Digital Privacy & Security

WYLD Network Annual Meeting 2019
Kate Mutch & Desiree Saunders
Overview

• What do you need to protect?
• Whom do you want to protect it from?
• What’s the worst that could happen?
• Where do you start?
What do you need to protect?

- Personal Information – protect Personally Identifying Information (PII)
- Banking accounts, health information
- Social media history
- Browsing history
- Location tracking
- Important documents, photos, etc.
Whom do you need to protect it from?

- Bad guys!
- Identity thieves
- Financial fraud schemes
- Online harassment
- Background checks (are you job seeking?)
What’s the worst that could happen?

- Identity theft
- Lost access to critical accounts
- Data loss
- Expose your workplace to threats
- Personal safety
Workplace Considerations

• Public PCs have security software? Is it up to date?
• Public PCs & other equipment physically secure?
• Who has access to passwords?
• Do you change important passwords when there is staff turnover?
• Do you have backups for important data?
• Is your library website secure?
Workplace Considerations, cont.

• Check your vendors to review their privacy & security policies. What data do they retain?
• Do you have privacy policies that staff must follow? [http://www.ala.org/advocacy/privacy/toolkit](http://www.ala.org/advocacy/privacy/toolkit)
• Have you trained staff on how to recognize security threats like phishing schemes?
• Phishing Quiz - [https://phishingquiz.withgoogle.com/](https://phishingquiz.withgoogle.com/)
Securing Devices

- Keep software and apps updated!
- Use trusted sources to download apps
- Limit app permissions
- Set a lock screen
- Use 2 factor authentication
- Use strong passwords
- Beware of public Wi-Fi
- Considering a VPN? Do your research (encryption, permissions, data mining?)
- Turn off automatically connect to Wi-Fi & Bluetooth
Securing PCs & Laptops

- Use security software to scan for viruses, malware, etc.
- Learn to recognize phishing scams
- Password protect your account
- Keep secure backups
- Laptop? Beware of public Wi-Fi & enabling Bluetooth when unnecessary
- Laptop camera
- Disable Adobe Flash from running automatically
Securing Accounts

• Use strong passwords
• Try a password manager like LastPass
• Use 2-Factor authentication when possible
• Log out of accounts when not in use
• Delete old accounts if no longer needed
• Consider creating an email for online use (e.g. shopping) and one for personal use
More about passwords

- It’s HARD!
- Don’t re-use passwords
- Don’t use easily guessed info (your pet’s name)
- Use a password manager – then you only have to remember the master password
- Think carefully about storing passwords in a browser – if someone gains access to your computer, they have access to those passwords
Passwords or Random Phrases?

Tr0ub4dor &3

~ 28 BITS OF ENTROPY

2^28 = 3 DAYS AT 1000 GUESSES/SEC

DIFFICULTY TO GUESS: EASY

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: HARD

correct horse battery staple

~ 44 BITS OF ENTROPY

2^44 = 550 YEARS AT 1000 GUESSES/SEC

DIFFICULTY TO GUESS: HARD

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.
Passwords – Work related

• Shared passwords should be changed on a regular basis
• Always change passwords when there is staff turnover
• Only share what you need to share
• Review who has access to what services regularly
Locking down information online

• Privacy checkups in Social Media
• My Activity in Google (years of data!)
• Google yourself
• Remove unneeded accounts
• Identity theft monitoring?
• Stored credit cards?
Browse safe

- Use HTTPs
- Use secure sites for online purchases
- Popup blockers & Ad blockers
- Cookies & browsing history
- Are you paranoid? Browse with a plugin like Duck Duck Go
- Public Wi-Fi is not secure and can be spoofed
- Are you over-sharing?
Who needs to know this stuff?

- Everyone!
- Kids are on social media, gaming sites, chat rooms ALL THE TIME… talk to them about privacy and being safe online
- Parents and older adults – Kate has a story!
Resources

- The Electronic Frontier Foundation
- Wired Guide to Digital Security
- Motherboard Guide to Not Getting Hacked
- ALA Privacy Guidelines
- Consumer Reports
- Phishing Quiz - [https://phishingquiz.withgoogle.com/](https://phishingquiz.withgoogle.com/)
- KidsHealth.org
- Internetsafety101.org / Enough.org