Office of the Chief Information Security Officer

Cybersecurity Tips

How To Be Cyber Safe While Online

The Internet is part of our everyday lives at work and home. We rely on it for our entertainment, connecting with friends and family through smart phones, car navigation systems, and sending daily messages via the web and texting. Our civilization is technology dependent and our daily routines would come to a grinding halt without it.

DIR has these tips to stay safe while you are online:

CONNECT WITH CARE, BE CYBER AWARE

Update

- Best defense against viruses and other online threats.
- Keep your devices, security software and web browsers updated with the latest patches.

Clicking

- Be wary of email and online advertising links.
- This is a common way criminals use to gain access to your computer.
- Remember if it sounds too good to be true, it probably is.

WiFi

- Be extra vigilant when using unfamiliar WiFi hotspots.
- Do not conduct sensitive work on public WiFi.
- Adjust your device security settings to limit who can access your phone.

Delete

- When in doubt, throw it out.
- If a link, email, tweet, post, online ad looks suspicious, even if you know the source, its best to delete or, if appropriate, mark as junk email.

Fortification

- Keep a clean machine. Keep all software on internet-connected devices, including PCs, smartphones and tablets, up to date to reduce the risk of infection from malware.
- Lock down your login: Fortify your online accounts by enabling the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device. Usernames and passphrases alone are not enough to protect key accounts like email and banking.

Browsing

- Before sending or entering sensitive information online, check the security of the website. Look for web addresses with https:// which indicates the site takes extra measures to help secure your information, while http:// is not secure.
- Pay attention to the website's URL. Malicious websites may look identical to legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .net versus .com).

Passwords

- Make your passphrase a sentence: A strong passphrase is a sentence that is at least 12 characters. Focus on positive sentences or phrases that you like to think about and are easy to remember (for example, "I love country music."). On many sites, you can even use spaces!
- Unique account, unique passphrase: Having separate passphrases for every account helps to thwart cybercriminals. At a minimum, separate your work and personal accounts. Make sure that your critical accounts have the strongest passphrases.

Email

- Do not reveal personal or financial information in an email, and do not respond to email solicitations for this information. This includes following links sent in email.
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly through information provided on an account statement, not information provided in an email.
- Think before you act: Be wary of communications that implores you to act immediately, offers something that sounds too good to be true, or asks for personal information.