CHILTON TRUST

Cybersecurity: Protecting Yourself & Your Family

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 from potential cyber threats.

Below are some basic tips and reminders to help lower your vulnerability and maintain awareness.

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 should do their job well. Passwords should ideally 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: You should not keep your passwords in a notebook or 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 and DashLane, have become highly regarded, as they generate, store, organize and encrypt passwords for you to make it harder for hackers to compromise. Dashlane, in particular, gives users the ability to change all secure passwords instantaneously with the click of a button, and allows for easy access and integration across all interfaces and corresponding iPhone/Android apps. Both providers rely on one master password to grant access to other passwords. You should therefore 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 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 online banking account through your email username, in order to fully gain access to your account, you must also enter a code that you would receive through a text message or through another 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.

2.) EMAILS & CALLS: Always Be Suspicious

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

Be Smart & Selective About the Information You Share: Never email personal and sensitive information such as social security or credit card numbers.

Exercise Caution with Spam Emails: Utilizing spam filters 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.

Always Be Aware of Strange Phone Numbers: Recently, there has been a preponderance of "spam" calls. These calls, often directed from numbers within your area code, attempt to trick you into sharing sensitive information over the phone. By pretending to be a representative from a service or cable provider that you use, these attackers will often ask you to verify your account information, claiming that your account has been "locked" or a "software update" is needed immediately. We advise that you ask for their number and contact information so that you can give them a call back on another line. This will allow you to confirm who you are speaking with, the number they are calling from, and will give you the time to verify the number they provided matches that of the generic help-line for the provider in question. In general, do not give away your personal information unless you have contacted the provider directly.

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://" (without the "s" for secure) 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 utilizing 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 (SSID10) 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 set up 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.

www.ChiltonTrustCompany.com

Charlotte	New York	Palm Beach	Stamford	Wilmington
5925 Carnegie Boulevard	300 Park Avenue	396 Royal Palm Way	1290 East Main Street	1105 North Market Street
Charlotte, NC 28209	New York, NY 10022	Palm Beach, FL 33480	Stamford, CT 06902	Wilmington, DE 19801
Phone: (980) 227-3101	Phone: (212) 843-6882	Phone: (561) 598-6330	Phone: (212) 843-6882	Phone: (302) 466-3501