TOP FIVE STEPS TO STAYING SECURE

Regardless of what technology you are using or where you are using it, here are five fundamental steps you should take to protect yourself. Learn more at www.securingthehuman.org/ouch.

1 YOU

The most important part to staying secure is you. Cyber attackers have learned that the easiest way to get something is to simply ask for it. As a result, common sense is your best defense. If an email, message or phone call seems odd, suspicious or too good to be true, it may be an attack.

2 UPDATING

Ensure your computer, mobile device and apps are updated and always running the latest version of their software. Whenever possible, enable automatic updating.

3 ENCRYPTION

Use encryption whenever possible. Use Full Disk Encryption (FDE) for laptops or computers, which will automatically encrypt everything on your hard drive. When browsing online, make sure the address of the website you're visiting starts with "https:" and has an image of a closed padlock next to it.

4 BACKUPS

Make sure you do regular backups of any important information. Often, the only way you can recover from a computer or device that has been hacked, lost or stolen is to recover from your backups.

5 PASSWORDS

Passwords are the keys to your kingdom, guard them well.

- Always use long, strong passwords; the more characters you have, the better. Even better, use two-step verification whenever it is possible.
- Use a unique password for every device and account. Can't remember all of your passwords? Use a password manager for securely storing and retrieving your passwords.
- Never share your passwords with anyone, including your coworkers or your supervisor.