BLACKCLOAK®

Personal Cybersecurity for Family Offices:

Essential Strategies to Protect Wealth and Privacy

blackcloak.io

Contents

"We often see high-net-worth families taking action only after an incident has occurred, which is unfortunately too late. Financial losses can be permanent, and reputational harm can have severe, long-lasting consequences. It's worth sacrificing a small amount of convenience to establish good cyber hygiene and personal security – which can prevent the costly, time-intensive efforts necessary to repair and recover when cybercriminals succeed in their missions."

– Ingrid Gliottone, Chief Experience Officer, BlackCloak

Introduction

> "Wealth creates a unique cybersecurity challenge. For cybercriminals, a high-net-worth individual or Family Office isn't just a target; they're an entire supply chain of high-value data."
>
> – Daniel Goldenberg, Founder & Principal, Seventh Sense Security

In today's world, the combination of AI's widespread availability with several other factors puts high-net-worth individuals (HNWIs) and their families directly in the crosshairs of hackers' sophisticated attack methods. HNWIs, who are often business executives and people in the spotlight, may think they're protected by a corporation's cybersecurity program, but that is typically not the case. Corporate cybersecurity rarely extends beyond the company-issued laptop or phone, and protecting the personal digital lives of business leaders is often not a top priority for most cybersecurity teams, given other urgent issues.

Additionally, HNWIs commonly have limited knowledge and skills in cybersecurity and self-protection. Family Offices themselves typically don't have the necessary cybersecurity skills to protect their clients. As a result, numerous gaps exist in defenses across HNWIs' personal lives, devices, and networks, as well as those of their families.

Simply put: HNWIs, their families, and their Family Offices are an attractive, high-value target of cyberattacks – and their digital doors are left wide open.

The answer? A proactive, layered approach to cybersecurity is essential to protect their wealth, privacy, and legacy.

But who is responsible for ensuring the appropriate guardrails are in place?

This eBook details the issues and preventive measures that Family Offices should understand and communicate to the principal and other family members to safeguard them and their legacy.

The escalating risks facing HNWIs

Recent studies reveal that 43% of Family Offices have experienced a cyberattack in the past 12 to 24 months[1], and 83% of U.S. Single-Family Offices rank cyber risk as a top concern[2]. HNWIs are viewed as goldmines of data, where stolen identities, along with financial and health records, command top dollar on the dark web. Consequently, sophisticated attackers approach these targets with persistence and precision. Compounding the issue, 60% of breaches stem from human error, while 30% involve third-party partners[3], such as personal accountants or real estate agents, underscoring the need for stronger defenses on every front.

The issues facing HNWIs and their families are numerous. First, while their wealth is substantial, their security is not. High-value, high-profile families can have comparable wealth to large financial institutions with $100 million cybersecurity budgets. Yet, they often lack the same enterprise-grade protections, relying instead on consumer-grade malware protection and a credit monitoring subscription. Attackers exploit weak points such as personal email, social media, poorly secured home networks, and unprotected devices – including those used by children. From guessable or reused passwords to unsecured gaming consoles and smart televisions, cameras, and more, vulnerabilities are everywhere, and HNWIs and families are sorely exposed.

Additionally, most people are aware of scam text messages but don't understand the real danger of skilled, sophisticated "Ocean's 11 hackers" and the lengths to which they go to find the right opportunity. For example, the average dwell time for an attacker in someone's network is 200 days – a considerable amount of time to gather information and wait for a travel or liquidity event to occur, when they can strike. Without proper awareness and training, family members are vulnerable to phishing and other nefarious attacks that grant cybercriminals access to sensitive information, account logins, and schedules.

The stakes are high: the average data breach now costs more than $4.5 million, but reputational damage and loss of trust can be far more costly in the long run. Family Offices can help by establishing the necessary guardrails for their clients and assisting them in adopting a holistic approach to cybersecurity, striking a balance between convenience and protection. Essential safeguards include regular device assessments, robust data privacy practices, reduced digital footprints, and hardened accounts with multi-factor authentication. Just as importantly, Family Offices should implement processes to serve as a counterweight to potential attacks, conducting due diligence and ensuring readiness.

What's needed to protect today's HNWIs and their families is a comprehensive approach to personal privacy and security through proactive, layered cyber defenses. This type of digital protection is no longer optional; it is the foundation for preserving the wealth and legacy of high-net-worth families.

1. The Family Office Cybersecurity Report, 2024 - Deloitte
2. 2024 RSM Family Office Operational Excellence report
3. 2025 Data Breach Investigations Report - Verizon

Kering example:

Kering, the parent company of luxury brands Balenciaga, Gucci, and Alexander McQueen, was breached in June 2025. The personal information of millions of customers was compromised, including names, email addresses, phone numbers, physical addresses, and customers' total spending amounts. Falling into the hands of cybercriminals, this information could then be used to access customers' other accounts – particularly those that use the same login information – and cause financial harm.

When such an event occurs – particularly one that specifically targets HNWIs – Family Offices can advise their impacted clients to take the following steps:

- Change their passwords, especially on any sites that use the same password
- Enable two-factor authentication on all accounts
- Be on the lookout for suspicious emails and text messages
- Always verify that the sender is a trusted contact before taking any action

"I work with breached high-net-worth individuals every day. We often find that a hacker has been sitting in their email inbox, watching their activities, waiting for the right time to strike. Unfortunately, high-net-worth family members don't stand a chance of detecting the 'Ocean's 11 hacker.' These are professionals who spend months researching and observing the family. Like a digital cat burglar, the money will quickly be redirected and stolen without a trace."

– Sarah Rosen, Managing Director of Private Client Services, BlackCloak

What are the threats?

20%

of home networks are vulnerable to unauthorized access[5]

76%

of clients' personal devices were actively leaking data before using BlackCloak[5]

70%

of connected homes have exposed account passwords[5]

39%

of new BlackCloak clients had been hacked without their knowledge[5]

87%

of new BlackCloak clients had no security on their cell phones or tablets[5]

Victims lost

$16.6 billion

to internet-enabled crimes in 2024[6]. The top crimes included:

- Phishing / Spoofing
- Extortion
- Personal Data Breach
- Non-Payment / Non-Delivery
- Investment

5. BlackCloak
6. 2024 Internet Crime Report - ic3.gov

The cyberattack maze: How cybercriminals target HNWIs

Cybercriminals are skillful in deploying many types of attack methods to target HNWIs and their families. Many of these start with a bad actor buying an individual's information that was accessed in a breach and released on the Dark Web for $10. They begin with basic information, such as compromised personal information scraped from data broker websites, stolen credentials from previous breaches, or publicly available details found online. These data points serve as the essential raw material that malicious actors weaponize into sophisticated, operational attacks.

Just like any profession, hackers have best practices and methodologies for efficiently performing their jobs, which they share with one another. The most effective methods become common scams and are therefore more detectable since cyber defenders know what to look out for and how to prevent them. Below is a comprehensive list of primary attack methodologies, illustrating how digital weaknesses can provide other pathways to cause financial and physical harm.

1. Account & identity hijacking exploits

These attacks focus on bypassing or weaponizing the basic personal information that is often used to authenticate the victim digitally.

Attack Method	Description
SIM Swapping / Port-Out Fraud	The attacker uses social engineering to convince the mobile carrier to transfer the victim's phone number to a device controlled by the criminal. This immediately enables them to bypass SMS-based Multifactor Authentication (MFA), reset passwords for email and financial accounts, and initiate fraudulent wire transfers, often resulting in swift, catastrophic financial losses.
Session Hijacking / Cookie Theft	Using sophisticated malware (often delivered via phishing), the attacker steals the user's active session cookies from a browser. This allows them to bypass the login screen and MFA entirely, therefore duplicating an actively logged-in user session on highly sensitive platforms (e.g., bank portals, cloud storage, trading accounts).
Credential Stuffing (Stolen Passwords)	Attackers use large databases of credentials leaked from previous breaches (stolen passwords, emails) and automate attempts to log into the victim's other, more valuable accounts (e.g., banking, investment). This works due to password reuse and lack of MFA/2FA.
Domain Hijacking (DNS/ Registrar Attack)	Gaining control of the executive's personal website domain or business domain registrar. This allows the attacker to redirect email traffic and website visitors, using the hijacked email for massive, convincing phishing campaigns.

The scam: A devastating SIM swap attack impacted one victim shortly after she purchased a new phone, resulting in the rapid takeover of multiple critical accounts, including her Apple ID, emails, and social media. Bad actors immediately initiated fraudulent financial activity, opening new lines of credit and attempting withdrawals.

The solution: BlackCloak's incident response team initiated a multi-hour recovery and defense protocol, successfully regaining account access, establishing an authenticator app for primary MFA, and implementing preventative measures that curtailed further financial loss and fortified the client's long-term security.

2. Malware, phishing, and social engineering

These remain the foundational methods for gaining initial access, often utilizing AI to boost authenticity.

Attack Method	Description
Deepfake Impersonation	Using AI-generated audio or video (created from publicly available samples, including those gained from social media) to impersonate an executive, a trusted family member, or a colleague in a video call or voicemail. The goal is often to manipulate an assistant, employee, or family member into making an urgent wire transfer or releasing confidential information.
Spear-Phishing and Vishing	Highly customized email or voice attacks that leverage private information (e.g., mentioning a recent vacation or a child's name) to establish trust. They trick the victim into clicking a malicious link, downloading ransomware, or revealing credentials.
Unprotected Devices & Networks	Exploiting the fundamental lack of security on personal laptops, tablets, and insecure home Wi-Fi networks (lack of encryption, default passwords, no separate guest network) to gain direct, unrestricted access to connected work assets.
Targeted Ransomware / Extortion	While ransomware is common, HNWIs face targeted extortion, where the attacker threatens to publish embarrassing or proprietary stolen data (files, emails, photos) to demand payment, leveraging the executive's high reputation.

The scam: A targeted phishing scam disguised as an urgent technical support alert sent to an individual's personal email tricked her into clicking the malicious link, inadvertently granting scammers remote access to her computer and rendering it inoperable.

The solution: BlackCloak's concierge incident response team swiftly engaged, identifying active threats and restoring the computer, underscoring the vital need for personal digital protection and prompting the family to fortify their defenses against future scareware and phishing attacks.

3. Physical-Digital convergence exploits

These attacks exploit digital information to facilitate real-world crime and pose personal safety risks.

Attack Method	Description
Doxxing & Stalking	Attackers compromise or aggregate vast amounts of Personally Identifiable Information (PII) – home address, cell number, travel plans, family names, etc., from data broker sites and breaches, and publish it online. This exposure directly facilitates physical harassment, stalking, or "swatting" (calling in false emergency reports to the victim's home).
Insecure Smart Home/IoT Exploits	Exploiting vulnerabilities in weakly secured IoT devices (smart locks, cameras, voice assistants, thermostats, connected appliances) to gain remote control. This provides the attacker with real-time intelligence on the family's routines, vulnerabilities, and potential windows for physical intrusion, or allows them to disable security systems remotely.
Geospatial Tracking	Exploiting flaws or data sharing in personal devices (e.g., smartwatches, improperly secured location data in apps, or connected vehicle systems) to monitor the victim's real-time movements and patterns. This is often used for planning kidnappings, burglaries, or targeted harassment.
Crypto-Wallet Abduction / Extortion	A high-stakes crime where digital intelligence about cryptocurrency holdings is combined with a physical threat (kidnapping or home invasion) to force the victim to transfer digital assets under duress.

The scam: In one case, activists used erroneous email addresses and internet activity to cross the divide of cyber and personal security and accuse a corporate executive of illicit activity, assaulting her and her family with a camera crew on the streets of NYC and threatening to run a public relations attack on media outlets the following morning

The solution: Working with BlackCloak, the executive's internet presence was minimized and forensic resources were provided to assist her with legal protective measures. BlackCloak's experts worked with the institution's public relations, media, counsel, and CSO to provide supporting evidence of the executive's innocence and protect her against future attacks.

4. Supply Chain & Third-Party Risk

These attacks compromise the victim via the small, trusted organizations or vendors they rely on daily.

Attack Method	Description
Third-Party Vendor Exposure	Compromise of a small, trusted service provider – such as a personal assistant, a family foundation's vendor, a gardener, or a construction contractor – can leak highly sensitive PII, which is then used for targeted spear-phishing against the executive's primary accounts.
Vulnerable Plugins / Integrations	Exploiting flaws, or "holes," in software used on a personal website, blog, or productivity software to inject malware or perform client-side data scraping. A software update, like the ones Apple sends regularly, often contains a "patch" that closes that "hole." Individuals who delay "patching" software can become vulnerable to attack.

The scam: Family Offices often employ remote workers, which creates an emerging risk involving deepfake impersonations, where threat actors pose as trusted employees to gain authorized access.

The solution: To offset this risk, the Family Office should have protocols in place to thoroughly screen potential hires and ensure individuals are experienced, genuine, and trustworthy.

Common signs of an attack

While the scenario may seem grim, there are red flags that can signal bad actors at work and prompt HNWIs and the Family Office to take measures to stop cybercriminals in their tracks. Below are signs to watch for to identify potential malicious activity:

Financial & Account Activity

- Micro-deposit requests - often used by attackers testing access to bank or investment accounts
- Unexplained password resets or login failures - could signal credential stuffing or someone trying to hijack accounts
- Unrecognized logins or devices on email, cloud, or social accounts
- Unexpected MFA/2FA prompts that weren't initiated by the user – e.g., a code sent to an individual's email that they did not request

Device & Network Behavior

- Blocked access to accounts - attackers may lock out legitimate users to buy time
- Very slow internet speeds - can be a symptom of malware, crypto-mining, or data exfiltration
- Unexplained spikes in power consumption or device heat - often linked to hidden processes like crypto-mining malware
- Missing or altered files/data - signals of ransomware or data theft
- Unexpected pop-ups, crashes, or software installations - potential malware infection

Communications & Social Engineering

- Unusual or overwhelming text messages - part of SMS flooding to drown out legitimate 2FA codes
- Urgent emails, texts, or calls - attackers create panic to override skepticism ("act now" pressure)
- Messages with misspellings, odd formatting, or strange sender details - subtle phishing indicators

Broader Risk Signals

- Family/friends receiving strange messages from your accounts - indicates compromised credentials
- Unusual access times (e.g., logins at 3 a.m. from foreign IP addresses)
- Security software warnings suddenly disabled or not functioning
- Urgent, unexpected communication from "family" requesting money or help

Protecting the family requires a comprehensive approach

Protecting high-net-worth individuals and their families requires a multi-layered approach that covers every possible point of entry for highly motivated and resourceful threat actors.

1. Begin with a thorough assessment of the digital landscape

Quick Checklist:

- ✓ Inventory all devices in the household (computers, phones, tablets, IoT, gaming devices, smart home)
- ✓ List all online accounts and services used by family members
- ✓ Document Wi-Fi networks and confirm router settings and updates
- ✓ Review each family member's social media platforms and sharing habits
- ✓ Assess password practices and use of multifactor authentication
- ✓ Evaluate overall cyber awareness and identify training needs
- ✓ Identify tech provided by children's schools and related accounts, as well as the primary point of contact at the schools for their management

Benchmark your Family Office's cybersecurity against best practice with our quick, self-guided online tool. After completion, you will receive your results along with a complimentary report containing personalized recommendations to strengthen your security procedures. The report will identify any cybersecurity gaps and provide practical steps to protect your Family Office, its principals, and their families against the growing number of sophisticated cyber attacks targeting high-net-worth individuals.

2. Reduce public exposure by minimizing the digital footprint

Quick Checklist:

- ✓ Opt out of data broker listings
- ✓ Remove property photos from Zillow and real estate sites
- ✓ Blur your home on Google Maps
- ✓ Limit GPS/location tracking on apps
- ✓ Avoid oversharing on social media

Definition

Data brokers collect, analyze, aggregate, and sell large amounts of personal data about individuals to third parties, often without a person's direct knowledge or consent. They gather information from diverse sources, including public records, online activity, loyalty programs, and financial transactions, and compile it into detailed profiles that are then sold to various entities, such as advertisers for targeted marketing, insurance companies for risk assessment, and political campaigns for voter targeting. These profiles are also accessible to cybercriminals and can help them track your activities online.

3. Harden all personal accounts and devices

Quick Checklist:

- ✓ Use multifactor authentication everywhere (email, banking, healthcare, social)
- ✓ Store credentials in a password manager like 1Password or LastPass
- ✓ Never reuse passwords—make each one unique
- ✓ Keep all devices and operating systems updated automatically
- ✓ Install anti-malware and avoid clicking on unknown links or attachments

(More on this can be found on our blog.)

Definition

"Harden" means to use the native cybersecurity settings and ensure the toggle options are not inadvertently exposing data.

4. Ensure home networks and connected devices are secure

Quick Checklist:

- ✓ Use a separate, non-identifiable guest network
- ✓ Keep all smart devices patched with the latest firmware
- ✓ Update and secure home automation systems with your A/V provider
- ✓ Regularly inventory connected devices
- ✓ Automate updates wherever possible

5. Exercise extreme caution when traveling

Quick Checklist:

- ✓ Avoid public Wi-Fi – always use a VPN
- ✓ Never scan QR codes to connect to Wi-Fi
- ✓ Use RFID-protected wallets and bags
- ✓ Turn off location sharing while traveling
- ✓ Log out of sensitive accounts when not in use
- ✓ Consider using a "travel phone" only equipped with essential services rather than your primary personal phone while on the road

6. Create a sustainable culture of security through ongoing education and strong processes

Quick Checklist:

- ✓ Use privacy settings on all social media accounts
- ✓ Only accept friend requests from known contacts
- ✓ Verify unexpected or urgent requests using a code word
- ✓ Teach children and teens to recognize phishing attempts
- ✓ Pause before clicking – if in doubt, don't act hastily

Taken together, these measures create a holistic defense strategy – reducing risks, enhancing resilience, and giving families the confidence that their wealth, privacy, and legacy are protected against an increasingly sophisticated cyber threat landscape.

Practical steps for Family Office managers

Family Office managers can build digital risk management into their operations through the following actions:

Be Proactive in Understanding or Quantifying Risk:
Ask each household to self-assess using the 20-question self-assessment provided above.
(See page 13)

Conduct Full Digital Footprint Audits:
Map all personal and professional devices, accounts, domains, and connected entities.

Educate and Empower:
Deliver regular briefings on new threats and tactics. Conduct phishing simulations and hygiene reviews.

Adopt Zero Trust Principles:
No implicit trust — even for family members or close aides. Use strict access controls and authentication.

Monitor Online Presence:
Establish active reputation and impersonation monitoring, especially for social media and public-facing platforms.

Establish Internal Processes to Counteract Fraudulent Requests:
Implement multiple steps to prevent scams and malicious requests from succeeding. For example, require signatures or approvals from 2-3 Family Office staff members before a payment is made.

Partner With Experts:
Work with trusted cybersecurity subject matter experts for ongoing monitoring, incident response, and forensic services.

Conclusion

The reality for Family Offices is that digital protection of their principals and clients can no longer be an afterthought – it is the foundation upon which to maintain wealth and legacy in the 21st century. Given the high percentage of Family Offices that rank cyber risk as a top concern, and with over half having experienced a recent attack, inaction guarantees future compromise. To truly fulfill their mandate of preserving generational wealth, Family Offices must proactively champion and implement cybersecurity best practices across every facet of the principal's life. This holistic, layered defense strategy is the only effective countermeasure to sophisticated, AI-driven threats, ensuring that the convenience of the connected world does not come at the cost of the family's security, privacy, and peace of mind.

BLACKCLOAK®

For more information or for an initial consultation, contact BlackCloak.

info@blackcloak.io | www.blackcloak.io