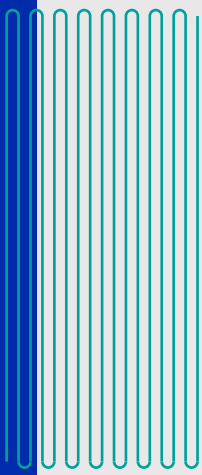
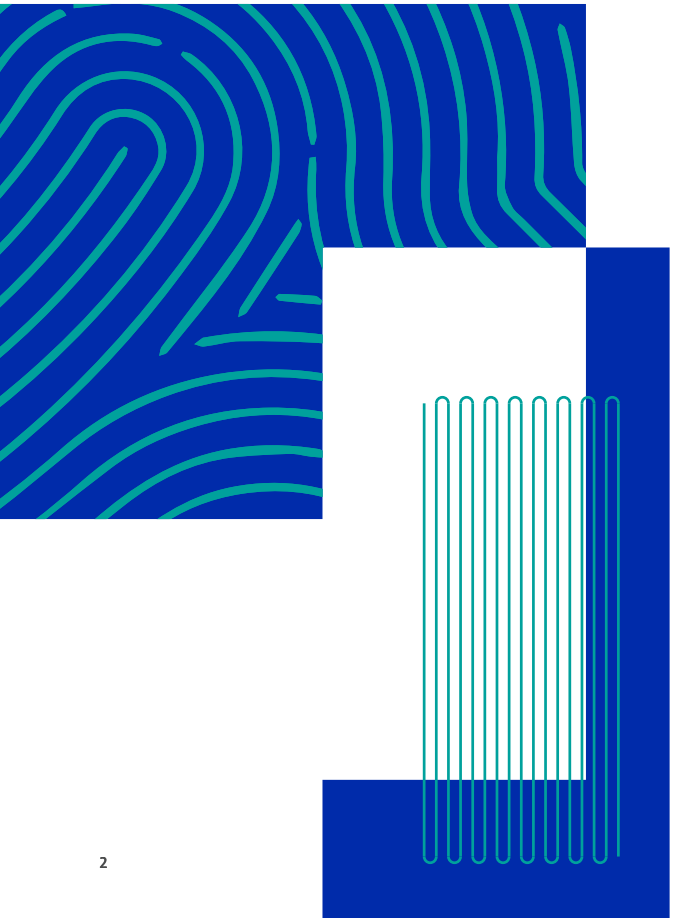
DIGITAL SECURITY

BASICS



Understanding basic digital security concepts, and knowing where to go for more help, is a great first step for all who work in libraries. Not only will these skills help make the library and its data more secure, they also allow staff to better help users to be more secure online. This guide is intended for individuals aiming to learn digital security skills and for those hoping to have privacy and digital security education for library staff.



4 Creating Strong, Secure Passwords

6 Passwords are out. Passphrases are in.

8 Password Managers

10 Multi-Factor Authentication

12 Phishing

14 Malware = Malicious Software

16 Ransomware

18 Network Privacy

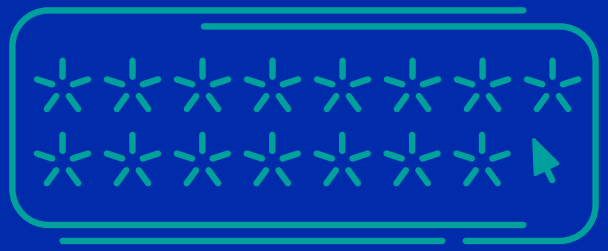
20 Staff and User Training

22 Digital Security Detective

Creating Strong, Secure Passwords

Do you lock your house when you leave for the day? Most of us probably answered yes to this question. Why do we secure the door? We lock our homes because we have things inside that we don't want anyone else to have access to or steal. Creating a strong password is like having a unique key and lock to your house. We have to make sure that those locks are strong!

Passwords are out. Passphrases are in.



Remembering passwords for 80 different accounts is a challenge. We want to have unique passwords for every account, and it gets out of control quickly. How can a human be expected to come up with a secure password that can also be remembered? Passphrases!

QUICK TIP

Forget about replacing "i" with "1" or "for" with "4." These techniques are so common now that the computer programs that crack passwords know them too.

EXERCISE

Practice making a passphrase. The strongest passphrases will have at least 17 characters, spaces count!

- Think of a set of words that have meaning to you and that you'll remember. Do not include any personal information such as birthdates, addresses, or names. String together a combination of these words to create a random phrase.
- Add numbers and symbols to the phrase at the beginning, middle, or end.
- Now, test your passphrase (https://bit.ly/securepassphrase) and see how quickly it can be broken.

Password Managers

How many passwords are you expected to remember at work? Do you have them written down on a sticky note that's placed "discreetly" under your keyboard or an office drawer? Believe it or not, one of the most common ways hackers gain access to accounts is through the human responsible for keeping their accounts safe. One solution to too many passwords is using a password manager.

Password managers generate and store complex passwords for you. You just have to remember one (very secure and unique) master password for the manager itself, and everything else is taken care of for you. Also, organizations can purchase a team password manager to manage shared accounts.

- Explore the password manager suggestions in this guide. Set up an account and try it out for a week.
- Use your strongest passphrase as the password for your password manager.

TRY A PASSWORD MANAGER

Dashlane
https://bit.ly/dashlanepw

1password
https://bit.ly/1passwordpw

LastPass
https://bit.ly/lastpasspw

QUICK TIP

Saving your passwords with your browser? Watch out. This is not secure and easily hacked. Password managers make it much harder for anyone to access your complex passwords and phrases.

Multi-Factor Authentication

Adding a Deadbolt to Your Online Doors

For accounts that hold a lot of our personal information, we want to make sure we're the only ones with access. Multi-Factor Authentication (MFA) means that just entering a password on the computer isn't enough for someone to gain access to your account. The term 2-Factor Authentication is commonly used as well, and is a subset of MFA that only requires one additional factor in addition to your password to grant access.

With MFA, when you enter a password into a digital account you will be prompted to verify your identity through another means. Most often you will be texted a code to the phone number on file. That code would then need to be entered into the account to gain access. Sometimes MFA will utilize an authorization app, use a physical object like a security token, or request a biometric identifier.

If you ever see one of these texts come to you when you're not trying to access the account, then you know someone else is attempting to break-in. This is a good time to change your password.

EXERCISE

- Review your personal accounts and enable MFA where possible.

ACCOUNT	MULTI-FACTOR AUTHENTICATION (Y/N)
Email	*Y - password, text code, second email verification, phone call*

- Multi-factor authentication can also be used at the library. Can you think of any accounts that could benefit from adding multi-factor authentication?

Phishing

Most libraries have filtering software for their email accounts, but this doesn't mean you shouldn't be on the lookout for malicious emails.

AVOID GETTING CAUGHT

- Only click links in email from trusted sources.
- Don't download an attachment unless you know who it's from.
- Don't enter your personal information into any form you have reason not to trust.
- Use context clues and listen to your gut. Just because an email looks like it's from a coworker doesn't guarantee it is. A hacker can send a message that appears to be from your coworker by hacking or spoofing their email address.
- Look at the entire URL you are being asked to click on. Is it exactly the same as the site address you normally type?

QUICK TIP

If you click on a link you think might be malicious, let your IT staff know right away.

Q: What are the phishing red flags in this email between employees at different libraries?

A:

- The email domain is from AOL. This is not a typical domain used by libraries.
- The response email asked for money.
- There are several typos.
- The recipient is asked to visit a link and provide personal information.

Malware = Malicious Software

Malicious software is software designed to do damage or other unwanted actions to your computer or smartphone. Usually this type of software is installed on your computer when you download attachments in emails or click on unknown links or ads. It can also be installed when someone puts an external flash drive into your machine. If you open an email and don't know what the attachment is, don't download it!

QUICK TIP

Check to see if your work or personal email has been compromised by going to https://bit.ly/pwnedemail

ACTIVITIES TO SECURE THE LIBRARY WORKPLACE

- Check if your computers have antivirus software installed. Do the computers for users have the same protections as staff computers?
- Check to see if your mobile devices are updated to the latest version of the operating system (OS).
- Create a schedule to regularly update OS and software when updates are released since malware can exploit security holes. This includes computers and all mobile devices!
- Does your library allow the use of external flash drives? Create procedures that do not allow staff to put external flash drives from users into staff terminals.

Ransomware

One type of malware gaining in popularity is ransomware. How does it work?

Attackers gain access to your computer when you accidentally download malware, and then they hold your information hostage. The attackers may lock all your files or shut down your entire network, and they will require you to pay them to regain access. If files are important to you, make sure to back them up to external drives or a cloud server.

These attacks often focus on businesses and governments so watch out for suspicious emails at work! If it feels wrong, report it to IT. If you see a suspicious email in your personal account, mark it as spam (if possible) and delete the email without clicking on anything.

QUICK TIP

Regularly update your devices! Updates are often security patches. Your apps and software are only protected when you're running the latest version.

EXERCISE

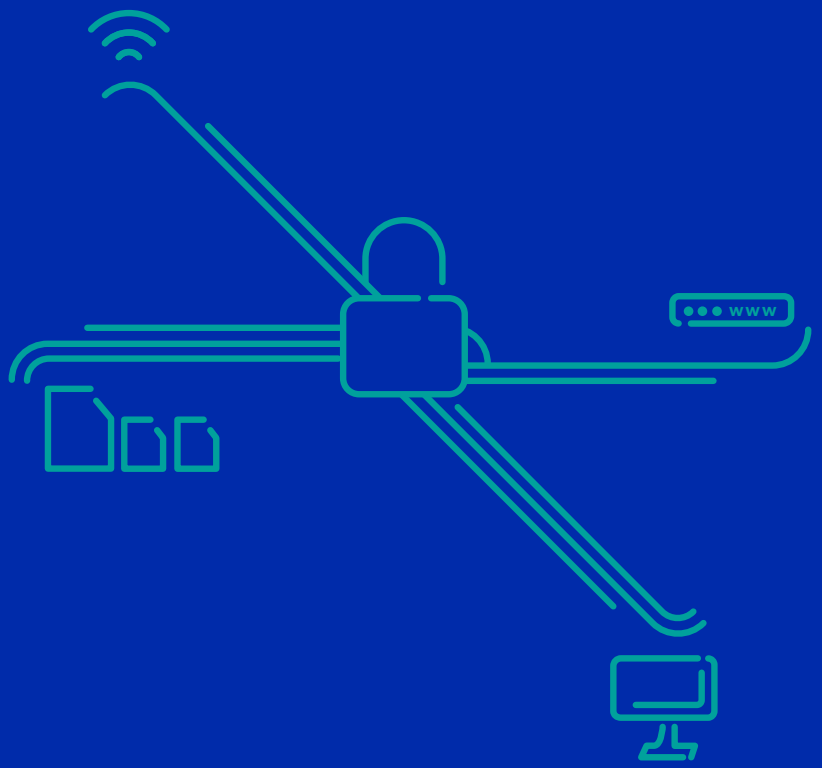
- Perform a search for ransomware attacks in libraries. How many libraries can you find that have experienced attacks?

_____

_____

- Does your library have a plan in place for a ransomware attack? Connect with your IT department and ask these questions. If no plan exists, try to develop one.
  - How will staff be contacted without access to email?
  - How will users be notified?
  - Does the library have a method to check out materials without access to the ILS?

Network Privacy



Pull up your library website. Look in the address bar. Do you see a little lock that's closed or open? Does your web address say HTTP or HTTPS? The 'S' at the end of HTTPS stands for 'Secure'. It means all communications between your browser and the website are encrypted, so no one can see the data that is being sent.

It is very important that your library website is using HTTPS, especially on the accounts page. People visiting your site without HTTPS may also get warnings from their browsers telling them your site is not secure.

Treatment of HTTP pages

Current (Chrome 67)	ⓘ example.com
July 2018 (Chrome 68)	ⓘ Not secure | example.com

GETTING YOUR WEBSITE TO HTTPS

- Connect with your IT manager or get ready to start the process if you're the one with network access. Seek out options for purchasing SSL/TLS certificates If costs are a concern, check out Let's Encrypt (http://bit.ly/httpsencrypt). Let's Encrypt offers free certificates to anyone who owns a domain name. There is a robust community of support available to help install the certificates and get your site secured.

EXERCISE

- Go to your library's website. Is it secured with HTTPS?
- If your site is still operating with HTTP, connect with the IT Department or get ready to start the process if you're the one with network access. Seek out options for purchasing SSL/TLS certifications.
- If your site is secured, visit a few library vendors to see if their sites are secure.

Staff and User Training

Once you understand the basics, it's time to share that knowledge in your library! When thinking about staff training, consider:

- How to get staff buy-in. Explain why privacy is important and vital to library operations.
- The technical skills of your staff; start out with the basics. This guide is meant to support all staff, including those who are less tech savvy.
- Ways to measure improvements after training and ways to keep the conversation going.

Even a short staff development session with the topics above will make the library, the staff, and your users safer. Use the lessons and activities from this guide to host a staff or user training session. You can also use library privacy and security training materials that are available online.

Staff training resources from NYC Digital Safety: Privacy and Security, Data Privacy Project, and the Library Freedom Institute: https://bit.ly/librarystaffprivacy

Programming for students at academic libraries: https://bit.ly/privacyacademic

User programming for public libraries: https://bit.ly/privacypublic

Lesson plans for students at K-12 libraries: https://bit.ly/privacyschoolplan

Digital Security Detective

You've now learned the basics of digital security. Practice your new skills by reading these accounts of library workers in the field.

MEET JAMIE

Jamie works in technical services at a nearby community college library and also does a few hours at the reference desk. Jamie comes to work and logs into her computer, the ILS, a messaging app to communicate with colleagues, and the intranet. She was using one password for all the accounts, but was told to create complex, unique passwords for each account by IT staff. It was too hard to remember them all so she keeps a handwritten list in her desk drawer.

When she's working at the reference desk she has to log into everything again and remember to log out at the end of her shift since she's using a shared computer. Sometimes Jamie brings her list with all the passwords out to the reference desk where she keeps it in an unlocked drawer. At the end of every shift she brings it back to her desk, except for a couple of times when she's forgotten and picked it up the next morning. What recommendations would you make to improve their digital security practices?

MEET MEL

Mel works as an adult librarian at a busy public library. Yesterday, a user came to the service desk explaining that he was having trouble with the computer. He told them that he wanted to print a very important document, but was not able to do it from the public terminal. Mel started walking the user back to the public terminals only to discover all of them were being used. They felt a moment of panic. The user told Mel that he was late to a job interview and needed to bring this document with him or he wouldn't be hired. He told Mel that he had a USB drive and asked them if they could print the document by using a staff computer.

Mel, wanting to help the user get that job, agreed. They took the USB drive to their desk in the back, opened the document, printed it, and returned the USB drive to the user. He seemed overwhelmingly thankful and left the library in a hurry. When Mel came into work today all of the computers were offline and IT staff were running around frantically. Mel found a manager who explained that the library was hit with a ransomware attack. All of the computers across the entire system were locked and the perpetrators were demanding a large payment of Bitcoin to return access to the library. What digital security mistakes were made?

ALA American Library Association

PRIVACY ADVOCACY GUIDES

Privacy is a core value of librarianship, yet it often feels like an overwhelming and onerous undertaking. Use these Privacy Field Guides to start addressing privacy issues at your library. Each guide provides hands-on exercises for libraries. Check out all the available guides at **bit.ly/PrivacyFieldGuides.**

INSTITUTE of Museum and Library SERVICES

This project was made possible in part by the Institute of Museum and Library Services LG-36-19-0073-19.

Designed by PixelbyInch.com