WINTHROP WEALTH

109 State Street
2nd Floor
Boston, MA 02109

P 617.530.1010
F 857.265.2382
winthropwealth.com

GONE PHISHING: PROTECTING AGAINST ONLINE ATTACKS

Identity theft compromises the personal data of millions of Americans every year. There are steps you can take to minimize your online risk and protect your sensitive data from cyber-attacks.

Identity theft is a growing concern that impacts millions of Americans every year. According to a recent study,[1] more than 14 million Americans fell victim to online theft in 2018, with 23% of those incurring unreimbursed personal expenses, up three-fold from just two years prior.

Identity theft occurs when a thief obtains your personal information — account numbers, Social Security number, personal ID and password, banking information — and uses that information to commit fraud. They can use that information to steal money from your accounts, take out credit cards or obtain loans in your name, and commit various other types of financial fraud.

Thieves can steal your personal information both offline and online, and their attacks are growing increasingly sophisticated, making them more difficult to identify and prevent.

Cyber Attacks

Cyber-attacks continue to dominate news headlines and have been responsible for compromising the data of millions of Americans. There are two primary methods that cyber thieves use to steal personal information — social engineering and phishing.

Social engineering happens when a thief tricks online users into performing an online action that gives them access to your system and its data. They may send a text message that includes a link that when clicked, leads the user to a website where the thieves then collect personal information.

A phishing attack happens when the cybercriminal lures a victim to a website that appears to be legitimate, but in fact is a front that tricks the victim into entering their personal information.

During these and other attacks, cyber criminals can infect your system with malicious code via email attachments, infected search engine results, and documents on social networking sites. They can also attack smartphones by corrupting otherwise legitimate apps that when installed, provide the criminals with access to the device and its information. They can even sometimes control the device remotely.

Protect Your Devices and Personal Information

The Federal Bureau of Investigation offers a number of tips to help protect yourself from cyber-attacks:

- Never divulge credit card information or other personal identifying information online or over the phone unless you initiate the communication.
- Regularly reconcile your financial statements and notify your bank of any discrepancies immediately.

109 State Street
2nd Floor
Boston, MA 02109

P 617.530.1010
F 857.265.2382
winthropwealth.com

- Monitor your online accounts regularly, reporting unauthorized transactions to your bank, credit card company, and law enforcement.
- Review your credit report annually, notifying the credit bureau in writing if you discover any questionable entries.
- Report any instances of people receiving mail from financial institutions in the names of others to law enforcement.

If you discover that your identity has been compromised, ask the credit bureau to enter that information into your credit report.

Finally, review any solicitation from an email or text message for you to update your personal information, activate an account, or enter your personal information. Be careful, too, when downloading any attachment or file from the Internet. And make sure that your computers are protected with cybersecurity software.

This material was prepared by LPL Financial, LLC.