The Rise of Cyber Crime Against Affluent Individuals

Cybercriminals target affluent individuals. Learn how to build cyber protection in a digital world.

The Rise of Cyber Crime Against Affluent Individuals

The COVID-19 pandemic has widened avenues of attack on affluent and high-net-worth individuals. Executives are working from home, and much of banking and shopping has moved online. Social media connects us in a socially distant world. IoT devices are linking everything from home security systems to music playlists.

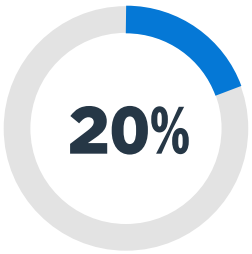
COVID-19 accelerated digitization for many industries by as many as seven years.[1] According to the FBI, there's been a 400% spike in cybercrimes since the onset of the COVID-19 pandemic.[2]

Because of their wealth, name recognition and access to corporate assets, high-net-worth individuals are prime targets. The potential cost to an individual is enormous: In addition to direct financial losses, individuals face costs associated with forensic investigations, enhanced security measures, potential lawsuits and other associated indirect costs.

In addition, with the sudden boom in remote work, high-net-worth individuals, their kids, household staff and guests are often all working off a single, cloud-based home network, leaving them more vulnerable than ever.

Worse, many may think cybercrime only happens to other people — but as many as 20% of family offices have knowingly experienced a cyber security attack prior to the coronavirus pandemic.[3] It's likely that this number is significantly higher today.

Learn how to build protection from the surge in cybercrime. HUB International helps breakdown the various risks, how to reduce ones digital footprint and what to do if fallen victim to a cyber breach.



Of family offices have knowingly experienced a cyber security attack.

Most common forms

76%
PHISHING

33%
MALWARE

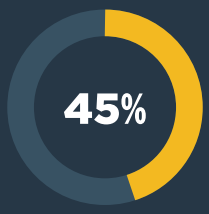
33%
SOCIAL ENGINEERING

SOURCE: UBS Global Family Office Report 2019 | UBS Global — *ubs.com*

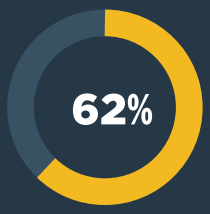
[1] McKinsey & Company, "How COVID-19 has pushed companies over the technology tipping point—and transformed business forever," October 2, 2020.
[2] MonsterCloud.com, "Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic," August 11, 2020.
[3] UBS, *Global Family Office Report 2019*, September 30, 2020.

23% Nearly 1/4 Americans have been victims of identity theft.

Of these cases report the victim losing money



Of these cases, the loss is more than **$1,000**



Of the time the victim gets their money back

47% Of Americans have been victims of credit card fraud

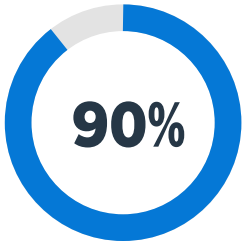
SOURCE: Identity Theft and Credit Card Monitoring Consumer Shopping Study: 2020 — *Security.org*

Bad Actors Play the Long Game

When scouting possible targets and planning major attacks, cybercriminals can infiltrate your accounts and remain undetected for months at a time.

When they make their move, these hackers will have had access to your accounts, email and personal information for weeks or months. Cybercriminals play the long game, acting only after they've gathered enough information to be dangerous. For example, with the right information, a hacker can trick a wealth manager into wiring tens or even hundreds of thousands of dollars from your brokerage to your bank account, then siphon it to an untraceable account abroad.

Today's cybercriminals have incredible patience, which maximizes opportunities. Their activities are extremely lucrative — reportedly, they can illicitly obtain as much as $2 million a year.[4]



Of cyber claims stem from some type of human error or behavior.

SOURCE: Almost 90% of Cyber Attacks are caused by Human Error or Behavior — *chiefexecutive.net*

[4] ComputerWeekly.com, "Cyber criminals earn up to $2m a year, study shows," April 10, 2018.

Cyberthreats: Old tactics, updated for our times

The top cybersecurity threats are familiar to most, but they've been updated for the times, including new aspects or threat vectors. Three of the most common cyberthreats include identity theft, reputational threats, and social engineering:

1. IDENTITY THEFT

In one of the oldest types of cybercrime, fraudsters will access your identity, either selling it immediately or using it later for a bigger payout. Identity theft is also one of the hardest breaches for a victim to uncover.

And recovering from a single incident of identity theft can take an individual six months and as much as 40 hours of effort.[5] Identity theft plays itself out in many ways:

- **Credit monitoring accounts opened with Experian or Equifax in victims' names.** Thieves will scan your credit report for accounts or credit cards you're not using. They'll have a new card issued and sent to them.
- **Hacking into cell phones, computers or tablets.** When a device is connected to public WiFi, thieves can swipe personal information. They'll grab login IDs and passwords to financial institutions, email address and password, and any other personal data stored on the device.
- **Leverage breach data.** Thieves will obtain personal information — including Social Security numbers, email addresses, passwords and more — from major data breaches, like the Cit0Day breach that leaked more than 23,000 databases containing more than 13 billion records.
- **Using sites like Google Maps, Zillow or Redfin to locate upscale neighborhoods.** Thieves will canvass upscale neighborhoods and collect mail containing personal information they can sell or leverage to uncover more information.

CASE STUDY

An 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 — the FBI got involved but the funds were never recouped.

More than **37 billion records were exposed globally in 2020**, an increase of 141%.

SOURCE: New Research: No. of Records Exposed Increase of 141% in 2020 — *RiskBasedSecurity.com*

[5] CNBC, "The latest ways identity thieves are targeting you — and what to do if you are a victim," February 27, 2020.

2. REPUTATIONAL THREATS

Criminals are not just interested in your wealth, but also your influence. A hacker will extort people through compromising photos, private information or travel plans. In return for not releasing information that may prove damaging, cybercriminals will demand a large ransom.

3. SOCIAL ENGINEERING

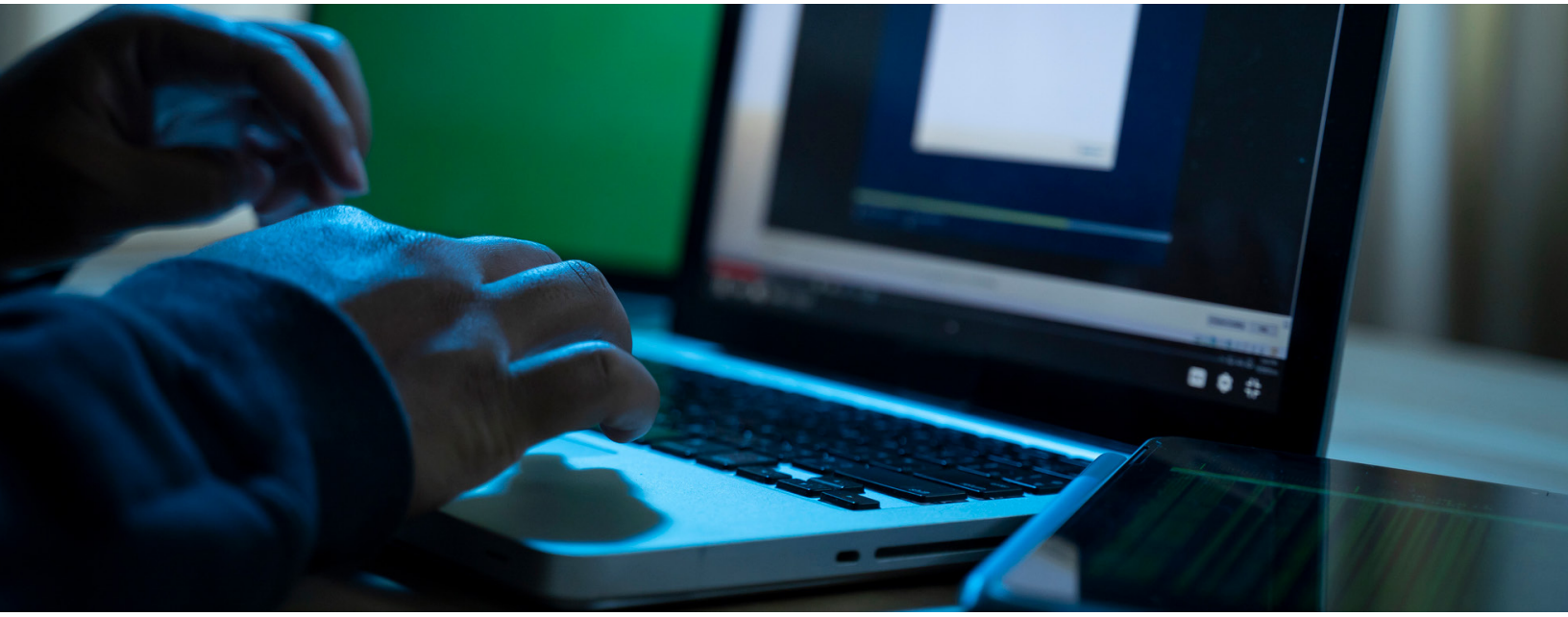
Manipulating someone into releasing money or information (which can lead to bigger sums), often through an email or telephone scam is common and profitable. Social engineering usually at its core, requires human error for success, making it the most preventable form of cybercrime.

Although tactics involving mass spamming remain in vogue, sophisticated hackers often target victims. A criminal may have been in the victim's network for weeks or months and studied their habits and actions, so the hacker knows what will result in a large windfall. What's more, criminals can even gain entry to a cell phone, tablet or laptop through its camera. This allows them to unlock your device and track your habits, learn your passwords and more.

CASE STUDY

Innocent photos become an extortion tool

The son of a high-profile real estate mogul uploaded pictures of himself at a party to his Facebook account. A hacker who had been following the teen downloaded and altered the pictures and uploaded them to a website, so he could extort the family.



How to Build Cyber Walls Around Your Assets

Like a medieval castle with a moat, drawbridge and knights, a multi-tiered approach to cyber security 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 Password1 to create and organize strong, complex passwords for each individual 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 kids as well.

TWO-FACTOR AUTHENTICATION. Four out of five hacking-related breaches leverage either stolen or weak passwords.[6] Using two-factor authentication — a password and a passcode sent through a different medium — provides a double-locked gate for important information.

TIP: *While using your phone as the second-factor authentication works fine, but an app authenticator like Authy or software tokens or hardware such as Yubikey offer even greater protection.*

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 using the network. Creating segments in your home network, such as a guest network and segments for other family members, personal matters and work provides extra levels of protection.

CASE STUDY

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.

[6] SecureLink, "80% of Hacking-Related Breaches Leverage Compromised Passwords," December 10, 2020.

STRENGTHEN YOUR WIFI 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 WiFi name. Anonymous names are more private and therefore more secure.

NEVER USE PUBLIC WIFI

Airport lounges, hotel lobbies and coffee shops are hot spots 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.

TIP: *Cybercriminals will often go into public areas of airports and malls to set their computer as an additional hotspot. Be aware of your phone's WiFi automatically connecting to them. Go to your WiFi settings and turn off "Auto-Join Hotspot."*

USE A VIRTUAL PRIVATE NETWORK

Airport lounges, hotel lobbies and coffee shops are hotspots for hackers, so 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.

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 cyber security 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.

CASE STUDY

Setting sail aboard the wrong ship

One family office manager received an email from his boss asking to wire money to a specific account for the purchase of a new yacht. The manager knew the boss was in the market for a boat, so he wired the money. Unfortunately, a hacker — who had access to the victim's email and lurked for some time — had sent the email and received the funds. The crime was only uncovered when the real boss phoned the manager asking to wire money for his real boat purchase.

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 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, including the IT forensics investigation and state 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 somewhere between a couple thousand dollars to more than $100,000.[7] 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 a reimbursement for financial losses sustained during and because of the cyber breach. This may include business interruption (BI) coverage for the lost work time, as well as for any federal or state fees resulting from the breach.

CASE STUDY

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.

3.2 million

people reported being victim to fraud or identity theft in 2019

20% IDENTIFY THEFT

20% IMPOSTER SCAMS

Median loss by age	
20-29 years	**$448**
70 years	**$800**
80+ years	**$1,600+**

1 in 10

people lost money in imposter scams, with **$667 million** reported lost, **$700** median loss

SOURCE: Federal Trade Commission, January 2020 report — *ftc.gov*

[7] Vestige, "How Much Does Digital Forensics Cost?", accessed February 23, 2021.
Securitymetrics.com, "What Does a Cyber Forensic Investigation Do and How Much Does It Cost?", August 17, 2016.

What cyber coverage is right for you?

Remember: Cyber coverage for your personal assets is not a stand-alone policy. Instead, it's an endorsement to your homeowner's or property policy, and it's an endorsement not all insurance carriers will offer.

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 — when tricked into sending money, for instance — 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 opens credit cards in your name, that's considered an offline breach that the right endorsements will cover.

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 these, the only solution is to be proactive and safeguard your assets.

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:

1. **Call the cyber response hotline attached to your cyber coverage.** The insurance representative will give you instructions to help stop continuing fraud. They'll also get the ball rolling to engage your cyber coverage.

2. **Contain the breach.** Take any breached device offline immediately. If you've built strong walls around your data (see "How to Build Cyber Walls Around Your Assets" on page 6), you should be able to locate and isolate the attack.

3. **Engage experts.** Your cyber insurance team will connect you to a privacy attorney who specializes in cyber breaches, and to an IT forensics team that can pinpoint the site of your breach to eliminate it. The faster you can get expert eyes on the problem, the better chance of limiting the damage.

Safeguard your family and assets *now*

Most hackers or gangs aren't criminal masterminds. They're usually successful only with a careless victim. Understanding your online vulnerabilities is the first step to protecting yourself and your family from an unwanted intrusion. Next, engage the resources and tools at your disposal to safeguard you and your family from any type of cybercrime.

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 your clients today while anticipating their needs and guiding them through tomorrow.

HUBPCA.com

Ready for tomorrow.

Risk & Insurance | Employee Benefits | Retirement & Private Wealth

HUB