You're the target.

You may think fraudsters aren't interested in your family's personal information or what you do on the job. But they are. Taking a few simple steps can go a long way toward protecting yourself, your loved ones and your employer.

The 4 Biggest Threats

Phishing: Emails and texts that look legitimate but are not. Bad guys send alerts saying you've made a purchase or need to verify a refund, are having computer issues and need to take action, or are having some sort of banking issue. One trick involves hiding malicious text in an Office 365 document.

Ransomware is up 600% in the past year and often targets Windows and Android devices. One warning sign: a document asks the user to "turn on Macros." Crooks block the victim from accessing computer files until they're paid a ransom. Even after payment is made, files are often not restored.

"Internet of Things": High-tech devices from smart refrigerators to home security cameras that use Wi-Fi are easily hacked. Manufacturers ship these products with default passwords that are easily cracked by cyber thieves. Often, consumers don't take time to change the passwords.

Insiders: From employees to vendors to delivery people, not everyone is ethical. Theft of sensitive documents, employees sharing passwords, and posting of company information online are examples why over half of organizations were victims of theft due to insiders in 2020.

4 Ways to Stay Safe

A

Ask.
Question the authenticity of emails, texts or phone calls you receive, particularly if they're of an urgent nature or ask for personal information.

B

Be skeptical.
Sounds too good to be true? You know the drill. Trust your instinct when a text, email or website looks suspicious.

C

Change the password.
Getting a new high tech-device for your home? Take time to change the default password that came with it.

D

Don't click.
If an email looks suspicious (if it requires immediate action or claims to be an important download), don't click and alert your supervisor.

AMBOY Bank