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 make 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.
   - “Creating Strong Passwords,” Electronic Frontier Foundation, Surveillance Self-Defense,
Privacy and Security Online: Best Practices for Cybersecurity

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.
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.
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).

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.
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).
3. Install an ad blocker. If you don’t want to see ads based on pages you’ve browsed, install an ad blocker.

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). 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.

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. 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


Security Experts to Follow


Backups


Phishing and Ransomware


VPNs: Virtual Private Networks


Passwords and Mobile Payments


Biometric Authentication


Data Breaches and Identity Theft


General Privacy


Targeted Advertising


Private Browsing and Searching


Location Tracking


Encrypted Messaging and Email

Anonymous Browsing


Webcam Privacy


Internet of Things Privacy


Notes


3. For more information, see “How to Organize a Crypto-Party,” CryptoParty wiki, last modified September 29, 2017 (https://www.cryptoparty.in/organize/howto).
