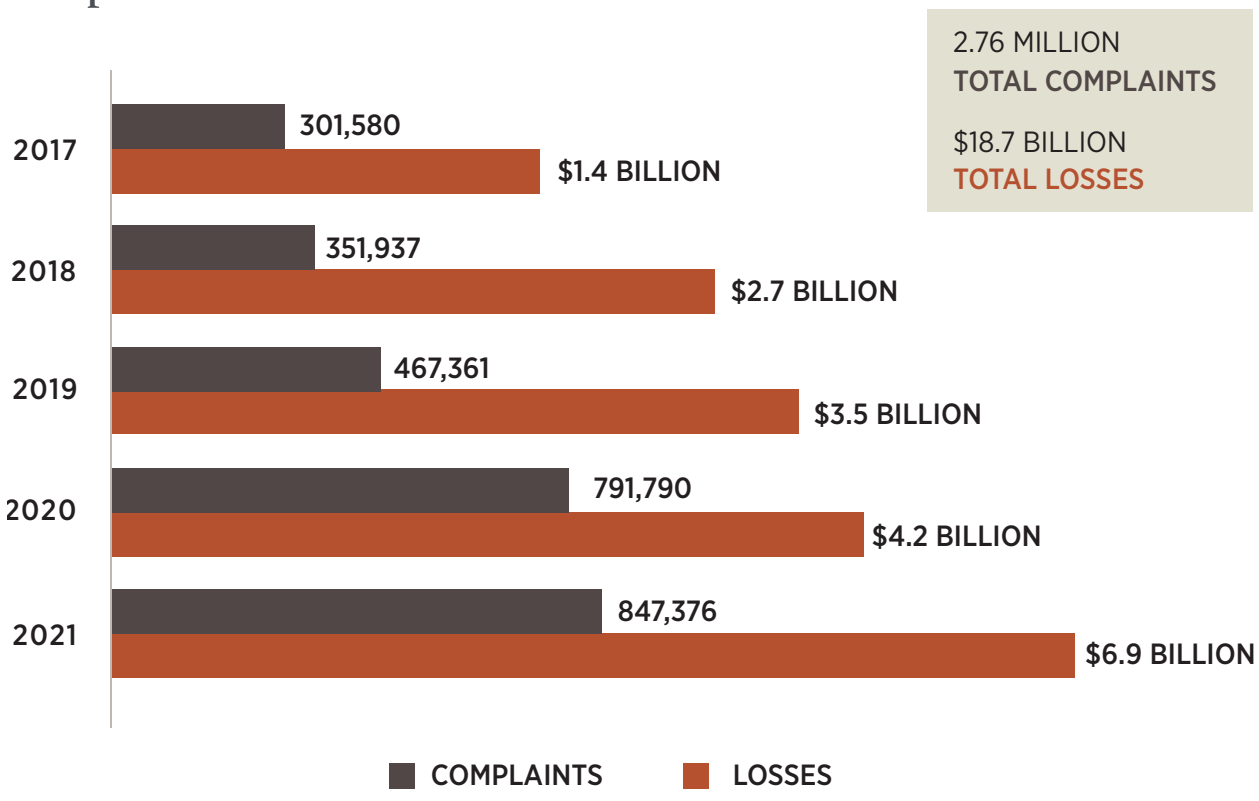
7 Practices to Protect Against Cyber Crime

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 2021, with potential losses exceeding $6.9 billion.[i]

FBI INTERNET CRIME COMPLAINT CENTER STATISTICS

Complaints and Losses over the Last Five Years



Source: Federal Bureau of Investigation Internet Crime Report 2021.

The good news is that a few relatively straightforward best practices can go a long way toward strengthening your cybersecurity defenses. Here are seven 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 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 — whenever offered.

02 | When in doubt, delete: 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.

03 | 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.

04 | Connect with caution: Avoid conducting any sensitive transactions, including purchases, when on a public Wi-Fi network. Also, avoid using free charging stations in airports, hotels or other public places. Cybercriminals use these public USB ports to introduce malware and monitoring software onto devices that access them.[ii]

04 | 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.

06 | Use caution on social media: Think before posting about yourself or others online. Consider what a post reveals, who might see it and how it might affect you or others. Encourage your family to do the same.

07 | 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 continually evolving our defenses to help keep your data safe as we communicate with you.

DISCLOSURES

[i] *Federal Bureau of Investigation Internet Crime Report 2021, retrieved from https://digitalguardian.com/blog/cybercrime-cost-us-69-billion-2021#:~:text=The%20FBI's%20annual%20look%20at,data%20breach%20statistics%20is%20out. Accessed September 8, 2022.*

[ii] *FBI, "The Cyber Threat," retrieved from https://www.fbi.gov/investigate/cyber#What-You%20Should%20Know. Accessed September 9, 2022.*