
Digital Privacy: Hands-on Tactics & Tools for Libraries



Workshop 2



About Us

This is a collaboration with:

- Brooklyn Public Library
- Metropolitan New York Library Council (METRO)
- New America and London School of Economics
- Data & Society
- Research Action Design (RAD)

Funded by the Institute for Museum and Library Sciences (IMLS)



This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 License](https://creativecommons.org/licenses/by-sa/4.0/).

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. Brooklyn Public Library and Research Action Design. New York: Data Privacy Project. Available at: <http://www.dataprivacyproject.org>.

Workshop Motivation

Libraries have served a critical role in providing free access to the web, especially to underserved populations.

BPL and New America conducted research to understand librarian concerns, challenges, and questions about digital privacy and security.¹ This workshop was one of the recommendations.

-
1. For further reading related to this research, see Morrone, M., & Witt, S. (2013). Digital Inclusion, Learning, and Access at the Public Library. *Urban Library Journal*, 19 (1). <http://academicworks.cuny.edu/ulj/vol19/iss1/8> and Gangadharan, S. (2015) The downside of digital inclusion: expectations and experiences of privacy and surveillance among marginal internet users. http://eprints.lse.ac.uk/64156/1/Downside_digital_inclusion.pdf

Workshop Goals

- 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



Workshop Agenda

- Introductions
- Risk Assessment
- Passwords, 2-Factor Authentication & Password Managers

Break (10min)

- Privacy on Public Networks and WiFi
- Browsing Privacy and Anonymous Browsing
- Malware
- Review & Eval



Introductions



Risk Assessment



Risk Assessment: Questions

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?



Risk Assessment Report back



Passwords



How strong is your password?

<https://password.kaspersky.com/>

Test: Try a password you think would be good

But, Don't use your own password



Strong Passwords from Phrases

She was more like a beauty queen from a movie scene

→ SWMLABQFAMS

→ \$wml@BQf@m\$

You can also use a **long sentence** (but **NOT common**):

Silver socks float around rivers



Library PINS

Do's	Dont's
<ul style="list-style-type: none">- Information of a person other than you (ex. last 4 of your childhood friend's phone number)- Modify personal information (ex. birth year backwards)- Have the patron enter their own PIN	<ul style="list-style-type: none">- Personal information birthdate MMYY MMDD- birthyear (ex. 19xx or 20xx)- Other personal info: last 4 of SSN, last 4 of your phone number- sequential digits (ex. 1234)- repeated digits (ex. 7777)



2-Factor Authentication



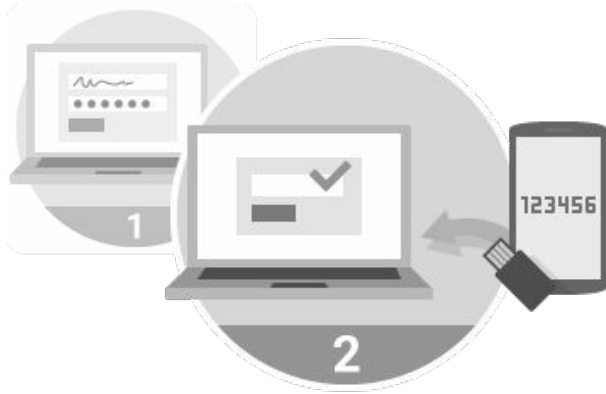
2-Factor Authentication

Something I **KNOW**
&
Something I **HAVE**



Hands-on: 2-Factor Authentication

YOUR BANK



GMAIL

Google accounts

Two-step verification

Enter the verification code generated by your mobile application.

Enter code:

Remember verification for this computer.

[Get a new verification code](#)

<https://www.google.com/landing/2step/>

<http://twofactorauth.org>



Device Passwords & Encryption

You should also put a password on your personal computers and mobile devices like smartphones and tablets.



Password Managers

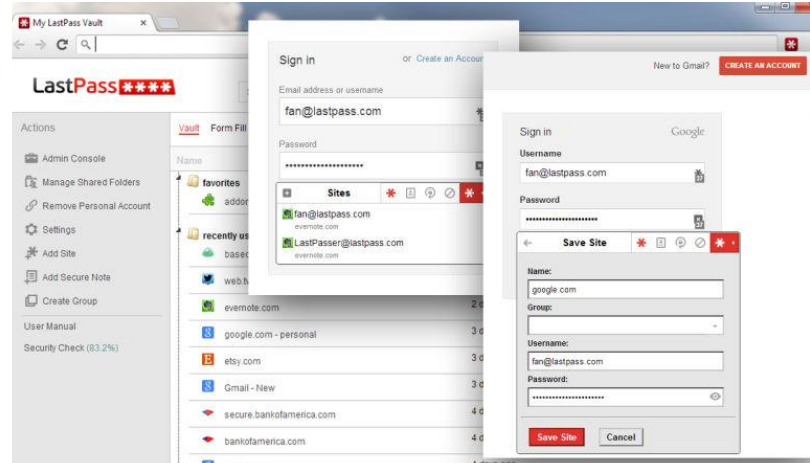


Demo: Password Managers

Demo: LastPass

<https://lastpass.com>

/



Other Password Managers

- Dashlane, <https://www.dashlane.com>
- KeePass, <http://www.keepass.info>



Password Takeaways

- Create **UNIQUE** passwords for the most sensitive accounts
- **Change** passwords every 6 months
- Use a **LONG** password (more than 12 characters)
- **DO NOT** include anything obvious (your birthday)
- **CAREFUL** of **phishing**
- Use **2-factor** authentication
- Use a **password manager** to store complicated unique passwords
- **DO NOT** store passwords in browsers!




BREAK



Privacy on Public Networks & Wifi




BPL's WiFi EULA



Wireless Internet Access

Stay connected to BPL while on the go!
Download the [My BPL mobile app](#) for iPhone® and Android™.








Agree & Continue



Brooklyn Public Library is happy to provide you with free WiFi internet access

- Use of BPL's wireless networks to commit any crime – including identity theft, the viewing and downloading of child pornography, and the illegal downloading of copyrighted materials is strictly prohibited. Violators may be prosecuted.
- The Library's wireless network is not secure. Information sent to and from your laptop can be captured by anyone else with a wireless device and the appropriate software.
- Library staff is not able to provide technical assistance for your device. BPL cannot guarantee a wireless connection.
- The Library assumes no responsibility for the safety of equipment or for laptop configurations, security, or data files resulting from connection to the Library's network.
- Laptops, cords and adapters must be properly connected to electrical outlets in a safe manner.

Get a Library Card Connect with BPL

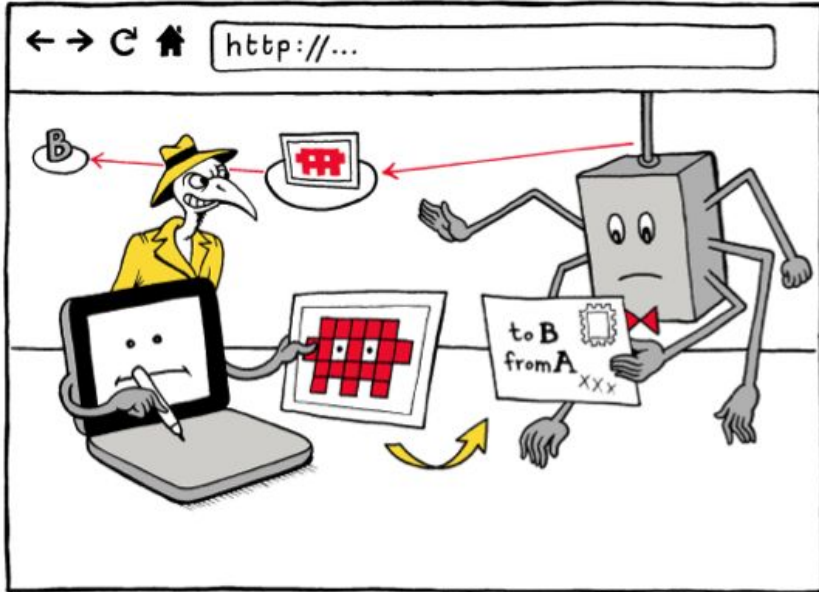
 Sign up now for a BPL library card.

Powered by:  



HTTP vs. HTTPS



vs.

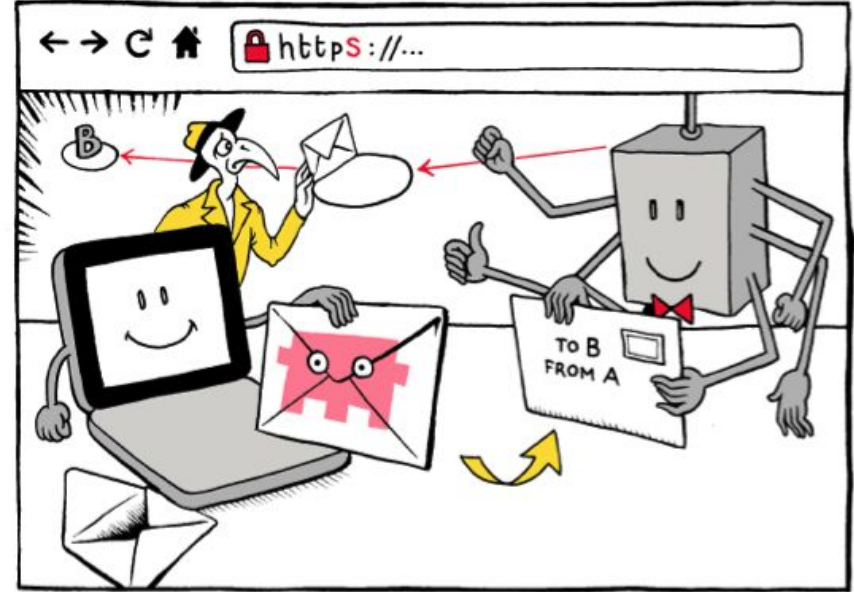


Image source: <http://binaire.blog.lemonde.fr/page/7/>



HTTPS Pledge

The Pledge for Libraries:

1. We will make every effort to ensure that web services and information resources under direct control of our library will use HTTPS within six months. [dated_____]
2. Starting in 2016, our library will assure that any new or renewed contracts for web services or information resources will require support for HTTPS by the end of 2016.

The Pledge for Service Providers (Publishers and Vendors):

1. We will make every effort to ensure that all web services that we (the signatories) offer to libraries will enable HTTPS within six months. [dated_____]
2. All web services that we (the signatories) offer to libraries will default to HTTPS by the end of 2016.

The Pledge for Membership Organizations:

1. We will make every effort to ensure that all web services that our organization directly control will use HTTPS within six months. [dated_____]
2. We encourage our members to support and sign the appropriate version of the pledge.

Library Freedom Project:
<https://libraryfreedomproject.org/ourwork/digitalprivacypledge/>



Digital Fingerprints



What is **my fingerprint**? Go to:

- <https://www.whatismybrowser.com/>
- <https://panopticklick.eff.org> and click “Test Me”

YOUR WEB BROWSER IS:
Chrome 48 on Mac OS X (Mavericks)

IS YOUR WEB BROWSER UP TO DATE?
✓ Your web browser is up to date.

YOUR WEB BROWSER'S CAPABILITIES:

Is JavaScript enabled?	Yes	How to enable JavaScript
Are Cookies enabled?	Yes	How to enable Cookies
Is Flash installed?	Flash 20.0 is installed	✓ Up to date
Is Java installed?	Java is not installed, or is disabled	How to install Java

MORE INFO ABOUT YOUR SYSTEM:

IP ADDRESS [47.18.209.196](#)

This is your IP Address.
There are many like it, but this one is yours.
[Learn more about IP Addresses](#)

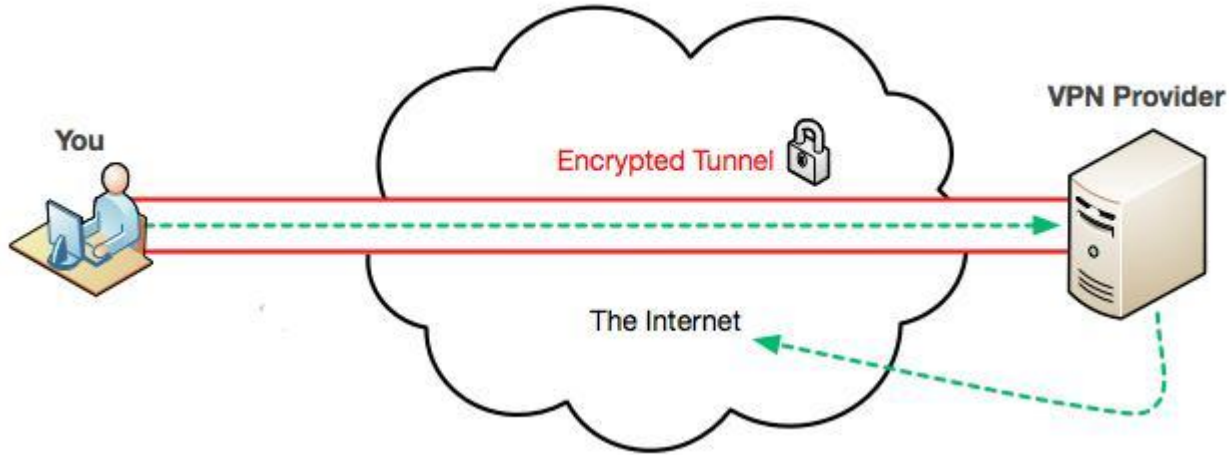
LOCAL IP ADDRESS	192.168.1.3
The local IP Address of your computer on your network.	
LOCATION	United States, Brooklyn <i>(Approximate)</i>
Your IP address can reveal your location.	
COMPUTER SCREEN	1280 x 800 pixels 24 bit
The dimensions/resolution and color depth of your screen.	
BROWSER WINDOW SIZE	969 x 778 pixels <i>(resize your browser to see this change!)</i>
Including your toolbars.	
"DO NOT TRACK" SETTING	"Do Not Track" is Enabled
Ask websites to not track you.	
DETECTED ADDONS	Ad blocker
Your browser announces that it has these extra addons.	



VPN



How a VPN works



VPN Demo



<https://www.privateinternetaccess.com>



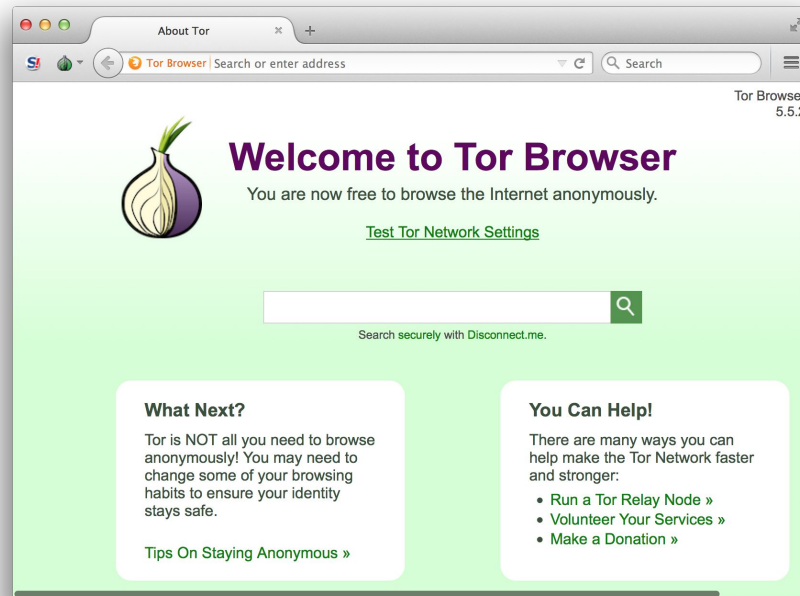
VPN features and services

Some VPN Services

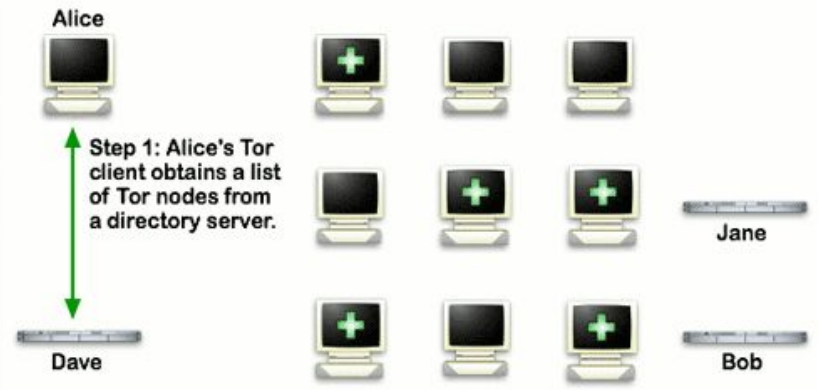
- Private Internet Access, for fee, <https://www.privateinternetaccess.com>
- Riseup VPN, free, <https://help.riseup.net/en/vpn> for Linux, Android and Microsoft Windows
- Psiphon, free, <https://psiphon.ca>, Microsoft Windows and Android.
- Your Freedom, free, <http://your-freedom.net/>, and pay for Linux, Mac OS and Microsoft Windows



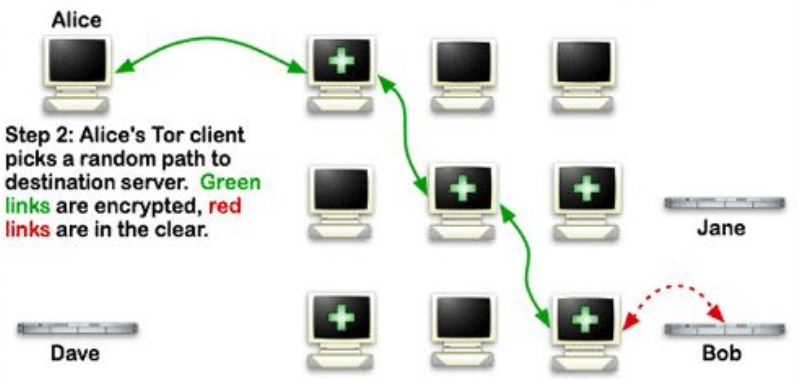
Anonymous Browsing with Tor: Demo



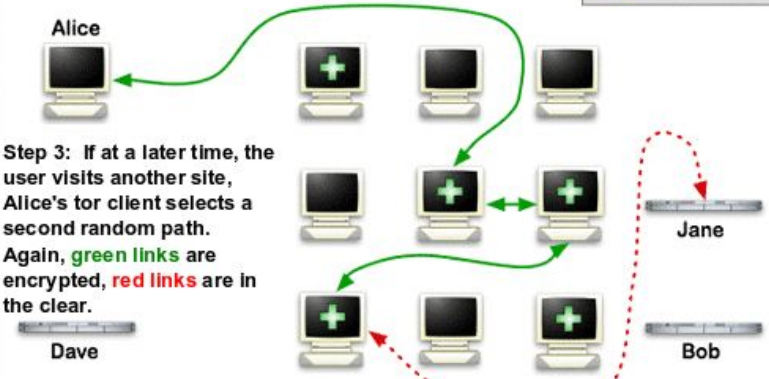
How Tor Works: 1



How Tor Works: 2



How Tor Works: 3



Network Privacy Takeaways

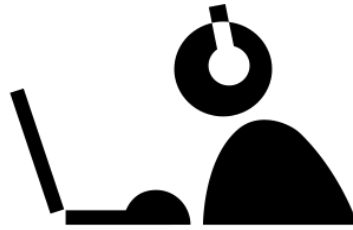
1. Only login on secure sites using encryption: **HTTPS**



2. Don't use the same **username** and **password** for different sites
3. Save the most important tasks for home or secure private connection (ex. your own hotspot).
4. Maximum Security: Use a **VPN**



Browsing Privacy



Browser settings, Tracking and 3rd Party Services



Privacy and Browsing

Who am I on the internet?

- My browser & browser cookies
- My accounts when I'm logged in
- My fingerprint

Hands-on with Internet Privacy

- Browser settings
- Actively blocking tracking
- Opting out of tracking



comic by Gegen Den Strich, gegen-den-strich.com



What does your library do?

Library browsing privacy: BPL's computer terminal reset.

When a patron's session ends or they log off:

- Clear Browser Data including browsing history, form data, user and passwords;
- Clear downloaded files;
- Clear temporary files;



What Browser are you using?

We recommend...



Chrome



Firefox



What are cookies?

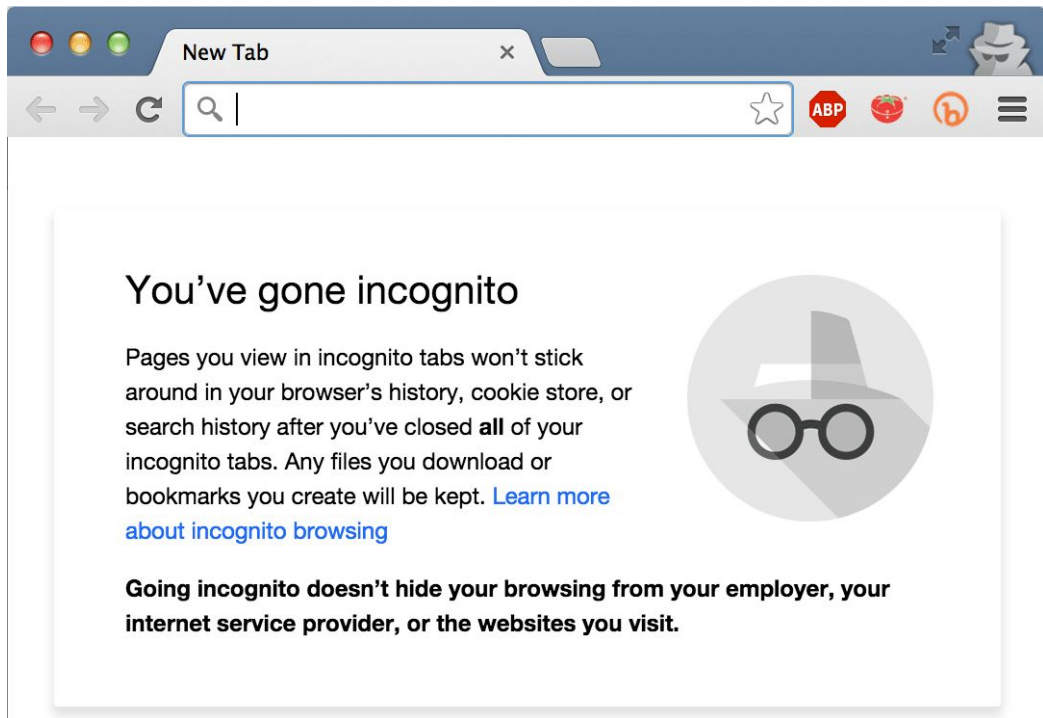


Wall Street Journal Video: **How Advertisers Use Internet Cookies to Track You**

<https://vimeo.com/12204858>



What is Private Browsing Mode?




Hands-on: Bye Cookies & History

View cookies, How To:

<http://www.wikihow.com/View-Cookies>

Delete the browsing history and cookies

- a. **Chrome:** Preferences>History>Clear Browsing Data>Select all from Beginning of Time
- b. **Firefox:** Menu  Button()>History>Clear Recent History
- c. **IE:** Tools> Safety> Delete Browsing History, Select Cookies checkbox and click Delete
- d. **Safari:** Safari>Preferences>Privacy>Remove all website data



Mobile Browser Privacy Settings

Mobile browsers offer settings:

- Cookie and History Deletion
- Private Browsing
- “Do Not Track”



Hands-on: Disable Flash

Chrome: Preferences>Settings>Content Settings>Plugins>Individual Plugins

Firefox: Tools>Add Ons>Shockwave Flash (Ask to activate)

Enabling Flash on specific sites. <http://hulu.com>



Plugins to prevent Third Party Tracking

Hands-on with the Privacy Badger Plugin

Go to: <https://www.eff.org/privacybadger>

Chrome or Firefox

Other similar plugins:

- Disconnect, <https://disconnect.me/>
- Adblock Plus, <https://adblockplus.org/>
- Ghostery, <https://www.ghostery.com/>



Social Media Privacy Settings

Let's look at some settings:

Privacy Settings and Tools		
Who can see my stuff?	Who can see your future posts?	Friends
	Review all your posts and things you're tagged in	
	Limit the audience for posts you've shared with friends of friends or Public?	
Who can contact me?	Who can send you friend requests?	Everyone
Who can look me up?	Who can look you up using the email address you provided?	Everyone
	Who can look you up using the phone number you provided?	Everyone
	Do you want search engines outside of Facebook to link to your profile?	No



Privacy in Browsing Takeaways

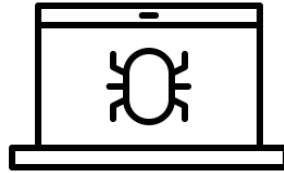
BPL automatically mimics “Private Browsing” mode on logout by deleting history, form data, and usernames/passwords;

Steps we can take:

- 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
- Anonymous Browsers and Anonymous VPNs



Malware



Anti-malware software

BPL's anti-malware practice:

- **McAfee** Antivirus Enterprise, mcafee.com - Windows
- **Gatekeeper**, Macs
- Update virus protection daily; scan computers and files

Other popular software:

- **AVG**, <http://www.avg.com/> **Avast**, <https://www.avast.com/> - Free trials, scan & cleanup;
- **Kaspersky**, kaspersky.com - Free scan 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")



Turn on your Firewall

Mac: Apple Menu>System Preferences>Security & Privacy>Firewall

Windows:

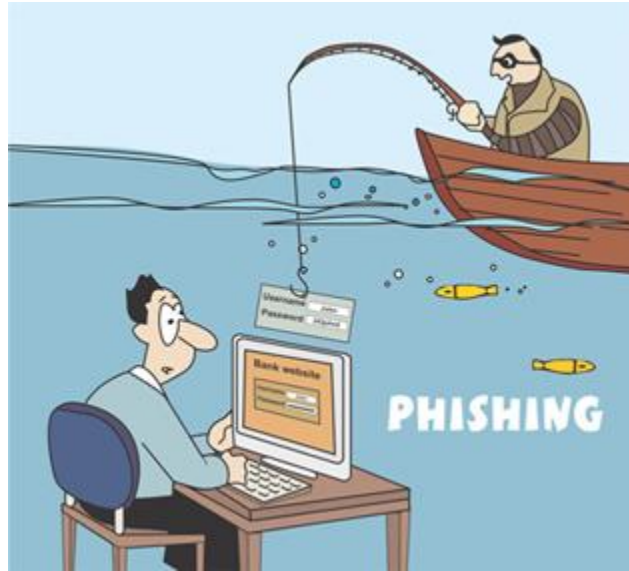
- In Search, type “firewall”, and then select Windows Firewall.
- Select Turn Windows Firewall on or off. You might be asked for an admin password or to confirm your choice.



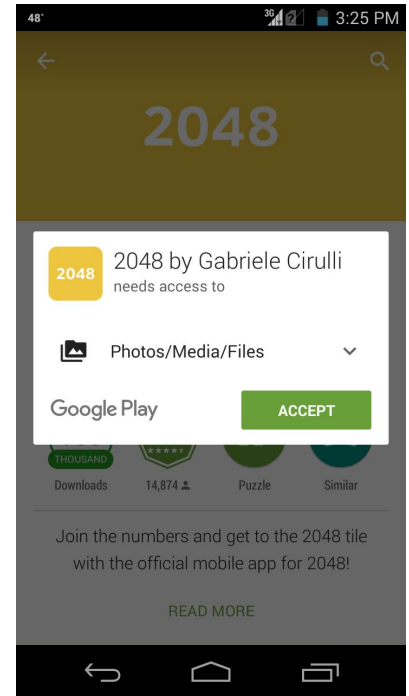
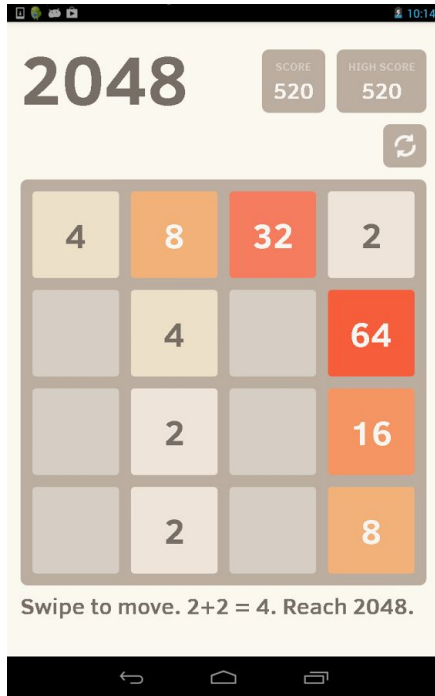
Update your software!



Avoid Phishing & Click Bait



Mobile Antimalware



Anti-malware Takeaways

- **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.** Research the best app for the job. Don't follow **unknown links** or download **unknown attachments**; scan files if you don't trust them; be careful in granting permissions (mobile)
- **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;*
- **Tell people** if they send you malware;



Revisiting Your Risk Assessments



dataprivacyproject.org



Step 1. Library user logs on.

A web user logs in at the library home screen.

She enters her patron ID and password onto the screen. Once the library's Integrated Library System validates her log-in credentials, she can use the computer to access the web.

TERMS

Integrated Library System: a relational database with patron-facing and staff-facing interfaces that allows the library to manage acquisitions, cataloging, circulation and reserves, serials holdings, and the online public access catalog.

log-in credentials: a username and password created by the user

Review: <http://www.dataprivacyproject.org/mapping-data-flows/#login>



Thank You & Exit Survey!

Please complete the Exit Survey!

Project website: <http://dataprivacyproject.org>

For more information about the project, email
dataprivacy@bklynlibrary.org.

