HUB Private Client

HUB PRIVATE CLIENT

CYBERCRIME IN THE AGE OF AI

Wealthy families are prime targets for cyber criminals. Here's how you can reduce the odds of becoming their next victim.

Fueled by AI-enabled scams, crypto theft and other increasingly sophisticated attacks, cybercrime continues to increase at a dramatic rate. The FBI reports that U.S. cybercrime losses reached $16.5 billion in 2024 – a 33% year-over-year increase[1] – while Canadian losses reached a record high of nearly $4 billion.[2] While virtually every North American with an internet connection has some degree of vulnerability, ultra-high-net-worth families and their family offices are especially desirable targets. A recent cybersecurity report shows that 43% of all family offices surveyed experienced a cyberattack in the past year, including 62% of those managing more than $1 billion in assets.[3]

The potential cost of a serious cyberattack can go well beyond direct financial losses. Depending on the nature and severity of the breach, high costs may be associated with forensic investigations, enhanced security measures, potential lawsuits, operational disruptions and other indirect costs. The potential damage to a family's reputation and peace of mind is incalculable.

Despite the apparent risks, relatively few affluent families are aware of the potential vulnerabilities, and fewer have taken adequate measures to mitigate the threat. In keeping with HUB International's commitment to helping our clients live safer and more financially secure lives, we offer these insights into the most serious and rapidly growing risks, some expert advice on reducing your exposures and measures to take if you fall victim to a cyber breach. Should you wish to discuss these issues in the context of your specific personal and/or business risk exposures, please consult your HUB Private Risk Advisor.

IMPERSONATION SCAMS BECOME A LEADING THREAT

Here's a scenario that is becoming an increasingly common occurrence in both Canada and the United States:

> A wealth advisor receives a call from a long-time client, asking him to wire $200,000 for a down payment on an offshore fishing boat. The advisor not only recognizes the voice but also knows his client is an avid fisherman and upgrades his boats every few years. A brief chat about family events and the weather in Florida erases any initial suspicion the advisor might have about the slightly awkward phrasing his client is using. So, he wires the money, which unwittingly goes straight into a fraudulent account overseas. As this request may well be ruled a "voluntary transfer," the loss would not be covered by the advisor's financial institution.

These types of impersonation scams surged 148% between April 2024 and March 2025, and those ending in losses of more than $800,000 rose eightfold during the same period.[4] Many of these high-dollar crimes are the result of an illegal intelligence gathering effort that may have lasted for months. Cybercriminals scout potential targets, seeking access to email and social media accounts and personal information from other sources. These sources provide the information they need to craft a compelling narrative, capture voice samples and train their AI system to perpetrate the crime.

So how do you reduce your vulnerability to attacks of this nature? Start with strict adherence to general cybersecurity practices, as they will complicate the task of gathering information

on you, your family and employees. Be aware of the warning signs that a voice – which sounds real – may be an AI-generated fake:[5]

- It may sound detached or robotic and/or have unusual pauses or an odd rhythm.
- You may hear a faint buzzing or strange background noise intended to cover imperfections in the voice.
- The speaking style may sound too "perfect" and lack the typical pauses, "ums and ahs" and other nuances of human speech. Also, natural laughter is difficult for AI to recreate convincingly.
- Be suspicious of repetition and awkward phrasing, especially if you ask a question and get a slightly rephrased version of a previous statement.

Know that even the most savvy individuals can be deceived, and as AI-generated impersonation tools continue to advance, UHNW families must remain alert, verify requests and adopt preventative controls to reduce risk. And because technical sophistication alone cannot prevent impersonation fraud, families must establish simple, enforceable verification controls to reduce exposure.

TIP: Establish a pre-shared safe word with family members and any individual authorized to initiate or approve financial transactions. Any request for a wire transfer or urgent payment – regardless of how credible the caller appears – must be authenticated using the safe word before funds are released.

CRYPTOCURRENCY THEFT AND FRAUD ON THE RISE

As cryptocurrency adoption accelerates, so too does crypto-related theft and fraud. Nearly $1.93 billion was stolen in digital asset crimes in the first half of 2025 alone, surpassing all of 2024 and putting the year on track to become the worst on record for crypto theft. Among the most common schemes are phishing attacks targeting cryptocurrency users – often through fake exchange websites – which increased 40% between mid-2024 and mid-2025.[6]

Cryptocurrency – particularly crypto ATMs – is also emerging as a preferred payment method for cybercriminals. Approximately 50,000 crypto kiosks now operate in retail locations across the United States and Canada,[7] converting cash into digital currency. While most are registered and used legitimately, these machines were exploited to facilitate more than $65 million in fraud in the first half of 2024 alone.[8] Law enforcement authorities report growing use of crypto ATMs in scams ranging from romance and government-impersonation schemes to fraudulent "grandchild-in-distress" emergencies.[9] Any request to send funds via a crypto ATM should be treated as a significant red flag and approached with heightened caution.

TIP: Treat any unsolicited request involving cryptocurrency – particularly those requiring payment via crypto ATMs – as inherently high risk. Never act under urgency, independently verify the request through a trusted secondary channel and remember that once cryptocurrency is transferred, the transaction is typically irreversible.

OLD THREATS REIMAGINED

Many of today's most significant cybersecurity threats are familiar, but they have evolved, incorporating new technologies, tactics and attack vectors. Among the most prevalent are identity theft, extortion and social engineering.

IDENTITY THEFT

One of the oldest forms of cybercrime, identity theft occurs when criminals gain access to personal information and either monetize it immediately or exploit it later for larger financial gain. It is also among the most difficult breaches for victims to detect. Recovering from a single identity theft incident can take six months and require up to 40 hours of effort.

Identity theft manifests in several common ways:

- Unauthorized credit activity. Fraudsters open or reactivate credit accounts in a victim's name – often through major credit bureaus such as Experian or Equifax – then request replacement cards sent to addresses they control.
- Compromised personal devices. When smartphones, tablets or laptops connect to unsecured public Wi-Fi, attackers can intercept personal data, including login credentials for financial institutions, email accounts and stored personal information.
- Exploitation of breach data. Criminals leverage information obtained from large-scale data breaches – such as those affecting AT&T and Dell in 2024, which exposed data for more than 122 million individuals – to fuel identity fraud and account takeovers.
- Targeted physical mail theft. Using publicly available tools like Google Maps, Zillow or Redfin, thieves identify affluent neighborhoods and harvest mail containing sensitive personal or financial information.

Email hack leads to a major loss

A high-net-worth individual's email was hacked, and after watching interactions with her bank for 30 days, the hackers posed as her and asked to have several hundred thousand dollars wired to their account. The bank complied after asking the standard security questions, which the bad actors were able to answer. An additional request two weeks later led to the bank calling the account holder, uncovering the fraud. By then, she had lost several hundred thousand dollars. Despite the FBI getting involved, the funds were never recouped.

EXTORTION

Cybercriminals may compromise browser histories, webcams, email accounts or other digital channels to obtain sensitive or embarrassing information. They then demand ransom payments in exchange for not releasing the material publicly or to personal and professional contacts.

The rapid advancement of AI-generated deepfakes has significantly escalated these threats, enabling criminals to fabricate highly realistic images or videos depicting behavior that never occurred. These capabilities have fueled a surge in personalized sextortion attacks, which may include photos of a victim's home or other personal details to lend credibility to false claims that webcams or devices have been hacked.[10]

SOCIAL ENGINEERING

Social engineering involves manipulating individuals into disclosing sensitive information or transferring funds – often through email, text or phone-based scams. While these schemes can lead to substantial financial losses, they are also among the most preventable forms of cybercrime, as they rely primarily on human trust and error rather than technical exploits.

Beyond mass phishing campaigns, sophisticated attackers frequently conduct targeted reconnaissance, sometimes remaining inside a victim's network for weeks or months. By studying habits, relationships and transaction patterns, they time their approach to coincide with moments of financial activity or heightened urgency. In some cases, criminals gain access to personal devices through cameras or other vulnerabilities, enabling them to monitor behavior, capture credentials and escalate fraud attempts.

HOW TO BUILD CYBER WALLS AROUND YOUR ASSETS

Like a medieval castle with a moat, drawbridge and knights, a multi-tiered approach to cybersecurity provides extra layers of protection. There are several steps you can take to build these layers and safeguard your assets.

- **Don't skip the basics.** Simple tools and best practices are an important first layer of protection. For example, consider installing password managers like Dashlane or Password to create and organize strong, complex passwords for each account, use webcam covers to ensure privacy and restrict access to your credit report. Also, be careful about the links you click on, and teach good cyber hygiene to your children as well.
- **Two-factor authentication.** Four out of five hacking-related breaches leverage either stolen or weak passwords.[11] Using two-factor authentication — a password and a passcode sent through a different medium — provides a double-locked gate for important information.
- **Use different emails for different things.** By using an email address for work, another for personal use and another for banking, it's easier to identify suspicious communications or compromised accounts. For instance, you'll be able to identify a phishing scam asking for banking information if that email address is not used for finances.
- **Segment your home network.** While we may trust guests in our homes, it's best to have a separate network for them. An infected device or malicious program inadvertently downloaded to your home network can corrupt all devices that use the network. Creating segments in your home network – such as a guest network and segments for other family members, personal matters and work – can provide extra levels of protection.
- **Strengthen your Wi-Fi security.** An unlocked internet router gives intruders access to every single device connected to it. Hackers can easily search for default router logins, so change the default name and avoid using personal identifiers in your Wi-Fi name. Anonymous names are more private and therefore more secure.
- **Never use public Wi-Fi.** Airport lounges, hotel lobbies and coffee shops are hotspots for hackers. It's best to use secure networks instead. Unlike most home and office wireless networks, the data flowing around a public hotspot is often not encrypted and can serve as a window into any device connected to it. Use a virtual private network (VPN).
- **Identify vulnerabilities.** Work with a professional to test the barriers you've constructed. Turnkey vendors like Blackcloak can help with password monitoring, data broker removal, device hardening and establishing privacy settings across your devices.
- **Have a cyber breach response plan.** Identify possible scenarios and categorize the importance of data before your identity gets compromised. It's also essential to know who to call in case of a breach. If you have cybersecurity insurance, this will be your broker or carrier, who will have a privacy attorney start the formal IT forensic process to determine how the perpetrators got in — and if they're still there.

TIP: While using your phone as a second authentication works fine, an app authenticator like Authy, software tokens or hardware such as YubiKey, offers even greater protection.

Innocent photos become an extortion tool

The son of a high-profile real estate mogul uploaded pictures of himself at a party to one of his social media platforms. A hacker who had been following the teen downloaded, altered and then uploaded the photos to a website to extort the family.

TIP: Cybercriminals will often go into public areas of airports and malls to set their computers as an additional hotspot. Be aware of your phone's Wi-Fi automatically connecting to them. Go to your Wi-Fi settings and turn off "auto-join hotspot."

CYBER INSURANCE: AN ESSENTIAL BACKSTOP

Data breaches are expensive, with potential costs coming from forensic investigations, notification expenses, lawsuits or even extortion attempts. Just as you purchase insurance to protect your physical assets, cyber coverage can help protect your digital assets. There are essential elements that any cyber insurance should cover:

- **Privacy attorney.** A data breach investigation and resolution process is complex. A privacy attorney will champion the entire post-breach process, helping victims manage and understand the process, such as IT forensics investigations, along with state, provincial and federal laws and regulations.
- **IT forensics investigation.** An IT forensics investigation helps determine the who, what, where, when and why of a data breach. While the exact cost of such an investigation depends on a variety of factors, it can range from a couple of thousand dollars to more than $100,000.[12] Cyber coverage that pays for forensic investigation is a fundamental part of any robust insurance plan.
- **Financial losses.** Depending on the policy, cyber coverage will provide reimbursement for financial losses incurred from the cyber breach. This may include business interruption (BI) coverage for lost work time, as well as for any fees or charges that may arise for the breach.

More specialized coverages are also available to protect against cryptocurrency theft and vicarious liability coverage to protect family officers, CPAs, wealth advisors and others who were tricked into making a fraudulent payment on your behalf.

WHAT CYBER COVERAGE IS RIGHT FOR YOU?

While shopping for the right policy endorsement, keep the following in mind:

- **Go for the max.** Individuals adding a cyber endorsement to their property policy may be tempted to settle for the lowest limit available, often just $50,000 worth of coverage. But think about a fraudulent wire transfer, the most common form of cyber fraud for high-net-worth individuals. This crime almost always results in losses exceeding $50,000. When you can, buy the maximum coverage.
- **Mind the exclusions.** Social engineering – such as being tricked into sending money – is the major exclusion to watch for. Though it's one of the most common forms of fraud, some insurance companies and policies do not consider social engineering to be cyber fraud.
- **Don't forget about offline breaches.** The right policy can cover both offline and online breaches. For example, if someone sells your personal information, including your Social Security number or Social Insurance number, or opens credit cards in your name, that's considered an offline breach, and the right endorsements will cover it.

Cyber insurance coverage will help minimize your financial loss and contain any damage, but the impact of a cyber breach or stolen identity on your reputation, as well as the inconvenience and the anxiety it causes, cannot be insured. For this, the only solution is to be proactive and safeguard your assets.

Dinner table talk goes viral

A private equity executive discussed a high-profile acquisition at the dinner table. His teenage son shared the information with a friend in a social media chat room. The company had flags in place to alert the business anytime its name was mentioned on social media. The executive lost both the deal and his job.

WHAT TO DO IF YOU GET HACKED?

If you fall prey to a cybercrime, you should immediately act to contain the damage and move toward resolution. Here are three important steps in case you become a victim:

- Call the cyber response hotline attached to your cyber coverage. The insurance representative will provide instructions to help stop continuing fraud and get the ball rolling to engage your cyber coverage.
- Contain the breach. Take any breached device offline immediately. If you've built strong walls around your data, you should be able to locate and isolate the attack.
- Engage experts. Your cyber insurance team will connect you to a privacy attorney who specializes in cyber breaches and an IT forensics team that can pinpoint the source of your breach to eliminate it. The faster you can get expert eyes on the problem, the better chance of limiting the damage.

A loss for charity

A bad actor broke into the charity account of a famous U.S. sports figure. The hacker was able to divert funds away from the player's charity over to his own personal account overseas. The player never recovered those funds.

SAFEGUARD YOUR FAMILY AND ASSETS NOW

Most hackers and cybergangs are not criminal masterminds; they typically exploit lapses in awareness and target the most vulnerable victims. Understanding where your exposures lie is the first step in protecting yourself and your family from unwanted intrusion. From there, leverage the tools, controls and resources available to reduce risk – and ensure appropriate insurance coverage is in place to provide financial protection should preventative measures fall short.

Experts in Private Client Personal Insurance

We understand that personal wealth often comes with a complex mix of business, professional and personal interests that can be jeopardized at any moment without proper risk management. Our insurance and risk management experts specialize in developing tailored solutions to protect you today while anticipating their needs and guiding them through tomorrow.

---

[1]Federal Bureau of Investigation, "FBI Releases Annual Internet Crime Report," April 23, 2025.

[2]Statista, "Estimated annual cost of cybercrime in Canada from 2017 to 2028," January 8, 2026.

[3]Deloitte, "The Family Office Cybersecurity Report, 2024," accessed January 15, 2026.

[4]Federal Trade Commission, "FTC Data Show a More Than Four-Fold Increase in Reports of Impersonation Scammers Stealing Tens and Even Hundreds of Thousands from Older Adults," August 7, 2025.

[5]McAfee, "A Guide to Deepfake Scams and AI Voice Spoofing," accessed January 14, 2026.

[6]Kroll, "2025 Cyber Threat Landscape Report: Cybercrime in the Crypto Era," August 22, 2025.

[7]CBC, "How fraudsters use crypto ATMs to launder millions from Canadian scam victims," October 7, 2025.

[8]WCF Bank, "Beware of Bitcoin ATMs!" accessed January 15, 2026.

[9]AARP, "What to Know About Cryptocurrency ATMs and Why Criminals Love Them," March 29, 2024.

[10]Krebbs on Security, "Sextortion Scams Now Include Photos of Your Home," September 3, 2024.

[11]OX IT Solutions, "How dangerous are weak passwords to your IT infrastructure?" October 18, 2025.

[12]Vestige, "What is the cost of Digital Forensics Services?" accessed January 16, 2026.

ABOUT PRIVATE CLIENT

Liability exposures are evolving—and so are the stakes. HUB Private Client helps affluent individuals and families safeguard their wealth with tailored excess liability solutions and expert risk guidance. Whether it's a serious auto accident, an injury on your property, or a lawsuit tied to travel, staff, or social media, our advisors help ensure you're protected well beyond the limits of standard coverage. We assess your full risk profile, uncover gaps, and recommend strategies that reflect the way you live today.

Connect with your HUB Private Client Risk Advisor for a personalized review and proactive risk strategies designed to protect your assets, reputation and legacy.

HubPrivateClient.com

This information is provided for general information purposes only. HUB International makes no warranties, express, implied, or statutory, as to the adequacy, timeliness, completeness, or accuracy of information in this document. This document does not constitute advice and does not create a broker-client relationship. Please consult a HUB International advisor about your specific needs before taking any action. Statements concerning legal matters should be understood to be general observations and should not be relied upon as legal advice, which we are not authorized to provide.

© 2026 HUB International Limited. All rights reserved