Identity Theft

CYBER THREATS

While computers and the Internet offer huge benefits, they also offer cyber criminals opportunities to steal personal information. Cyber crooks have shown they can keep up with the fast-paced growth of technology. They constantly develop new tools and methods to trick and exploit people though computer and Internet use. The more aware you are of cyber threats, the more prepared you are to avoid them.

"Malware" is a broad term for the many forms of malicious software designed to disrupt, harm or hijack a computer system or data. It includes viruses and spyware. Secretly installed without your knowledge or consent, malware programs can damage your privacy and the security of your computer or mobile device. They can capture your personal information in a variety of ways and secretly send it to identity thieves.

Computers and mobile devices are commonly infected with malware through email attachments, downloads and the links within emails or pop-up windows.

Carefully read all disclosures, including the privacy statement and licensing agreement, before downloading and installing software. Malware may be bundled in with it. Look for wording about personal information collection, Internet activity monitoring or additional programs.

Warning Signs of Malware

- Slow or sluggish performance
- Computer crashes
- Repeated error messages
- Being automatically sent to websites you didn't mean to visit
- An unintended reset to a new Internet home page that can't be undone
- Getting bombarded with pop-up ads and/or ads popping up when a browser is not open
- Finding a new toolbar added to your browser
- Seeing new icons on your desktop
- Your online search results page shows only ads
- Emails sent from your account that you didn't write
- Decreased battery life, interrupted or dropped calls and crashing apps on mobile devices are also warning signs of a malware infection

Malware can be hard to remove. If you suspect it immediately stop all online activities that require you to enter any kind of personal information, update and then run your security software and seek reliable tech support if possible.

Identity Theft

CYBER THREATS (cont.)

Catfishing

When a person creates a fake identity on social media, usually targeting a specific victim for abuse, deception or fraud. Catfishing is often used for romance scams on dating website.

Phishing

When cyber thieves send you emails that try to lure you into providing or confirming personal information. The emails look like they're from legitimate organizations, often ones you know. These ordinarily used threats, warnings or enticements to create a sense of urgency. You're usually asked to click on a link. If you do, it can lead to a spoof website. The site looks real enough to trick you into entering personal information. Signs of phishing emails could include:

- Request (usually urgent) for you to make contact through a provided link
- Spelling and grammar mistakes
- Generic greetings, like "Dear User"
- Unsolicited attachments

Smishing and Vishing

Very similar to phishing, this is when criminals use automated dialing systems to call or text you with messages intended to trick you into sharing personal information. The message will direct you to a phone number or website that asks you for the information.

Clicking on links, opening attachments or going to web addresses provided through phishing, smishing and vishing frequently cause identity-stealing malware downloads.

Avoid Phishing, Smishing and Vishing

- Never click on links from unknown senders. Be cautious about clicking emails and text message links even from known senders.
- Don't trust contact information provided in emails, text messages or pop-ups. Verify it on your own.
- Don't respond to text or automated voice messages on your mobile phone if they're from an unknown or blocked called.
- Know that most legitimate companies and organizations won't request personal information via email.
- Be cautious about downloading email attachments. Ensure you know and trust the sender.