- Never give out login credentials (over the phone, in person, email). Any competent IT department would never ask for your login credentials in any circumstance.
- Roll the mouse pointer over a link to reveal its actual destination, displayed in the bottom left corner of the browser. In Microsoft Outlook it is displayed above the link.
- When using public Wi-Fi, refrain from sending or receiving private information.
- Report any loss or theft of your company issued smartphone/tablet/laptop immediately to IT.
- Be leery of items from unknown sources or even suspicious links from trusted sources. When in doubt, chuck it out!
- Stop. Think. Click. Think twice before clicking that link.
- Report any security incident (ex. responding to a scam email with your login credentials) to IT immediately. Do not fear reprisal or be ashamed, such incidents are expected given today's threat landscape.
- Use a different password for every website. If you have only one password, a criminal simply has to break a single password to gain access to all your information and accounts.
- Practice good password management. Use a strong mix of characters, and don't use the same password for multiple sites. Don't share your password with others, don't write it down, and definitely don't write it on a post-it note attached to your monitor.
- If you have difficulty remembering complex passwords, try using a passphrase like "I love getting to work at 7:00!" Longer passwords are harder to crack than shorter complex passwords.
- Never leave your smartphone, tablet, or laptop unattended in a public place.
- Realize that you are an attractive target to hackers. Don't ever say "It won't happen to me."
- Always be careful when clicking on attachments or links in email. If it's unexpected or suspicious for any reason, don't click on it. Double check the URL of the website the link takes you to: bad actors will often take advantage of spelling mistakes to direct you to a harmful domain.
- Sensitive browsing, such as banking or shopping, should only be done on a device that belongs to you, on a network that you trust. Whether it's a friend's phone, a public computer, or a cafe's free WiFi—your data could be copied or stolen.
- Back up your data regularly, and make sure your anti-virus software is always up to date.
- Be conscientious of what you plug in to your computer. Malware can be spread through infected flash drives, external hard drives, and even smartphones.
- Watch what you're sharing on social networks. Criminals can befriend you and easily gain access to a shocking amount of information—where you go to school, where you work, when you're on vacation—that could help them gain access to more valuable data.
- Offline, be wary of social engineering, where someone attempts to gain information from you through manipulation. If someone calls or emails you asking for sensitive information, it's okay to say no. You can always call the company directly to verify credentials before giving out any information.
- Be sure to monitor your accounts for any suspicious activity. If you see something unfamiliar, it could be a sign that you've been compromised.