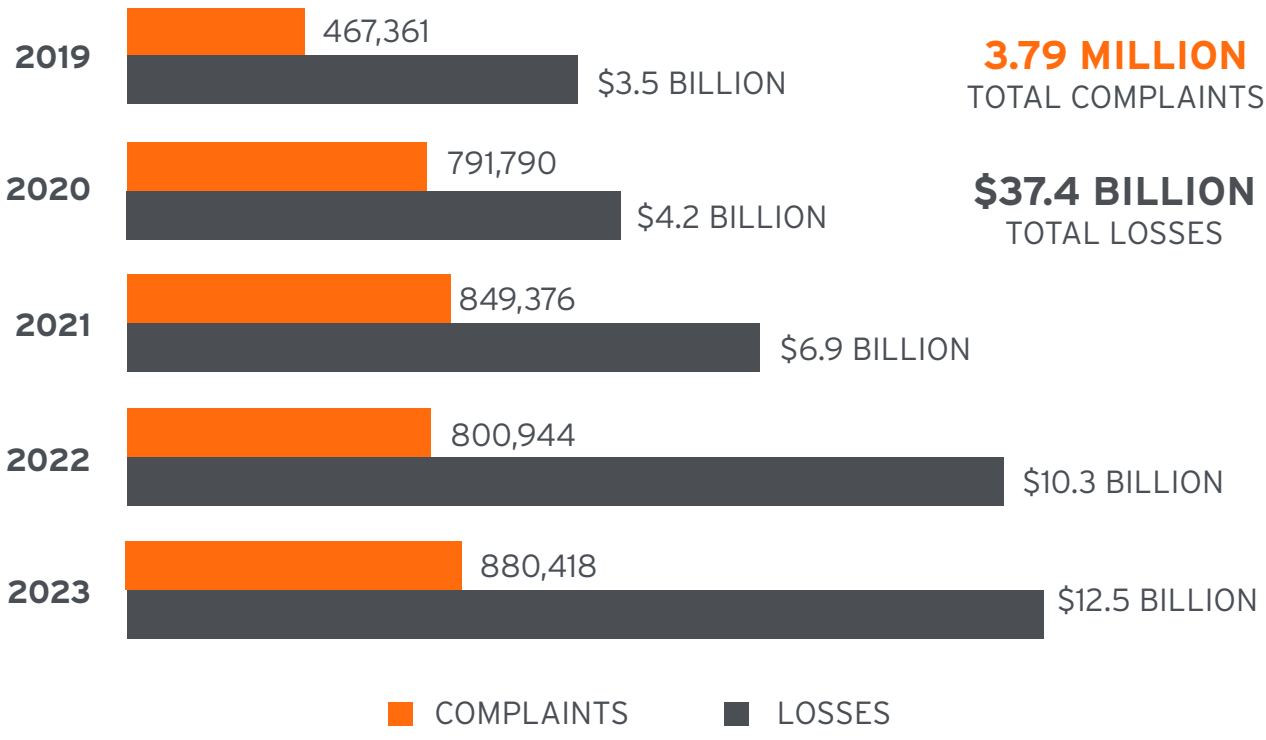
HIGHTOWER
Westchester

8 Practices to Protect Against Cybercrime

Cyber criminals are relentless. As individuals and businesses adopt new behaviors and technologies to stave off attacks, they evolve their techniques and find new targets. Highlighting this unfortunate trend – and perhaps, more optimistically, growing awareness around it – the FBI continued to receive a record number of cybercrime complaints in 2023, with potential losses exceeding $12.5 billion.[1]

COMPLAINTS AND LOSSES OVER THE LAST FIVE YEARS[1]



Source: Federal Bureau of Investigation Internet Crime Complaint Center. Accessed September 18, 2024

The good news is that a few relatively straightforward best practices can go a long way toward strengthening your cybersecurity defenses. Here are eight recommended by Sarah Khan, who, as chief information security officer for Hightower Advisors, helps protect advisor businesses and clients in one of the most highly targeted industries: financial services.

01

Use Strong, Unique Passwords and a Password Manager

Weak or reused passwords are one of the most common causes of cybercrime, leading to account takeovers, data breaches, and identity theft. Use long, complex, and unique passwords for every account. Implement a password manager to generate and securely store passwords. A compromised password from one account can expose many others, making strong, unique passwords essential for online safety.

02

Use multifactor authentication whenever possible

Usernames and passphrases are not enough to protect important accounts such as those for email, banking and social media. Strengthen the security of your online accounts by using multifactor authentication tools (MFA) — like biometrics, security keys or a unique, one-time code through an application on your phone.

03

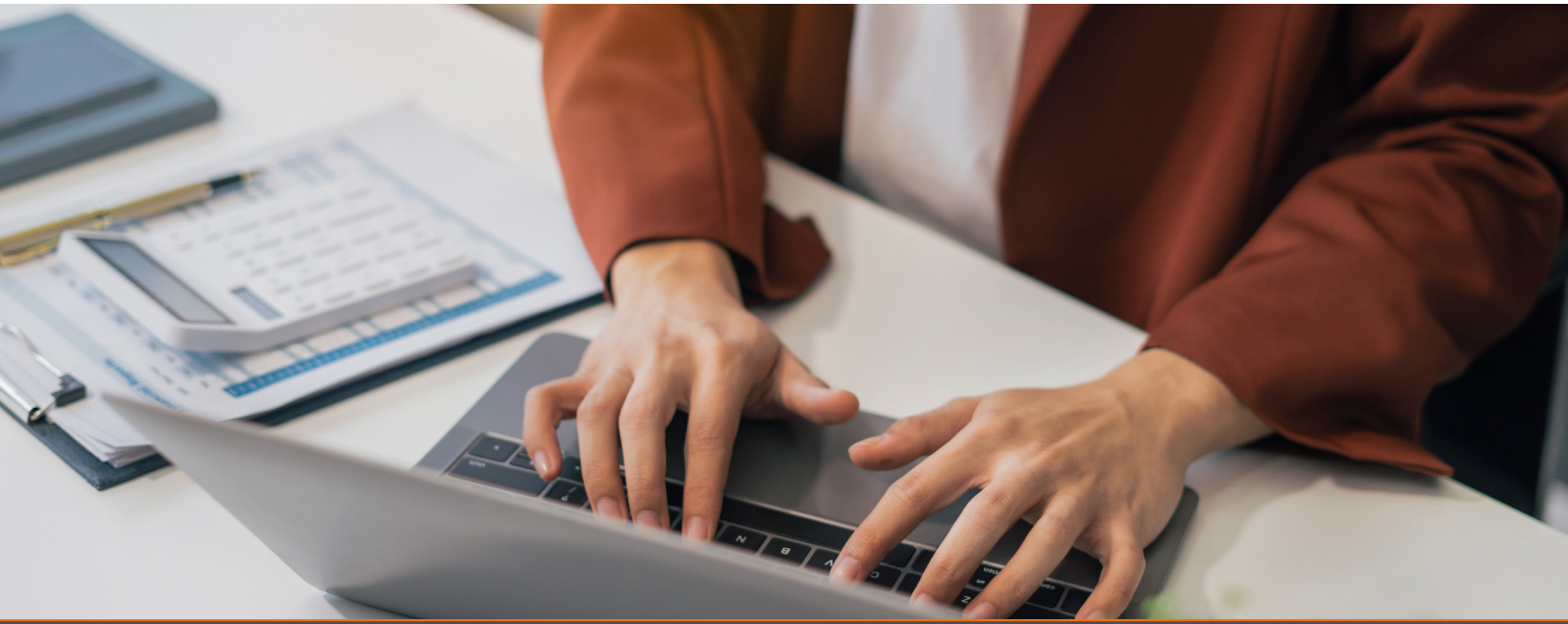
When in doubt, delete

Phishing attacks trick users into providing personal information or clicking malicious links, often leading to account takeovers or malware infections. Links in social media posts (and private messages), emails and online advertising are often how cybercriminals attempt to compromise your information. If there is any doubt in your mind about a link's security, even if you know the source, delete it, or mark it as junk.

04

Keep your machine clean

Cybercriminals use viruses, botnets, malware and spyware to infect or take over your machine. Use antivirus software to defend against these technical attacks; most new machines come with preinstalled antivirus software that you can trial and then purchase. Keep this software — and all other software on your internet-connected devices (and those of family members), including personal computers, phones and tablets — current to reduce risk of infection from cyberattacks.



05

Connect with caution

Avoid conducting any sensitive transactions, including purchases, when on a public Wi-Fi network. Unsecured public Wi-Fi networks can expose your data to cybercriminals, who can intercept your internet traffic or steal login information. Also, avoid using free charging stations in airports, hotels or other public places. Cybercriminals can use these public USB ports to introduce malware and monitoring software onto devices that access them.

06

Carefully select your online privacy settings

Companies and websites track your online activity. Ads, social media platforms and websites collect information about your location, browsing habits and more. The more information available and shared about you, the more vulnerable you become to cyberattacks. Keep this in mind and set the privacy and security settings on websites accordingly — based on your comfort level for information sharing and with the understanding that ultimately the best way to contain your personal information is by not sharing it in the first place.

07

Monitor Financial Accounts and Credit Reports

Cybercriminals may attempt to steal your identity or make unauthorized transactions using your financial information. Regularly check your bank accounts, credit card statements, and credit reports for any suspicious activity. Set up alerts for unusual transactions. Early detection of fraudulent activity can minimize financial loss and allow for faster responses to identity theft.

08

Back it up

Even the best computers and devices may become compromised and crash. Regular backups to an external hard drive and/or secure cloud provider will help you recover your valuable work, music, photos and other digital information in the aftermath of these stressful situations.

As the above practices highlight, cybercriminals may be relentless, but their methods can be thwarted with continual awareness and caution — while you still enjoy the many advantages offered by the digital age. Please also know that we are evolving our defenses to help keep your data safe as we communicate with you.

HIGHTOWER

Westchester

440 MAMARONECK AVENUE,
SUITE 506
HARRISON, NY 10528
(914) 825-8630
HIGHTOWERWESTCHESTER.COM

[1] Federal Bureau of Investigation: Internet Crime Report 2024. (2024). Federal Bureau of Investigation. Retrieved September 18, 2024, from https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

[2] FBI, "The Cyber Threat," retrieved from https://www.fbi.gov/investigate/cyber#What-You%20Should%20Know. Accessed September 9, 2023.