Spotting Scams

Learn the warning signs and prevention techniques for computer, phone, text, and online scams.

Slow Down | Stop and Think | Be Skeptical

Email and Computer

Phishing
Sending **messages** claiming to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Spear Phishing
Targets a **specific person or group** and often includes information known to be of interest to the target, such as current events or financial documents.

Whaling
Directed at **high-profile CEOs and celebrities**. Attackers masquerade as trusted entities and encourage a victim to share highly sensitive information.

Pharming
Directing users to a **bogus website** that mimics the appearance of a legitimate one, in order to obtain personal information such as passwords, account numbers, etc.

Spot the Scam!

- The email address is unrelated to the supposed organization
- Email content is vague and not personalized
- Poor grammar and spelling
- It was unsolicited…. you never requested to change account settings
- Sense of urgency, e.g. "your account will be suspended immediately"
- "Click here" – never click links within a suspicious email

An ounce of prevention

- Don't respond!
- 2-factor authentication (password plus an additional layer of security)
- Junk folders and blocking
- Unsubscribe to emails you no longer need. Only use this if you know you joined their mailing list.
- Install Antivirus, Anti-malware, Windows Security
- Update your browser. Consider Firefox, Brave, or DuckDuckGo, which are browsers and search engines that clear personal data, or don't collect it at all
- To force-close windows or pop-ups:
    - CTRL-ALT-Delete (windows)
    - Command-Option-Esc (mac)

Never return a call by using the phone number included in a suspicious email, text, or voicemail. Instead, use a search engine (or call the library!) to find the real number.

Phone and Text

Vishing

Calling or leaving **voicemails** claiming to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Smishing

Using **text messages** to induce individuals to reveal personal information.

Most popular categories of phone and text scams:

- Telemarketing
- Government
- Tech Support
- Banks or financial Institutions
- Loved one in an emergency situation

Spot the Scam!

- It seems like an official-sounding, or at least recognizable organization
- There's a problem or prize
- Pressure to act immediately
- Instructed to pay in a specific way (wire transfers, gift cards)
- Unknown phone numbers

An ounce of prevention

- Stop and think
- Don't answer the call if you don't recognize the number
- Block unwanted calls and messages
- Don't give out personal information when you didn't initiate the call
- Slow down, do not give in to pressure tactics
- Do not agree to unusual payment methods (cryptocurrency, wire transfers, gift cards)
- Talk to someone you trust
- Forward text to 7726 (SPAM) – universal reporting system

Voice Cloning:

Scammers can use audio clips to mimic the sound of a loved one's voice. If this happens, hang up and call a phone number you KNOW is theirs!

Online, Video and Social Media

Deepfake
Video or photo of a person in which their face or body has been digitally altered so that they appear to be someone else, typically used maliciously or to spread false information.

Online Marketplace
A buyer or seller attempts to defraud an individual by not following through with the promised item.

Job Scam
Job offers that are deceptive or dishonest towards those seeking genuine employment possibilities.

Romance Scam
Using a fake online identity to gain a victim's affection and trust. Uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim.

Spot the Scam!

Deepfake
- Background: Blurry or crooked
- Glasses: Mismatched connections, too much or not enough glare.
- Eyes: eyes in the same spot in the frame ("deepfake stare")
- Jewelry: strangely attached; embedded into the skin.
- Collars and shoulders: Misshapen or Unmatching

Online Marketplace
- You're asked to send the item before receiving payment
- It sounds too good to be true
- Overpayment or odd forms of payment
- They ask for verification with a texted code
- Bait and switch
- Giveaways that require you to fill out a form

Job Scam
- Fake check scam
- Reshipping and reselling
- Vague or no details about the position
- Fees and upfront payment demands

Fake Check Scam

Someone you don't know asks you to deposit a check.

It's for more than they owe.

They ask you to send the extra back to them or someone else.

When asked, they give a shady explanation for why you can't keep all the money.

Do not fall for this! The check will bounce, but your bank will still want their money!

An ounce of prevention

Online Marketplace

- Pick up in-person and inspect before paying
- Meet-up in a safe spot
- Never refund an overpayment
- Never send back codes texted to your phone
- Verify rental status by contacting the property listing manager. Do not fill out rental agreements until verified.
- Always use a tracking number for shipping packages
- Only use established forms of payment (cash, zelle, paypal)
- Guard your personal information
- Change social media settings to private
- Reverse Image Search helps spot fake profile pics

Romance Scams

- Be careful what you post and make public online.
- Use reverse image search
- Go slowly
- Are they too good to be true?
- Requesting inappropriate photos or information, or attempting to isolate you are major red flags
- Beware if you haven't met in-person after a few months
- Never send money to anyone you haven't met in-person.

Job Scams

- Check out employers before providing sensitive information
- Don't send money up front (beware the fake check scam)
- Get the details in writing
- Talk to someone you trust

Text code verification?

A marketplace buyer wants to "verify your identity" by sending a code to your cell phone. They ask you to reply to them with the code.

This is a scam! Sending these codes can be used to hack your accounts or set up a Google voice number in your name.

Resources

Reverse Image Search Instructions from PC Magazine

- Sign up for Scam Alerts: www.consumer.ftc.gov/features/scam-alerts
- IL Attorney General Senior Citizens Consumer Fraud Hotline: 1-800-243-5377
- Report Scams to the FTC: reportfraud.ftc.gov
- Milton Township SALT (Seniors and Law Enforcement Together) provides a quarterly Scams Report: miltontownshipsalt.com/