Published on *University of Colorado* (https://www.cu.edu)

Week 4: Cybersecurity Starts with You [1]

Every time you use the Internet, you face choices related to your security. Should a link be clicked, website accessed, and wireless networks be joined? Your security and the security of your family, friends, coworkers, and fellow students depends on making secure online decisions. Making the Internet more safe and secure requires all of us to take responsibility for our own cybersecurity posture.

Why is Cybersecurity Important?

Cybersecurity is the art of protecting networks, devices, and data from unlawful access or criminal use and the practice of guaranteeing confidentiality, integrity, and availability of information. Communication, transportation, shopping, and medicine are just some of the things that rely on computers systems and the Internet now. Much of your personal information is stored either on your computer, smartphone, tablet or possibly on someone else's system. Knowing how to protect the information that you have stored is of high importance not just for an individual but for an organization and those in it.

Potential Threats

• Phishing. Phishing scams use emails and malicious websites that appear to be trusted organizations, such as charity organizations or online stores, to obtain user personal information.

• Malware. A computer can be damaged or the information it contains harmed by malicious code (also known as malware). A malicious program can be a virus, a worm, or a Trojan horse. Cybercriminals are in it to make money off these software flaws. Despite their benign intentions and curiosity, their actions are usually contrary to the intended uses of the systems they exploit.

• Identity Theft and Scams. Identity theft and scams are crimes of opportunity, and even those who never use computers can be victims. There are several ways criminals can access your information, including stealing your wallet, overhearing your phone call, dumpster diving (looking in your trash) or picking up a receipt that contains your account number. While you cannot guarantee that you will not be a victim of identity theft, you can lower your risk by practicing secure behaviors at home, work, and school.

Simple Tips

• Use antivirus software. Antivirus software is very important. It's an important protective

measure useful against cybercriminals and malicious threats. It can automatically detect, quarantine, and remove types of malware. Automatic virus updates should always be enabled to ensure maximum protection against the latest threats.

• Keep software up to date. Cybercriminals have been known to take advantage of well-known problems and vulnerabilities. Making sure you install software patches and utilizing automatic updates for your operating system will help keep you protected.

•Utilize strong passwords. Creating passwords that will be difficult for cybercriminals to guess is vital. Use different passwords for different programs and devices. It is also best to use long, strong passphrases or passwords that consist of at least 15 characters. Consider a password manager to generate and remember different, complex passwords for each of your accounts. (See Creating a Password Tip Sheet below.)

•Double your login protection. Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring. (See Multi-Factor Authentication How-to-Guide below.)

•Watch for Phishing. The goal is to gain information about you and use your information to make unauthorized purchases or gain access to a secure system. Be suspicious of unexpected email sand always check email address sources to make sure the email is not coming from a fake website.

Learn More

Webinar October 27, 2021, 12:00 - 1:00 p.m. MT: Kerry Tomlinson, Cyber News Reporter, Click to join webinar: Working from Home Safely [2]

Attachments:
creating-passwords-tip-sheet.pdf [3]
mfa-tip-sheet.pdf [4]
Groups audience:
Office of Information Security

Links
[1] https://www.cu.edu/security/week-4-cybersecurity-starts-you
[2] https://cuboulder.zoom.us/j/98525523059
[3] https://www.cu.edu/doc/creating-passwords-tip-sheetpdf
[4] https://www.cu.edu/doc/mfa-tip-sheetpdf