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 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.