TOP 5 CYBER PRACTICES TO KEEP YOU SAFE

People assume that staying safe from cyber hackers requires a lot of money. While spending money in the right area is important, common sense features costing little to no money and are the most effective defenses to thwart a cyber attack. Let's face it, no one is 100% safe from cyber hackers so each of us needs to be vigilant to protect our personal information. Below are some basic cyber practices that are easy to employ and do not break our wallet.

Passwords keep our private data private. This is completely in our control, yet every day people still create weak passwords that are simple to guess or hack. Creating long and strong passwords with a minimum of 14 characters that includes numbers, uppercase, lowercase and symbols is essential. Of course, the stronger the password is, the harder it is to hack, but also the more difficult it will become to remember. So don't write down and store your passwords on a sticky note on your keyboard. If you are guilty of this, try a password manager. It might just help you stay organized and secure. There are dozens of password managers available. I personally use and recommend Dashlane because it is secure, effective, and free. If you are old school, give PassowordsFast a try. It looks like a calculator but allows you to manually store all your login credentials on one device that cannot be connected to the internet or Wi-Fi. This might seem inconvenient but all data is encrypted and stays securely in your pocket.

One day on a whim, I tried to guess my friend's password by thinking about his favorite sport, hockey. I already knew his favorite player which he often talked about, so I decided to start from there. I was dumbfounded when on the first attempt, I was able to compromise his account. It is not uncommon for people to create easy, guessable passwords with common things they can

remember, but what happened next blew my mind. I decided to see if he was foolish enough to use the same password across multiple sites and he was! **Password reuse is one of the greatest problems in cybersecurity.** More than half of all Internet users reuse passwords across multiple sites. Don't believe me, ask a few colleagues if they ever reuse the same password across more than one site. You might be surprised by their answer. When a hacker compromises a user's password, the first thing they do is try that same password across multiple platforms looking for reuse. There are even tools available that automate the hacking process for reused passwords automatically as well as 'paste' sites where attackers publicly post the email addresses and passwords they've stolen. It's no mystery as to why at a web summit in Lisbon, Alex Stamos, Chief Security Officer at Facebook, declared "The reuse of passwords is the No. 1 cause of harm on the internet."

Don't be too social on social media. With all the catfishing and online fraud, you would think that people would be more wary of online strangers and connections but people are too trusting. Everything we post on social media is on the Internet, and thus, available to everyone, including hackers. Don't be too quick to 'Like' or Tweet something. Each interaction forms a digital footprint of the individual that can be used against them. All modern browsers provide private browsing modes. Use them for normal browsing to lessen your digital footprint. And if you don't trust Apple's or Google's privacy policies, consider a secure browser that does not collect cookies at all such as Duck Duck Go for truly anonymous browsing.

You know those annoying birthday questions and automated wishes from all of your connections? I recommend you lie about your birthday in order to make it more challenging for hackers trying to steal your ID or take credit out in your name. For example, I've posted my birthdate incorrectly across numerous social media sites so if or when a hacker calls a bank posing as me with my credentials and provides the wrong birthdate, the conversation is over. Always think twice before posting information that could be used against you. Social media implies that we share things freely and socially with our friends and colleagues but strangers lurking around or posing as our friends are the ones who truly benefit from that information.

It's ok to lie about your security challenge questions. Honesty is normally the best policy but that does not apply when we are asked a security challenge question such as 'What high school did you attend?' This is where I create a unique password or response that only I know. Why is it dangerous to answer honestly? Answers to some personal questions regarding high school, street names and pets are practically public knowledge thanks to the Internet and social media. A quick search can yield detailed results in seconds.

Stop clicking on those attachments. Phishing attacks are huge and cost individuals and companies over $5 billion dollars each year. So who falls for these scams? Every day over 80,000 people click on attachments in which malware and ransomware are then downloaded. Even with a good firewall, junk filter, spam filter, virus and malware software, there will be a small percentage of malicious email that still gets through. When going through email, take your time by hovering your mouse over any links embedded in the body of the email before clicking on it. Observe the link address to see if it looks weird and if so, DO NOT CLICK on it. Always type out the website address directly in the new browser window unless you are expecting a specific email from that source.

Also look for telltale signs such as poor spelling and grammatical errors as many hackers do not speak or write English as their primary language. If an email is asking for personal information such as your address, credit card or social security number, a red flag should immediately go up. Most email scams also invoke a sense of urgency, motivating the user to click before it is too late. And of

course, when the email is encouraging you to win 5 million dollars just by clicking and it seems to good to be true, then it is too good to be true.

Regularly update security patches. We have become accustomed to annoying reminders to update security patches to the point of numbness but that doesn't make them any less crucial. Next time you receive an update reminder, do not put it off until later. Take action and immediately update to the recommended security patch. The same holds true applications as well as (OS) Operating System updates.

The best way to stay safe on the Internet is to minimize the size of the targets on all of our backs. Hackers will never give up completely, but they will move onto easier targets. Stay Safe…