echo-and-go-1794697554.
28. Lee Rainie and Janna Anderson, "The Internet of Things Connectivity Binge: What Are the Implications?" Pew Research Center, June 6, 2017, www.pewinternet.org/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the-implications.
29. Ibid.

Chapter 4

Applying Best Practices

Why It's Important to Practice Effective Security

Now that you've read about all the different types of security issues and possible invasions of privacy, you might be feeling overwhelmed. When does one even begin to have time to deal with any of this? You may feel that you have nothing to hide anyway and that there are minuscule chances of anyone wanting to find your data. Many people feel this way, and it's not uncommon to throw up your hands and say that if someone did want to hack your data, there would be nothing you could do to prevent it anyway.

You may not be an interesting target or have very important data to protect, but what you do as an individual does makes a difference to others on the internet, for several reasons. First, your devices might be infected to become part of a "botnet" used to launch large-scale denial of service attacks. An example is the attack that happened in October 2016, where many hacked Internet of Things devices (cameras, routers, DVRs, and printers) were used in an attack on a large internet infrastructure provider.[1] This created huge bottlenecks that made it hard for people to access major sites powered by that provider, like Amazon, Twitter, Netflix, and Spotify. This malware worked by scanning the internet for hardware that was powered by default usernames and passwords.

In addition, your email account could be compromised and used to send email to everyone in your address book in the hopes of breaching their accounts. Or you could be targeted by ransomware that demands that you infect your friends in order to get the key to unlock your computer.[2]

When it comes to government surveillance, you might not feel that it matters for you, but journalists and political activists depend on privacy tools to do their work. Tools like Signal, DuckDuckGo, and Tor are worth using and supporting with donations because when more people use them, individuals are less likely to be singled out and thought suspicious because they use encryption. And with more users, these tools can get more donations to keep their services running.

So even if most people don't need all of the different types of tools mentioned in this report, it's likely that using some of them in specific situations makes sense for everyone. And it's important to have a basic understanding of this entire topic as a part of today's digital literacies so that you can protect yourself and better assist library users.

Tips for Getting Started

We've covered a large number of tools and tips in this report. If you'd like to know which practices are most important to begin with, read on.

Where to Start with Security

These are the top four most important security practices as a starting point:

1. Use a password manager. Use the following two sources for recommendations on choosing one and also for how to create a strong password for those few that you keep in your head.
   - Alan Henry, "The Five Best Password Managers," Lifehacker, August 22, 2017, http://lifehacker.com/5529133/five-best-password-managers.
   - "Creating Strong Passwords," Electronic Frontier Foundation, Surveillance Self-Defense,

last reviewed October 16, 2017, https://ssd.eff.org/en/playlist/want-security-starter-pack#creating-strong-passwords.

2. Set up Find My iPhone or the equivalent on Android. It's important to have a way to remotely erase your data if your device goes lost or missing.
   - "Find My iPhone," Apple, accessed January 8,2018,https://www.apple.com/icloud/find-my-iphone.
   - Chris Smith, "Google Can Help You Track Down Your Lost iPhone and Android Devices," BGR, June 1, 2016, http://bgr.com/2016/06/01/google-find-your-phone-iphone-android.
3. Set up regular backups, both local and remote. It's important to have backups on local drives and also on a remote cloud service in case anything happens to your devices.
   - Joe Kissell, "The Best Online Cloud Backup Service," Wirecutter, last updated October 3, 2017, http://thewirecutter.com/reviews/best-online-backup-service.
4. Use a VPN on public Wi-Fi. Get a VPN app for those times when you use your computer or mobile devices on public Wi-Fi (airports, coffee shops, and more).
   - "Choosing the VPN That's Right for You," Electronic Frontier Foundation, Surveillance Self-Defense, last reviewed June 9, 2016, https://ssd.eff.org/en/module/choosing-vpn-thats-right-you.

Where to Start with Privacy

These are the top three practices for protecting your privacy:

1. Use private browsing. Make sure you know how to browse privately.
   - Matt Klein, "How to Enable Private Browsing on Any Web Browser," How-To Geek, February 15, 2017, https://www.howtogeek.com/269265/how-to-enable-private-browsing-on-any-web-browser.
2. Use a private search engine. Use a private search engine for those searches you don't want associated with your accounts on Google (or other search engines).
   - DuckDuckGo (search engine that doesn't track you) homepage, accessed January 8, 2018, https://duckduckgo.com.
3. Install an ad blocker. If you don't want to see ads based on pages you've browsed, install an ad blocker.
   - John Corpuz, "Best Ad Blockers and Privacy Extensions," Tom's Guide, July 6, 2017, http://www.tomsguide.com/us/pictures-story/565-best-adblockers-privacy-extensions.html#s1.

For most people, using the practices above will give you a strong foundation for keeping your data safe.

Assisting Library Users

As librarians, we aren't in a position to give legal advice, but we can serve as resources for guiding people to the best information about privacy and security.

As we do with many other topics, we can offer privacy and security information in a number of ways. You might want to offer guides on your website or create printed handouts. Perhaps you'd like to offer workshops, run either by your own library staff or by local security experts that you invite.

Another option might be to familiarize yourself with the CryptoParty movement. It's a decentralized, global, grassroots movement for spreading the word about security and privacy basics and training the general public. You can learn more about it on the CryptoParty wiki (https://www.cryptoparty.in).[3] Your library meeting rooms might be a useful place for those in your local community who wish to organize these meetings.

If you would like one single best source to recommend to people, make sure your staff members know about this site: Surveillance Self-Defense, Electronic Frontier Foundation (https://ssd.eff.org/en). It's a comprehensive guide to best practices for security and privacy. It offers "playlists" or selected guides to which parts of the site to read if you are from any of the following groups: academic researchers, activists or protestors, human rights defenders, journalism students, journalists on the move, LGBTQ youth, Mac users, or online security veterans.[4]

If you would like to set aside time to learn more about implementing these best practices, consider signing up for my online course on this topic, Online Privacy and Security: Best Practices for Librarians.[5] Taking this course will give you time to learn to use these tools effectively, so you can in turn train your library users.

I hope that you will enjoy empowering yourself and your users with this information. There is no need to be a security expert to make use of this information and to spread the word to others. By using this guide and the sources it refers you to, you can serve as an information resource for your community on this important topic. Understanding this information can also help you avoid feeling overwhelmed by fear-based headlines that come up so often about security and privacy breaches. Remember to check with trusted security experts for balanced information. By using the tools recommended in this report, you can greatly reduce the chances of having your own information compromised.

Bibliography

General Security

Cunningham, Andrew. "A Beginner's Guide to Beefing Up Your Privacy and Security Online." Ars Technica, December 1, 2016. https://arstechnica.com/information-technology/2016/12/a-beginners-guide-to-beefing-up-your-privacy-and-security-online.

Electronic Frontier Foundation. "Assessing Your Risks." Surveillance Self-Defense. Accessed December 12, 2017. https://ssd.eff.org/en/module/assessing-your-risks.

———. "An Introduction to Threat Modeling." Electronic Frontier Foundation. Accessed December 12, 2017. https://ssd.eff.org/en/module/introduction-threat-modeling.

Pew Research Center. "Cybersecurity Knowledge Quiz." Internet and Technology. Accessed December 12, 2017. http://www.pewinternet.org/quiz/cybersecurity-knowledge.

Wolff, Josephine. "Practicing Good Personal Cybersecurity Isn't Just about Protecting Yourself." *Slate*, February 7, 2017. http://www.slate.com/articles/technology/future_tense/2017/02/everyone_needs_to_take_computer_security_seriously.html.

Security Experts to Follow

Brian Krebs. Follow his site, *Krebs on Security*, https://krebsonsecurity.com.

Bruce Schneier. Subscribe to his *Crypto-Gram Newsletter*. https://www.schneier.com/crypto-gram.

Backups

Kissel, Joe. "The Best Online Cloud Backup Service." Wirecutter, October 3, 2017. https://thewirecutter.com/reviews/best-online-backup-service.

———. *Take Control of the Cloud*, 2nd ed. Take Control Books, 2017. https://www.takecontrolbooks.com/the-cloud.

Krajeski, Justin, and Kimber Streams. "The Best Portable Hard Drive." Wirecutter, October 24, 2017. https://thewirecutter.com/reviews/best-portable-hard-drive.

Phishing and Ransomware

Better, Kim. "4 Ways to Protect against the Very Real Threat of Ransomware." *Wired*, May 13, 2016. https://www.wired.com/2016/05/4-ways-protect-ransomware-youre-target.

Electronic Frontier Foundation. "How Do I Protect Myself against Malware?" Surveillance Self-Defense. Last reviewed October 31, 2014. https://ssd.eff.org/en/module/how-do-i-protect-myself-against-malware.

Palmer, Danny. "What Is Phishing? How to Protect Yourself from Scam Emails and More." ZDNet, September 6, 2017. www.zdnet.com/article/what-is-phishing-how-to-protect-yourself-from-scam-emails-and-more.

VPNs: Virtual Private Networks

Electronic Frontier Foundation. "Choosing the VPN That's Right for You." Surveillance Self-Defense. Accessed June 9, 2016. https://ssd.eff.org/en/module/choosing-vpn-thats-right-you.

Passwords and Mobile Payments

Bluefin. "The Security of 'Traditional' Payments vs. Alternatives: Mobile Wallets." May 12, 2016. https://www.bluefin.com/bluefin-news/security-traditional-payment-methods-vs-alternatives-spotlight-mobile-wallets.

Electronic Frontier Foundation. "Creating Strong Passwords." Surveillance Self-Defense. Accessed October 16, 2017. https://ssd.eff.org/en/playlist/want-security-starter-pack#creating-strong-passwords.

Golbeck, Jennifer. "How to Set Up Two-Factor Authentication." *Slate*, February 15, 2017. www.slate.com/articles/technology/future_tense/2017/02/how_to_set_up_two_factor_authentication.html.

Kissel, Joe. "The Best Password Managers." Wirecutter, August 3, 2017. Last updated December 8, 2017. https://thewirecutter.com/reviews/best-password-managers.

———. *Take Control of Your Passwords*, 2nd ed. Take Control Books, 2016. https://www.takecontrolbooks.com/passwords.

Schneier, Bruce. "Choosing Secure Passwords." *Schneier on Security* (blog), March 3, 2014. https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html.

———. "Stop Trying to Fix the User." *IEEE Security and Privacy* 14, no. 5 (September–October 2016): 96. http://ieeexplore.ieee.org/document/7676198 (requires login).

Biometric Authentication

Couch, Paul. "Biometric Authentication Overview, Advantages and Disadvantages." *Heimdal Security* (blog), July 28, 2017. https://heimdalsecurity.com/blog/biometric-authentication.

Low, Cherlynn. "Our Fingerprints, Eyes, and Faces Will Replace Passwords." Engadget, October 10, 2016. https://www.engadget.com/2016/10/10/future-of-biometric-security.

Mogull, Rich. "Face ID Is the Future of Security (Authentication)." *Securosis Blog*, November 9, 2017. https://securosis.com/blog/14884.

———. "Face ID's Innovation: Continuous Authentication." TidBITS, November 9, 2017. http://tidbits.com/article/17621.

Data Breaches and Identity Theft

AnnualCreditReport.com homepage. Accessed December 12, 2017. https://www.annualcreditreport.com.

Consumer Reports. "Don't Get Taken Guarding Your ID: Do-It-Yourself Safeguards Are Just as Effective as Paid Services." January 2013. https://www.consumerreports.org/cro/magazine/2013/01/don-t-get-taken-guarding-your-id/index.htm.

Have I Been Pwned? Check if You Have an Account That Has Been Compromised in a Data Breach homepage. Accessed December 12, 2017. https://haveibeenpwned.com. See also the list of websites that have suffered breaches: "Pwned Websites," accessed January 8, 2018. https://haveibeenpwned.com/PwnedWebsites.

IdentityTheft.gov. "Report Identity Theft and Get a Recovery Plan." Federal Trade Commission. Accessed December 12, 2017. https://www.identitytheft.gov.

Privacy Rights Clearinghouse. "Data Breaches." Accessed December 12, 2017. https://www.privacyrights.org/data-breaches.

———. "What to Do When You Receive a Data Breach Notice." November 2, 2017. https://www.privacyrights.org/consumer-guides/what-do-when-you-receive-data-breach-notice.

Ross, Katherine. "How Much It Costs in Every State to Freeze Your Credit Report." ValuePenguin. Accessed December 12, 2017. https://www.valuepenguin.com/states-where-freezing-your-credit-will-cost-you-most.

General Privacy

Boykis, Vicki. "What Should You Think about When Using Facebook?" February 1, 2017. https://veekaybee.github.io/2017/02/01/facebook-is-collecting-this.

Cope, Sophia, Amul Kalia, Seth Schoen, and Adam Schwartz. *Digital Privacy at the U.S. Border: Protecting the Data on Your Devices and in the Cloud*. San Francisco: Electronic Frontier Foundation, March 8, 2017. https://www.eff.org/wp/digital-privacy-us-border-2017.

Kelly, M. J. "Facebook Privacy Tips: How to Share without Oversharing." *Internet Citizen, Mozilla Blog*, January 25, 2017. https://blog.mozilla.org/internetcitizen/2017/01/25/facebook-privacy-tips.

Kissel, Joe. *Take Control of Your Online Privacy*, 3rd ed. Take Control Books, 2017. https://www.takecontrolbooks.com/online-privacy.

Targeted Advertising

Corpuz, John. "Best Ad Blockers and Privacy Extensions." Tom's Guide. July 6, 2017. https://www.tomsguide.com/us/pictures-story/565-best-adblockers-privacy-extensions.html.

Martinez, Antonio Garcia. "Facebook's Not Listening through Your Phone. It Doesn't Have To." *Wired*. November 10, 2017. https://www.wired.com/story/facebooks-listening-smartphone-microphone.

Me and My Shadow. "Tracking . . . So What? 7 Things We Know You're Going to Say." October 19, 2016. https://myshadow.org/tracking-so-what.

Private Browsing and Searching

Klein, Matt. "How to Enable Private Browsing on Any Web Browser." How-To Geek. February 15, 2017. https://www.howtogeek.com/269265/how-to-enable-private-browsing-on-any-web-browser.

Mundrha, Ashish. "5 Reasons to Search the Web Using DuckDuckGo." Guiding Tech, July 5, 2017. https://www.guidingtech.com/11797/5-reasons-to-search-web-with-duckduckgo.

Rusen, Ciprian Adrian. "What Is DuckDuckGo and What Are the Benefits of Using It?" Digital Citizen, November 28, 2017. https://www.digitalcitizen.life/what-is-duckduckgo.

Location Tracking

Me and My Shadow. "Location Tracking." February 15, 2017. https://myshadow.org/location-tracking.

Encrypted Messaging and Email

Electronic Frontier Foundation. "How to: Use Signal for Android." Surveillance Self-Defense. Last reviewed March 17, 2017. https://ssd.eff.org/en/module/how-use-signal-android.

———. "How to: Use Signal on iOS." Surveillance Self-Defense. Last reviewed March 17, 2017. https://ssd.eff.org/en/module/how-use-signal-ios.

———. "Why Metadata Matters." Surveillance Self-Defense. Last reviewed August 10, 2015. https://ssd.eff.org/en/module/why-metadata-matters.

Me and My Shadow. "What Are Digital Traces?" October 20, 2016. https://myshadow.org/digital-traces-content-and-metadata.

Pinola, Melanie. "ProtonMail Is the Easiest Way to Send and Receive Encrypted Emails." Lifehacker, March 17, 2016. https://lifehacker.com/protonmail-is-the-easiest-way-to-send-and-receive-encry-1765491376.

Wolber, Andy. "Simple Security: How Gmail, Mailvelope, and Virtru Make Encrypted Email Easier." TechRepublic, July 13, 2016. https://www.techrepublic.com/article/simple-security-how-gmail-mailvelope-and-virtru-make-encrypted-email-easier.

Anonymous Browsing

Brodkin, Jon. "How ISPs Can Sell Your Web History—and How to Stop Them." Ars Technica, March 24, 2017. https://arstechnica.com/information-technology/2017/03/how-isps-can-sell-your-web-history-and-how-to-stop-them.

Electronic Frontier Foundation. "How to: Use Tor for Linux." Surveillance Self-Defense. Last reviewed September 5, 2017. https://ssd.eff.org/en/module/how-use-tor-linux.

———. "How to: Use Tor on MacOS." Surveillance Self-Defense. Last reviewed September 5, 2017. https://ssd.eff.org/en/module/how-use-tor-macos.

———. "How to: Use Tor for Windows." Surveillance Self-Defense. Last reviewed September 5, 2017. https://ssd.eff.org/en/module/how-use-tor-windows.

Nicol, Will. "A Beginner's Guide to Tor: How to Navigate through the Underground Internet." Digital Trends, January 19, 2016. https://www.digitaltrends.com/computing/a-beginners-guide-to-tor-how-to-navigate-through-the-underground-internet.

Webcam Privacy

Brogan, Jacob. "What's the Best Way to Cover Your Webcam?" *Future Tense* (blog), *Slate*, September 15, 2016. www.slate.com/blogs/future_tense/2016/09/15/the_best_ways_to_cover_a_webcam.html.

Snyder, Chris. "Hackers and Governments Can See You through Your Phone's Camera—Here's How to Protect Yourself." Business Insider, March 7, 2017. http://www.businessinsider.com/hackers-governments-smartphone-iphone-camera-wikileaks-2017-3.

Yates, Mark. "Time to Tape over the Camera on Your Laptop." AVG, September 26, 2016. https://www.avg.com/en/signal/why-you-should-cover-the-camera-on-your-laptop-or-tablet.

Internet of Things Privacy

Nield, David. "How to Lock Down Your Privacy on the Amazon Echo and Google Home." Gizmodo Field Guide, April 27, 2017. https://fieldguide.gizmodo.com/how-to-lock-down-your-privacy-on-the-amazon-echo-and-go-1794697554.

Rainie, Lee, and Janna Anderson. *The Internet of Things Connectivity Binge: What Are the Implications?* Washington, DC: Pew Research Center, June 6, 2017. www.pewinternet.org/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the-implications.

Notes

1. Brian Krebs, "Who Makes the IoT Things under Attack?" *Krebs on Security* (blog), October 3, 2016, https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack; Brian Krebs, "Hacked Cameras, DVRs Powered Today's Massive Internet Outage," *Krebs on Security* (blog), October 21, 2016, https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage.
2. Darrin Pauli, "Ransomware Scum Offer Free Decryption if You Infect Two Mates," *The Register*, December 11, 2016, www.theregister.co.uk/2016/12/11/ransomware_offer_pay_us_a_770_ransom_or_infect_two_friends.
3. For more information, see "How to Organize a CryptoParty," CryptoParty wiki, last modified September 29, 2017 (https://www.cryptoparty.in/organize/howto).
4. See "Playlists," Electronic Frontier Foundation, Surveillance Self-Defense, accessed January 8, 2018, https://ssd.eff.org/en/playlist.
5. For more details, including the course outline, see Nicole Hennig, "Privacy and Security Online Course," accessed January 8, 2018, http://nicolehennig.com/courses/privacy-security-best-practices-library-users.

Notes

Notes

Library Technology
REPORTS

Upcoming Issues	
May/June 54:4	**Accessibility, Technology, and Librarianship** edited by Heather Moorefield-Lang
July 54:5	**Integrating Learning Tools Interoperability into Learning Management Systems** edited by Amanda Clossen
August/ September 54:6	**Virtual and Augmented Reality** by Hannah Pope

Subscribe
alatechsource.org/subscribe

Purchase single copies in the ALA Store
alastore.ala.org

alatechsource.org

ALA TechSource, a unit of the publishing department of the American Library Association