DIGITAL LITERACY IN THE AGE OF CYBERSECURITY

Introductions

Christa Van Herreweghe, MLS, Library Director at Kirkwood Public Library

Ruthie Rochman, MBA, MLIS Candidate, Library Assistant at University City Public Library and Logan University Learning Resources Center (Library)

Intro

What is digital literacy: Digital literacy can be defined as those sets of abilities, skills and competencies and fluencies that relate directly to technology.

What is cybersecurity: Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyber attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

You may have heard of…

- SolarWinds - Probably initiated in Russia, allowed access to data in the U.S. government and many tech companies.

- Equifax Credit Reporting Agency - 148 million people affected.

- Every credit card ever issued? - Not 100% certain but it sure feels like it

Threats to service

- Malware
- Virus threats
- Phishing attacks
- Denial of service
- Ransomware

Malware

According to Tech Terms.com, short for "malicious software," malware refers to software programs designed to damage or do other unwanted actions on a computer system.”

Virus Threats

As defined by Malwarebytes Labs, ‘a computer virus is “malware attached to another program (such as a document), which can replicate and spread after an initial execution on a target system where human interaction is required. Many viruses are harmful and can destroy data, slow down system resources, and log keystrokes.”’

Phishing Attacks

According to Imperva.com, “phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.”

Denial of Service

According to Tech Terms.com: A denial of service attack is an effort to make one or more computer systems unavailable. It is typically targeted at web servers, but it can also be used on mail servers, name servers, and any other type of computer system.

In other words, a website is getting pinged so much, it can't answer back. Usually it is an "attack" and is temporary.

Ransomware

According to Tech Terms.com, “Ransomware is a type of malware that prevents you from using your computer or accessing certain files unless you pay a ransom. It often encrypts your files so that they cannot be opened.”

What is at risk in your library?

- Patron privacy
- Functioning online presence
- Internal computer network
- Financial data

Cyber Security Attacks on Libraries

- 2017: Ransomware attack paralyses St Louis Public Libraries as hackers demand bitcoins
- 2018: Ransomware attack on Spartanburg County Public Library (SCPL) - $36,000 in bitcoins
- 2019: Onondaga (NY) County Public Library was disabled by a cyber attack
- 2020: Ransomware attack on Contra Costa (SF Bay Area) Library System causing a network outage affecting all 26 branches and administration office

Key information for staff

- Don’t click on links or attachments from unknown sources.
- Do not open emails from unfamiliar senders.
- Beware of phone calls asking for equipment information.

Key information for staff

- Monitor for extensions like .exe or .zip that may have executable files.
- Avoid installing software that is not vetted by your IT department.
- Review the sending email address before opening since many attackers may use very similar sounding names of people or organizations.
- Guard your password(s).

Examples from MoreNet on potential attacks

You've been contacted by phone, email or text:

- There's a problem with your computer and we need to help you fix it.
- Your iCloud account has been compromised.
- We've noticed suspicious activity on your credit card.
- Your package is waiting for delivery information.
- COMPUTER SCAN ALERT! Suspicious activity detected on your computer. Contact a live technician now. 1-800-xxx-xxxx

According to MoreNet, here is how to help defend against a potential attack:

- Ask yourself is if this is a company that you do business with. If not, ignore it.
- Do not reply to emails or respond to calls that request a login or personal information. Call the company or open a browser and visit the website directly. Do not use the links, attachments or robocall directories to respond.

According to MoreNet, here is how to help defend against a potential attack:

- Hang up on robocalls. If you did not contact them for assistance first then you don't need their assistance. Never trust caller ID. Attackers will spoof a company's number to make you think they are legitimate, or they will make it look like a local area code. Screen your calls by letting unrecognized numbers go to your voicemail.
- Don't succumb to a sense of urgency or threats. If you are being pressured to act immediately, you should question it.

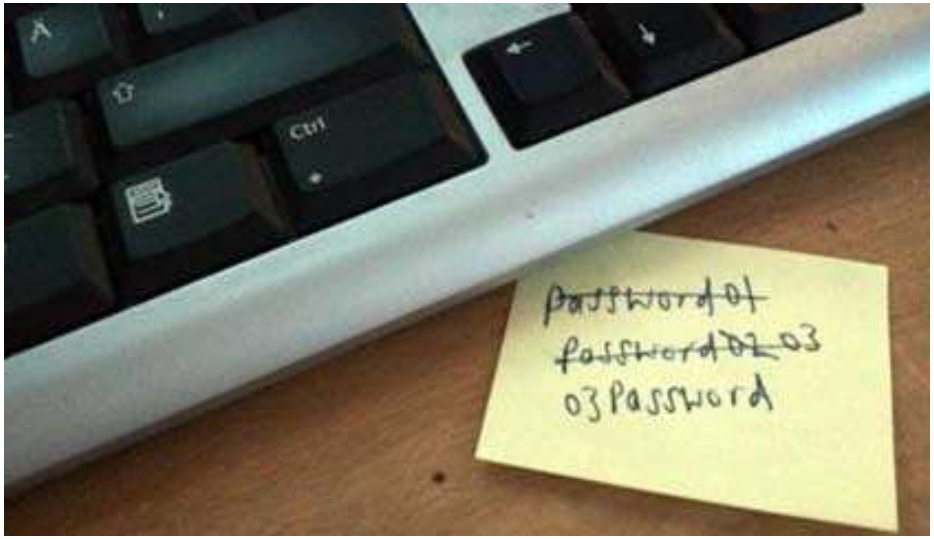
Remember, many companies and organizations will NEVER call you and ask for personal information. That includes credit/debit card numbers, Social Security numbers and passwords.

Delivering the message

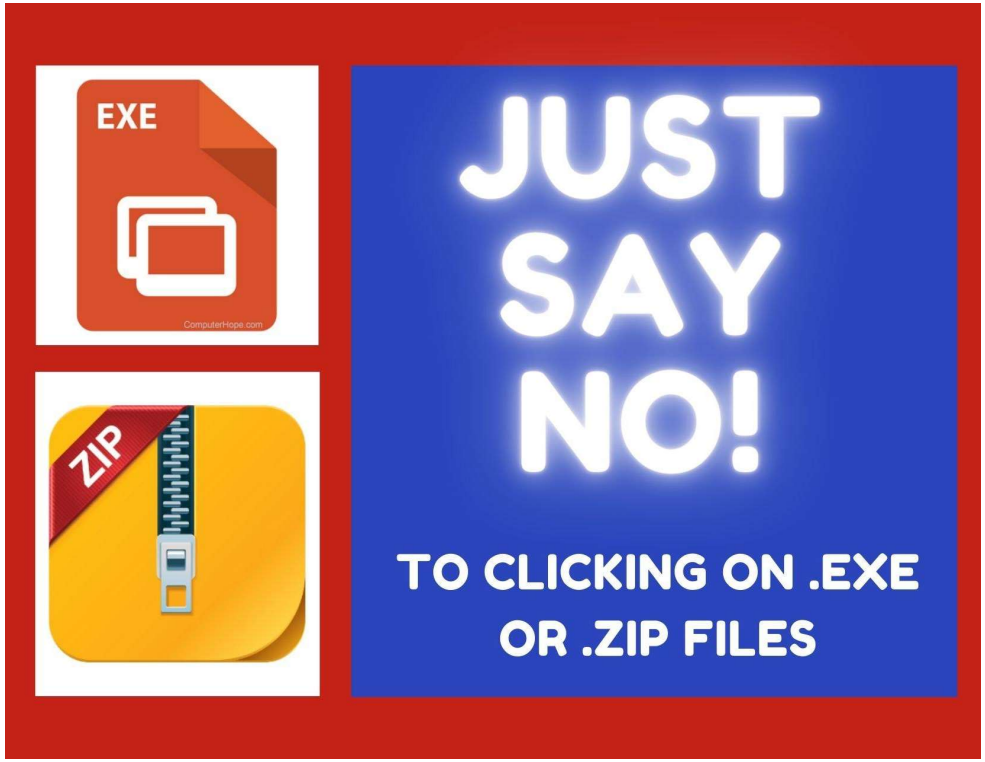
- Repetition is the key to learning
- Your staff probably won’t want long trainings focused on this topic
- Integrate Cyber Security into other meetings
- Results of our survey last year - staff doesn’t think they are being trained

Email Tip

What is your keyboard for?



Microwave Minute



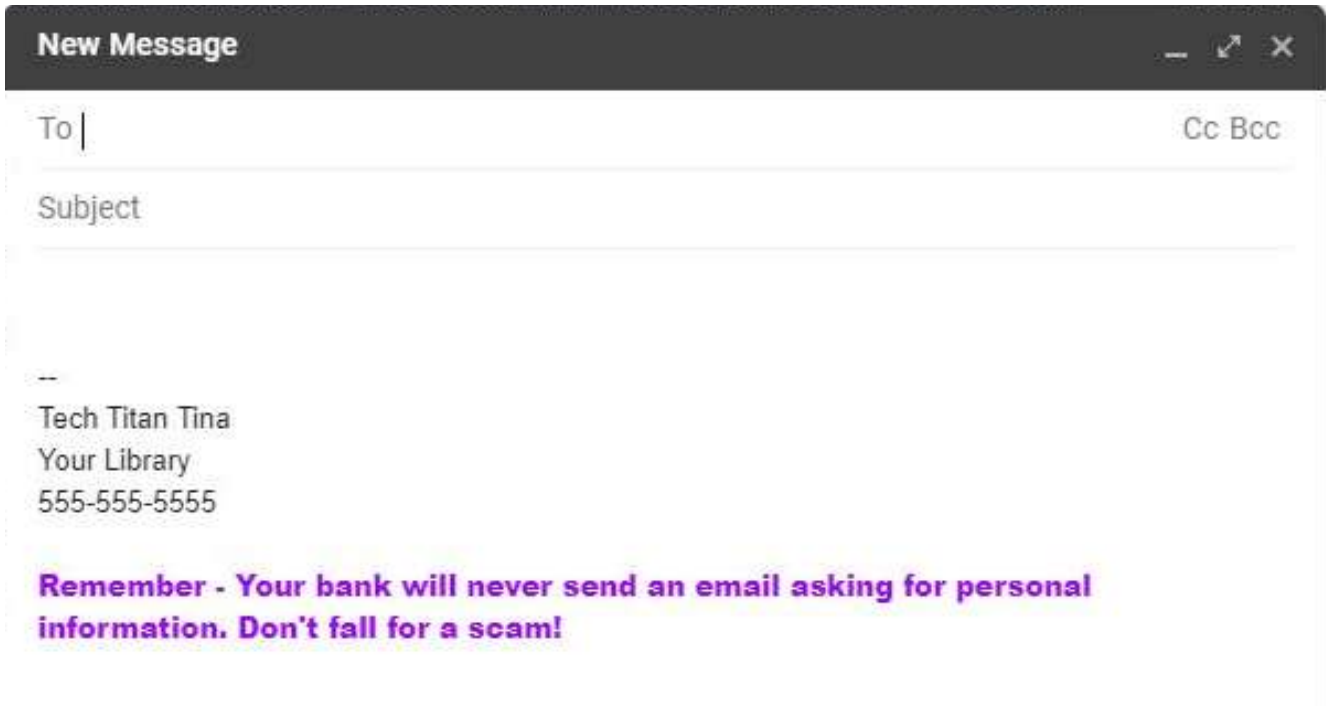
Integrate a tip into each staff meeting

Meeting Agenda

March 2, 2021 2:15pm

I. Tech tip
II. Old Business
III. New Business

Internal email signature



Security Quiz

Security Quiz

Choose all that apply.

Which of these might be a tip off for a phishing email?

- [ ] Your iCloud account has been compromised. Click here to fix this problem.
- [ ] We've noticed suspicious activity on your credit card. Login to your account to find out more.
- [ ] COMPUTER SCAN ALERT! Suspicious activity detected on your computer. Contact a live technician now. 1-800-xxx-xxxx
- [ ] Your cat is in my yard!

Questions?

Contact us!

Christa Van Herreweghe: christa@kirkwoodpubliclibrary.org

Ruthie Rochman: ruthie@ucitylibrary.org

References

https://www.vable.com/blog/cyber-security-what-your-library-needs-to-know

https://blog.techsoup.org/posts/cybersecurity-checklist-for-when-your-library-reopens

www.malwarebytes.com

www.imperva.com

www.techterms.com

https://www.more.net/news/is-that-for-real-4922

More References

https://www.stltoday.com/entertainment/books-and-literature/book-blog/st-louis-public-library-reassures-patrons-of-safety-after-ransomware-attack/article_de787695-a88d-56bd-aafc-da1857191d99.html

https://www.cybersecurity-insiders.com/ransomware-news-on-spartanburg-public-library-and-gandcrab/

https://americanlibrariesmagazine.org/latest-links/cyberattack-shuts-onondaga-county-library-network/

https://pioneerpublishers.com/library-system-recovering-from-crushing-cyber-attack/