



Digital Privacy: Hands-on Tactics and Tools for Libraries

Workshop 2

ABOUT THIS TRAINING

This is a 3-hour workshop with one 10 minute break in the middle. Maximum registration is 25 participants and we will have 2 facilitators in each workshop.

Activities in this workshop include: group lecture and discussion, small group, and self-guided. Each participant will have a computer.

The main goal of this workshop is for library staff to deepen understanding and have hands-on practice with privacy and security tools that they can share with patrons. This includes tools that the library has already put in place as well as other tools that are freely available online. The second goal is for library staff to deepen understanding and have hands-on practice with privacy and security tools that they can use in their work and personal computing. A third goal is to introduce other people and libraries focusing on privacy and security in US public libraries so library staff can explore perspectives on libraries and privacy education.

This training was developed by Research Action Design (rad.cat) in collaboration with:

- Research Action Design worker-owners: Bex Hurwitz and Chris Schweidler
- Digital Privacy and Data Literacy Leadership Team: Melissa Morrone and Seeta Peña Gangadharan
- Members of the Digital Privacy Curriculum Advisory Committee: Ali Seden, Brian Hasbrouck, Carl Fossum, Chris Cotton, Jessica Ng, Jose Arellano, Larissa Larier, Luz Diaz, Robert Weinstein
- Additional support from: Ann Joseph, Arlene Ducao, Bonnie Tijerina, Corina Bardoff, Harlo Holmes, Priscilla Yuen, Ronella Fraser-Jackson, Ryan Gerety, Tara Adiseshan, Thomas Garcia
- Training plans shared with us by Library staff members Corina Bardoff and Priscilla Yuen, who are teaching digital privacy and security at their branches
- It also draws on resources from the EFF's Surveillance Self Defense, Frontline Defenders, Library Freedom Project, and Tactical Technology Collective



This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 License](https://creativecommons.org/licenses/by-sa/4.0/). Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use. ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

Suggested Citation:

Hurwitz, B., Morrone, M., Gerety, R., Gangadharan, S. P., and Schweidler, C. (2016, December). [Digital Privacy: Hands-On Tactics and Tools for Libraries, Workshop 2](http://www.dataprivacyproject.org). Brooklyn Public Library and Research Action Design. New York: Data Privacy Project. Available at: <http://www.dataprivacyproject.org>.

PRE WORKSHOP MATERIALS & PREP ITEMS

MATERIALS

- Slides Workshop 2
- Large Paper with adhesive top (2 large pads, will use with walls)
- Markers
- Whiteboard and markers (in room, markers in podium)
- Name tags
- Small pads/paper + pens or pencils (participants can take personal notes)

HANDOUTS

- Workshop Intake & Exit Survey
- Digital Privacy: Hands-on Tactics and Tools for Libraries
- Patron Profiles for Risk Assessment

BEFORE WORKSHOP

- Print Handouts ~25 participants
- Prepare laptops for participants. People are encouraged to bring their own, but there are PC laptops that METRO staff can retrieve from the classroom closet if necessary.
- Prepare printed Intake & Exit Surveys to handout prior to workshop.
- Projector with connection to Facilitators' computer. METRO will set up the projector.
- Arrange the room with tables in clusters of 2 tables.
- Pickup final registration list of attendees
- Set up facilitator laptop with projector, plug in audio, load links in tabs
- Facilitator - install software including Privacy Badger, LastPass plugin, Tor
- Test the audio
- Test slide advancement, & toggling between Slides & Browser on the projector
- Facilitator's personal computer (for slides) and Software demos (password manager, Privacy Badger, Tor)
- Prepare large paper with written Workshop Agenda including times and breaks to post on wall. Include training website & contact email.
- Identify main and support facilitation roles for agenda items.
- Place pens or pencils and small pads/paper on each table.
- Prepare large Risk Assessment paper for each team
- Prepare large Paper and Markers for Parking Lot










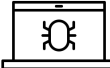


ADDITIONAL TIPS FOR TRAINERS

- **Harm Reduction:** As we move through the workshop, often someone will raise the concern that it is not possible to keep digital information private to just the intended parties. We use the frame of harm reduction to say that we follow a set of best practices around digital privacy in order to reduce the possibility of harm to ourselves if our information is not private.
- **Physical Analogies:** We have found that using physical analogies is quite useful for library staff to consider how to speak with patrons. For example: if you are using a browser and looking at sensitive information, say your bank account information, consider it like you would a paper statement. In the same way you would not get up from a public area at the library and leave your paper bank statements on the table, do not leave an active terminal session open with your bank or other sensitive material.





WORKSHOP 1: FACILITATOR'S AGENDA WITH TIMING

	Agenda Item	Time	Facilitation Roles	
			Main	Scribe/Support
	WELCOME	5 min		
	INTRODUCTIONS & NAME YOUR TEAM	10 min		
	RISK ASSESSMENT	35 min		
	PASSWORDS	15 min		
	BREAK	<i>10 min</i>		
	PRIVACY ON PUBLIC NETWORKS AND WIFI, HANDS ON WITH VPN AND TOR	40 min		
	BROWSING PRIVACY	30 min		
	MALWARE	10 min		
	FINAL EXERCISE	15 min		
	WRAP UP & EVALUATION	5 min		

Total Workshop Time: 3 HOURS



Welcome [5 min]

Materials

- Name stickers
- Large paper with Agenda, training website info and contact email posted on wall
- Pens/pencils, notepads on each table
- Handouts

Slide:	TITLE SLIDE - DIGITAL PRIVACY: HANDS-ON TACTICS AND TOOLS
Actions:	People arriving, ask everyone to write their First Name and Library System.
Prompt:	Ask them to start completing the Intake Questions of the Intake and Exit Survey.

Slide:	WORKSHOP GOALS
SPOKEN:	<p>SLIDE: WORKSHOP GOALS</p> <ul style="list-style-type: none"> • Digital privacy and security practices to share with patrons • Assess and communicate privacy risks with patrons • Protecting accounts with strong passwords and 2-factor authentication • Hands-on internet browsing privacy controls & tools • Malware and virus prevention and protection • Resources and practices available to library institutions <p>Facilitator SAY: Welcome to Hands-on Data Privacy and Digital Security at METRO.</p> <p>The main goal of this workshop is for library staff to deepen understanding of data privacy and have hands-on practice with privacy and security tools that they can share with patrons. This includes tools that the library has already put in place as well as other tools that are freely available online.</p> <p>Specifically, we'll be:</p> <ul style="list-style-type: none"> • Practicing assessing and communicating about privacy risks with patrons • Protecting accounts with strong passwords and 2-factor authentication • Getting hands-on with internet browsing privacy controls & tools • Discussing malware and virus prevention and protection • Sharing resources and practices available to library institutions <p>We are also offering another workshop that looks more generally at how information flows through the Internet, and how patron data privacy is impacted by library systems, federal and state policies, agreements with third party companies like bibliocommons, and terms of use of Internet companies. You can sign-up for those on the METRO website -- that class is offered once each month.</p>



Slide:	WORKSHOP AGENDA
SPOKEN:	<p>Facilitator SAY: And this is what the day will look like with a break in the middle.</p> <ul style="list-style-type: none"> • Welcome (5min) • Introduction & Name your team (10min) • Risk Assessment (35min) • Passwords (15min) <p><i>BREAK (10min)</i></p> <ul style="list-style-type: none"> • Privacy on Public Networks and WiFi, Hands-On with VPN and TOR (40min) • Browsing Privacy (30min) • Malware (10min) • Final Exercise (15min) • Eval (5min)

Introductions [10 min]



Goals

- team building
- get a sense of the experience in your group

Slide:	INTRODUCTIONS
Activity:	Organize people by library type for small group introductions, reportbacks will follow
SPOKEN:	<p>Facilitator SAY: “Who here is from a public library?” “Who here is from an academic library?” (FYI = community college, university, etc.) “Who here is from a school library?” (= K-12) “Who here is from a special library?” (which could be a law library, medical library [like in a hospital], museum, cultural organization, municipal agency...)</p>
Prompt 1:	<p>Facilitator Prompts Group for Activity:</p> <ul style="list-style-type: none"> • Please join with the librarians from your type of library. • Introduce yourself to each other. Share your name, gender pronouns, your library system and role. • Come up with a name for your group.
Prompt 2:	<p>Facilitator Prompts Group for Report Back -</p> <ul style="list-style-type: none"> • Share your Group Name!
SPOKEN:	<p>Facilitator SAY We’ll do a few group exercises and will be asking you to follow along with us in a few parts. Please think of your team as a first line of support in these exercises.</p>



Risk Assessment in Teams [35 min]



Materials:

- Whiteboard & pens
- Printed Patron Profiles (1 copy)


Goals:

- Participants begin to work as a team
- Participants share experience & understanding of patron security & privacy risks
- Participants will practice weighing risks and choosing which risks to address
- Library staff practicing using tools to support conversations with patrons about assessing likelihood of online risks

Slide:	RISK ASSESSMENT																			
ACTION:	<p>Draw the columns and column headings as below on the whiteboard and use the table as the participants generate examples. Fill in examples as participants speak them.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 20%;">1. Information</th> <th style="width: 20%;">2. Who? How likely?</th> <th style="width: 20%;">3. Already doing</th> <th style="width: 20%;">4. Impact</th> <th style="width: 20%;">5. New Effort</th> </tr> </thead> <tbody> <tr> <td><i>Job applications, SSN, work history</i></td> <td><i>other library patrons are likely to access any information he leaves behind at the terminal;</i></td> <td><i>logging off; not leaving printed copies on tables; using a privacy screen</i></td> <td><i>possible identity theft; very impactful;</i></td> <td></td> </tr> <tr> <td><i>Social media accounts on computers and mobile phone;</i></td> <td><i>family members likely to access on his mobile;</i></td> <td><i>using library terminals;</i></td> <td><i>accessing personal messages; impersonating; bothersome but not very impactful</i></td> <td></td> </tr> </tbody> </table>					1. Information	2. Who? How likely?	3. Already doing	4. Impact	5. New Effort	<i>Job applications, SSN, work history</i>	<i>other library patrons are likely to access any information he leaves behind at the terminal;</i>	<i>logging off; not leaving printed copies on tables; using a privacy screen</i>	<i>possible identity theft; very impactful;</i>		<i>Social media accounts on computers and mobile phone;</i>	<i>family members likely to access on his mobile;</i>	<i>using library terminals;</i>	<i>accessing personal messages; impersonating; bothersome but not very impactful</i>	
1. Information	2. Who? How likely?	3. Already doing	4. Impact	5. New Effort																
<i>Job applications, SSN, work history</i>	<i>other library patrons are likely to access any information he leaves behind at the terminal;</i>	<i>logging off; not leaving printed copies on tables; using a privacy screen</i>	<i>possible identity theft; very impactful;</i>																	
<i>Social media accounts on computers and mobile phone;</i>	<i>family members likely to access on his mobile;</i>	<i>using library terminals;</i>	<i>accessing personal messages; impersonating; bothersome but not very impactful</i>																	
SPOKEN:	<p>Facilitator Discuss Risk Assessment and Introduce the Method</p> <p>Facilitator SAY: We have formal and informal methods for assessing risks to our privacy, the potential impacts on ourselves, and choosing tools to try to maintain privacy.</p> <p>This method is shared on the handout and is a modified version of the EFF’s Threat Modeling exercise, link in the handout.</p> <p>In this first exercise, we’ll share a simple method for assessing risks and choosing tactics for maintaining our privacy. This is called a Threat Model or a Risk Assessment. Formalizing the method helps us to make sure that we’re being thorough in our assessment and choosing to act on our privacy concerns for our most sensitive</p>																			



	<p>information and for the information that is most at risk of being accessed without our permission.</p> <p>A Risk Assessment is specific to a person and a context. In this exercise, we'll consider threats that patrons face and develop a shared understanding of how we would assess those threats and support patron privacy based on this assessment.</p>
--	--

Slide:	RISK ASSESSMENT: QUESTIONS
Prompt:	<p>Facilitator SAY: When Conducting an Assessment, There are 5 Main Questions you Should Ask Yourself.</p> <ol style="list-style-type: none"> 1. What information do you want to keep private? 2. Who might try to access that information without your consent? How likely is it that they will succeed? 3. What are you already doing to keep it private? 4. What are the consequences and how impactful would the consequences be for you? <p>Facilitator/Scribe - DO AN EXAMPLE TOGETHER and write on the whiteboard</p> <p>Facilitator ASK:</p> <ul style="list-style-type: none"> • What information do you want to keep private and what are you doing to keep it private? <p>Scribe WRITE:</p> <ul style="list-style-type: none"> • Participant answers on the whiteboard to complete as the examples after we introduce the questions below. <p>Facilitator/Scribe - Use the examples people have shared and answer the subsequent questions; if people seem confused, do more examples</p>
ACTION	Hand out Patron Profiles
Prompt 1:	Facilitator ASK: Each group to think of 3 distinct pieces of information that your patron wants to protect
Prompt 2: (15 min)	<p> Activity: Patron Risk Assessment on Paper</p> <p>Facilitator DO: Give each group a piece of large paper</p> <p>Facilitator INSTRUCT: Each group to scribe their responses on the large paper, and label the patron name & patron number, e.g. "Patron 1: Cecilia"</p> <p>Facilitator SAY: Now you'll do threat modeling in groups.</p> <p>Facilitator DO: Hand each group a patron profile.</p>



Facilitator SAY: Read your Patron profile together, give it a name, talk about who they are. Now answer the questions as you imagine the patron would answer them.

Start by giving them a name.

- Patron 1, 20s: has smartphone and uses it for calls, texts, apps and occasionally for surfing the web. They use desktop computers at the library to apply for jobs and also to shop online and to use Facebook.
- Patron 2, an older adult: their only internet access is on library terminals, and they set up their first email account on a library terminal. They attend library classes for older adults on digital literacy.
- Patron 3, 30s: they are a freelance journalist who frequently brings their laptop to the library and uses the public wifi. They conduct skype interviews with sources in public places, use facebook and twitter to communicate with sources and to promote stories
- Patron 4, 20, is a college student. While doing research, they search for journal articles through Google Scholar and in subscription databases such as ones from ProQuest and EBSCO. Sometimes they use their own laptop and sometimes they use computers in the campus library. They get course readings and assignments and upload their completed coursework to an online learning management system.
- Patron 5, 20s, accesses their library only online. They borrow ebooks through OverDrive and other platforms, and they access subscription databases to find articles and other media. They also use apps on their smartphone including Flipster to read magazine articles and the library's own app to manage their account. They stay perpetually logged in to some or all of their accounts across multiple devices.
- Patron 6, 14 years old: has their own smartphone which is on a family plan that is both surveilled and limited by the plan's subscriber. They come into library and use computers for personal use including gaming, email, social media, and to complete school work.
- Patron 7, 12 years old, using school library computers to play games such as Minecraft and do homework through their school's portal. They attempt to go around school filters using 3rd party websites to access games/social media. Games are multiplayer and they interact with others online.

Facilitator aid:

Facilitators walk around and support groups who are stuck. Here are some examples created in our training of trainers day:

Patron 1, 20s: has smartphone and uses it for calls, texts, apps and occasionally for surfing the web. They use desktop computers at the library to apply for jobs and also to shop online and to use Facebook.

Name: Casey, 27: Looking to switch careers

1. *job application materials including SSN; passwords to social media accounts*



- and online shopping sites; contacts; contents of messages*
2. *logging off; not leaving printed papers job applications on shared desks; using library desktops; limiting use of web; passwords; people looking over shoulder;*
 3. *cybercriminals/identity theft; friends/family who might access his phone; other library patrons; government; private sector ads*
 4. *very likely that family members in the house will access his accounts; likely that cybercriminals will succeed if they try; government actually isn't trying to access his information; advertisements are definitely accessing his data*
 5. *identity theft of credit scores and job applications would be very impactful and could require a lot of time and attention;*
 6. *more willing to use more time to protect his professional and government related data; less willing to use as much effort in protecting personal accounts like social media*

Patron 6, 14 years old: has their own smartphone which is on a family plan that is both surveilled and limited by the plan's subscriber. They come into library and use computers for personal use including gaming, email, social media, and to complete school work.

1. *Social info (photos, messages, dates), financial info because uses phone to order food, email*
2. *Justin protects himself (by necessity) by using multiple devices. Parents "protect" Justin surveilling his phone and both his parents and BPL are filtering data on his phone.*
3. *Justin's parents are monitoring his use. They are absolutely succeeding, monitoring through software they install and controls they can set via their mobile phone provider.*
4. *Consequences of Justin seeing that he is using his phone in ways that they prohibit could lead to punishment. Justin's parents are concerned that consequences could be criminal.*
5. *Justin is willing to put effort into circumventing filters -- uses his phone, BPL devices, friend's computers. When he gets into a bind, he is willing to go to more trouble and will seek help from BPL staff and friends. His parents put in a lot of effort learning about software and filtering via their provider.*

Patron 3, 30s: they are a freelance journalist who frequently brings their laptop to the library and uses the public wifi. They conduct skype interviews with sources in public places, uses facebook and twitter to communicate with sources and to promote stories

Name: Clarice

1. *sources' identities, own identity, contents of interviews*
2. *passwords, VPN when using public wifi, cloaking phone numbers*
3. *government, other journalists, corporations who are the subject of the articles she writes, other patrons and people around her*



	<p>4. <i>depends on the topic of her story. If it's corruption, likely; it's it a story about a cute puppy, unlikely</i></p> <p>5. <i>loss of credibility, depends on location, she is responsible for sources</i></p>
--	--

Slide:	RISK ASSESSMENT REPORT BACK
Prompt:	<p>FACILITATOR ASK: Each group to choose one person to report back:</p> <p>(a) Share your patron description;</p> <p>(b) What is their risk assessment?</p> <p>Facilitator ask questions to get more information or when something is vague.</p> <p>FACILITATOR ASK: Does anyone have any additional concerns for this patron?</p>
SPOKEN:	<p>Facilitator review this list and connect these tools and tactics to things BPL is doing and parts of the workshop's agenda. Say that each team is the champion for the patron they have gotten to know through this exercise. Throughout the training, we will ask you to add to the tools that your patron could be using to support their privacy goals.</p>

Passwords [15 min]



Goals:

- Participants will learn about threats to passwords
- Participants will learn about tools for creating strong passwords
- Participants will practice creating strong passwords
- Participants will learn about 2-factor authentication
- Participants will learn about tools for managing passwords

Slide:	PASSWORDS
SPOKEN	Facilitator SAY: Passwords are a primary tool to keep computer & accounts private.
Prompt	<p>Facilitator ASK Discussion Questions:</p> <ul style="list-style-type: none"> • What makes a strong password? • What's a strong password? <p><i>Random, memorable, does not use personal information</i></p>
SPOKEN	<p>Facilitator Recap and/or share tips for passwords</p> <ol style="list-style-type: none"> 1. Create long, complex passwords (always over 12 characters) 2. Don't use something obvious (like your birthday) 3. Use a unique password for important accounts 4. Change your password regularly 5. Don't get phished! 6. We will talk about applications to help you with this later!



Slide:	HOW STRONG IS YOUR PASSWORD?
Prompt	<p>Facilitator SAY: Test it: How strong is your password? Try a password you would normally use (but not your actual password): https://blog.kaspersky.com/password-check/</p> <p>Facilitator DO: As you notice people are writing and testing, ask, “anything surprising?” “how long did it take to break the password?”</p>
SPOKEN	Facilitator WRAP: Passwords are a critical part of digital privacy risk assessment and should be a part of privacy practice. We know that people come to the library and create accounts, library accounts, service accounts, email accounts.

Slide:	STRONG PASSWORDS FROM PHRASES
SPOKEN	<p>Facilitator SAY: Strong passwords are difficult to guess -- not just by people who know you and may know information that is important to you, but also by computer programs designs to guess passwords. Here is a method we recommend for creating a password that is hard to guess and includes a variety of characters.</p> <p>Facilitator SAY: Think of a phrase, lyrics to a song, a sentence that is memorable for you. Write it down. Take the first letter of each of the words. Change some of the characters to similar special characters and capitals.</p> <p>Example: <u>S</u>he <u>w</u>as <u>m</u>ore <u>l</u>ike <u>a</u> <u>b</u>eauty <u>q</u>ueen <u>f</u>rom <u>a</u> <u>m</u>ovie <u>s</u>cene → SWMLABQFAMS → \$wml@BQf@m\$</p>

Slide:	LIBRARY PINS
SPOKEN	Facilitator SAY: Library Pins are an example of passwords that are often not very secure.
Prompt	Facilitator Ask: What does your library system use?
SPOKEN	<p>Facilitator SAY: At BPL, PINs are very short and by default are made based on a patron’s birth month and year. So here are some tips we can share when people sign up for new cards or when people reset their PINs.</p> <p>Do’s</p> <ul style="list-style-type: none"> ● information of a person other than you (ex. last 4 of your childhood friend’s phone number) ● birthyear backwards ● have the patron enter their own PIN <p>Don’ts</p> <ul style="list-style-type: none"> ● Personal information birthdate MMYM MMDD ● birthyear (ex. 19xx or 20xx) ● Other personal info: last 4 of SSN, last 4 of your phone number



	<ul style="list-style-type: none"> • sequential digits (ex. 1234) • repeated digits (ex. 7777)
--	--

Slide:	2-FACTOR AUTHENTICATION (Title only)
Prompt	<p>Facilitator ASK:</p> <ul style="list-style-type: none"> • Is anyone using 2-Factor Authentication already? What accounts? How does it work? • What services do you use and what you want to add 2-factor authentication for?
SPOKEN	<p>Facilitator SAY:</p> <p>It's important to have a strong password, but passwords can be broken or stolen through Phishing. Phishing is when you receive an email asking for you to log into a service to change or check something.</p> <p>What if someone else guesses your password, because they crack it, know it, or steal it? You can use 2-Factor Authentication to add another step to your login. You go to your account, log in, & receive a message another way - say through your mobile phone, or email address - then enter a code or another piece of information to log in.</p>

Slide:	2-FACTOR AUTHENTICATION
SPOKEN	<p>Facilitator SAY:</p> <p>The 2 factors are: Something I know - typically a password or phrase Something I have - could be a code sent to us on our mobile, software we use to generate a code, or a hardware code</p> <p>Facilitator SHARE Examples:</p> <p>Example of a software and a hardware token; a token sent to your mobile or that you generate using software; a token that is generated by a physical object like the key in the right image</p>

Slide:	HANDS-ON: 2 FACTOR AUTHENTICATION
ACTION	<p>Facilitator DO: Show the settings in gmail, and explain what would happen.</p> <p>Support the participants to set up 2 factor on (1) Google or (2) a financial institution of their choice. They can turn it off or on once they have it set up.</p> <p>For people who have Google accounts, go to: https://www.google.com/landing/2step/</p> <p>For people who setting up 2 Factor on another account, find instructions through: http://twofactorauth.org</p>



Slide:	DEVICE PASSWORDS & ENCRYPTION
SPOKEN	<p>Facilitator SAY: We've been speaking mostly about passwords for services and accounts. You should also put a password on your personal computers and mobile devices. Passwords on devices can be linked to other security features as well.</p> <p>For example: Apple iPhone encryption. By default now, iPhones are encrypted -- with an unencrypted phone, someone can make a copy of your data and view it as you do. If your data is encrypted, a person can copy your data, but would need to unencrypt it with your own password, otherwise it looks like code. Apple's system is designed so that if you guess the wrong password <u>_times_</u>, the device destroys its own data.</p>
Slide:	PASSWORD MANAGERS
SPOKEN	Facilitator SAY: Many browsers offer to save your passwords for you. This is not secure. Instead, try a password manager.
Prompts	<p>Facilitator ASK:</p> <ul style="list-style-type: none"> - Who is using an online password manager? - How are you using it? Do you store all of your passwords in it? - How did you choose it? <p>Facilitator ASK/Discuss: When are Password Managers a good option?</p> <ul style="list-style-type: none"> - Use on your personal computers, not shared ones - Use a browser-based password manager anywhere - Secured with a password or 2-factors - Store on your computer encrypted or in the cloud <p>Facilitator ASK: What tools are people interested in trying? Already using?</p> <ul style="list-style-type: none"> - Keychain - Apple Computers; local - KeePass - LastPass (online and on your computer) - DashLane
INFO	<p>Info/Notes For Facilitators to Support Discussion</p> <p>How to choose:</p> <ul style="list-style-type: none"> - Online and offline access - 2-factor authentication - Browser integration - Automatic Password Capture - Automatic password changes - Automatic Security Alerts - Portable/Mobile Apps - Security Audits - Import/Export - One-Time-Use Password Sharing - Password Sharing



	<p>Resource: “You need a password manager. Here are some good free ones.” http://www.wired.com/2016/01/you-need-a-password-manager/</p> <p>WHO MIGHT USE THIS: The patron profile of the older person who can’t remember passwords</p>
--	--

Slide:	DEMO: PASSWORD MANAGERS
INFO	<p>Facilitator use prepared, customized info to demonstrate a password manager. Demo account on LastPass: Go to: lastpass.com and log in; Show adding a site;</p> <p>With a paid version, you can share folders with other people; they need accounts and can access those shared passwords and usernames here.</p> <p>Login: password:</p> <p>Features you can show:</p> <ol style="list-style-type: none"> 1. One password encrypting the accounts 2. Generating passwords 3. How to use the passwords
SPOKEN	Facilitator SAY: you should never have the browser remember your password, instead use a password manager.

Slide:	PASSWORD TAKEAWAYS
SPOKEN	<p>Facilitator SAY: Summing up, these are some of the key takeaways related to passwords.</p> <ol style="list-style-type: none"> 1. Create long, complex passwords (always over 12 characters) 2. Don’t use something obvious (like your birthday) 3. Use a unique password for important accounts 4. Change your password regularly 5. Don’t get phished! 6. Use a password manager, DO NOT save passwords in the browser
Prompt	Facilitator: Ask the groups to return to their Risk Assessment, and add using a different color marker, any new tools/tactics to the “Already Doing” column that you can share with your patron to support their privacy goals.



Break! [10 min]



Facilitator: Ask participants to return promptly.

Privacy on Public Networks and Wifi [40 min]

Goals:

- Evaluate the risks of using WiFi at the library, public WiFi
- Practice some steps for keeping your data private or secure

Slide:	PRIVACY ON PUBLIC NETWORKS AND WIFI
ACTION	Facilitator DO: Introduce this portion of the workshop, including goals.

Slide:	BPL'S WIFI EULA
SPOKEN	Facilitator SAY: This is the pop up that BPL shows you when you log onto the BPL wireless.
Prompt	Facilitator ASK: <ul style="list-style-type: none"> • Why does the Library give this warning? • Discuss the library as a free internet access point. • What can you do to protect yourself and what can you do to support patrons' privacy?
SPOKEN	Facilitator SAY: The same is true of many public networks that we get onto -- cafes, airports, restaurants, transit -- that we don't know who else is on the network, that they can see our traffic, that the network operator also can see our traffic. Not all give you a warning. Facilitator, Additional Discussion: <i>open vs passworded router (a password on a network offers some encryption and protects traffic from would-be sniffers outside the network, but anyone connected to that network with bad intentions might be able to view unencrypted traffic)</i>

Slide:	HTTP VS HTTPS
SPOKEN	Facilitator SAY/EXPLAIN: When you are viewing a site, these are 2 ways you can send and receive information.



	<p><u>Using HTTP</u>, the information that you send and receive is sent like a postcard, so anyone on your network can see what you are sending and receiving. This may be fine, say, if the information you're asking for and receiving is New York Times articles.</p> <p><u>Using HTTPS</u>, this information is sent encrypted, as though it's in an envelope and anyone on your network could see that you are sending and receiving data, but not exactly what that data is. This is particularly important when you're sending sensitive information like your username/password.</p> <p>So, when you're on a website, you can check HTTP or HTTPS and you might try now or later, if you go to your favorite site, you'll see that it has HTTP or HTTPS.</p>
INFO	Facilitators! Diagram explanation: the many-armed guy is the INTERNET!
Slide:	HTTPS PLEDGE
SPOKEN	<p>Facilitator SAY:</p> <p><u>The Library Freedom Project</u> was started by a librarian to develop knowledge, practice and policy that reinforces the ability of libraries to be spaces of intellectual freedom.</p> <p>The Library Freedom Project is asking libraries to sign onto an HTTPS Pledge that the libraries will commit to using HTTPS on all pages they create and will require services they use to implement HTTPS.</p> <p>https://libraryfreedomproject.org/ourwork/digitalprivacypledge/</p> <p>BPL Policy: BPL has implemented HTTPS on all webpages that involve people entering in personal data. When BPL has a new website (planned for later this year), the whole site will be HTTPS.</p>
Prompt	Facilitator ASK: Does anyone know your library's policy? You might go back to your library system and ask what they will be doing.
Slide:	DIGITAL FINGERPRINTS
Prompt	Facilitator ASK: What does the network and/or a destination server know about you? What is your data fingerprint, or "identity" on a network?
Prompt	<p>Facilitator PROMPT: Find out what your fingerprint is: Open in your browser: https://www.whatismybrowser.com/ You can also look at: https://panopticlick.eff.org/</p> <p>Facilitator ASK: Does it know where you are?</p>



Slide:	VPN
Section	VPNs, including on-screen demo (10 min)
Prompt	Facilitator ASK: <ul style="list-style-type: none"> • who is using a VPN? Who has? • What were you using it for? • What risks were you addressing?


Slide:	HOW A VPN WORKS
SPOKEN	Facilitator SAY: A Virtual Private Network is a way for you to access a network you trust from a network you don't trust. It's described as a tunnel, the tunnel is protective and your data can flow to and from the secure network through the tunnel. <u>The most important thing you need to know about a VPN:</u> It secures your computer's internet connection to guarantee that all of the data you're sending and receiving is encrypted and secured from others -- people on your network, your ISP. The VPN service you use does see the data you are sending and receiving.

Slide:	VPN DEMO
ACTION	Facilitator DO: Lead on-screen demo of a VPN (PIA). Open Private Internet Access Turn it on, show that it says it's active.

Slide:	VPN FEATURES & SERVICES
SPOKEN	Facilitator SAY: VPNs don't keep logs, protect your anonymity, don't discriminate against traffic or protocol types, offer exit servers to help you get around location-restricted content blocks, and deliver the best bang for your buck. It takes a lot to make a VPN service worth your trust, but there are some good ones out there. Here are some of the ones you thought were the best, in no specific order

Slide:	ANONYMOUS BROWSING WITH TOR
Section	<i>Tor discussion and demo (15 min)</i>
SPOKEN	Facilitator SAY. We know from our RISK ASSESSMENT that we can be identified on the internet by our:



	<ul style="list-style-type: none"> Browsers, cookies, accounts, and fingerprint
Prompt	Facilitator ASK: <ul style="list-style-type: none"> Who here is using a tool to make their browsing more anonymous? What are the risks you are concerned about? Who would be looking at your internet use? What would the consequences be?
SPOKEN	Facilitator SAY: The Tor software protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked.
ACTION	Facilitator DO: On screen demo - open up Tor and run https://www.whatismybrowser.com/
SPOKEN	Facilitator SAY: If you want to install, you can download Tor: https://www.torproject.org/download/download.html.en
Slide:	HOW TOR WORKS
ACTION	Facilitator DO: Describe/explain the tor graphics.
Slide:	NETWORK PRIVACY TAKEAWAYS
SPOKEN	Facilitator SAY: To sum up, here are some key takeaways: <ol style="list-style-type: none"> It's easy for other people on your network to see your activity on the network. Only login on secure sites using encryption: HTTPS  Don't use the same username and password for different sites Save the most important tasks for home or secure connection (hotspot). Maximum Security: VPN or Anonymous Browser
Prompt	Facilitator REQUEST: Ask the groups to return to their Risk Assessments and add using a different color marker, any new tools/tactics to the "Already Doing" column that you can share with your patron to support their privacy goals.



Browsing Privacy [30 min]



Goals:

- We will discuss how we know that we are being tracked on the internet
- We will learn about the companies that track
- We will get hands on with seeing who we are on the internet
- We will install browser plugins to block adware and spyware in browsers
- We will implement browser settings that will make it harder to track us

Slide:	BROWSING PRIVACY
ACTION	Facilitator DO: Review workshop section goals.
WATCH	Facilitator DO: Play video about digital trail: https://episode1.donottrack-doc.com/en/
Prompt	<p>Facilitator ASK: When you're surfing the net, you are looking at websites and websites are looking at you. How do you know that websites and web services are looking at you?</p> <ul style="list-style-type: none"> • Patrons or acquaintances follow you on social media. • Those pants that keep following you as an advertisement. • Predatory ads. • Companies tracking you online. • My identity on the internet: I am my account(s) when I'm logged in, I am my browser and my machine, I am my IP address • Deleting cookies, Flash cookies
Prompt	<p>Facilitator ASK: What are some steps you're taking to prevent tracking?</p>

Slide:	PRIVACY AND BROWSING
SPOKEN	<p>Facilitator SUMMARIZE: There are 3 ways that you can be tracked while you're on the internet, and we'll talk about 3 tactics to prevent this when you don't want to be tracked.</p> <ul style="list-style-type: none"> • My browser and browser cookies • My fingerprint • My accounts when I'm logged in
SPOKEN	<p>Facilitator SAY: In this section, we'll look into all of these pieces:</p> <ul style="list-style-type: none"> • Deleting cookies and browser history • Opting out of tracking • Actively blocking trackers



Slide:	WHAT DOES YOUR LIBRARY DO?
SPOKEN	<p>Facilitator SAY:</p> <p>BPL IT has browser privacy defaults linked to patron sessions. When a patron signs out or their session ends, BPL computer terminals:</p> <ul style="list-style-type: none"> • Clear Browser Data including browsing history, form data, user and passwords; • Clear downloaded files; • Clear temporary files;
Slide:	WHAT BROWSER ARE YOU USING?
SPOKEN	<p>Facilitator SAY:</p> <p>We recommend using Firefox or Chrome. Internet Explorer and Safari are less secure. They have more known security holes, are less hardened. Firefox and Chrome have more security features.</p>
Slide:	WHAT ARE COOKIES?
SPOKEN	<p>Facilitator SAY:</p> <p>Cookies are small text files that websites download to your computer when you visit them. At the start, cookies were invented so that shopping sites could remember items you were shopping for even if you left and returned to the site. A cookie is downloaded to your computer identifying it and when you return to a site, the site asks for existing cookies, if it recognizes you, it will show you your past items or preferences.</p> <p>Now, advertisements are often connected through third party advertising networks -- sites A and B may both have ad banners with content from one advertising network that uses one cookie across all of the sites it's on. This is called a third party cookie and allows your activities to be linked and a profile to be built about you across sites.</p>
INFO	<p>Facilitators, a link to more info for participants is presented on the slide:</p> <p>Wall Street Journal Video: How Advertisers Use Internet Cookies to Track You https://vimeo.com/12204858</p>
Slide:	WHAT IS PRIVATE BROWSING MODE?
SPOKEN	<p>Facilitator SAY:</p> <p>When you use your browser, your browser stores information about your browsing - history of sites you have visited, cookies from sites you have visited, possibly data you've typed into forms. You can erase this either manually through our browser settings or by using private browsing mode.</p>
Prompt	<p>Facilitator ASK:</p> <p>Why would I want to use private browsing or delete my history? Who might use this: reference the teenager with a computer at home; sharing a computer</p>



SPOKEN	<p>Facilitator SAY:</p> <p>This is a control on your browser:</p> <ul style="list-style-type: none"> • Prevents saving history of sites you visit • Prevents saving usernames and passwords • Prevent saving form data • Can automatically delete cookies <p>Does not:</p> <ul style="list-style-type: none"> • Prevent other people from storing a history of the sites you visit (ex. your ISP) • Prevent sites you visit from tracking your behavior • Prevent fingerprinting
ACTION	<p>Facilitator DO:</p> <p><i>ON SCREEN DEMO: Open a Private Browsing Window</i></p>
SPOKEN	<p>Facilitator SAY:</p> <p>If you want your browser to not remember your history and save data by default, you can use private browsing. Show this slide with instructions about how to open a private browsing window in Chrome, Firefox, IE, Safari.</p>

Slide:	HANDS-ON: BYE COOKIES & HISTORY
SPOKEN	<p>Facilitator SAY:</p> <p>You can delete browser history manually also. We'll demo deleting cookies and browsing history.</p>
ACTION	<p>Facilitator DO: ON Screen Demos</p> <ol style="list-style-type: none"> 1. On Screen Demo: show cookies then delete cookies and history 2. On Screen Demo: showing cookies - http://www.wikihow.com/View-Cookies. Open a cookie and show that it is a small amount of text. Look for a file that seems to just be marking that you have visited the site. 3. On Screen Demo: Follow the slide steps to delete history -- you should see a list there of sites you have visited. 4. On Screen Demo: Delete the history and the cookies and show that there both are gone.
SPOKEN	<p>Facilitator SAY:</p> <p>Some, but not all of your mobile browsers will have similar settings for clearing history, cookies and incognito modes: example screen from Chrome for Android</p>

Slide:	MOBILE BROWSER PRIVACY SETTINGS
SPOKEN	<p>Facilitator SAY:</p> <p>Some, but not all of your mobile browsers will have similar settings for clearing history, cookies and incognito modes: example screen from Chrome for Android</p>



Slide:	HANDS-ON: DISABLE FLASH
SPOKEN	<p>Facilitator SAY:</p> <p>Flash is a type of digital media that often looks like animation or a video with graphics. Many advertisements use Flash animations and these require a plugin to play in the browser. The plugin, however, has a lot of security weaknesses and viruses attack through these plugins.</p> <p>For that reason, we disable it!</p>
ACTION	<p>Facilitator DO:</p> <p><i>ON SCREEN DEMO:</i></p> <p><i>Disable Flash Player in your browser (show either Chrome or Firefox)</i></p> <p><i>Explain that some sites will require Flash to play the content you want to see on the site. Example includes Hulu - go to hulu.com and enable Flash for this site only.</i></p>
Slide:	PLUG-INS TO PREVENT THIRD PARTY TRACKING
SPOKEN	<p>Facilitator SAY:</p> <p>You can install tools in your browser called Plugins or Extensions. We've listed a few here that we recommend for blocking tracking.</p> <p>Privacy Badger is a browser add-on that stops advertisers and other third-party trackers from secretly tracking where you go and what pages you look at on the web. If an advertiser seems to be tracking you across multiple websites without your permission, Privacy Badger automatically blocks that advertiser from loading any more content in your browser. To the advertiser, it's like you suddenly disappeared.</p> <p>If you want to install this, you can follow this link (https://www.eff.org/privacybadger) and click the install instructions. This is available for Chrome and Firefox.</p>
SPOKEN	<p>Facilitator SAY:</p> <p>HOW DOES THIS WORK? - When you view a webpage, that page will often be made up of content from many different sources. (For example, a news webpage might load the actual article from the news company, ads from an ad company, and the comments section from a different company that's been contracted out to provide that service.) Privacy Badger keeps track of all of this. If as you browse the web, the same source seems to be tracking your browser across different websites, then Privacy Badger springs into action, telling your browser not to load any more content from that source. And when your browser stops loading content from a source, that source can no longer track you.</p>
ACTION	<p>Facilitator DO - On Screen Demo: Privacy Badger</p> <p>Open the New York Times and click on the Badger icon to show how many trackers</p>



	<p>Privacy Badger sees. Describe the states. <i>If you have just cleared your cookies, all trackers will look green because there's not yet history of tracking across multiple sites.</i></p>
SPOKEN	<p>Facilitator SAY as show during demo:</p> <p>Green means there's a third party domain, but it hasn't yet been observed tracking you across multiple sites, so it might be unobjectionable. When you first install Privacy Badger every domain will be in this green state but as you browse, domains will quickly be classified as trackers.</p> <p>Yellow means that the third party domain appears to be trying to track you, but it is on Privacy Badger's cookie-blocking "yellowlist" of third party domains that, when analyzed, seemed to be necessary for Web functionality. In that case, Privacy Badger will load content from the domain but will try to screen out third party cookies and referrers from it.</p> <p>Red means that content from this third party tracker has been completely disallowed.</p> <p>Privacy Badger analyzes each third party's behavior over time, and picks what it thinks is the right setting for each domain, but you can adjust the sliders if you wish.</p> <p>At a more technical level, Privacy Badger keeps note of the "third party" domains that embed images, scripts and advertising in the pages you visit. If a third party server appears to be tracking you without permission, by using uniquely identifying cookies (and, as of version 1.0, local storage super cookies and canvas fingerprinting as well) to collect a record of the pages you visit across multiple sites, Privacy Badger will automatically disallow content from that third party tracker. In some cases a third-party domain provides some important aspect of a page's functionality, such as embedded maps, images, or stylesheets. In those cases Privacy Badger will allow connections to the third party but will screen out its tracking cookies and referrers.</p>
Prompt (10 min)	<p>NOTE TO FACILITATORS: HANDS-ON Privacy Badger Installation</p> <p>Facilitator SAY: Everyone open https://www.eff.org/privacybadger Click Install and install - will work on Chrome and Firefox</p> <p>Facilitator DO: Support participants to install.</p>
Slide:	SOCIAL MEDIA PRIVACY SETTINGS
SPOKEN	<p>Facilitator SAY: Facebook, Twitter and Google all allow you to opt-out of customized ads based on the habits they track.</p>
Prompt	Facilitator ASK (popcorn style):

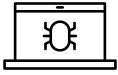


	<p>What are social media habits that concern you and what would support patrons to learn best practices in your own library?</p> <p>Facilitator SAY: We're going to look at our privacy settings on Facebook. If you have an account, log on and if not, look on with someone near you.</p>
Prompt	<p>Facilitator ASK (during discussion):</p> <ul style="list-style-type: none"> • Who can see what? • What does your profile look like from other people's eyes? • Are you sharing your location? • What apps have access to your account? • How do you report problems? • How do you delete your account? <p>Facilitator ASK: Are there questions? What are people's biggest concerns?</p>
INFO	<p>For Facilitators - Additional Notes can be found here:</p> <ul style="list-style-type: none"> • http://www.informationweek.com/software/social/facebook-privacy-10-settings-to-check/d/d-id/1269438?image_number=2 • http://mashable.com/2013/07/09/facebook-privacy-how-to/#eE8lpsPwqaqL

Slide:	PRIVACY IN BROWSING TAKEAWAYS
SPOKEN	<p>Facilitator SAY: BPL automatically mimics "Private Browsing" mode on log out by deleting history, form data, and usernames/passwords;</p>
SPOKEN	<p>Facilitator SAY: Steps we can take:</p> <ul style="list-style-type: none"> • Browser settings: Deleting history and cookies, Private browsing • Opt-Out of some Tracking • Using a diversity of software providers • Block and prevent some Tracking using plugins
Prompt	<p>Facilitator REQUEST: Ask the groups to return return to their Risk Assessment and to add using a different color marker, any new tools/tactics to the "Already Doing" column that you can share with your patron to support their privacy goals.</p>



Malware [10 min]



Goals:

- Define the many forms & purpose of malware
- Familiarity with anti-malware software and strategies

Slide:	MALWARE
Prompt	<p>Facilitator ASK: Ask the room to share experiences:</p> <ul style="list-style-type: none"> • Has anyone had a virus or malware on their computer? • How did you know? • What did you do about it?
SPOKEN	<p>Facilitator SAY: What is Malware? Malware is any malicious code. You may have heard these names: virus, adware, spyware, worms, trojan, ransomware</p> <p><i>Optional definitions: Malware, malicious code:</i></p> <ul style="list-style-type: none"> • <i>Virus - a contagious piece of software that infects a host computer and spreads to other computers;</i> • <i>Adware - watches computer and internet use for the purpose of showing advertisements to the user;</i> • <i>Spyware - spies on internet activities to gather information about a user's behaviors; ex. Keyloggers</i> • <i>Worms - self replicating software that destroys data on the host computer;</i> • <i>Trojan - disguised as a safe or useful program, a Trojan is designed to take a user's personal information and to take over the computer and networks that the computer is a part of;</i> • <i>Ransomware - limits computer access until a user pays a fee;</i>
SPOKEN	<p>Facilitator SAY: What is the purpose?</p> <ul style="list-style-type: none"> • at first, many were experiments or pranks and now most are to steal personal information • some are designed to take over your computer and turn it into a scam -- sending spam email or illegal files
SPOKEN	<p>Facilitator SAY: How does malware get onto computers?</p> <ul style="list-style-type: none"> • Downloads: clicking on advertisements • exploiting software weaknesses; people figure out how to use the software you knowingly installed to install malware • Downloading files - via email, over the internet • If you don't know the emailer, don't download • If you don't trust the file, scan it • If you don't trust the website, don't download • Try to download from the creator of the file



SPOKEN	<p>Facilitator SAY:</p> <p>What to do if you have a virus:</p> <ul style="list-style-type: none"> • Run a scan. If your virus software is able to locate and delete this file, you are in luck. • If you cannot locate the file, you may need to bring your computer to someone at work or another service who can scan your computer and remove the virus. • Let your friends know.
Slide:	ANTI-MALWARE SOFTWARE
Prompt	<p>Facilitator ASK:</p> <p>What is your library or institution using for antivirus?</p>
SPOKEN	<p>Facilitator SAY:</p> <p>BPL's Antimalware practice:</p> <ul style="list-style-type: none"> • McAfee Antivirus Enterprise, mcafee.com - Windows • Gatekeeper, Macs • Update virus protection daily; scan computers and files
SPOKEN	<p>Facilitator SAY:</p> <p>Other popular software:</p> <ul style="list-style-type: none"> • AVG - http://www.avg.com/ - Free trials; • Avast - www.avast.com - Free scan software and cleanup; • Kaspersky, kaspersky.com - Free scan software and cleanup; • Malwarebytes, malwarebytes.org - Free scan and cleanup; • Norton, norton.com - Free trials; • Sophos, sophos.com - Free tools for home use (click "Free Tools") <p>How it works:</p> <ol style="list-style-type: none"> 1. Download the program of your choice 2. Scan your entire computer, folders, or even single files 3. Your software will alert you if it recognizes malware and supports you in deleting and repairing your computer or device; 4. Some software will search for malware-like behaviors also
Slide:	TURN ON YOUR FIREWALL
SPOKEN	<p>Facilitator SAY:</p> <p>Your computer can make connections to network, other devices, and other devices can try to connect to your machine. A Firewall controls the connections other devices can make.</p>
ACTION	<p>Facilitator DO:</p> <p>Turn this on now:</p> <p>Demo: Apple Menu>System Preferences>Security & Privacy>Firewall</p> <p>Windows: Open Windows Firewall by clicking the Start button. ...</p> <ol style="list-style-type: none"> 1. In the left pane, click Turn Windows Firewall on or off. ... 2. Click Turn on Windows Firewall under each network location that you want to



	help protect, and then click OK
Slide:	UPDATE YOUR SOFTWARE
SPOKEN	<p>Facilitator SAY: Everyday, people are finding holes in software. Often when you receive a software update, it is patching a security hole. Be sure to keep your software up to date, this includes your operating system.</p>
Slide:	AVOID PHISHING & CLICK BAIT
SPOKEN	<p>Facilitator SAY: Phishing - when you receive an email or a message that is targeted to you and asks you to take an action; Click-bait - sensational content; are commonly linked to malware.</p> <p>If you receive a message instructing you to take action, especially if you are being redirected to a website, instead of following the link you have been sent, open a browser window and type in the address. This way you can be sure you are going to the site or service you seek.</p>
Slide:	MOBILE ANTI-MALWARE
SPOKEN	<p>Facilitator SAY: There is also malware for mobile devices.</p> <ul style="list-style-type: none"> • Commonly, we download and install mobile malware knowingly -- installing fake apps • Or, trusted apps are exploited and used to infect our devices <p>Mobile Apps can be Mobile Malware</p> <ul style="list-style-type: none"> • Research best app for the job • Install apps from developers you trust • Think twice if it asks for a lot of permissions <p>Mobile Security Apps</p> <ul style="list-style-type: none"> • Avast, Kaspersky, McAfee, Norton, Sophos • Mobile features like locating if lost, turning off if lost
SPOKEN	<p>Facilitator DESCRIBE some of this example: Here's an example: 2048 Spooof</p> <p>Trojan:Android/Voxv.B is a trojanized version of the legitimate and popular game app 2048 Puzzle. The trojan uses the same name and look as the original app, but requests more permissions than the legitimate game, including permission for writing, reading and sending SMS messages. Due to the similarity between the legitimate and trojanized apps, users would need to be alert to the additional permissions requested by the trojan to be able to differentiate between them.</p>



	<p>Once installed, the trojan collects the following details from the device: International Mobile Subscriber Identity (IMSI) number International Mobile Equipment Identity (IMEI) number Device type, brand, model and release version Device ID, SIM serial number and phone number (line1) API level and display type List of installed apps These details are silently forwarded to specified remote servers; some of the details are also sent via SMS to a specified phone number.</p> <p>In addition to data harvesting, the trojan also checks the device for the presence of a specific app with the package name 'com.lbe.security' (LBE Security Master Application). This appears to be a security utility program intended for Chinese language users. https://www.f-secure.com/v-descs/trojan_android_voxv_b.shtml</p>
--	--

Slide:	ANTI-MALWARE TAKEAWAYS
SPOKEN	<p>Facilitator SAY: Here are some takeaways for malware:</p> <ul style="list-style-type: none"> ● Backup! Make a copy of your computer files and programs on an external drive. ● Update your software including your Operating System (OS); ● Be careful of links and downloads. Don't follow unknown links or download unknown attachments; scan files if you don't trust them; ● Screen for Malware. Install and use Antivirus/Antimalware software on your personal computers to scan your computer and suspicious files; ● BPL scans using Antivirus/Antimalware software on all of its computers; ● Keep all of your software updated including your Operating System (OS); ● Tell people if they send you malware
Prompt	<p>Facilitator REQUEST: Ask the groups to return return to their Risk Assessment and to add using a different color marker, any new tools/tactics to the "Already Doing" column that you can share with your patron to support their privacy goals.</p>



Risk Assessment - Final Exercise [15 min]



Goals:

- Participants make final revisions to risk assessment

Slide:	REVISITING YOUR RISK ASSESSMENTS
Prompt	<p>Facilitator REQUEST: In your groups, review your risk assessments.</p> <p>Also ask yourselves: What additional tools could your patron use? What tools is the library already using to support your patron's privacy?</p>
Prompt	<p>Facilitator REQUEST Reportbacks: Ask each group to share back what has changed. Ask the other groups if they have anything to add.</p> <p><i>Try to add in as many of the tactics and tools as you can that we discussed in the workshop!</i></p>

Wrap Up & Evaluation [5 min]



Goals:

- Thank participants
- Participants complete exit survey
- Participants informed about resources and dataprivacy.org project

Slide:	DATAPRIVACYPROJECT.ORG
ACTION	<p>Facilitator DO: Open: http://www.dataprivacyproject.org/mapping-data-flows/</p>
SPOKEN	<p>Facilitator REVIEW handouts, course site, contact info:</p> <p>REVIEW HANDOUTS</p> <ul style="list-style-type: none"> • You're leaving with one handout. <p>SHARE COURSE SITE</p> <ul style="list-style-type: none"> • http://dataprivacyproject.org <p>SHARE CONTACT INFO</p> <ul style="list-style-type: none"> • For more information about the project, email dataprivacy@bklynlibrary.org.



Slide:	THANK YOU & EXIT SURVEY
Prompt	Facilitator ASK: Please take some time to answer the Exit Questions and hand it to us. (pause for about 5 minutes to allow people to complete the exit survey)
SPOKEN	Facilitator THANK participants for attending, before closing the workshop.
ACTION	Facilitators DO <ul style="list-style-type: none"> • Collect and review Intake and Exit Surveys and Signs/Handouts generated in final exercise • Store materials at METRO

END Workshop 2.

