SIMPLE STEPS TO ONLINE SAFETY

Make cybersecurity a priority

1 DOUBLE YOUR LOGIN PROTECTION.

Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in.

2 SHAKE UP YOUR PASSWORD PROTOCOL.

According to National Institute for Standards and Technology (NIST) guidance, you should consider using the longest password or passphrase permissible.

3 IF YOU CONNECT, YOU MUST PROTECT.

Whether it's your computer, smartphone, game device, or other network devices, the best defense against viruses and malware is to update to the latest security software, web browser, and operating systems.

4 PLAY HARD TO GET WITH STRANGERS.

Cybercriminals use phishing tactics, hoping to fool their victims. If you're unsure who an email is from — even if the details appear accurate — or if the email looks "phishy," do not respond and do not click on any links or attachments found in that email.

5 NEVER CLICK AND TELL.

Limit what information you post on social media — from personal addresses to where you like to grab coffee. Disable location services that allow anyone to see where you are – and where you aren't – at any given time.

6 KEEP TABS ON YOUR APPS.

Most connected appliances, toys, and devices are supported by a mobile application. Your mobile device could be filled with suspicious apps running in the background or using default permissions you never realized you approved — gathering your personal information without your knowledge while also putting your identity and privacy at risk.

7 STAY PROTECTED WHILE CONNECTED.

Before you connect to any public wireless hotspot – like at an airport, hotel, or café – be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate.

OWN SECURE PROTECT IT. OCTOBER 2019 National Cybersecurity Awareness Month #BeCyberSmart

INTERNETWORK ENGINEERING