Online Safety and Practical Strategies for Avoiding Internet & Phone Scams

Types of Online Scams

- Romance Scams
- Malware and Spam
- Faulty Purchases
- Employment Scams
- Investment & Banking Scams
- Telephone Scams
- Census-Related Fraud
- Government grant scams
- Lottery and sweepstakes scams
- Charity scams

Important Terms:

Phishing: "a cybercrime in which targets are contacted by someone posing as a legitimate institution to lure individuals into providing sensitive data"

Spoofing: "a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity"

Practical Strategies for Increasing Personal Internet Safety

Online Shopping

- **Double check the URL** - If you think a website is suspicious, look at the URL. For example, f it looks like Target but doesn't begin with https://www.target.com exit the page and directly type in the website into your browser.
- **Payment method** - Paying with a credit card versus a debit card when shopping online can make the dispute process easier if needed
- **Read the fine print** - Some "deals" are not deals at all but scams. Check what you are signing up for when signing up for "free" trials.

Protect your devices and accounts with Passwords

- Password Do's:
  - Use different passwords for different accounts
  - Include a variety of numbers, symbols, uppercase and lowercase letters in your passwords
  - Make passwords at least 10 characters long
  - Change your passwords frequently (approximately every 3 months)
- Password Don'ts:
  - Track passwords in a place close to your devices or on your computer
  - Use repeat passwords for multiple accounts
  - Use familiar names, phone numbers, dates, common phrases or number sequences in your passwords

SALUS UNIVERSITY
Occupational Therapy Institute

Email: OTI@salus.edu
Phone: 215.276.3646
Website: SalusUhealth.com/OTI

Online Safety and Practical Strategies for Avoiding Internet & Phone Scams

Practical Strategies for Increasing Personal Internet Safety

Social Media Use

- **Photo Use** - Be careful of what photos you share online, some scammers use headshot like photos in identity theft scams.
- **Public Sharing Settings** - Be aware of who can see your posts and what information you are sharing with the public on social media platforms
- **Be wary of your online interactions** - Don't accept friend requests or messages from people you don't know. Don't click on links sent by strangers.
- **Be critical of what you are consuming.** Not everyone will fact check what they are sharing, so think critically when reading articles or posts from your friends or groups online.

General Tips

- Have an **antivirus software** installed on your computer and run it on a regular basis to monitor your computer for viruses (Examples: Norton, McAfee)
- Follow the guideline **"when in doubt, throw it out."** If you are unsure about a message, piece of mail, an email, send it to spam, delete the message or throw it in the trash.
- If you don't recognize the phone number calling, ignore the call or let it go to voicemail.
- Trust your instincts - if something feels suspicious online, close the browser, exit the website.
- Register your phone number on the **National Do Not Call Registry**
- Organizations for resources and to report fraud or scams:
    - Better Business Bureau (BBB), US Securities and Exchange Commission (SEC), North American Securities Administrators Association (NASAA), Federal Trade Commission (FTC)

References

AARP (2019, May 7). *Strategies for Staying Safe and Secure Online*. Personal technology.https://www.aarp.org/home-family/personal-technology/info-2019/privacy-for-seniors.html

Australian Competition and Consumer Commission. (n.d.). *Spot the scam signs*. About scamwatch.https://www.scamwatch.gov.au/about-scamwatch/tools-resources/online-resources/spot-the-scam-signs

Button, M., McNaughton Nicholls, C., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology, 47*(3), 391-408. https://doi.org/10.1177/0004865814521224

Federal Communications Commission. (2021, March 17). *Caller ID Spoofing*. Consumer guides. https://www.fcc.gov/spoofing

Federal Trade Commission. (2019, September). *Phone Scams*. Privacy, identity & online security. https://www.consumer.ftc.gov/articles/0208-phone-scams

KnowBe4. (n.d.). *What is phishing?*. Phishing.org

USAGov. (2021). *Common Scams and Frauds*. Scams and frauds. https://www.usa.gov/common-scams-frauds

SALUS UNIVERSITY
Occupational Therapy Institute

Email: OTI@salus.edu
Phone: 215.276.3646
Website: SalusUhealth.com/OTI