The Investment Letter

Volume 89, No. 7 July 2018

An Ounce of Prevention is Worth a Pound of Cure

Cybersecurity 101: What to Watch for and How to Protect Yourself

Last month alone,we received panicked calls from three different clients who had become potential victims of cyber-theft. One client had his email hacked. The hacker obtained personal information, ghosted his email and then requested a wire transfer. A second called when his computer locked up and he received a call from a remote technology company claiming to be able to offer help. Instead, they only made unauthorized withdrawals from his bank account. A third opened an email containing tracking software that stole confidential information contained on her computer. Additionally, someone attempted to open a cell phone account under my name. Fortunately, due to fast actions, none of these attempts were successful.

Identity theft, perhaps the gravest personal risk to arise from cybersecurity attacks, resulted in $16 billion in stolen assets in the US in 2016, and impacted some 154 million people. And the attacks are growing larger and more frequent; cases of identity theft increased 16% between 2015 and 2016. Identity theft doesn't always mean someone is out there in the real world with a pocketful of fake IDs with your name on them. Identity theft also happens when someone hacks into one of your bank, email or social media accounts and pretends to be you.

Money motivates. Wherever thieves discern the possibility of financial gain, they will invest their time and effort into chasing it. They use a whole toolbox worth of methods to access your private information:

Password Cracking - Password cracking represents a common threat in the cybersecurity landscape. A form of identity theft, password cracking happens when thieves guess your password. Armed with your password, the key to assume your online rights, they enter the system and cause mischief, or worse, start stealing. Either results in costly lessons.

Viruses - Computer viruses, like biological ones, reproduce by distributing copies of themselves. They're also stealthy, and are often hard to detect before they cause harm. Viruses hide in computer files and arrive in any number of ways, e.g., through social media messaging, emails, texts, or they may even be activated when you load a web page.

Ransomware - Ransomware locks you out of your machine, and away from your data. Ransomware works much the same as if someone places a lock on your bicycle while you're away. You come back, ready to ride to your next destination, and you find yourself

trapped, and at the mercy of whoever placed the lock on your bike, or, at least someone who knows how to remove it. Ransomware demands payment to restore access to your machine. Alternatively, you can bring your machine to a specialist for costly repairs that may imperil some or all your data.

Phishing - In the last two months, my wife has received bogus (but authentic-looking) receipts from Apple, Facebook messages from someone pretending to be her sister, and emails from scammers pretending to be our bank. All of these bogus communications emerge with one malicious objective – someone is phishing for confidential financial information so they can obtain access to assets that aren't theirs.

Trojan Horses - Trojans arrive seemingly as a gift, and potentially from the hacked email or social media account of a trusted friend or colleague. The victim downloads the file or program and activates it, installing the Trojan on his or her machine. Once installed, Trojans allow cybercriminals to watch their victims' actions; steal, delete, or share their confidential data; and open the gates to their systems.

Protecting Yourself from Cybercrime: Be Vigilant

When something doesn't seem right, take a deep breath and act with care. The time you spend now may save much more later.

Suspicious communications can sometimes be spotted upon arrival. Emails from Not-Apple are missing key information, e.g., my billing address and the last four digits of my credit card. Also, the sender's email address is never an Apple.com domain. Those phishing Facebook messages from my not-sister-in-law never read quite right. She's not an English language learner, has lived in Chicago her entire life and we've never had a conversation with her regarding get-rich-quick schemes.

Scammers build your trust before you realize what's happening. They send links or attachments that install malware on your computer. They spoof your trusted friends and businesses, even sometimes creating fake log-in screens to capture your ID and password.

The Do's and Don'ts of Cybersecurity – A Primer

Do's

- Use strong, complex passwords to help protect your online identity. Use combinations of letters, numbers, and special characters. Change your password often and avoid using the same password on multiple accounts.
- Answer security questions with responses that only you would know. Avoid responses easily gleaned from publicly available information.
- Get a good antivirus/anti-spyware program, and subscribe to automatic updates. Keep your browser up-to-date too.
- When installing software from the internet – know what it is and what it does. Installing Adobe Acrobat so you can open .pdf files is okay. Installing software sent via Instant Messenger or email from someone pretending to be your friend is not.
- Consider a firewall, which allows you to control the flow of information between your computer and network. Firewalls help hide your computer from scammers too.

Don'ts

- Don't create passwords using your name or the name of a family member. Don't use birthdates or words found in the dictionary. Also, don't use letter or number sequences that are easily guessed.
- Don't post the answers to your security questions to social media quizzes that ask for this information. It's fun to reminisce about your childhood phone number or the name of your first-grade teacher, but cybercriminals have been known to mine these responses for potential security question answers that they can use to reset your password.
- Don't try to save money by letting your anti-malware subscriptions lapse. The money you save now may cost you much more later.
- Don't click on links embedded into emails, or on attachments that look suspicious.
- When you receive an email seeking your personal information, don't reply, or, if it appears to come from a trusted source, call to verify.

Lastly, and perhaps most importantly, monitor your credit. Under federal law, you're allowed one free credit report per year from each of the national credit reporting agencies.

We subscribe to LifeLock.com for credit monitoring and Keeper.com for password security. We encourage you to consider doing the same.

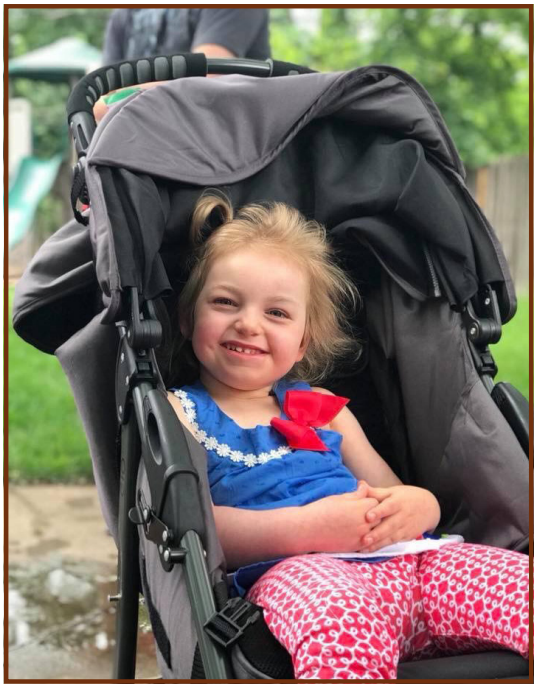
All malware creates mischief – sometimes for profit, sometimes just to ruin someone's day. However, vigilance, common sense, and some money spent now may save you much more later if you become a victim of a cybersecurity attack. ■

Investment Counsel News

Inside the Office

As further protection for your portfolio, we have implemented a new policy that requires us to call you for a verbal confirmation before we will execute any withdrawal or transfer request.

Outside the Office



Dorothy participated in the 2018 Metro Detroit Summer Stroll for Epilepsy. Her granddaughter, Abby, is pictured here.