William Blair

Private Wealth Advisory

Cybersecurity: A Self-Defense Guide

“The first crucial step in protecting yourself from a cyberattack is to assess your digital footprint.”

Your Privacy Is Under Attack

As we become more digitally connected, cybersecurity risks will continue to rise. The Equifax breach, which compromised the identity of 145 million Americans, and the Capital One breach, affecting an estimated 106 million, are the latest reminders of how vulnerable we are, and will remain, to cybercriminals.

Digital commerce and communities have made the world faster, more efficient, and more connected. The internet has also fundamentally changed the definition of privacy. Cyber threats and cybercrime have kept pace, with more sophisticated attacks and potentially more serious consequences. The theft of your social security number or credit card information to obtain money or credit has evolved to today's cyberattacks on your digital existence, used to steal your most private information, professional and personal patterns of life, practices of behavior, medical records, etc., which can be far more devastating for individuals and families.

William Blair's Chief Information Security Officer, Ralston Simmons, provides suggestions on how investors can improve their cybersecurity. Keep in mind that even though the tips are intended to help prevent the loss of personal data, exposure to cyber risk increases every day as digital collection and storage data continue to grow exponentially.

Where Are You Vulnerable?

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. The first crucial step in protecting yourself from a cyberattack is to assess your digital footprint.

Number of devices
The more devices you use, the more networks you are connected to. Cellphones, laptops, and tablets are the more commonly used, but consider also home security systems, appliances, technology-enabled cars, and even medical equipment and children's toys that plug directly into the internet of things (IoT) network. Connecting these devices to the cloud may leave them exposed.

Multiple homes
Do you own multiple homes, each with a separate network?

Social media accounts
Are you active on social accounts such as Facebook, Twitter, LinkedIn, Google+, and YouTube?

Websites visited, including all online purchases
Do you regularly shop online, whether it is at traditional stores or online retailers?

Public Wi-Fi at airports, hotels, coffee shops, homes
Do you connect to public Wi-Fi? If so, you are opening your mobile devices to public internet traffic. Cybercriminals are able to spoof signals, making it appear as though you are dialing into the public Wi-Fi. Should you dial into the fake box, the criminal would have access to your personal information.

Email addresses, user names, passwords
Hacking most commonly occurs via poor user names and password management. The average user has 130 accounts assigned to a single email address.

Quick Reference List

- Number of devices
- Homes
- Social media accounts
- Online Purchases
- Public Wi-Fi
- Email addresses

The larger your digital footprint, the greater your cyber risk.

Account takeovers

Account takeovers occur when a fraudster steals personal information and login credentials and takes over your bank, credit card, email, or other online accounts.

Blackmail/extortion

A blackmail or extortion plan may start with a hacker accessing your computer and searching for information or photos, and then threatening to release the information unless a ransom is paid.

Hacking

The criminal invasion and theft of digital records comes in all shapes and sizes. Hackers target massive computer databases, ATM banking codes, social media networks, email, and messaging.

Identity theft

Identity theft, a more common form of cybercrime, occurs when someone uses your identity (social security number, credit cards, and personal bank accounts) to obtain credit or money, often opening credit accounts or using the stolen personal information to make purchases.

Fake account creation

Fake account creation is on the rise. A criminal can establish a fraudulent account in a client's name, transfer assets from the client's account to the fake account, and then quickly move the money out of that account. Cybercriminals are also able to alter wire instructions to transfer clients' funds to an account controlled by the criminal.

Poor management of your digital footprint can result in a slew of cyber risks affecting your finances and your reputation.

Most Common Targets

Malware and ransomware

Malware is malicious software—viruses, spyware, and ransomware—that automatically captures your credentials, records your keystrokes, and tracks your online behavior and transactions without you knowing. The attacks can last for weeks or months. Equifax, TransUnion, Sony, and Target are just a few of the many companies that have been victimized by malware. Ransomware, a practice whereby a criminal threatens to publish a victim's data or blocks access to a victim's accounts unless a ransom is paid, is on the rise.

Phishing

Phishing is a popular criminal attack that typically comes via email. Clicking on an unfamiliar link can launch malware to steal your personal login credentials. Some of the more sophisticated phishing emails divert you to another website that may make you think you are logging into your real provider. Others may be disguised as spam asking you to click on an unsubscribe link to prevent more emails, but instead the link launches a malware attack.

Your email inbox is the most common target for cyberattacks.

Social engineering

Through social and other digital media, cybercriminals gain your trust over time and convince you to give up personal information. Scammers will contact you and leverage something they have learned about you such as an address or account ID. Their goal is to convince you to offer additional personal information—a social security number, a driver's license, an account number, a password—which they can use to commit fraud.

USB attack

An attacker will leave a USB key on the ground. When you pick it up and plug it into your computer, it will activate and install malware onto your machine, allowing the attacker to gain access to your personal information.

Smart and mobile hacks

Smartphones are now being targeted for attacks, underscoring the need to update iOS and operating systems on mobiles. Do not let anyone have access to your device without your permission.

Think before you click.

Never click on an unfamiliar link.
Never click on a link from someone you don't know personally.
Always delete unfamiliar emails without clicking.

Protect passwords

- Use passwords with 12 to 16 characters, and a mix of characters and numbers. Malicious software, available on the darknet, allows criminals to crack a six-character password in seconds. By contrast, a 14-character password would take the same malware many years to break.
- Don't reuse passwords. Use different passwords for each account.
- Avoid commonly used words and phrases.
- Don't save passwords in your phone notes app.
- Consider using a password management app. Create a master password for the app, which then creates strong passwords for all your accounts. The application resides on your smartphone, your tablet, and your laptop.

Two-factor authentication

This process adds an extra layer of protection to ensure you are the only person who can access your account. It has been among the most important personal cybersecurity steps you can take to protect your account.

1. Sign into your account using your password;
2. A second passcode is sent by email or text to your laptop and mobile, which allows you to continue the login process.

Secure digital assets

- Make sure antivirus software is installed and up to date and your firewall is turned on.
- Install updates when released. Malware is a constant danger. It is vital that you apply security updates as soon as they are released.
- Keep your home router, which connects your digital activity to the internet, up to date and maintain best practices for passwords. Separate personal use and guest use on your home router and Wi-Fi networks. Most routers today have the technology to partition guest use.
- Only buy IoT devices that allow password changes.
- Avoid public Wi-Fi. To connect while traveling, use the hot spot on your iPhone or use a MiFi device—a wireless router that acts as a mobile Wi-Fi hotspot.

Take control of your digital footprint

- Access your online accounts and review privacy settings.
- Use a separate email account when signing up for one time offers.
- Educate all family members on digital risks. Do not post vacation whereabouts real-time on social media. You're broadcasting where you are and where you're not, putting your home assets at risk.
- Avoid opening multiple windows while online in personal accounts.
- Log out completely after completing a transaction or message.
- Consider an identity managing service which will notify you when there is suspicious activity involving your data.

William Blair's Information Security Program

William Blair has a multistep 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 chief information security officer and his team lead the firm's cyber risk management program and are 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. Cybercriminals continuously try to create new ways to break into systems and the technology environment is far from static. 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, and 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.

November 2019 This information has been prepared solely for informational purposes and is not intended to provide or should not be relied upon for accounting, legal, tax, or investment advice. The factual statements herein have been taken from sources we believe to be reliable, but accuracy, completeness, or interpretation cannot be guaranteed. All views expressed are those of the author, and not necessarily those of William Blair & Company, L.L.C.