THE ULTIMATE

PRIVACY FIELD GUIDE

A WORKBOOK OF BEST PRACTICES

EDITED BY ERIN BERMAN AND BONNIE TIJERINA
ALA OFFICE FOR INTELLECTUAL FREEDOM (OIF)

ALA Editions
CHICAGO 2023

ERIN BERMAN is a fierce privacy advocate who led the Privacy Subcommittee of ALA's Office for Intellectual Freedom from 2018 to 2022. During her time as innovations manager for the San José Public Library, she published the book *Your Technology Outreach Adventure: Tools for Human-Centered Problem Solving*. Currently, she works as the division director of the Learning Group for the Alameda County Library in California.

BONNIE TIJERINA is a researcher, librarian, and community convener. She is currently focused on creating opportunities for education and discussion in the library profession and beyond on the role libraries and librarians can play in the increasingly complex issues of the digital world. In that space, she has worked on several grant-funded projects that involve privacy and big data research ethics, and she is the coeditor of *Protecting Patron Privacy: A LITA Guide*. She is also the founder and annual coordinator of the Electronic Resources & Libraries Conference.

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

Extensive effort has gone into ensuring the reliability of the information in this book; however, the publisher makes no warranty, express or implied, with respect to the material contained herein.

ISBN: 978-0-8389-3730-3 (paper)

Library of Congress Cataloging-in-Publication Data

Names: Berman, Erin, editor. | Tijerina, Bonnie, editor.
Title: The ultimate privacy field guide : a workbook of best practices / edited by Erin Berman and Bonnie Tijerina, Office for Intellectual Freedom.
Description: Chicago : American Library Association—ALA Editions, [2023] | Includes bibliographical references and index. | Summary: "Designed for use in school, public, and academic settings of all shapes and sizes, this easy-to-use workbook is packed with practical, hands-on exercises to guide you towards creating a more privacy-focused library"—Provided by publisher.
Identifiers: LCCN 2022029484 | ISBN 9780838937303 (paperback)
Subjects: LCSH: Privacy, Right of. | Intellectual freedom.
Classification: LCC JC596 .U57 2023 | DDC 323.44/8—dc23/eng/20220729
LC record available at https://lccn.loc.gov/2022029484

Original design by Heejung Yoon, Ryan Carnrick at PixelbyInch.com.
Layout adapted by Kim Hudgins.

∞ This paper meets the requirements of ANSI/NISO Z39.48-1992 (Permanence of Paper).

Printed in the United States of America
27 26 25 24 23 5 4 3 2 1

CONTENTS

INTRODUCTION

With the creation of ever larger datasets and methods to track users' every movement online, library workers need to have a deep understanding of privacy, confidentiality, and security. While privacy is a core value of librarianship, it often feels like an overwhelming and onerous undertaking. Library workers need easy-to-use tools that will help them create private and secure spaces for users to express their intellectual freedom.

The editors of this book, Bonnie Tijerina and Erin Berman, saw that there was a lack of practical how-to guides for making concrete privacy changes in the library. As a librarian and researcher, Bonnie has focused on the role libraries play in supporting their communities in the digital space. As an active member and then chair of the Privacy Subcommittee of ALA's Office for Intellectual Freedom, Erin has heard often from library workers who feel passionately about supporting users' privacy rights but feel unprepared, not tech-savvy enough, or not in the right position of leadership to make a change.

To address the concerns voiced by library workers, Bonnie and Erin partnered to create the "Privacy Field Guides." Sponsored by the Institute of Museum and Library Services and the American Library Association, these short online guides are designed to work in school, public, and academic libraries, making it easier to talk about privacy and take steps, even small steps, to improve the library's or its users' privacy in some way.

This publication gathers those guides together into one workbook, with each chapter representing a guide that covers topics important to library workers, including the basics of digital security, understanding the data lifecycle, performing library privacy audits, and writing or reading privacy policies. The chapters also help libraries learn how to talk about privacy with stakeholders, how to work with vendors to secure privacy requirements, and what to consider around nontechnical privacy issues.

This workbook has been thoroughly reviewed and then vetted in real-world library settings. Library stakeholders from across the country participated in surveys, trainings, workshops, and focus groups to provide input and guidance about the content and format of these guides. Library privacy experts wrote the guides, which were then put through real-world testing before reaching their final versions.

The workbook chapters are structured to give library workers the tools they need to create and be advocates for a safer, more secure library. Each chapter will give an introduction to the topic and then provide several exercises for you to implement privacy changes at your library. Each chapter follows the same easy-to-use format. You can read this workbook cover to cover, but we imagine you will choose a chapter that interests you or is in an area that your library would like to work on. Then you can revisit this workbook several times to learn about other aspects of privacy.

While some of the work in these chapters may not seem like big steps, these small but consistent actions can have large implications for your community. Learning the language to advocate for privacy, tweaking physical spaces, using new digital security tools, rethinking policies and practices, and asking questions within your organization will make a difference. With many libraries taking these steps, there is the possibility for powerful, collective change.

CHAPTER 1

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, but they will also allow staff to better help users to be more secure online. This chapter is intended for individuals who want to learn digital security skills and for those hoping to provide privacy and digital security education for library staff.

In This Chapter

Creating Strong, Secure Passwords

Do you lock your house when you leave for the day? Most of us probably would answer “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 eighty different accounts is a challenge. We want to have a unique password for every account, and this can get out of control quickly. How can a person be expected to come up with a secure password that can also be remembered? Passphrases!

EXERCISE

Practice making a passphrase. The strongest passphrases will have at least seventeen characters (and spaces count).

1. 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.
2. Add numbers and symbols to the phrase at the beginning, middle, or end.
3. Now, test your passphrase (https://howsecureismypassword.net) and see how quickly it can be broken.

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.

Password Managers

TRY A PASSWORD MANAGER

Dashlane: dashlane.com

1password: 1password.com

LastPass: lastpass.com

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 in an office drawer? Believe it or not, one of the most common ways hackers gain access to accounts is through the person 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 utilize a team password manager to manage shared accounts.

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

Multi-Factor Authentication

QUICK TIP

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

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. In the table below, list the current accounts you have, whether or not they have multi-factor authentication, and if they do, what that verification involves.

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

Phishing is the practice of sending fraudulent e-mails that claim to be from reputable sources to trick users into revealing personal information that can then be used for illicit or malicious purposes. Most libraries have filtering software for their e-mail accounts, but this doesn't mean you shouldn't be on the lookout for phishing e-mails.

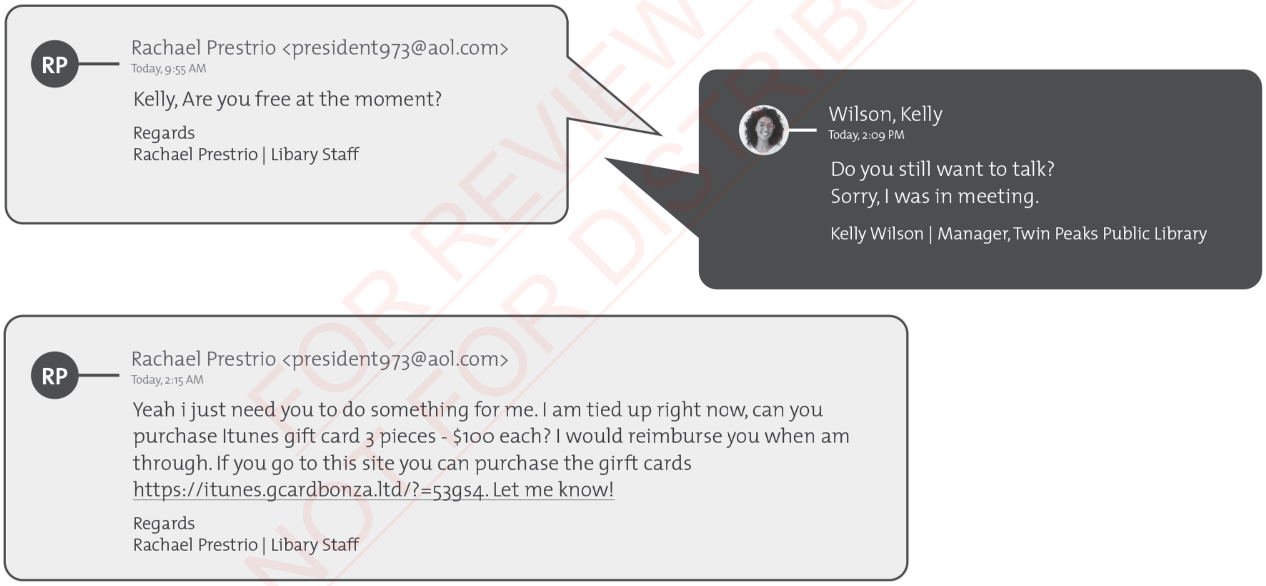
Avoid Getting Caught

- Only click links in e-mail 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 e-mail looks like it's from a coworker doesn't guarantee that it is. A hacker can send a message that appears to be from your coworker by hacking or spoofing their e-mail 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 have clicked on a link you think might be malicious, let your IT staff know right away.

Example of a Phishing Scam



Rachael Prestrio <president973@aol.com>
Today, 9:55 AM

Kelly, Are you free at the moment?

Regards
Rachael Prestrio | Libary Staff

Wilson, Kelly
Today, 2:09 PM

Do you still want to talk?
Sorry, I was in meeting.

Kelly Wilson | Manager, Twin Peaks Public Library

Rachael Prestrio <president973@aol.com>
Today, 2:15 AM

Yeah i just need you to do something for me. I am tied up right now, can you purchase Itunes gift card 3 pieces - $100 each? I would reimburse you when am through. If you go to this site you can purchase the girft cards https://itunes.gcardbonza.ltd/?=539s4. Let me know!

Regards
Rachael Prestrio | Libary Staff

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

A:
- The e-mail domain is from AOL. This is not a typical domain used by libraries.
- The response e-mail 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 e-mails 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 e-mail and don't know what the attachment is, don't download it!

QUICK TIP
Check to see if your work or personal e-mail has been compromised by going to https://haveibeenpwned.com.

Activities to Secure the Library Workplace

- Check if your computers have antivirus software installed on them. 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) they use.
- Create a schedule to regularly update the OS and software when updates are released, as malware can exploit security holes. You should check 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 e-mails at work. If it feels wrong, report it to your IT department. If you see a suspicious e-mail in your personal account, mark it as spam (if possible) and delete the e-mail 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 of them.

EXERCISE

1. Perform a search for news reports of ransomware attacks on libraries. How many libraries can you find that have experienced attacks?

   ____

   ____

   ____

2. Does your library have a plan in place for a ransomware attack? Connect with your IT department and ask them the questions below. If no plan exists, try to develop one.

   - How will staff be contacted without access to e-mail?
   - How will users be notified of a ransomware attack?
   - Does the library have a method for users 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 that all communications between your browser and the website are encrypted, so no one else can see the data that is being sent.

It is very important that your library website use HTTPS (rather than just HTTP), especially on the accounts page. People visiting your site without HTTPS may even get warnings from their browsers telling them your site is not secure.

Getting Your Website to HTTPS

How can you move your library's website from HTTP to the HTTPS protocol? First, connect with your IT manager, or get ready to start the process yourself if you're the one with network access. Seek out the options for purchasing certificates for either SSL or TLS—the two standard security technologies that are used in HTTPS. If costs are a concern, check out Let's Encrypt (https://letsencrypt.org). 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

1. Go to your library's website. Is it secured with HTTPS?
2. 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.
3. 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 the following:

- How to get staff buy-in. Explain to your staff why privacy is important and vital to library operations.
- How to upgrade the technical skills of your staff with regard to digital security and privacy. Start out with the basics. This chapter is meant to support all staff members, including those who are less tech-savvy.
- Consider 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 chapter to host a staff or user training session. You can also use library privacy and security training materials that are available online. You can find all of the following resources at www.ala.org/advocacy/privacy/training:

- Staff training resources from NYC Digital Safety: Privacy and Security, the Data Privacy Project, and the Library Freedom Institute
- Programming for students at academic libraries
- User programming for public libraries
- Lesson plans for students at K–12 libraries

INDEX