Cybersecurity Awareness & Internet Safety Tips

Remember, if something looks "suspect", report it. It's better to be safe than sorry.

Cybersecurity Awareness: Malware Tips

Criminals use malware to steal or destroy your data and compromise the security and integrity of your equipment and/or systems. Malware is a serious and persistent threat, but there are ways to help protect your sensitive information.

Quick Tip: Cyber criminals can modify how their names initially appear in emails. Hover over the sender's name to display the real address from which the email was sent.

Reduce Your Risk of a Malware Infection

- Keep your security software, web browser and operating systems up to date – including your smart phone operating system. Turn on and take advantage of automatic updates.
- Install anti-virus and anti-malware software only from a trusted source and scan your system often.
- Make sure your firewall is on. Update settings to maximize protection for all network locations—home, work, public.
- Do not install software you did not specifically seek out. Do not download software from untrustworthy or unknown sources. Remove / uninstall software you are no longer using.
- Avoid using USB and other plug-in devices. Use online storage as an alternative.
- Back up computer data. Use an external hard drive or network to ensure you have access to your information in the event your computer or mobile device becomes corrupted.

Watch What you Click

- Do not click on e-mail or phone text links in pop-ups or spam—even those claiming to offer anti-virus software—as they also may install spyware or ransomware.
- Be careful what you click; unfamiliar links can expose you to malicious software programs that scan your computer or track keystrokes, including your passwords and account numbers.

Things aren't always what they seem

- Pay attention to anti-virus and anti-malware warnings, such as when you are trying to access websites that may be unsafe.
- Pay attention to message boxes and the fine print when installing programs because some intentionally include malware. Cancel any installation if you believe it may be harmful.
- Be wary of suspicious-looking email. Even email from people you know can contain malware links or attachments if their accounts have been compromised.
- Be careful following links in incoming email. Whenever possible, visit websites by entering the desired address directly in your browser.
- Scan files with security software before opening. Do not assume emailed files or those given to you on a disc or flash drive are safe.
- Do not trust pop-up windows asking you to download software. Their goal is to convince you that your computer has been infected and downloading the software will take care of the problem. Close this window immediately, making sure not to click on anything inside the pop-up window.
- Avoid file-sharing sites because most are illegal. In these types of services, there is little policing for malware, which can be disguised as a popular movie, song or program.

Cybersecurity Awareness: Internet Safety Tips

Every device connected to the internet can be hacked. Hackers can create clones of well-known websites or push phishing attacks to capture personal information, such as user credentials, direct deposit bank information, fake vendor invoices, tax IDs, credit card information, etc. Then they use the stolen information to access banking and other accounts.

Quick Tip: Multi-factor authentication ("MFA") is one of the strongest cybersecurity measures available and adds an extra layer of protection against attacks from cyber criminals.

Precautions to Take Online

- Update your browser software frequently and maintain a medium or higher level of security on your browser settings.
- Browse securely by checking that "https://" begins the URLs of websites you visit. Some browsers feature a padlock icon with the URL to indicate a secure/encrypted connection. Remember, "http://" is not secure.
- Log out after using an internet banking service to ensure your session has closed.
- Clear cookies and browser cache so hackers cannot access your history and obtain information.
- Always block pop-ups and ads and never respond to pop-ups asking you to submit or resubmit your login information.
- Avoid file-sharing sites or similar sites that provide illegal downloads or content. Even if you do not download any files, you can be vulnerable to viruses and/or malware that can infect your computer.

What to Avoid

- Do not download anything from unknown sources. Download and install software only from sources you trust.
- Do not allow your internet browser or websites you visit remember your passwords or credit card information.
- Do not accept calls from a computer company, e.g. Dell, Apple, Microsoft, Google, or a telecom company, e.g. Verizon, AT&T, Comcast, Time Warner/Spectrum, the IRS, etc. Those companies would not call out to you – they are very likely fraudsters trying to 'social engineer' access via computer password.
- Do not link accounts across websites. If one is compromised, all of them may be compromised.

What to Remember

- Regularly check your banking and credit card transaction histories for suspicious transactions, and set up easy transaction alerts on your accounts. Reconcile bank accounts promptly.
- Enable private browsing whenever possible.
- Prevent cookies and browsing history from being stored or saved to your device.
- Use trusted bookmarks for important sites—note-mail links or popups.
- Use the **X** in the upper right-hand corner to close windows containing pop-up ads or unexpected warnings. Avoid clicking the "close" button or anywhere within the window to close it.
- Do not buy anything promoted in a spam message. Even if it's not a scam, your purchase encourages spamming.
- Use multi-factor authentication ("MFA") whenever possible. You confirm your identity in two steps each time you use an ATM—with a debit card and PIN. Do the same online.
- Maintain separate email accounts and use MFA with each of them. Multi-factor authentication is one of the strongest cybersecurity measures available and adds an extra layer of protection against attacks from cyber criminals.