Eight Ways to Keep Hackers and Cyberthieves at Bay

Cyberfraudsters are working around the clock to devise new ways to steal what is rightfully yours. But you don't need to be their next victim. Late last year, Yahoo revealed a pair of massive data breaches from 2013 and 2014 that compromised more than 1.5 billion accounts.[1] While Yahoo accepted the blame, the incident cast a harsh light on a reality all too easy to ignore: Cyberfraud can victimize anyone at any time. And it's not going away anytime soon. In 2015, some 13.1 million U.S. consumers fell prey to online fraudsters at a cost of more than $15 billion.[2]However, the financial loss isn't necessarily the worst part. Recovering from identity theft can take six months and 200 hours of work, on average[3], often exacting its heaviest cost in the form of depression, sleep disorders, health issues and lost wages according to a study by the FINRA Investor Education Foundation. Admittedly, there are no ironclad ways to completely shield yourself from hackers, snoops and identity thieves. But there are actions you can take to significantly lower your risk. Consider the following:

1. **Choose a smart password.** When choosing a password, use the longest amount of characters possible, as the length of the password makes it harder to crack. Try using a phrase that only you can guess instead of a single word. Obvious though it may seem, "password" and "123456" are not smart passwords, yet they top the list of most common passwords year after year. To create a secure password, mix upper and lowercase letters, numbers and symbols – and don't use your child's birthday, your mother's maiden name or your Social Security number. Never use security questions that are common knowledge or easy for others to figure out. For instance, don't use information available in your social media profiles, like your pet or best friend's name.

2. **Keep your passwords to yourself.** Don't share your passwords with anyone. Also, never use public computers or unsecured Wi-Fi hotspots to log on to bank or investment accounts.

3. **Lock down your login.** While a complex password may effectively thwart most hackers, you can make it even harder to access your information by adding "strong authentication," such as the use of a fingerprint or a one-time code. These protections are available from a growing number of online services, retailers and financial services firms.

4. **Ignore and delete "ishers."** "Phishing" is a ruse aimed at stealing personal information or money through the use of fake emails purportedly from a legitimate business. If a suspicious but sort-of-official-looking email lands in your in-box, delete it without responding and never click on a link or attachment. Be similarly on guard against "vishing" and "smishing"- phone- and text-based attempts to steal your information.

5. **Inventory your wallet.** If your pocket were picked, your first move would probably be to cancel your credit cards, notify your bank and get your driver's license replaced. But can you be sure you'd remember every item and the numbers to call? Losing your wallet is traumatic enough without having to dig through old bills and account statements to straighten things out. To be prepared, go through your wallet card by card and record the information you would need to report your loss, such as account numbers, card expiration dates and fraud phone numbers. Keep a hard copy in a safe place; don't save the information to your computer.

6. **Shred first, then toss.** Identity thieves have many ways of accessing your personal information without even going online, from dumpster diving to purse snatching to mail theft. To avoid leaving a paper trail, shred sensitive documents and even junk mail and old bills before discarding.

7. **Don't leave your mobile device exposed.** Create a password for your home screen, download apps only from sources you trust, and update to the latest operating system as soon as it becomes available. That way you'll know you're getting the most current protection against malware – software programs designed to infiltrate your device and steal your information.

8. **Review account statements monthly.** Check account statements and healthcare benefits explanations as soon as they come in for fraudulent or questionable charges. The sooner you spot suspicious activity, the sooner you can report it and nip the problem in the bud.

Keep Your Kids Safe from Harm

Children may not even know what a credit card is, but they're a ripe target for fraudsters who are becoming increasingly adept at using a child's Social Security number to create a "synthetic identity" that can be used to apply for bank accounts, credit cards or loans. Furthermore, unlike adults who can quickly learn their identities have been stolen, for example, after being rejected for a credit card or loan, it can take years to discover a child has been a victim of identity theft. Fortunately, parents can proactively protect their children by contacting the major credit bureaus (Equifax, Experian, Innovis and TransUnion) and requesting a credit freeze for their child. That will block unauthorized credit inquiries, keeping fraudsters at bay and your child's identity safe.