TIP SHEET

CYBERSECURITY 101

CYBERSECURITY 101 Cybersecurity is the art of protecting networks, devices, and data from unlawful access or criminal use, and providing confidentiality, integrity, and availability of information. Much of your personal information is stored either on your computer, smartphone, or tablet. Knowing how to protect your information is important, not just for individuals but for organizations, as well. Every time you use the internet, you face choices related to your security. Your security and the security of the nation depends on making responsible online decisions. Making the internet safe and secure requires all of us to take responsibility for our own cybersecurity behavior.

KNOW YOUR CYBER BASICS

• Think Before You Click: Recognize and Report Phishing: If a link looks a little off, think before you click. It could be an attempt to get sensitive information or install malware.
• Update Your Software: Don't delay – if you see a software update notification, act promptly. Better yet, turn on automatic updates.
• Use Strong Passwords: Use passwords that are long, unique, and randomly generated. Use password managers to generate and remember different, complex passwords for each of your accounts. A password manager will encrypt passwords securing them for you!
• Enable Multi-Factor Authentication: You need more than a password to protect your online accounts, and enabling MFA makes you significantly less likely to get hacked.

POTENTIAL THREATS

• Malware. A computer can be damaged or the information it contains harmed by malicious code (also known as malware). A malicious program can be a virus, a worm, or a Trojan horse. Hackers, intruders, and attackers are in it to make money off these software flaws.
• Identity Theft and Scams. Identity theft and scams are crimes of opportunity, and even those who never use computers can be victims. There are several ways criminals can access your information, including stealing your wallet, overhearing a phone call, looking through your trash, or picking up a receipt that contains your account number.
• Phishing. Phishing attacks use emails, texts, and malicious websites that appear to be trusted organizations, such as charity organizations or online stores, to obtain user personal information.

HOW CRIMINALS LURE YOU IN

Phishing is one of the most common forms of cyber scams that you are likely to experience. The key is that both emails and texts should come from a trusted source. Know what to look for—here are examples of phishing that might be seen in an email to lure you in:

"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below, and confirm your identity."

"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."

"Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."