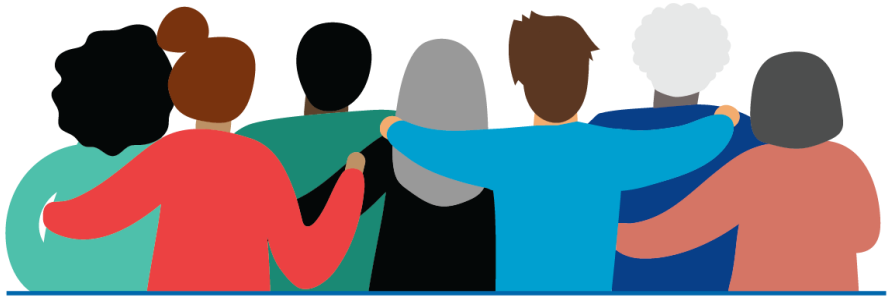

SENIOR LAW DAY
COLLABORATIVE

westchester
LIBRARY SYSTEM
Empowering libraries. Empowering communities.

Online Security Essentials

7 THINGS TO DO NOW

Who I Am

- WLS Technology Training Coordinator
- Background in education, technology and art
- 15+ years technology, internet, and cyber security training
- 20+ years in libraries

Poll #1

What do you worry about most?

- That your passwords will be stolen
- That your phone or laptop will be stolen
- That you will lose pictures or information in a ransomware attack
- That you will be compromised using hotel or airport WiFi

Let's talk about

- Why does it matter?
- Protect your machines
- Set up your accounts and passwords
- Use email safely
- Share on social media with caution
- Use Wifi with care
- 7 Key To-Do's

Why does it matter?

In 2022, cyberattacks **have risen by 38% compared to** 2021.

Data breaches and access have become profitable business.

Attacks are getting **more sophisticated every day.**

YOU are the key to your own security!

westchester LIBRARY SYSTEM
Empowering libraries. Empowering communities.

Protect your machines

- Computers, phones, tablets, smart devices
- Set up automatic updates
- Use antivirus and anti-malware software
- Back up your data
  - Use your device's scheduler
  - Back up in at least 2 ways
    - To a separate USB or other drive
    - To the cloud

Never plug in unknown USB (flash) drives - They could be infected with malware!

Set up accounts and apps

- Set up a lock screen and log in with a pass phrase, code, fingerprint or facial recognition
- Download apps only from your app store
- In Settings, for each app, make the usual Location *Only when in use*

Passwords – the problems?

Most common (Bad) passwords: latest 2023 statistics from Cybernews

Passwords are often stolen with digital tools and guesses based on social media posts

Tools to check your security

- How Secure Is My Password?
- Pwnd Passwords checker
- See if you've been part of a breach

1. 123456
2. 123456789
3. qwerty
4. password
5. 12345
6. qwerty123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890

westchester LIBRARY SYSTEM
Empowering libraries. Empowering communities.

Password solutions

Use a password manager and/or randomly generated passwords

- Use an online password generator
- Use dice and words from a word list

Use PINs or Biometrics

Use unique passphrases for strong passwords

- The longer the better!
- Don't reuse old passwords!
- Avoid family, pet, sports team, or place names, and birthday and anniversary dates
- Don't use obvious letter replacements like a = @, e = 3, i = !

Poll #2

Which method of making passwords sounds best for you?

- Using a password manager and generator
- Online random password generator
- Dice and word lists
- 12 word sentence that's meaningful but not personal

Multifactor authentication

1. MFA (Multifactor Authentication)
2. 2FA (two-factor authentication)
3. Password + OTP (one time password)

westchester LIBRARY SYSTEM
Empowering libraries. Empowering communities.

Multifactor authentication

Uses at least 2 pieces of information to log in

- Something you know (password or PIN)
- Something you have (card)
- Something you are (digital fingerprint)

Authenticate with a second account like a Firefox browser/Gmail message

Use a security key fob as the 2nd factor

Stand-alone Authenticator Examples

- Authy.com
- Google Authenticator

Strong credentials protect...

1. Your email account
2. Social Media use
3. Public Wi-Fi

westchester LIBRARY SYSTEM
Empowering libraries. Empowering communities.

Use email safely

What to watch for?

- Phishing emails that "lure" you to click a bad link, log in, or enter PPI (Protected Personal Information)
- Requests for immediate action, especially about your accounts, passwords, or money
- Spear Phishing, Vishing, and Smishing may be targeted lures

What to do?

- Pause and count to 5 before clicking!
- Beware a sense of urgency!
- Go to the source for confirmation
- Report phishing emails to your email provider

westchester LIBRARY SYSTEM
Empowering libraries. Empowering communities.

The human factor

Social engineering attacks count on human psychology

Habits

- Hackers and scammers are paying attention to your online habits

Trust

- People **trust and want to trust those they know (leads to impersonation)**
- People **share to connect with others on Social media (leads to info gathering)**

Emotions

- Be wary of emotional **hooks** that cause **fear and worry**

Beware of

- **Urgent messages from friends or connections**
- **Cryptocurrency, wire transfer, or gift card payment requests**
- **Requests for romance**
- **Deals that are too good to be true**

westchester LIBRARY SYSTEM

Empowering libraries. Empowering communities.

The human factor: what to do?

Pause	Take a minute to assess the situation. Scammers use fear tactics to get victims to act quickly.
Don't over share	-Scammers use social media to learn your habits and gather information that can be used to hack your devices. -Don't post photos that may have sensitive info in them, don't share birthdays, locations, connections to family members.
Don't click links from unknown sources	Go to the business's website to verify if the links are legitimate.
Verify urgent messages with the source	Take a minute to reach out to the person or business that is trying to contact you or get you to act quickly.

westchester LIBRARY SYSTEM
Empowering libraries. Empowering communities.

Share on social media with caution

1. Set privacy settings and limit who can see your posts.
2. Opt-out of targeted advertising when possible.
3. Contact a friend if you get unusual messages or requests for money. They may have been hacked.
4. Read about romance scams.
5. Never send money to someone you haven't met in person.
6. Check out companies before you buy. Search online for its name plus "scam" or "complaint."

Use public Wi-Fi with care

Public Wi-Fi is **unencrypted**

What to do?

- Avoid logging in to key accounts like shopping or financial services
- Use your phone as a hotspot instead
- Install and use a VPN on your laptop and phone

Traveling?
Carry your own charger and USB cord and use an electrical outlet instead

westchester LIBRARY SYSTEM
Empowering libraries. Empowering communities.

VPNs - Virtual Private Networks

A secure tunnel for internet traffic

- PC Magazine has recommendations for free and paid, desktop and mobile, iOs and Android options
- Some browsers have VPN options or plugins

At home

- Use your own network and router – use WPA2 wifi standard
- Use strong passwords

westchester LIBRARY SYSTEM
Empowering libraries. Empowering communities.

Your choice

Security

Privacy

Convenience

Sharing

7 Key Things To Do Now

SET UP AUTOMATIC UPDATES AND BACKUPS AND CHECK YOUR SETTINGS

SET UP PASSCODES ON YOUR COMPUTER, PHONE, AND TABLET

USE LONG, UNIQUE PASSPHRASES AND SET UP MULTI-FACTOR AUTHENTICATION

CHECK YOUR DEVICE AND APP SETTINGS

COUNT TO 5 AND THINK BEFORE YOU CLICK OR SHARE

VERIFY URGENT MESSAGES WITH THEIR SOURCES AND REPORT PHISHING

CONNECT TO WIFI WITH A VPN OR USE YOUR PHONE AS A HOTPSOT

Poll #3

Which key thing will you start with today?

- Check to see if your computer or phone has automatic updates set up
- set up passcodes on all your devices
- Set up MFA on your email account
- Check your app's location settings
- Count to 5 and pause before you click or share
- Find out how to report a phishing email in your email provider
- Practice using your phone as a hotspot

Links & Support

- National Cyberserity Alliance Online Safety Basics
- Consumer Reports Security Planner and Tool For Regaining Control of Hacked or Compromised Accounts
- EFF's Surveillance Self Defense Basics
- Tom's Guide What is a USB Security Key?
- Use your phone as a hotpsot for Apple/iOS or Android
- Privacy Settings How-To's

westchesterlibraries.org