westchester
LIBRARY SYSTEM

Empowering libraries. Empowering communities.

Online Security Essentials

WLS CYBER SMARTS SERIES

Online Security Essentials – Learning Objectives

Keep your computers, devices, and accounts safe from threats you can see - and those you can't.

Learn and adopt key strategies and behaviors to protect yourself from cybersecurity attacks and reduce the risk to yourself and your library.

westchester LIBRARY SYSTEM

Empowering libraries. Empowering communities.

Online Security Essentials Agenda

- Why It Matters
- Common Risks
- Cybersecurity Systems
- Hardware Protections
- Human Protections
- Authentication, Email and Phishing Protections
- Social Media Protections
- Remote Work & Travel

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 first line of defense!

Threats Are Constantly Evolving

Common Malware Examples:

Viruses: a specific way software is secretly distributed, often by e-mail or instant messaging.

Ransomware: a type of malware that locks your files, data or the PC itself and extorts money from you.

Worms: worms are malicious software that aims at spreading as fast as possible once your PC has been infected.

Trojans: a type of malware disguised as useful software.

Social Engineering

Hackers use social engineering - psychological manipulation – to induce people to perform actions or divulge confidential information.

What makes social engineering especially dangerous is that it relies on human behavior which is harder to identify and thwart than vulnerabilities in software and operating systems.

- Relies on emotions from trust and caring for others to fear and anger
- Counts on human error and inattention.

SOCIAL ENGINEERING
The clever manipulation of the natural human tendency to trust.

Reasonable Cybersecurity

Technology, People, Processes, and Management

Everyone plays a part!

Involves all employees, from part-time staff to executives

Requires continual planning, assessment, monitoring, and responses

Reasonable Cybersecurity Components

There is no perfect cybersecurity solution, so you need to take legitimate steps to combat the risks that you and your company face.

If a breach happens, you will be able to show that you have done what you could to prevent cyber incidents:

1. Create cybersecurity policies and procedures
2. Budget for prevention
3. Assess and train your workforce
4. Insist on strong passwords
5. Utilize multi-factor authentication
6. Back up your data

westchester
LIBRARY SYSTEM
Empowering libraries. Empowering communities.

Physical Security

68% of companies have had a security breach. 69% of those breaches were physical.

What to do?:

- Clean up and shred any paper with sensitive information on a regular basis.
- Be alert for unfamiliar people in the workplace: WLS IT Staff visiting your library will introduce themselves and wear visible ID.
- Protect your devices, hardware, and software: Don't walk away from your device without signing out or locking it.
- Keep work materials OFF your personal devices.

Physical Security – Working from Home

- NEVER use a personal device for work.
- Information stored on your personal devices and accounts is subject to FOIA requests – and can even be confiscated!
- It is your library director's responsibility to make sure that staff has the appropriate equipment to work from home if necessary.
- For questions or comments, please contact WLS IT Director, Wilson Arana.

Software Security

Make sure your technology and devices are secure:

- **Back up!**
- **Set up automatic updates**: at work ask IT if you notice that your software isn't updating.
- Use antivirus software.

westchester LIBRARY SYSTEM

Empowering libraries. Empowering communities.

Device Protection

Phones, laptops, tablets, desktops

COVER DEVICE CAMERA WHEN NOT IN USE.

ONLY USE REPUTABLE APPS.

AVOID VISHING AND SMISHING SCAMS (VOICE AND TEXT PHISHING).

SET UP SECURE ACCESS ON YOUR DEVICES WITH STRONG PASSWORDS AND MFA.

DO NOT REUSE OLD PASSWORDS.

BIOMETRICS ARE PREFERRED.

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 - hackers use that trust to play on your desire to help people you know**
- People **share to connect with others on Social media – hackers use this to gather information to impersonate people you know**

Emotions

- People respond to emotional **"hooks" like fear and worry – hackers use this to tap into your emotions instead of your reasoning**

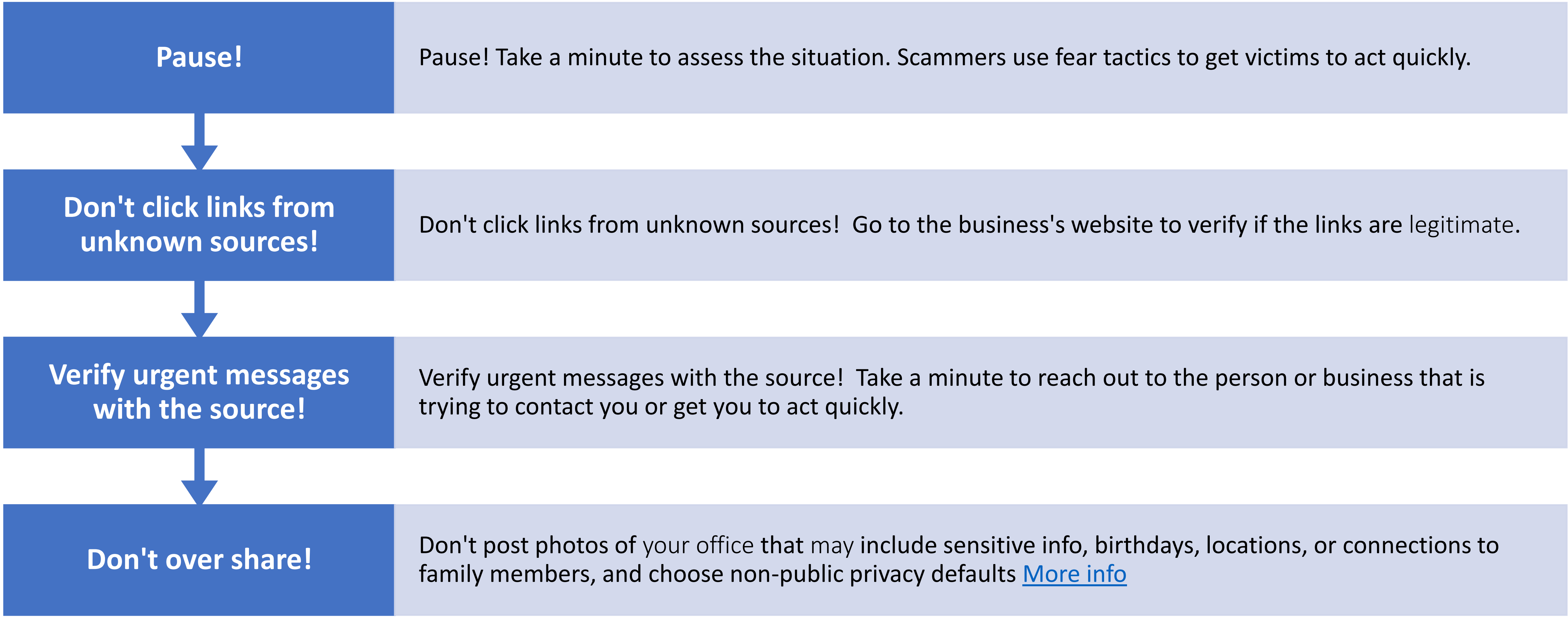
Beware of:

- 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!

Pause! Take a minute to assess the situation. Scammers use fear tactics to get victims to act quickly.

Don't click links from unknown sources!

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!

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.

Don't over share!

Don't post photos of your office that may include sensitive info, birthdays, locations, or connections to family members, and choose non-public privacy defaults [More info]

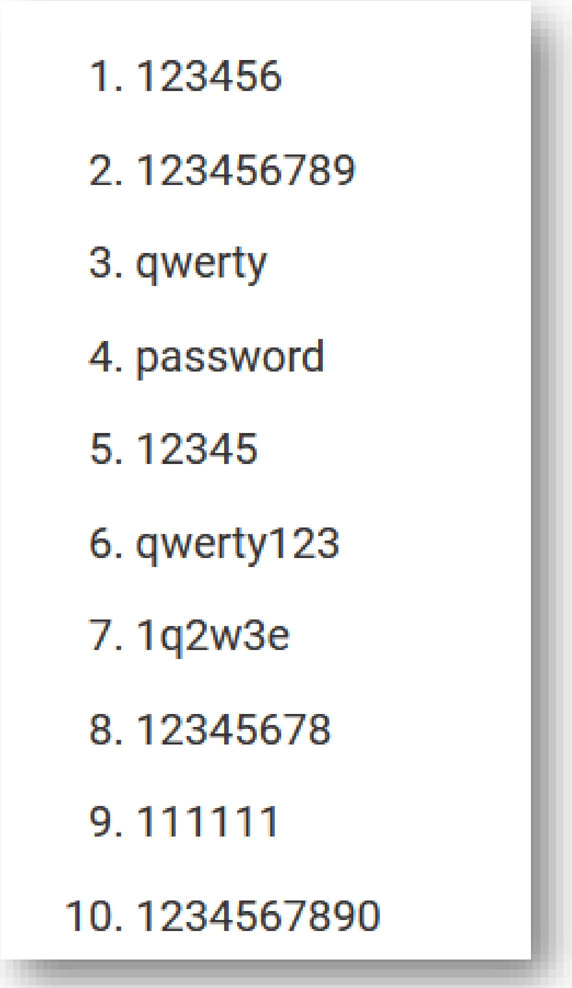
Password Problems

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

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

Cybernews Tools:

- 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 unique passphrases for strong passwords.

- Don't use obvious letter replacements (a = @).
- The longer the better!
- Don't reuse old passwords!
- Avoid common words, as well as family names, pet names, sports teams, or popular places.

Use a password manager and/or randomly generated passwords.

Use PINs or Biometrics instead.

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 off other software

- Email message
- Authentication app - Authy.com or Google Authenticator

External Device Authentication

- Phone or text message
- Key Fob Learn more

Strong Credentials Protect...

1. Your email account.

2. Social Media use.

3. Public Wi-Fi.

4. Your Library!

westchester LIBRARY SYSTEM
Empowering libraries. Empowering communities.

Your Email Inbox

What to watch for?

- Phishing emails that "lure" you to click a bad link and login or enter PPI (Protected Personal Information.)
- Spear Phishing - targeted lures.

What to do?

- Beware of urgency!
- Pause!
- Go to the source for confirmation.

westchester LIBRARY SYSTEM

Empowering libraries. Empowering communities.

Social Media

Stay safe while browsing social media platforms

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 • Learn 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."

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.

Public Wi-Fi

Public Wi-Fi is unencrypted.

What to do?

- Install and use a VPN.
- Use your phone hotspot instead.
- Use WPA2 (Wi-Fi Protected Access 2, a technology used for secure Wi-Fi connections) and a strong password.

westchester LIBRARY SYSTEM
Empowering libraries. Empowering communities.

VPNs - Virtual Private Networks

A secure tunnel for internet traffic

Ask your IT team for access to theirs or for a recommendation

- PC Magazine has recommendations for free and paid, desktop and mobile, iOs and Android options

Working from home

- Use a secure network.
- Use your own Router – use WPA2 wifi standard.
- Use strong passwords.

Protect You and Your Library
Intellectual Property – Customer Data – Employee Data

Patrons, library, and even you can be at legal and financial risk!

Never forward sensitive data to personal email accounts!

Know who should have access to what data – internally and externally.

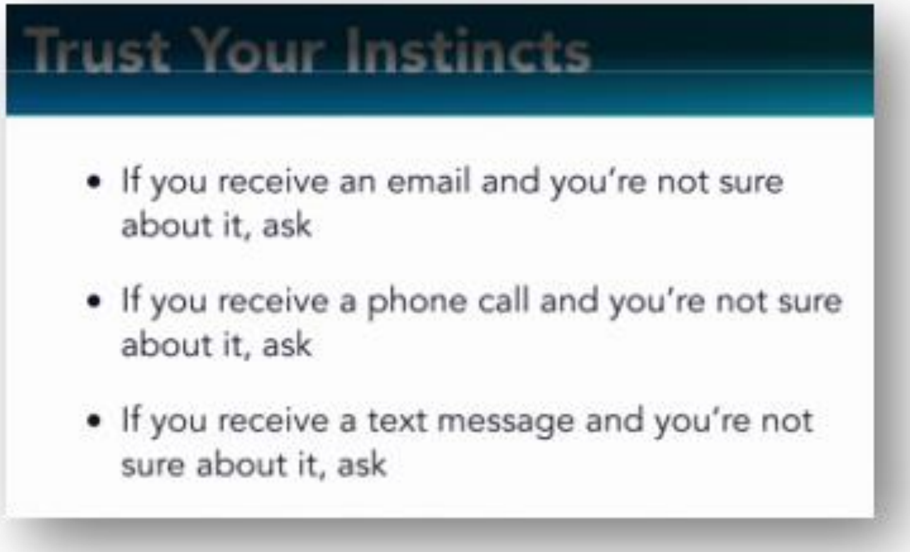
Know your library's data and digital standards policies!

westchester LIBRARY SYSTEM
Empowering libraries. Empowering communities.

Protect You and Your Library

Pause!

If something seems off or suspicious, trust your instincts and ask your security IT team, or the WLS IT Helpdesk for help.



Trust Your Instincts

- If you receive an email and you're not sure about it, ask
- If you receive a phone call and you're not sure about it, ask
- If you receive a text message and you're not sure about it, ask

westchester LIBRARY SYSTEM

Empowering libraries. Empowering communities.

New York Shield Act

The SHIELD law expands data security and breach notification requirements to cover any business that collects private data of New York residents, not just companies that conduct business in the state.

The Shield Act significantly strengthens New York's data security laws by:

- Expanding the types of private information that companies must provide consumer notice in the event of a breach, and
- Requiring that companies develop, implement, and maintain reasonable safeguards to protect the security, confidentiality and integrity of private information.

The NYS Shield Act

westchester LIBRARY SYSTEM
Empowering libraries. Empowering communities.

Key Takeaways

- Keep your mobile devices and work area secure.
- Keep software, especially antivirus software, updated and on.
- Keep professional and personal devices and accounts separate.
- Use Multi-factor Authentication, strong passwords, and a password manager.
- Don't click on links from unknown sources in emails. Verify urgent messages with their sources.
- Use a VPN when on a public Wifi network.

westchester LIBRARY SYSTEM
Empowering libraries. Empowering communities.

The Big Balance

- **Security**
- **Privacy**

- **Convenience**
- **Sharing**

Links & Support

- National Cyberserity Alliance Online Safety Basics
- Consumer Reports Security Planner
- Cybersecurity and Infrastructure Security Agency (CISA)
- CyberNews Best Password Managers For 2021
- PKF O'Connor Davies Newsletter Sign Up

- Training@wlsmail.org
- Support@wlsmail.org

Allison Midgley

- amidgley@wlsmail.org

westchester LIBRARY SYSTEM
Empowering libraries. Empowering communities.