Don't be a CyberVictim

By Claire E. Toth, JD, MLT, CFP™
Point View Wealth Management, Inc.
ctoth@ptview.com
(908) 598-1717

Edward Snowden and the NSA leaks may have grabbed most of last year's cyber security headlines, but in personal finance terms, we should have been far more concerned about data breaches at retailers like Target and Neiman-Marcus. Data theft grows ever more sophisticated. Although there is no guaranteed way to protect yourself, your information, and your accounts, there are steps you can take to make yourself a less attractive target and to limit the damage should you be hacked.

Cybercrime breaks into three principal categories: malware, phishing, and social media mining. Criminals often use a combination of these to steal from investors.

Malware is short for malicious software. The victim may innocently click on a link in a legitimate-looking email or web site; that installs the software on his system. The software may disrupt the computer's operation, gather sensitive data, or gain access to private computer systems. With phishing, a trustworthy-seeming email requests the recipient's personal data. Social engineering attempts to learn that information or access that data in social media websites and applications. These common attempts to steal your personal financial information are why you should never click on a link in an email, provide personal information in one, and be cognizant of what you share in social media.

Together, these crimes have resulted in the theft of untold millions, typically through wire or other electronic funds transfers. One recently-sentenced criminal used online data bases to identify likely victims, then moved onto social media sites to learn enough information about them to impersonate the victims in telephone calls to their banks. Using prepaid disposable cell phones, the crooks provided enough personal information to answer security questions and have at least $11 million wire transferred out of the country.

You can't guarantee you won't be the victim of cybercrime, just as you can't guarantee your car won't be stolen or your house won't be burglarized. Still, you can take concrete steps to protect yourself.

- Install a robust firewall and antivirus program—and keep them updated.
- Never click on a link in an email, even if you know and trust the sender. Instead, open that web browser and go to the site on your own. More and more, phishing emails look like the real thing. Even if it's your credit card company sending you the monthly email that your statement is ready, take the time to go to the website independently. This is particularly important with an urgent-sounding request. If you get an email that looks and smells like it's from your credit card company, warning you of potential fraud and inviting you to click on a link, don't. Go to your bookmarked website and contact the company through known channels. Better yet, pick up the phone and call the fraud department—the number is on the back of your card.
- Whenever possible, do not use your email address as part of a log-on. Your log-on and your password work together like a combination lock, and using your email gives away half the combination.

- If a website offers a third level of security—sending a text to your cell phone, or a stand-alone encryption device, take advantage of it. That third level makes your combination lock more robust.
- Particularly across your financial accounts and your email, use different, robust passwords. That way, if one account is compromised, the thief can't simply re-use your password to gain access to all of them. Change your passwords periodically, say every three months.
- The one place NOT to store passwords is in the notes section of your email account. Do that, and a thief who hacks your email now has access to every account you own. Clean out your email account often, to limit the amount of personal data in saved emails.
- Consider using a password aggregator/generator. There are several good ones, available either online or through anti-virus software. Not only can one of these store all your passwords securely across all your devices, but it can generate and save those painfully long and complicated secure passwords you know you should be using.
- Set up alerts on your financial accounts. For example, you can have your credit card company email you whenever there is a charge above a certain dollar amount, an overseas charge, or a charge without the card being present. This can help you nip cyber theft in the bud.
- While you're at it, check your accounts regularly, to be certain you recognize every transaction. Often cybercrime and identify theft begin with small charges to an account, on the theory that the owner isn't paying attention. Don't be that owner. If you look at your brokerage account every day, look at your bank account and your credit cards every day as well.
- Check your credit history regularly. You can review yours annually, for free, at https://www.annualcreditreport.com. (If you are reading this article on line, don't click the link—type it into your browser window yourself!) There are three credit reporting agencies, each with slightly different information. Consider reviewing one agency every four months, so reviews are more frequent than looking at all of them once a year—you are looking for inaccurate information or accounts you do not recognize. If a credit card has been used fraudulently, you can place a ninety day fraud alert on your credit files and receive new reports for free. The fraud alert prevents anyone from accessing your credit files without your consent, reducing the likelihood that a criminal can open an account in your name.
- If you are requesting an unusual money move, don't do it by email. Plenty of fraudulent emails exist, asking for wire transfers to third parties. They're growing more sophisticated, and investment professionals are on high alert. A conscientious investment professional won't initiate a third party wire transfer without speaking to you personally anyway, so pick up the phone yourself and speak to someone you know. If you begin your request with an email, and that conscientious investment professional can't reach you immediately by phone, he or she may respond by restricting your accounts, to prevent an unauthorized transfer.
- Limit your social media sharing. Just as we've learned not to trust that Nigerian email, criminals have likewise grown more sophisticated. Many of them mine personal information from our social media accounts, allowing them to target genuine-sounding emails to our online friends or to contact financial institutions. Some of these criminals have hacked cell phone numbers as well, forwarding calls to burner phones manned by people with that mined personal information, sometimes successfully appeasing anyone who phones to confirm the unusual email.

- On the subject of cell phones—be certain yours is password-secured, and opt for the complicated password, instead of the four-digit default. Set the phone to time out and require a new log in after five or fifteen minutes of inactivity. Keep the phone's operating system updated as well.
- Almost all cell phones support some sort of remote locking/wiping application. Be sure your phone has one and that you know how to use it. Many of these applications can also help you find a misplaced phone.
- Be wary of both apps and Wi-Fi hotspots, both of which can mask criminal activity that infiltrates your smartphone. Read reviews of new apps before downloading, and verify the legitimacy of your hotspot.
- If you suspect any of your personal information has been compromised, have an IT professional scrub your computer as part of your response, to ferret out any malware or worms.