

5 Tips To Protect Yourself From Cybercriminals

by A. Scott White, CFP®, ChFC®, CLU®
Uhler Vertich White Advisors

Wealthy individuals are increasingly becoming targets of cyber-attacks. From phishing scams to ransomware attacks, cyber threats can have serious consequences for individuals with high net worth, including financial loss, reputation damage, and identity theft.

“High-net-worth individuals (HNWIs) are more searchable online and therefore more vulnerable. Someone who owns a company, holds a C-suite position, frequently makes large donations to charity or is a public figure has a highly-visible online presence, making it easier for cyber thieves to profile them as potential victims,” according to Stacy Bertrand, manager of information security strategy and metrics at City National Bank, an RBC company.

Therefore, it’s critical that high net worth individuals take proactive measures to protect themselves and their assets from cyber threats by implementing robust cybersecurity practices.

1. Use strong and unique passwords: Strong passwords are complex and unique, consisting of a combination of letters, numbers, and symbols. Avoid using personal information such as your name, birthdate, or address. Instead, use a password manager to generate and store your passwords securely. A password manager creates unique, strong passwords for each of your accounts and stores them in an encrypted database, which is protected by a master password. This way, you only need to remember one password to access all of your accounts.

2. Enable two-factor authentication (2FA): Two-factor authentication provides an extra layer of security by requiring a second form of authentication, such as a code sent to your phone or an app, in addition to your password. This way, even if your password is compromised, the hacker won’t be able to access your account without the second factor. Many online services and apps support 2FA, so be sure to enable it wherever possible.

3. Keep your software up to date: Cybercriminals often target software vulnerabilities to gain access to systems. Ensure that your software, including your operating system, applications, and security software, is always up to date with the latest security patches and updates. Set your software to update automatically or regularly check for updates manually. If you’re unsure about how to update your software, consult with a trusted IT professional.

4. Use a virtual private network (VPN): A VPN encrypts your internet traffic, making it difficult for hackers to intercept your data. Use a reputable VPN service when using public Wi-Fi or accessing sensitive information online. When you connect to a public Wi-Fi network, you’re potentially sharing the network with other users who may be able to intercept your data. A VPN creates a secure, encrypted connection between your device and the internet, keeping your data safe from prying eyes.

5. Be cautious of social engineering attacks: Social engineering attacks use psychological manipulation to trick people into divulging sensitive information. Be cautious of unsolicited emails, phone calls, or text messages, especially if they ask for personal or financial information. Always verify the identity of the sender before responding or clicking on links. If you receive an email or message that looks suspicious, report it to your IT department or the relevant authorities. Remember that high net worth individuals are often targeted by cybercriminals, so it’s important to stay vigilant and be aware of the latest threats.

Though these five tips will keep generic cyberattacks at bay, many families of high-net-worth may also need enhanced security measures if they are especially prominent.

This material is being provided for information purposes only and is not a complete description, nor is it a recommendation. Raymond James is not affiliated with any of the external organizations mentioned. Certified Financial Planner Board of Standards, Inc. (CFP Board) owns the certification marks CFP®, CERTIFIED FINANCIAL PLANNER™, and CFP® (with plaque design) in the United States, which it authorizes use of by individuals who successfully complete CFP Board’s initial and ongoing certification requirements.

Certified Financial Planner Board of Standards Inc. owns the certification marks CFP®, CERTIFIED FINANCIAL PLANNER™, CFP® (with plaque design) and CFP® (with flame design) in the U.S., which it awards to individuals who successfully complete CFP Board’s initial and ongoing certification requirements.

Every investor’s situation is unique and you should consider your investment goals, risk tolerance and time horizon before making any investment. Prior to making an investment decision, please consult with your financial advisor about your individual situation.

The foregoing information has been obtained from sources considered to be reliable, but we do not guarantee that it is accurate or complete, it is not a statement of all available data necessary for making an investment decision, and it does not constitute a recommendation. Any opinions are those of Uhler Vertich White Advisors and not necessarily those of Raymond James.