8 InfoSec Tips

You Are A Target

Realize that you are an attractive target to hackers. Don't ever think or say, "It won't happen to me."

Offline Risk

Be wary of social engineering, malicious actors use manipulation techniques to gain sensitive information. If someone calls or texts you asking for sensitive information, it's best to say no or just simply hang up. A best practice is to call the company directly to verify credentials before giving out any information.

Strong Passphrases

Practice good password management. A passphrase should be at least 14 characters long and don't use the same password for multiple accounts. Don't share your password with others, don't write it down, and don't write it on a post-it note attached to your monitor nor place it under your keyboard.

Lock It Up

Never leave your devices unattended. If you need to leave your computer, phone, or tablet for any length of time—no matter how short—lock it up so no one can use it while you're gone. If you keep physical sensitive information, make sure to lock it up where no one else has access, unless they need to.

Practice Safe Clicking

Always be careful when clicking on attachments and/or links in an email. If it's unexpected or suspicious for any reason, don't click on it. Double-check the URL of the website by hovering your mouse over the link. Bad actors will often take advantage of spelling mistakes to direct you to a harmful site. Be alert for any red flags and always report any unusual activity to your IT or InfoSec department immediately.

Beware of Browsing

Whenever you're doing any sensitive browsing, such as banking or doing any purchasing, it should only be done on a device that belongs to you, on a secure network that you trust. Your data can be compromised, copied, or stolen by using a friend's phone, a public computer, or a public free Wi-Fi.

Share Less Sensitive Information

Watch what you're sharing on social networks. Cybercriminals 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.

Monitor Your Accounts

Be sure to stay on top of your accounts for any suspicious activity. If you see something unusual, it could be a sign that you've been compromised.

To report an incident, please contact your InfoSec team immediately.

Follow us on:

#SecLex

Contact us at:

(323)471-0057

contact@SecLexISC.com

SEC LEX

www.SecLexISC.com