WALDRON
Private Wealth

OnePaper

WHAT ARE SOME BASIC STEPS I CAN TAKE TO PROTECT MY PERSONAL INFORMATION ONLINE?

By John Waldron, Founder & CEO, and Ryan Fortier, Director - Operations

In recent years, cyber crime has evolved from scenarios involving individual hackers with specific pet projects to highly profitable, organized criminal organizations with detailed processes and best practices.

Financial institutions are required to maintain strict protocols to protect the data of their clients, but the clients themselves are under no such regulations and are often the most vulnerable access points for criminals to target. As a result, protecting your online presence has changed from a good thing to try to do, to an absolute necessity.

While there are many steps individuals can take to protect themselves online, we will provide guidance on a few of the most effective.

Strengthen your passwords: For how many sites do you use the same password, or a slight variation of the same password? Too many. How often do you change that password? Never. How long or complex is your password? (Hint: Your dog's name is not complex or long enough).

A simple way to solve this ever-growing password problem is to take a different approach: Use a password manager. Using a secure password manager allows you to have different, complex passwords for every online account, while requiring you to remember only one. As you can see below, a password does not have to be difficult to remember to be secure.

Using a password manager is a simple and inexpensive way to keep your online accounts organized and more secure.

Password	Password Strength*
Lassie	Weak
1AsD#$*@j2	Medium
My favorite food is pasta.	Strong
My #1 food is pasta.	Best

*According to Microsoft's Password Strength Checker

Also, make sure that your home Wi-Fi network is secured with a complex password. Most broadband companies now issue unique secure passwords with each new router, but if you haven't changed or upgraded your service recently, you could still be using a generic default Wi-Fi password. This could easily give a hacker access to your network.

Don't click the link: The easiest way for cyber criminals to gain access to your computer, and thus your personal information, is to get you to click a link in an email. It is no longer a safe assumption that if you receive an email from someone you know, that the email is legitimate. Hackers may have compromised the sender's account and may be impersonating his or her email address. Don't be click happy. Slow down and read the email, and make sure it makes sense. Were you expecting this email? Are there misspellings? Are there attachments that the sender is asking you to open that you were not expecting?

Educate yourself: Find a training session through a trusted service provider. Increasing your awareness is invaluable to your cyber defense. Educating yourself about the current methods cyber criminals are employing will give you a much better chance of identifying and avoiding these techniques. Here are some methods criminals are currently employing:

a. Phishing – a non-targeted email designed to get you to click a link so they can steal your information. Theory: Cast a wide net, you will catch some fish.

b. Spear phishing – a targeted email that appears to be from an individual or business that you know. Hackers may conduct limited research to create a more legitimate email thereby increasing the chances of you clicking it. They may combine this technique with spoofing.

c. Spoofing – changing the "from" and/or "reply to" address of an email to impersonate a real email address. At first glance, the receiver will not recognize that it is a bad email.

d. Malware -software that is intended to damage or disable computers and computer systems. Malware is normally delivered through a bad link on a website or in an email.

e. Virus - a piece of code that is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.

f. Social engineering – under the cover of a false pretense, convincing the user to follow precise steps which will allow the thief to access the information he or she is seeking.

A great, free resource for cybersecurity education is the *OUCH! Newsletter* at www.securingthehuman.org. *OUCH!* provides up-to-date information about protecting your cyber presence, as well as that of other important people in your life, such as less tech savvy parents, or children who may be extensive users of technology, but largely unaware of the security risks. It is written by security experts from around the globe, but in language that is easy to comprehend.

Stay updated: Make sure that you are running a supported operating system on your computer and that the operating system is receiving regular security updates (e.g. Windows XP is no longer supported. Windows 7 support will end on January 14th, 2020). Always keep your anti-virus software updated as well, to ensure that it has the latest library of virus definitions. And as the mobile world is outpacing the technology of desktops and laptops, you will want to take these same precautions with your mobile devices.

Segment Email Use: Similar to how most people have a business and a personal email address, you should have two personal email accounts, one "social", and the other strictly for "confidential information". Share your "social" email address with friends and family, but limit sharing your "confidential information" email address to medical and financial service providers. This way, if your social account is compromised the damage will be limited.

Back-ups: Create thorough back-ups to help you protect against the ever increasing probability that your system will be compromised. Even if a hacker isn't looking to steal your data, he or she may try to encrypt it and hold it hostage to extort a fee. While most of the time the hacker will provide encryption keys after you pay the fee, occasionally they won't. Also note that by paying the hacker, you are encouraging further criminal activity. The more frequently you back up your files, the better position you will be in, should your computer become compromised. DropBox and Google Drive offer simple cloud back-up solutions, or if you are interested in something more robust, PCMag.com has published a review of the top rated cloud storage services.

Credit Check/Credit Monitoring: At a minimum, you should pull your free annual credit report from each of the three main credit reporting agencies once a year. However, paying for credit monitoring services will provide you with nearly real time fraud warnings, and many of these services also include identity theft features which will help you overcome the damages caused should your identity be stolen. Often times if you are hacked, you might not find out until the criminal has already utilized your information for financial gain.

Although cyber security is a moving target, following these recommendations will put you and your data in a much safer position.

If you are a victim, report your crime by going to http://www.ic3.gov. This is a partnership between the FBI and the National White Collar Crime Center. The FBI is typically the best agency to report an internet complaint to because cyber crime typically crosses state lines.

With more than 30 years of wealth counseling experience, John's focus is on U.S. and international financial planning, and tax and investment management for high net worth and ultra-high net worth individuals. John is a well recognized leader and visionary in the wealth management industry. John serves on the Fidelity Institutional Wealth Services and Pershing Advisor Solutions Advisory Councils.

Ryan leads the operations team which is responsible for upholding Waldron's high standard for information security. Ryan's focus is on executing the firm's vision and continuing to enhance the client experience. He came to Waldron from The Boeing Company, where his main responsibility was the project management of testing military aircraft.