

Cyber Security Awareness Tips

Helpful tips for helping to keep your identity, personal information and data secure. More information can be found through the links listed below.

Phishing Emails

- Never respond to requests for personal information via email. Businesses will never ask for personal information in an email.
- Do not enter personal information in a pop-up screen.
- Do not click on any links listed in an e-mail message. Copy and paste the URL into your browser.
- Use anti-virus and anti-spyware software and update them regularly.

Dispose of Information Properly

- Destroy/shred hard copy confidential documents that contain personal information such as social security numbers, credit card numbers, bank account numbers, and health records.
- Ensure you are using the right tools when destroying and disposing of personal information or media storage from your computer and mobile devices.

Ethics - Be a good cyber citizen

- Do not engage in inappropriate conduct, such as cyberbullying, cyberstalking or rude and offensive behavior.
- Do not do something in cyberspace that you would consider wrong or illegal in everyday life.
- Do not impersonate someone else. It is wrong to create sites, pages, or posts that seem to come from someone else.
- Adhere to copyright restrictions when downloading material from the Internet.
- Do not use someone else's password or other identifying information.

Lock it when you leave

- It takes only a few seconds to secure your computer and help protect it from unauthorized access. Lock down your computer every time you leave your desk.
- Set up a screen-saver that will lock your computer after a pre-set amount of time and require a password to log back in.
- If your computer is used by more than one person, you may want to create individual accounts, with unique login and passwords for each user.
- Choose a strong password. A good password should always include upper and lowercase letters, numbers, and at least one special character. Do not set the option that allows a computer to remember any password.

Protect data on mobile devices

- Ask yourself "Is it really necessary that I transport this sensitive information?" If the answer is no, then do not copy the information.
- Choose a strong password. A good password should always include upper and lowercase letters, numbers, and at least one special character. Never use the same password for multiple devices or accounts.
- Store your portable devices securely. When not in use, store devices out of sight and when possible in a locked drawer or cabinet.

Protect mobile devices

- Password-protect your portable device.
- Be sure all critical information is backed up.
- Disable Bluetooth when not required.
- Make sure your firewall and anti-virus are up-to-date.
- Store your portable devices securely.
- Record identifying information such as serial number and label your equipment if possible.
- Report the loss or theft to the appropriate authorities as soon as possible.

National Cyber Awareness Tips: <https://www.us-cert.gov/ncas/tips>

MSISAC Daily Tip: <http://msisac.cisecurity.org/daily-tips/>

Department of Homeland Security: <http://www.dhs.gov/stopthinkconnect>

Stay Safe Online: <http://staysafeonline.org/>

FCC Smartphone Security Checklist: <https://www.fcc.gov/smartphone-security>