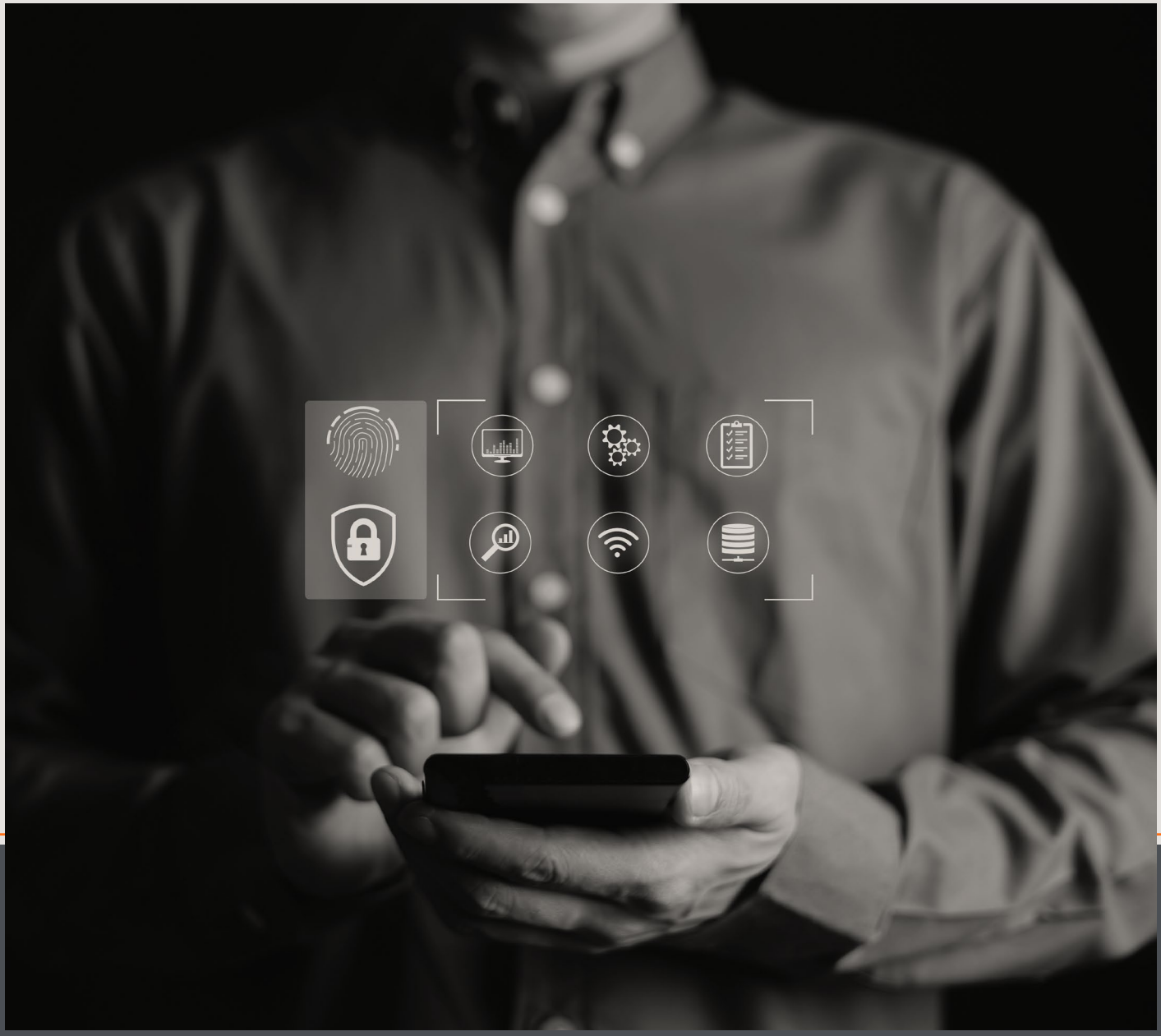
HIGHTOWER
Westchester



How to Defend Against Cybercrime

Cybercriminals are relentless. As individuals and businesses adopt new behaviors and technologies to stave off attacks, they evolve their techniques and find new targets. Losses from cybercrime continue to climb, with a record $10.3 billion in 2022 – which only includes those tracked by the FBI.[i] Actual losses are likely much higher.

FBI INTERNET CRIME COMPLAINT CENTER STATISTICS

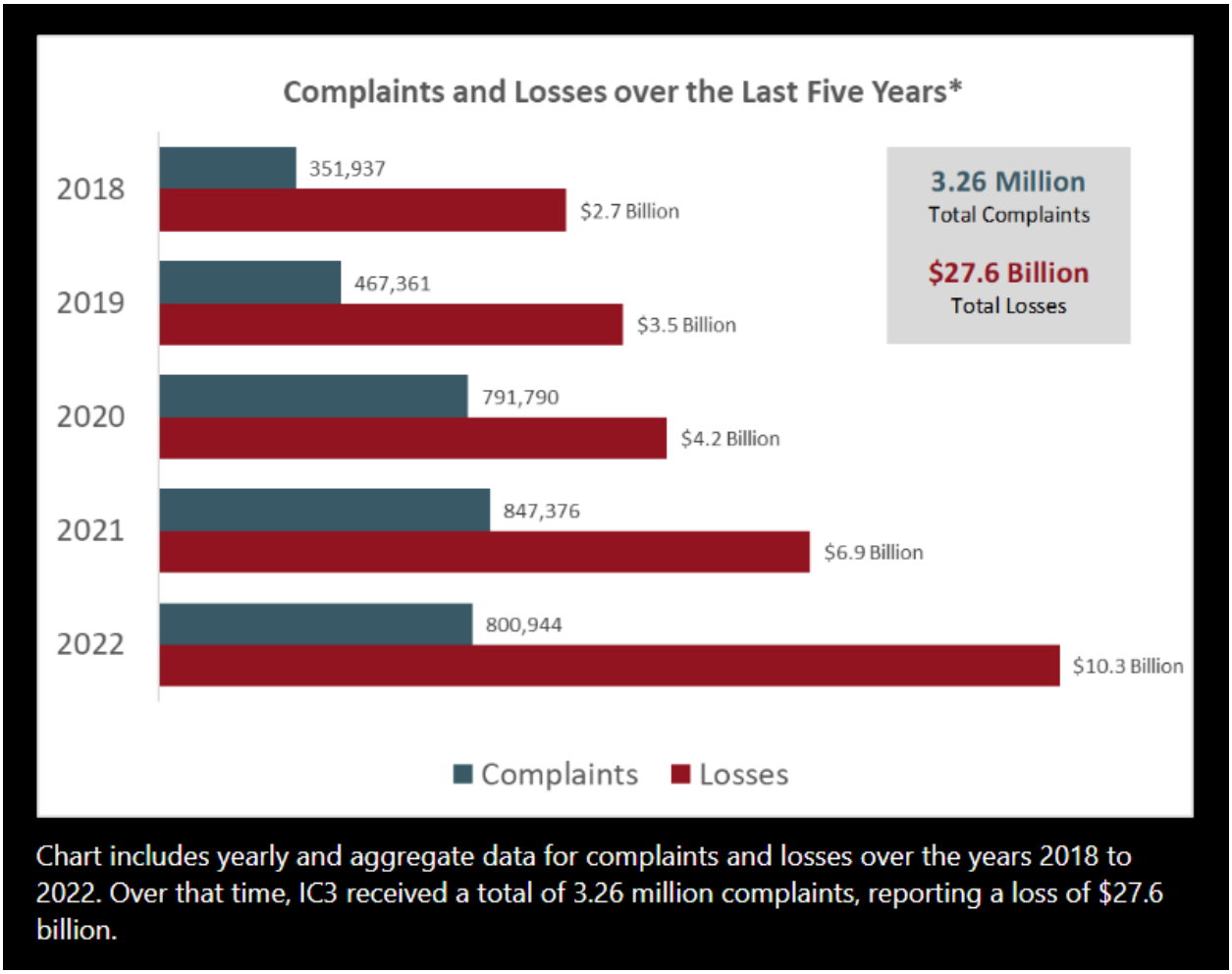


Chart includes yearly and aggregate data for complaints and losses over the years 2018 to 2022. Over that time, IC3 received a total of 3.26 million complaints, reporting a loss of $27.6 billion.

Source: Federal Bureau of Investigation Internet Crime Complaint Center. Accessed September 27, 2023.

The good news is that with education and a few relatively straightforward best practices, you can significantly strengthen your cybersecurity defenses. To that end, here are common scams to watch for and recommended best practices for avoiding them.

COMMON SCAMS

Though methods vary, cybercrimes usually share a common theme: The victim provides their personal information (either intentionally or unintentionally) with an unknown person or entity over the phone, on a computer or through a mobile device.

According to the U.S. Cybersecurity and Infrastructure Security Agency, here are some of the most common schemes criminals use to solicit information from their targets and how to minimize your risk of falling victim to them.[ii]

1 | EMAIL PHISHING

Cybercriminals design emails that mimic those coming from legitimate sources, including banks, government agencies and other services and businesses. They use these emails to collect personal and financial information and/or infect your device with malware or viruses.

Examples

- You receive an email that looks like it came from Amazon requiring immediate action to receive a refund. It includes Amazon's logo and at first glance appears legitimate, but if you hover over the Amazon.com link provided, you can see that it's not really Amazon's URL.
- You receive an email that looks like it came from your bank, warning that it will need to shut down your account unless you reconfirm your billing information. If you click on the link, it takes you to a bogus website designed to look like your bank's actual website.

How to Avoid

- Never input your login information through a link provided by an unsolicited email request.
- Never provide your personal information in response to an unsolicited email request.
- If you believe the request may be legitimate, contact the institution yourself.
- Never provide your password in response to an unsolicited email request.
- Never click on a link if you have any doubt about an email's legitimacy.

2 | IMPOSTER SCAMS

Criminals impersonate a government official, family member, colleague or friend asking you to wire money, often using personal information they have collected about you to sound more convincing.

Examples

- An IRS official calls you to warn that you owe back taxes but can avoid further penalties if you take care of the payment today over the phone.
- A friend of a friend who claims to have met you at a recent event in your community calls to ask you for a donation to a legitimate charity – she will match your donation if you provide your payment over the phone tonight.

How to Avoid

- Block unwanted calls or texts on your mobile or home phone.
- Do not answer calls from numbers you do not know.
- Never wire money — or provide a gift card — to someone you do not know.
- Never send money because someone contacted you, even if you feel like you might know the person or if the person says they are your friend or are related to you.
- If you find yourself on a suspicious phone call, hang up. If the person you spoke to claims to be calling from an institution, call back the official number for that institution.

3 | "YOU'VE WON" SCAMS

Cybercriminals email, call or text stating that you have won a prize, sweepstakes or lottery. You are told that to receive the prize, you must first pay a fee or tax. The call or message is usually full of congratulations and excitement.

Examples

- You receive an email that says you have won $2.5 million in the International Sweepstakes. The scammer claims to represent a legitimate sweepstakes, such as Publishers Clearing House. You are asked to pay a small fee via a link to cover processing and receive your winnings. The email provides assurance that the sweepstakes is safe and legitimate.
- You receive an email that appears to be from a relative stating that you have won a raffle. The relative asks you to reply with certain pieces of your financial information to collect your winnings.

How to Avoid

- Stop and think before you act. If an offer seems too good to be true, it likely is.
- Never pay a fee or provide personal information to collect winnings or a prize.
- Search online for the offer and contact from which it was received to see if there are any references to a scam.
- If a friend or family member sends or forwards you an offer via email or social media, confirm with them outside of email or social media that they really sent it.

4 | HEALTH CARE SCAMS

Criminals call, email or send a letter to promise big savings on your insurance, prescriptions or other health-care-related expenses. The communication usually requests your Medicare or insurance information, Social Security number or other pieces of personal information.

Examples

- You receive an email with the subject line of "Big Senior Discounts on Prescription Drugs," with a link to visit a new pharmacy offering low-cost drugs.
- You receive a text message that claims to be from Medicare. It says you may be eligible for a new 20% discount and asks you to follow a link to provide personal information to see if you qualify.

How to Avoid

- Stop and think before you act. Medicare and insurance companies will not reach out to you in this manner.
- Never provide personal or sensitive information in response to unsolicited communication.
- Search the promotion or offer online to see if there are any references to a scam.

5 | TECH SUPPORT SCAMS

Criminals call you or reach you via online popups and claim to be from a technology company contacting you to diagnose or fix a problem with your computer, software or other technology. The scammer is typically trying to gain remote access to your device or online account.

Examples

- A popup appears on your computer warning you that a virus has been detected. It asks you to contact a live technician at a provided phone number.
- Someone who says they work for Dell calls you claiming that they have detected an issue with your computer. They ask you to walk through certain steps with them to gain remote access to your device so that they can fix it.

How to Avoid

- Recognize that legitimate technology companies will not contact you by phone, email or text to inform you about a problem, nor by a popup that asks you to call them or click on a link.
- Never provide remote access to your computer to someone who contacts you unexpectedly.
- If you need help fixing your computer, device or other technologies, go directly to someone you trust.

6 | IDENTITY THEFT

Criminals use your personal information (e.g., your name, credit card number, Social Security number, etc.) to obtain money or credit. Usually this is made possible by the criminal obtaining multiple pieces of your information unbeknownst to you.

Examples

- Unauthorized charges show up on your credit card. A criminal has been able to make purchases by obtaining your credit card number and other personal information (e.g., your zip code).
- A criminal uses your personal information, including Social Security number, to file a fake tax return in your name and collect a refund.

How to Avoid

- Use multifactor authentication, do not respond to emails or other messages that ask for personal information and do not provide personal information on a computer in a public place.

- Physically secure personal identification (e.g., Social Security and Medicare cards) by keeping it in a safe place, shredding papers that contain it and retrieving your mail as soon as possible.
- Only provide your Social Security number to companies if absolutely necessary. Ask if you can use another type of identification.

BEST PRACTICES

Defending against cybercrime and identity theft also includes following best practices as you set up and interact with your devices, including:

1. Understand common signs of scams, including messages that:
   - Use subdomains (i.e., extra information added to a website's URL), misspelled URLs (e.g., amozon.com) or otherwise suspicious URLs
   - Claim to be from businesses or other organizations but use a public email address (e.g., Gmail)
   - Attempt to invoke fear or a sense of urgency
   - Request that you verify personal information, such as financial details or a password
   - Are poorly written with spelling or grammatical errors

2. 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 (MFA) tools — like biometrics, security keys or a unique, one-time code through an application on your phone — whenever offered.

3. Protect your phone number: Another common ploy of cybercriminals is to take control of your phone number. Once they do this, they can receive your incoming calls and messages, discover information about your contacts, and even access your private bank accounts. There are several ways to protect your phone number, such as setting a PIN for account access, using strong passwords on your phone and using additional safeguards your carrier may offer. Keeping your phone number protected also stops it from being used by hackers and spammers for robocalls.

4. 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.

5. 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.

6. **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.

7. **Adjust 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.

8. **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.

9. **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.

Vigilance Makes the Difference

As the above practices highlight, cybercriminals may be relentless, but their methods can be thwarted with continual awareness and caution. Please also know that we continue to evolve 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

[i] Federal Bureau of Investigation, Internet Crime Complaint Center (IC3), https://www.ic3.gov/. Accessed September 13, 2023.
[ii] U.S. Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/be-cyber-smart/common-scams. Accessed September 13, 2023.
[iii] FBI, "The Cyber Threat," retrieved from https://www.fbi.gov/investigate/cyber#What-You%20Should%20Know. Accessed September 9, 2023.