THE NORTHERN TRUST INSTITUTE

10 STEPS TO REDUCE YOUR RISK OF CYBER FRAUD

Reduce your risk significantly by adopting some basic best practices.

As the trend toward a more hybrid work environment has taken hold, cyber fraud has accelerated beyond an already-alarming rate. Government agencies, private companies and individuals are all potential targets of identity theft, transactional fraud and ransomware. Of 2.6 million fraud reports to the U.S. Federal Trade Commission, 24% reported a loss, which averaged $650, with older targets being impacted much more severely: $1,750 was taken from the average victim over 80, according to 2022 data from the agency.

And as the shift to cloud storage and quantum computing accelerates, security challenges will evolve. The following best practices will significantly increase the security surrounding your data, assets and overall online safety.

01 Continually Update Your Computer and Mobile Devices

Cybercriminals frequently gain access to information by using known flaws in the software and operating systems that run your computer or phone. The best defense is to keep software, web browsers, and operating systems up to date. This is the most effective measure you can take to protect your digital devices. Regularly updating your computer and mobile devices is crucial as it ensures that any known security flaws are patched, reducing the risk of exploitation by malicious actors. It prevents you from being a victim of a successful cyberattack.

Tip:

You can easily program your phone and computer to update automatically, effectively managing the patches for you. Here are instructions for iPhones and phones using Android and Microsoft operating systems.

02 Employ Antivirus Software and Anti-malware Protection on Your Computers

Cybercriminals also use technical attacks to deploy viruses, botnets, malware, keyloggers and spyware to infect or take control of your computer.

Many new computers come with a free trial of antivirus software preinstalled, which you can purchase once the trial is over. Additionally, there are hundreds of antivirus applications available in the market for you to choose from. Be sure to select software solutions that provide you adequate protection, keep them updated with the latest virus definitions, and schedule regular full scans, preferably at least once per week.

Tip:

Almost all internet service providers (ISP) offer a free subscription to antivirus software, as it is in their best interest to keep you secure. Check with your provider for download instructions, but keep in mind that free subscriptions may not be sufficient for small businesses, which may benefit from extra protection.

03 Use Good Password Habits

For each account, use the longest password permissible and update it regularly. Create strong passwords by combining uppercase and lowercase letters, unique characters

and numbers. Avoid including personal information in your passwords and never use the same password for multiple accounts. Don't write down your passwords on paper or share them with anyone. For mobile devices, set up a PIN (or passcode) or facial recognition setting and activate the auto-lock feature in your settings. When it comes to computers, consider maintaining multiple profiles, especially if you have younger children, as this allows you to apply restrictions to specific accounts.

Tip:

Be sure to enable multi-factor authentication (MFA) on all accounts that support it; this will add an extra layer of protection for your information. Whenever possible, always turn on MFA.

04 Strengthen Your Home Network

Malicious cyber actors may leverage your home network to gain access to personal, private and confidential information. To protect against these threats, start by setting a robust password for your Wi-Fi network and select the appropriate encryption, beginning with at least Wi-Fi Protected Access 2 (WPA2). Additionally, be sure to regularly update your router's software. It is also advisable to hide your network, keeping it concealed from unauthorized connections. To view a comprehensive guide regarding securing your home network, click here.

Tip:

You can purchase protection against cyberattacks for every internet-connected device in your home, including game consoles, smart TVs and appliances.

05 Protect Yourself from Phishing/Vishing Attacks

Phishing is when cybercriminals use deceptive emails or messages to trick you into revealing personal or financial information, while vishing involves fraudulent phone calls with the same goal. The best defense is staying vigilant. If you receive a request for personal or financial information from an unknown source, take a moment to verify their legitimacy. Contact the organization or individual directly through official channels to confirm the request's authenticity. Be cautious about clicking on links, opening attachments or sharing sensitive details.

Tip:

If you by accident click on a phishing link, here is what you should do.

06 Back Up the Data on Your Computer and Your Mobile Devices

Even the best machine or device may become compromised or crash. Backing up the data on your devices will help you recover your information in these situations. You can back up your information by regularly copying your files to an external hard drive, using cloud storage services or employing specialized backup software. These practices ensure that your data remains secure, easily recoverable, and protected against unexpected mishaps or device failures.

Tip:

You can now easily back up many mobile devices to the cloud storage space that is owned and hosted by a vendor such as Google, iCloud or Box. But use caution when sending financial information to cloud storage, which is more appropriate for photos, contacts and media. Learn more about cloud security from Norton, a leading digital security provider.

07 Talk to Your Children and Family About Internet Security

Young children are vulnerable to even the most basic of cyber tricks. Teenagers, while savvy, are online more frequently and often visit riskier sites, such as file sharing platforms for movies, videos and games. Older family members, on the other hand, often possess what cybercriminals are looking for: financial assets and limited digital knowledge. Encourage open dialogue to educate them about safe online practices, including the importance of strong passwords, recognizing malicious email attempts, and avoiding sharing personal information with strangers.

Tip:

Google, in partnership with iKeepSafe and The Net Safety Collaborative, has developed an online program that teaches children and families how to navigate the internet by learning the fundamentals of digital citizenship and safety.

08 Understand and Protect Against Identity Theft

Certain types of personal information can be used to commit fraud, such as account takeovers, unauthorized money transfers or new lines of credit opened in your name. This may result from malware on your computer, social engineering that tricks you into giving personal information over the phone or internet, or a thief stealing your mail or trash to access personally identifiable information. You can protect against identity theft by following several best practices — including shredding sensitive documents, avoiding interacting with suspicious links and attachments in your email, learning to recognize and block smishing attacks and reviewing your credit report on a regular basis.

Tip:

Opt in for electronic statements whenever possible to avoid the risk of stolen mail and eliminate the need for shredding.

Learn more about identity theft at usa.gov/identity-theft.

09 Know What To Do if You Become a Victim

If you discover that your information has been exposed, you may want to enable a fraud alert or a credit freeze on your credit information. A fraud alert on credit reports requires potential creditors to contact you and obtain permission to open new accounts or lines of credit. A security freeze may help block institutions or lenders from accessing your credit report, unless a pre-set PIN is provided to “thaw” the report, which prevents them from opening new accounts in your name.

Tip:

Consumers are entitled by law to receive a free credit report from each of the credit reporting bureaus once a year. Go to annualcreditreport.com or call 877-322-8228 and follow instructions to access your reports.

For more detail and additional actions to take after becoming a victim of identity theft, read the Federal Trade Commission's guidance.

10 Keep Control of Your Information

Be mindful of what you share online and with whom. Do not automatically provide social security numbers, account numbers, credit or debit card information or other highly sensitive information just because you are asked. Ensure that you only provide such details to trusted sources. When in doubt, verify the request first before proceeding. Regularly review your privacy settings on your online accounts to control who has access to your information.

Tip:

Organizations and businesses that request access to your social security number may not actually need it. Use alternative forms of identification whenever possible, and stay alert for medical, insurance or even tax fraud.

As the above best practices demonstrate, you do not need to be a technical expert to improve your security. But you do need to stay informed and adopt good habits. For additional education and other important steps to take, visit the Northern Trust Security Center.

Disclosures

This information is not intended to be and should not be treated as legal, investment, accounting or tax advice and is for informational purposes only. Readers, including professionals, should under no circumstances rely upon this information as a substitute for their own research or for obtaining specific legal, accounting or tax advice from their own counsel. All information discussed herein is current only as of the date appearing in this material and is subject to change at any time without notice.