Cybersecurity: How to Protect Yourself Against Identity Theft

westwoodgroup.com/insight/cybersecurity-how-to-protect-yourself-against-identity-theft/

Be cyber secure. Protect yourself against identity theft.

Cyber-crimes are on the rise, and Texas is a major target. According to the FBI's 2018 Internet Crime Report, email scams designed to get the victim to wire a payment through their personal or business account, along with other internet-based crimes, have continued to rise in recent years, and the crooks are continually devising more sophisticated strategies. In 2018 alone, email related reported crimes yielded losses of nearly $1.3 billion. As reference, one expert said that only ~15% to 20% of these crimes are reported. Texas, unfortunately, ranks high in the internet crime statistics, coming in at No. 2 in terms of victims per state (25,589) and No. 3 for reported losses ($196M) in 2018. The problem is real.

The question is, what can we do about it?

1

Be alert.

Don’t be fooled into the idea that it won’t happen to you. Thieves target people with good credit and money and those without, including youth. In fact, in 2018, there were nearly 10,000 internet crime victims under age 20. The continual news about data breaches may make it seem inevitable, and since there are so many breaches, there are questions around just exactly what these criminals are trying to accomplish. There are many different schemes designed to collect personal information to access, or steal, money, sell someone’s identity on the black market or commit either fraud or criminal acts with a victim’s identity.

2

The best offense is a good defense.

The best way to defend against these crimes is to monitor your accounts and your credit rating. Keep an eye on your accounts for unusual activity, and pull your credit at least annually to make sure there are no suspicious changes. Be sure to only use one of the three official credit bureaus (Equifax, Experian and TransUnion) to access your free annual report. You are allowed one free credit report from each agency. If you want to check your credit report three times a year for free, consider requesting a report from one agency every four months. Many times, identity theft victims have no idea that they’ve been compromised for months or even years. They find out when they are working on a financial transaction, or worse yet, when a collection agency calls, demanding payment.

3

Practice password hygiene.

Managing passwords can seem like it has taken on a life of its own with all the directives: *Don’t use the same password repeatedly! Replicate a sentence not just a word (G1veMe@ccess)! Use numbers, letters and symbols! Change your password every three months!* and so on. These are important, especially for financial accounts or other places where you store, keep or manage sensitive information. Many people have found that password vaults, software programs that store passwords in a secure location, are handy and remember, you can always reset a password if you forget it. Further, many organizations are now using multi-factor authentication, which requires the user to log in with credentials and verify their identity in some other way as well, either via the Internet Protocol (IP) address on their device, by answering security questions or by entering a code sent to a secondary means of contact, such as a mobile phone. You should also consider providing a trusted individual access to your online passwords in the event you become incapacitated.

4

Click smart.

Think twice before clicking on links or attachments in an email or text. If possible, navigate to a site through your browser, instead. For example, if you receive a message from Amazon that you need to log in to check on an order or change a payment method, go to your browser, type www.amazon.com and log in there. Similarly, if you receive a call requesting sensitive information, decline and call the company directly using a phone number that you know is valid.

5

Plan your plug-in.

Be careful with jump drives or other USB plug-ins, which could contain malware. Also, at the airport or other public spaces, consider plugging in “old school” vs. using the USB, as there have been instances of tampering with the USB “outlets” and criminals have contaminating devices, allowing them to track credentials and gain access to private information.

6

Keep it secure.

Lock your device(s), or any drive containing sensitive information, especially when you are in public. Similarly, avoid banking or other transactions (including shopping) unless you are on your personal device and you are connected to a network that you trust. Free or public Wi-Fi is notoriously suspect.

7

Share smart.

Before you share on social media, consider what could happen if it gets into the wrong hands. Friends’ accounts can be compromised, or you could accidentally connect to someone who is a criminal. Sharing information about being away for extended periods, your habits — work, school or details about your children or grandchildren — could put you and your family at risk.

8

Shred it.

Keep a separate bin for any materials with sensitive information. Set up a system to use a cross-cut shredder to shred this information on a semi-annual basis, before you toss it. Thieves have been known to dig through people’s trash looking for billing and account details, receipts, and birthdate and address information.

Learn the lingo

Phishing – Email that is designed to trick you into providing sensitive information, often replicating a website for an institution you trust in hopes you'll enter your login credentials.

Vishing – Voice calls impersonating a trusted institution seeking information.

Smishing – Text messages requesting you share personal details.

Hacking – The installation of malware or programs that can log your keystrokes and other computing history, compromising your data security without you ever suspecting wrongdoing.

Juice jacking – Criminals altering public USB ports to collect information or install malware providing access to texts, emails and other personal communications. Some security experts have likened using public USB ports to using a toothbrush you've found on the side of the road.

Source: Forbes

Sheana Suek
Vice President, Marketing Strategist

The information contained herein represents the views of Westwood Holdings Group, Inc. at a specific point in time and is based on information believed to be reliable. No representation or warranty is made concerning the accuracy or completeness of any data compiled herein. Any statements non-factual in nature constitute only current opinion, which is subject to change. Any statements concerning financial market trends are based on current market conditions, which will fluctuate. Past performance is not indicative of future results. All information provided herein is for informational purposes only and is not intended to be, and should not be interpreted as, an offer, solicitation, or recommendation to buy or sell or otherwise invest in any of the securities/sectors/countries that may be mentioned.