Chilton Trust

CYBERSECURITY:

Protecting Yourself & Your Family

By Sara B. Bernard & Katie Harrison

5 WAYS TO BOLSTER YOUR SECURITY

1.) PASSWORDS:
Your First Line of Defense

2.) EMAIL:
Always Be Suspicious

3.) PUBLIC INTERNET & WI-FI HOTSPOTS:
Prime Hacking Targets

4.) SYSTEMS & SOFTWARE:
Update, Update, Update!

5.) SOCIAL MEDIA & NETWORKS:
Think Before You Post

The rapid and ongoing advancements in technology and the interconnectedness of the devices we use on a regular basis have transformed the way we live and the ways we interact with each other. These innovations have meticulously and purposefully transformed our various technological devices into extensions of ourselves. Following suit with regards to pace and evolution, cybercrime has also continued to flourish, counterbalancing the convenience of these innovations, and ultimately posing serious threats to our security and the security of the world that we live in today. As a result, Chilton Trust devotes significant resources to maintaining the security of our networks, systems and software, including robust security for our email and online portal and app. We are committed to protecting our clients, and as part of this effort, we want to ensure that you are personally doing all that you can to protect yourselves and your families.

We have identified five key areas of vulnerability along with steps to help protect your confidential personal information and assets from potential threats.

1.) PASSWORDS: Your First Line of Defense

Create Strong Passwords: Get creative with your passwords. By focusing on dynamic combinations using all aspects of your keyboard (numbers, symbols, upper and lower case letters), passwords will do their job well. As most websites now require, passwords should be at least 20 characters and should never include personally identifiable information. Most, if not all of this information – your birthday, mother's maiden name, name of your first pet, place of birth – can be found instantly with a simple Google search. If it is easy for you, it is easy for hackers: use different passwords for each login rather than one across the board.

Secure your Passwords: First and foremost, you should not keep your passwords on a post it note (this also includes the "Notes" section on any of your devices). Rather, they should be stored in a secure and safe place. Secure password management tools, such as LastPass, have become highly regarded, as they help users to generate, store, organize, and encrypt their passwords to make it harder for hackers to compromise. These tools rely on one master password to grant access to other passwords, and as such, you should ensure that the master password includes the characteristics of a strong password. Using a phrase instead of a word – for example, "Where is Spot" – and run the words together, adding in symbols and numbers: "Wh3reIsSp@t", would significantly increase the strength of the password, versus using a one word password such as "@Spot13".

Two-Factor Authentication: This method of protection is extremely powerful, as anyone that attempts to sign into your account must go through a secondary layer of security. For example, if you are logging into your email, in order to fully log into your account, you must also enter a code that you would receive on your text message or through a verification code sent to a trusted device. This means that a hacker not only would have to have stolen your user ID and login, but they must also have possession of your phone or device. We recommend you turn two-factor authentication on for every app, program, and device where available.

Manage your Digital Legacy: Using a password service that will always be up-to-date, such as LastPass, can enable you to share your password within the App with your spouse or another trusted person so they have access to your digital presence upon your death. Alternatively, you could create a new email account and give the username and password to your executor; then, in a password service site such as LastPass, you could share the account details with this email address so no one else has access while you are living. Sites such as Legacy Locker and SecureSafe can also help in terms of identifying your online assets and login credentials to people who you trust to handle your online accounts after your death. In addition, you can create a digital will; however this requires keeping your digital asset information and up-to-date list of passwords on paper to be provided to your executor upon your death.

2.) EMAIL: Always Be Suspicious

Create Separate Email Accounts: Maintaining separate email accounts for business, friends and family, and for websites that require an email address in order to login will reduce your exposure to potential threats.

Share Smartly: Never email personal and sensitive information such as social security or credit card numbers.

Exercise Caution with Spam Emails: First, you should always utilize your spam filters as they will drastically reduce the risk of falling prey to malicious software and phishing scams received via email. Be mindful that email phishing scams have evolved and grown to be ever more cunning in this day and age. They often duplicate a legitimate website or service in order to grab your attention, altering a minor letter or character that a reader may easily overlook. Therefore, it is crucial that you verify the site's URL before you enter any personal information, password, or open any attachments. For example, bad actors may often direct you to a link such as this: microsoft.xyzdomain.com, rather than the correct and secure link of www.microsoft.com. Furthermore, as tempting as it may be, do not click the "Unsubscribe" link on your spam emails, as doing so could alert the spammers and potential bad actors that you are a "live" target.

Exercise Caution with Spam Emails: First, you should always utilize your spam filters as they will drastically reduce the risk of falling prey to malicious software and phishing scams received via email. Be mindful that email phishing scams have evolved and grown to be ever more cunning in this day and age. They often duplicate a legitimate website or service in order to grab your attention, altering a minor letter or character that a reader may easily overlook. Therefore, it is crucial that you verify the site's URL before you enter any personal information, password, or open any attachments. For example, bad actors may often direct you to a link such as this: microsoft.xyzdomain.com, rather than the correct and secure link of www.microsoft.com. Furthermore, as tempting as it may be, do not click the "Unsubscribe" link on your spam emails, as doing so could alert the spammers and potential bad actors that you are a "live" target.

3.) PUBLIC INTERNET & WI-FI HOTSPOTS: Prime Hacking Targets

Only Access Safe URLs: ALL secure websites start with https://, which stands for Hypertext Transfer Protocol Secure. URLs starting with simply "http" or "http://" allow harmful third parties to insert code onto the website, and should be avoided at all costs.

Be a Mindful Web Browser: Clear website cookies and internet browser histories frequently, and block ads and pop-ups whenever possible. When online banking, always log out after you have completed your task. Be cautious when downloading; do not download items from unsafe sites or unfamiliar links.

Perils of Public Wi-Fi or Wi-Fi Hotspots: Hacking can occur whenever and wherever there is internet. As one cyber security expert shared, "using public Wi-Fi is like walking through the airport barefoot". Hotspots and public Wi-Fi links have become very popular with cyber criminals. Alternatively, you should virtualize and secure your online access through a virtual private network service (VPN's). Virtual private networks create a virtual path to secure sensitive information, hide your identity, and establish a baseline level of security on public Wi-Fi.

Protect and Hide Your Home and Business Wifi: When you first set up your home or business Wifi network, be sure to immediately change the password given to you by the network company. Hackers can easily identify these generated passwords and gain access to the network as well as your personal information. As an additional precaution, take measures to hide your Service Set Identifier (SSID), also known as your network name, by configuring your router so that it does not appear publically.

4.) SYSTEMS & SOFTWARE: Update, Update, Update!

Don’t Wait to Update: The older your operating system, the more susceptible it will be to hackers targeting systems with vulnerabilities and security flaws. Use the latest version of the operating system of your choice (Microsoft, Windows, Apple, etc.), and when an update comes out, install the update immediately.

Keep All Your Smart Devices Up to Date: This includes devices not traditionally thought of as computers, such as your routers, smart appliances, smart TVs, and even Nest™ thermostats. Ensure you are setup to receive constant updates from the manufacturer.

5.) SOCIAL MEDIA & NETWORKS: Think Before You Post

Be Aware of What You Share: Social media continues to have a strong presence in our daily life, and it is virtually impossible to be hidden or invisible online. Hackers will do anything to obtain personally identifiable information (PII). It is important to recognize that everyone is a target, both children and parents. Hackers can befriend you or your children and easily gain access to an extraordinary amount of valuable information that could be used in attempt to gain greater access to you and your accounts. By using search engines, you can evaluate how much of your family’s personal information is public, and thereby determine how much intelligence a hacker may be able to gather online. You can use tools to evaluate you and your family’s social footprint, such as Maltego, which can help identify accessible information with the input of very basic personal information (i.e., name, address, email address, LinkedIn profile, Facebook profile). Once you are aware of how exposed you are, you can take steps to remove the information.

Chilton Trust is committed to helping protect you, your families, your privacy and your assets. As always, we are here to guide and assist you using our own internal robust resources along with external partnerships with experts in the field of Cyber Security. Please do not hesitate to reach out to us if we can help you engage in a thorough cyber security review of your digital assets.

Sara B. Bernard is a Vice President & Client Advisor at Chilton Trust Company. Ms. Bernard is an experienced relationship manager and wealth specialist, located in Chicago, who advises high net worth families, individuals, foundations and family offices. Ms. Bernard received her B.A. from the University of Virginia.

You may contact Sara B. Bernard at (646) 443-7860, or via email at sbernard@ChiltonTrust.com

Katie Harrison is an Associate Client Advisor at Chilton Trust Company. Ms. Harrison is located in New York, and works alongside experienced relationship managers and wealth specialists to advise high net worth families, individuals, foundations and family offices. Ms. Harrison received her B.A. from Yale University.

You may contact Katie Harrison at (646) 443-7834, or via email at kharrison@ChiltonTrust.com

Chilton Trust Company (together with Chilton Investment Services, its SEC-registered investment advisory affiliate, “Chilton Trust”) is a private, independent trust company to advise and provide wealth management, fiduciary and investment solutions to high net-worth individuals, families, trusts, foundations, endowments and other institutions. Chilton Trust was founded on the principles of service, expertise, trust and integrity. Chilton Trust offers full-service, bespoke investment management, open architecture advisory services, tailored asset allocation advice, family office, tax advisory and fiduciary services.

www.ChiltonTrustCompany.com

New York
300 Park Avenue
New York, NY 10022
Phone: (646) 443-7846

Palm Beach*
396 Royal Palm Way
Palm Beach, FL 33480
Phone: (561) 598-6330

Stamford
1290 East Main Street
Stamford, CT 06902
Phone:(203) 352-4000

*Fiduciary services may only be offered through the Palm Beach office.