N B
PRIVATE WEALTH

ANTHONY DeSANTIS
Chief Information Security Officer

Cybersecurity in Focus

Technology continues to heighten digital risks, but caution and common sense can go a long way toward protecting your information and accounts.

The headlines pop up almost daily. A bank, a retailer, a ticket reseller (or any number of other businesses) announces a data breach exposing the personal information of thousands, sometimes millions of people. It's probably a safe assumption that all of us have been caught in a breach at one time or another.

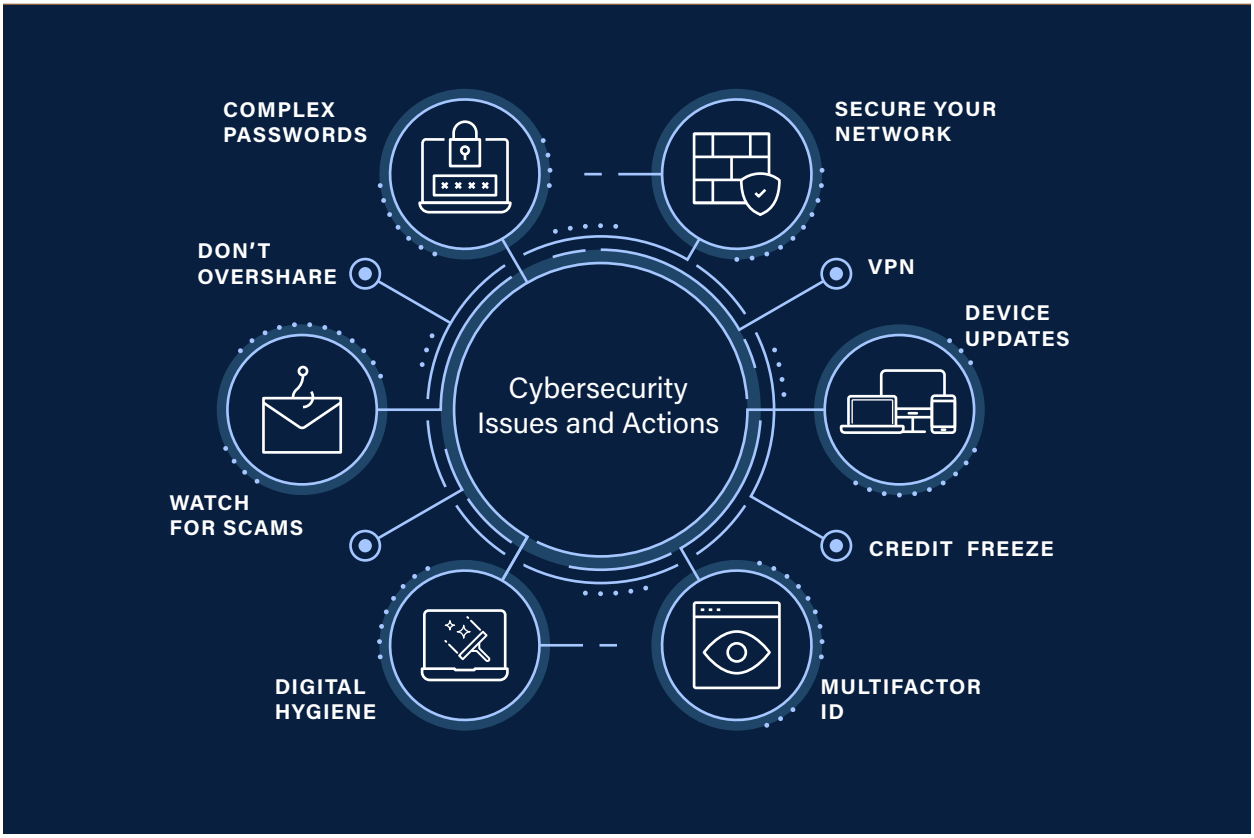
At the same time, the threat from con artists and other predators has only increased, as the tools at their disposal have become more effective and widespread. AI-powered algorithms are successfully sorting through millions of datasets to identify vulnerabilities. And while it was once easy to spot a fake "phishing" email—often riddled with typos and spelling mistakes—large language models are making it easier for bad actors to produce realistic, believable communications to manipulate potential victims. Cybercrime is a big business, which is estimated to reach an estimated $10.5 trillion in 2025.[1]

Fortunately, there are precautions you and your family can take to reduce exposure—some very easy and some more involved. How much you do is likely a personal decision, balancing your desire for both convenience and security.

Use Multifactor Identification. This is probably the most important step to protect your information and accounts, and you may be taking it already. It simply means that whenever you log into a financial website you receive a passcode (typically by text or email) to enter in order to access your account. Even if bad actors acquire your username and password, they can't get into your account without that passcode. Establishing multifactor ID for all your key accounts—including phone and email—can help seal off access to your information.

Bolster Your Passwords. Passwords can be hard to remember, so it's common to make them too basic or to use them across websites. Try creating long "passphrases" with multiple characters and numbers, and be sure to make them unique to each account you create. Crooks often take the username/password combinations obtained in a single data breach and run them against thousands of other websites. Using the password manager provided on your device or by a third-party vendor can help you avoid having to keep track of 100-plus different passwords. You can also just keep a written list—just be sure to keep it safe!

[1] Source: Cyber Ventures.



Freeze Your Credit. Ubiquitous online access has made the once onerous process of creating a credit alert or temporarily freezing your credit an easy process, via the websites of the three major credit bureaus. An alert warns lenders that they should take extra steps to verify your identity before granting credit; a "freeze" means that, even if your data is compromised, criminals will be unable to create an account in your name. If you need to apply for loan or to rent a car, you can unfreeze at a credit bureau and then re-freeze when you are finished. You can actually apply this principle to online accounts generally—turning them off and on at your convenience.

Safeguard Your Email. Your email account is a treasure trove of information for the digital criminal—often containing financial details, social security numbers, family information and much more. Most email traffic is encrypted in transit; rather, its presence on your computer or cloud servers is typically the issue. The defense mechanisms above (multifactor ID, password managers, etc.) apply to email, but you can consider taking another step: grooming your mailbox by deleting and/or archiving messages to a safer location.

Keep Your Devices Updated and Secure. One of the easiest ways to hack a computer or other device is to attack known security flaws where the owner has not uploaded software updates that would have fixed the issue. The more you keep your software up to date and the more sophisticated you make your computing environment, the less likely it is that this will happen to you. To bolster your defenses, consider purchasing security and/or antivirus software.

Protect Your Home Network. The router for your home WiFi network comes with a default password that is easy to decode, opening up your personal communications and data to outsiders. Be sure to customize the name of your WiFi network and set your own password to make this more difficult.

Be Wary of Public WiFi. Free networks at hotels and coffee shops are very convenient, but highly risky for users who don't have protection. Consider subscribing to virtual private network (VPN) service that creates a secure "tunnel" insulating your device from intrusion on public (or semipublic) WiFi. Be careful of rogue networks that may pretend to be affiliated with the hotel or other venues that you may frequent.

Curate Social Media. For better or worse, social media has become a central part of modern life, but carries certain risks. In our view, you should be careful about what you reveal online. Real-time location information and current vacation photos can alert criminals to when you may be away from your home. And excessive detail as to family members may set up you or a loved one for manipulation.

Watch for Scams. Especially with AI, email or text "phishing" attacks may look like they come from reliable senders, prompting you to click on links that expose your device to malware; unsolicited phone callers may ask for private information that can be sold or exploited. Be wary of urgent requests or offers that seem too good to be true. And stay alert for URLs that are similar to (with slight differences) a mainstream site. Rather than clicking on an email link, visit the provider website or call them independently. And never provide sensitive data like your Social Security number over the phone.

Secure Your Entire Family. When it comes to cybersecurity, family coordination is essential. As in a business organization, your security is only as strong as its weakest link. You should look to ensure that your whole family understands digital "hygiene," and maintains secure passwords, limits social media disclosures, updates computer software and is careful in clicking on questionable links.

Conclusion: Using Common Sense

At its most basic, effective digital security involves the same cautious approach that you might apply to safeguarding your home. Locks and alarms aren't foolproof, but they create a layer of obstacles that may encourage burglars to look elsewhere. Similarly, effective passwords, multifactor identification, timely software updates and general caution about sharing information can discourage cybercriminals. Be sure to check your account statements regularly. If they are compromised, you should act quickly to limit the damage—locking down credit and financial accounts as appropriate. That said, common sense precautions can go a long way toward securing your information and helping you enjoy the convenience of our digital age.

Resources

U.S. Cybersecurity & Infrastructure Security Agency: CIBA's website offers useful tips on securing your digital life at cisa.gov/secure-our-world.

Credit Bureaus: Contact each bureau individually to set up a credit freeze at Experian.com, Equifax.com and Transunion.com.

Annualcreditreport.com: Visit this website to receive your free credit report.

Identity Theft Resource Center: Offers assistance to identity theft victims, maintains breach database at www.idtheftcenter.org.

Haveibeenpwned.com: Find out if your email or passwords have been compromised in a data breach.

NEUBERGER BERMAN

1290 Avenue of the Americas
New York, NY 10104–0001
www.nbprivatewealth.com