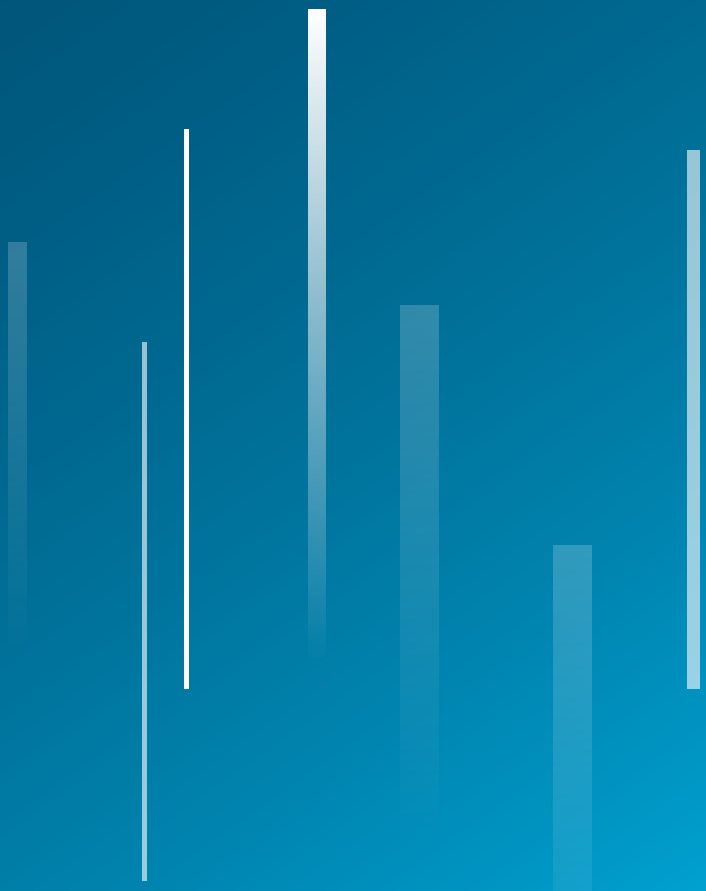
William Blair

Private Wealth Management
williamblair.com

Keeping Your Financial Information Secure
And Steps to Take if You Have Been Hacked

Explore our guide to help you keep your financial information secure, recognize digital risks, and identify next steps to take if your data has been compromised.

Always remain vigilant.
Regularly check your financial, personal, or sensitive accounts for any signs that someone else may be using your identity.



Introduction

As the world becomes more digitally connected, we encourage you to stay vigilant against the ever-present threat of identity theft and the many scams, hacks, and malware that can compromise your personal and financial information.

Your digital footprint includes all your online presence and activity—transactions, websites visited, postings on social media, digital communications, and comments on blogs and websites. Exposure to cyber risk increases every day as digital collection and storage of data continue to grow exponentially. In addition, the number of devices you use in your digital life now includes cell phones, laptops, and tablets; home security systems; appliances; technology-enabled cars; medical equipment; and more. Staying secure is of the utmost importance. Read more for next steps to take if your information has been compromised and how to protect your digital footprint.

Suspect You've Been Hacked? Here's What to Do

Best Practices for Keeping Your Financial Information Secure

Digital Risks

Suspect You've Been Hacked? Here's What to Do

Even if you follow precautions, fraudulent behavior or hacking can still occur. If you suspect that your personal or financial information has been compromised, you should act quickly to limit the damage and protect your rights.

Identity Theft

Account Access

If you still have access to your account, log in from a trusted computer and reset passwords with a new, unique password; set up multifactor authentication for all your online accounts if you have not already done so.

Contact Institutions

Contact any institution or company that is directly affected. If an online account is compromised, contact customer support. If there's a fraudulent charge on your credit card, call the card issuer to report it. If there's a fraudulent money transfer or activity, call the bank or financial institution. Use a trusted phone number, such as the one listed on the back of your credit card or on its website.

Email

If your email has been hacked, in addition to changing your password, verify that the active email account rules are the ones you have established. Fraudsters may try to set up rules in the compromised email account to divert emails to external accounts or hidden folders.

Inform Family & Friends

Let family and friends know that you have been hacked so they do not click on links fraudulently sent.

Fraud Alerts

If you haven't already done so, place a fraud alert on your credit reports by contacting one of the credit bureaus; the credit bureau will notify the other two.
Equifax Fraud Alerts
Experian Fraud Alerts
TransUnion Fraud Alerts

File a report with the Federal Trade Commission +1 877 438 4338 or *www.identitytheft.gov*.

Contact the Social Security Administration +1 800 772 1213 and/or the Internal Revenue Service +1 800 829 0433.

Contact your healthcare provider if your health insurance or medical records are involved.

File a report with your local police department.

Viruses on Devices

WiFi Connection

Disconnect your device from WiFi to stop hackers from accessing your computer remotely.

Computer Shutdown

Shut down your computer and contact your computer manufacturer's technology support by visiting its website.

Password Change

Change your passwords and set up multifactor authentication for all your online accounts, if possible.

Best Practices for Keeping Your Financial Information Secure

Sensitive Mail and Bills

Shred documents that contain personal or financial information.

Devices

Lock down devices when not in use.

Enable lock functions and passwords for each device, setting them to auto-lock.

Set up remote lock functionality and data wiping use.

Update your devices with new security software releases.

Activate biometric measures, like Face, Touch, or Voice ID.

Never plug your devices into public USB ports, always use your own charging block.

Passwords and Usernames

Use multifactor authentication whenever possible.

Use strong passwords and usernames with unique words/phrases; change them frequently; do not use your email as your username.

Do not save passwords in your web browser, phone notes apps, or a spreadsheet on your computer; do not share your passwords with others.

Do not use the same password for multiple accounts.

Consider using a password manager tool.

Networks

Avoid public WiFi whenever possible; use the hot spot on your mobile device or your wireless router; if you must use public WiFi, confirm the WiFi name with the operator of the property.

Use secure websites. Look for a lock icon or “http” in the address bar.

Install virtual private networks (VPNs) and antivirus software on your devices; install updates when released.

Make sure your home WiFi network is password-protected. Do not use the default password.

Avoid opening multiple browser windows while online in personal accounts; log out completely after a transaction or message.

Don’t allow internet cookies when loading new websites.

Best Practices for Keeping Your Financial Information Secure (continued)

Email

Think before you click on an unfamiliar link or attachment from an unknown contact.

Beware of emails requiring immediate attention or threatening circumstances.

Check emails alerting you of changes to your account or unknown sign-ons.

Social Media

Do not share personal information on social media.

Check your privacy settings.

Block unknown followers and report unusual activity.

Credit Cards, Financial Statements

Check bank and financial statements for unusual activity.

Consider freezing your credit with the three credit bureaus and lift the freeze if a potential creditor requires a credit check. Never do so in response to an unsolicited text or message.
Equifax Credit Freeze
Experian Credit Freeze
TransUnion Credit Freeze

Request a fraud alert for an additional layer of protection on your credit if you do not have a credit freeze.
Equifax Fraud Alerts
Experian Fraud Alerts
TransUnion Fraud Alerts

Carefully review credit reports, free from each of the credit bureaus.
Equifax Credit Reports
Experian Credit Reports
TransUnion Credit Reports

Digital Risks

Account Takeovers

Your personal information and login information are stolen and used to take over your bank, credit card, email, or other online accounts.

Identify Theft

Someone uses your identity (Social Security number, credit cards, and personal bank accounts) to obtain credit or money or open accounts.

Fake Account Creation

A criminal establishes a fake account in your name, transfers assets from your account to the fake account, and then quickly moves money out of that account. A criminal can also alter wire instructions to transfer your funds to an account controlled by the criminal.

Phishing

A popular criminal attack typically delivered by email. Clicking on an unfamiliar link can launch malware to steal your personal login credentials. Or, the link can divert you to another website. You may receive spam asking you to click on an unsubscribe link to prevent more emails, but instead, the link launches a malware attack.

Social Engineering

Scammers will contact you and leverage information they have learned about you, such as an address or account ID, to convince you to offer additional personal information.

Malware

Malware is malicious software—viruses, spyware, and ransomware—that automatically captures your credentials, records your keystrokes, and tracks your online behavior and transactions. It can manifest itself on your computer with:

Unexpected pop-ups

Missing files or programs

Slow performance or unusual browser behavior

Unexplained changes in settings

Alerts, pop-ups, redirects to unknown sources

Suspicious or unknown charges or transfers in your bank account

Family/friends notify you of unusual messages or invites

Emails notify you confirming changes to your online profile that you did not make, or that someone has logged onto your account without authorization

Email forwarding rules that you did not set up are found in your email account. Disable these if found and change your password.

William Blair's Information Security Program

William Blair has a multilayered information security program to deal with the wide variety of potential cyberattacks. These include tools, procedures, and controls to defend against the loss of data. The information security policies and procedures are based on the National Institute of Standards and Technology (NIST) Cybersecurity framework.

William Blair's information security team leads the firm's cyber risk management program and is dedicated full-time to our clients' information security.

Security practices are reviewed during an annual audit. The firm conducts regular tests of its networks and security using phishing campaigns, vulnerability scans, and penetration tests, promptly addressing any potential problems. William Blair is continually adapting its testing strategy to counter new risks.

Further, the program includes security controls around user access, third-party audit reviews, automated alerting, and incident response plans to address potential cybersecurity breaches. To provide additional protection, William Blair maintains cyber insurance coverage for potential internet, data, and network exposures.

Be vigilant

Always be vigilant. Regularly check your bank accounts, credit card accounts, and other sensitive accounts for any signs that someone else may be using your Social Security number or identity.