HUB

Under Lock and Key

Why high net worth individuals face unique exposures to cyber crime

hubinternational.com

Under Lock and Key

Why high net worth individuals face unique exposures to cyber crime.

Smartphones, tablets and wireless networks are connecting us in new ways every day. Along with this heightened connection comes increased risk.

Today, technology is multiplying at a faster rate than device security. Devices are coming to market with minimally imbedded defenses — and convenience is winning the race by a long shot. Smart devices are in demand with or without the most robust security and too many individuals are still thinking, "It won't happen to me."

But, it will. Fraudsters stole $16 billion from 12.7 million U.S. consumers last year; every two seconds there is a new victim of identity fraud.[1]

Cyber security breaches can take the form of theft, manipulation, destruction, extortion or a reduction of access to data and can happen for a variety of reasons. Some do it to destroy reputations, others for financial reasons, extortion and blackmailing.

The U.S. is the most targeted country in the world for cyber attacks - both by perpetrators across the globe and those within our own borders. That is because Americans have the wealth and economic capital cyber-criminals are looking for. In fact, high net worth individuals in the U.S. are 1.5 times more likely to fall victim to identity theft.[3]

"High net worth individuals have a uniquely high exposure because of how they interact with social media, in the banking sector and more," said Hart Brown, CORP, CBCP, LPQ, Vice President, Practice Leader, Organizational Resilience, HUB International. "Most prefer to use mobile banking and make online purchases. The exposure level of the high net worth individual and their cybercrime education level is disproportionate."

Learn how to protect yourself by understanding the risks, reducing your digital footprint and responding appropriately when you suspect that a cyber breach has occurred.

CYBER STATS

Fraudsters stole
$16 BILLION
from 12.7 million US consumers last year[1]

Every **TWO SECONDS**
there is a new victim of identity fraud[1]

Identity thieves stole
$10.4 MILLION
from more than 20,000 victims in Canada in 2014[2]

2/3 IDENTITY FRAUD VICTIMS
received a data breach notification[1]

47% or **110 MILLION** Americans, had their personal information exposed during 2014[7]

Understand Cybercrime Threats

Knowledge is power. Understanding today's most common cyber crimes and how personal data can be accessed is the first line of defense in snubbing the perpetrators.

"Historically bad guys would sit outside your office or house and choose the right time to break in. During that period, there were multiple opportunities to identify them," said Brown. "In a cyber environment that visibility doesn't exist – the bad guys can be as patient as they want. In most cases, we don't even know they're there. They don't have to be in close proximity to harm you." Cyber hackers have a number of tools they can use to infiltrate someone's cyber presence – and they use them from the office next door or from their bedroom across the ocean. Here is what is in their bag of tricks:

PHISHING. Email messages sent out in the hopes of acquiring usernames, passwords and credit card details. These emails often contain poor spelling and grammar as well as false links known to spread malicious software so the perpetrator can access an individual's computer. They are sent in the hundreds of thousands with the hope that just a few people will respond.

SPEAR PHISHING. Phishing from a familiar email address - either a person, organization or business known to the victim. This tactic will disseminate fewer, more targeted emails and may contain more detailed information.

WHALING. Phishing that specifically targets high net worth individuals or senior executives – aka "the big fish." Although fewer nets are cast and the data is harder for the cyber criminal to obtain, the potential payback is much greater.

BLUE JACKING. Criminals will try to download data directly from a wireless Bluetooth connection. It's simple - there is even a blue jacking program, downloadable for free.

JUICE JACKING. Unlike computers, cellphones were designed to charge and send data through a single port. Today, convention centers, airports and train stations all have free charging stations. Cyber criminals have been known to set up these stations and download all the data from an individual's phone while it's charging.

SOCIAL ENGINEERING. Social engineering is the act of obtaining personal information, like a mother's maiden name, first school attended, birth date, address and banking institution of choice, by skimming the individual's publicly available social media profiles. Because as many as 90% of high net worth individuals are active on social media, spending as much as 48 hours per week networking[4] - and it is estimated that as many as 54% of social media users are targeted by identity thieves[5] - high net worth individuals are a prime target for social engineering. By obtaining this information, a cyber criminal can answer security questions, gain access to one's bank or credit card accounts, and even use personal information for a virtual kidnapping scheme.

VIRTUAL KIDNAPPING: Could you be a target?

Virtual kidnapping, a scheme in which an individual or criminal organization alleges a kidnapping and demands ransom, has become big business in recent years. Thanks to a plethora of personal information available in real time on social media, known high net worth individuals may be at greater risk for this type of extortion.

Perpetrators leverage personal information to hook the family members when in reality the "victim" is simply on an airplane, sleeping in a hotel or unable to be reached by phone at the time. Virtual kidnapping requires very little investment in time and resources for the perpetrator and can be lucrative - initial demands run as high as $10,000 to $20,000.

Some warning signs include: a call from an international area code, not originating from the "victim's" phone; a landline call in which someone asks for a mobile number to call back; demands with nontraditional payment routes like MoneyPak, GreenDot cards, PayPal cards or wire transfers.

If targeted, stay calm. Trust your instincts and call the police. Avoid sharing personal information and instead ask the perpetrator to describe the "victim" and ask to speak to them directly. Call, text or email the "victim" to confirm they are okay.

Minimize Your Digital Footprint

Just as environmentalists work to minimize their carbon footprint, the high net worth individual needs to minimize their digital footprint. A number of simple strategies can help reduce an individual's vulnerability as well as the impact of cyber crimes and identity fraud.

PASSWORD PROTECTION. Password protection remains the most important step to protecting against a data breach. Make sure to change the default password on all devices and programs to one that is complex and unique. For example, instead of "life's a beach," a more secure password might be "Life%is*a^beach72." Regularly update passwords to reduce the value of those stolen in a data breach or through malware. Avoid using the same password on multiple accounts. Password managers can provide a convenient way to minimize the potential for compromise.

SECURE YOUR MOBILE DEVICES. Apply software updates as soon as they become available and take advantage of security capabilities built into cellphones, including protecting the device with a passcode or biometric fingerprint. These measures are designed to provide a baseline of protection but must be actively engaged.

BE RESPONSIBLE ABOUT YOUR SOCIAL MEDIA. Think before posting. This includes pictures and posts revealing someone's whereabouts. Also, consider all exposures, including friends, as they could post pictures of you. Know all default settings and understand how to change them. Take friend requests seriously and consider each tag for its content.

PRACTICE SAFE BROWSING. Some browsers are more secure than others. Online surfing habits are watched by retailers, advertisers and cyber criminals alike. Use bookmarks to access critical business and online banking sites. This will prevent people from landing on "one-off" websites (for example, "coffee shop" vs. "coffee shop 1") even for a minute, which is all a cyber criminal needs to download critical information directly from a computer.

Cyber breach prevention checklist:

- ○ Update passwords regularly
- ○ Apply software updates as soon as they are available
- ○ Think before posting on social media
- ○ Use bookmarks when browsing the web
- ○ Use two-factor authentication
- ○ Turn off wireless technology when not in use

USE DIFFERENT PHONES WHEN APPLICABLE. As recently as five years ago, people still had two or more cellphones - one for work, one for personal. In some cases, there is still a benefit to having different devices for different purposes. Multiple computers and email addresses could work the same way. For example, use one computer exclusively for banking.

TWO-FACTOR AUTHENTICATION. Using two factors (your password and then a unique password sent through a different medium on demand) to get into email or social media profiles will provide an added level of protection. Even if someone knows the password, they still can't get in. Almost all social media and email administrators offer a two-factor authentication option, but it has to be selected and used every time to provide protection.

EMAIL ENCRYPTION. Always available but rarely used, email encryption locks an email system and requires a different code or key each time it is opened. This can be inefficient, but it is an option. Different levels of encryption are available and can be implemented.

TURN OFF WHAT'S NOT IN USE. When not in the car, turn off the wireless Bluetooth to prevent data interception and disable the automatic sync on devices when not in use. Children will often leave apps running on a cellphone. Turning them off each time will eliminate the ongoing pop-up notification and create multiple security vulnerabilities. A recent study revealed that 98% of apps inherently harbor one or more security vulnerability.[6]

BE WARY OF PUBLIC WI-FI

While public Wi-Fi is a convenient way to connect to the Internet when outside the home or office, it presents its own host of risks. Most hot spots skimp on protection, never changing the default setting on their password, and many users are unaware of the potential risk this poses.

Unlike most home and office wireless networks, the data flowing around a public hot spot is usually not encrypted and therefore can actually serve as a window into any device connected to it. Every request from a device travels via an access point, before reaching the sites that users want to visit. Without any encryption of communication between users and the access point, it's easy for a cyber criminal to intercept data entered while using the Wi-Fi network.

Cyber criminals will often go into areas where a hot spot exists and set up their computer as an additional hot spot. Be aware of Wi-Fi passwords that are "one-off."

Syncing your device to the cloud when using public Wi-Fi can expose an entire computer's data. Some devices are set up to automatically sync when near a hot spot. Remember to turn the automatic data sync off and change settings with every upgrade.

For the traveling executive a public Wi-Fi connection can facilitate corporate espionage. Remember that outside of the U.S., most countries don't have the same privacy laws and the governments themselves can even be the perpetrators. For example, when logging onto the hotel network in another country, it may be possible for the government or other cyber criminals to access that individual's device.

When working in public places, experts recommend all individuals purchase their own hot spot.

You've been hacked!

Forty-seven percent or 110 million Americans had their personal information exposed during 2014.[7] That means there is a 50/50 chance of it happening to you. How does someone know if they've been hacked?

Here are a few common signs that someone has stolen your identity:

- Unexplained withdrawals from a bank account
- Bills and other mail are not delivered
- Merchants refuse an individual's checks
- Debt collectors call about debts that aren't accurate
- Unfamiliar accounts or charges appear on a credit report
- Medical providers bill for services not performed
- Health plan rejects a legitimate medical claim(s) because the records show the individual has reached his benefits limit
- The Internal Revenue Service (IRS) sends a notice that more than one tax return was filed in someone's name, or that there is income from an employer the individual doesn't work for
- Receiving a notice that information was compromised by a data breach at a company where an individual does business or has an account
- An individual is arrested for a crime someone else allegedly committed
- Receiving an extortion or blackmail threat

Now that it's happened – what can be done?

It can be overwhelming when an individual falls victim to a cyber crime data breach. What actions must be taken? Who should be notified first and how can an individual uncover the extent to which their personal information has been compromised? Here's a run down of the do's and don'ts post-breach, by violation.

ATM AND DEBIT CARDS Federal law limits liability for an unauthorized electronic transfer of funds that results from identity theft. Report an unauthorized withdrawal or purchase as soon as it is discovered.

CHECKING ACCOUNTS If checks are stolen, contact the bank or financial institution and ask them to close the account as soon as possible. Victims might be responsible for a loss if they knew about a problem but didn't report it to the bank in a timely manner.

CREDIT CARDS To dispute fraudulent charges, contact the credit card company within 60 days of receiving the bill with the fraudulent charges. Individuals are responsible for keeping track of their statements.

BANKRUPTCY FILED IN YOUR NAME Contact the U.S. Trustee in the region where the bankruptcy was filed. The U.S. Trustee Program refers cases of suspected bankruptcy fraud to government offices for possible investigation and prosecution.

INVESTMENT ACCOUNTS If an identity thief has tampered with investments or brokerage accounts, contact the broker, account manager and the U.S. Securities and Exchange Commission (SEC). If the investment adviser attempts to handle the issue exclusively, this could be a red flag. Don't be afraid to go to the SEC directly.

DEBT COLLECTORS To stop collection action, contact the debt collector, the business that opened the fraudulent account and the credit reporting companies.

MISUSE OF SOCIAL SECURITY NUMBER If a Social Security number is stolen, it can be sold or used to obtain a job or other benefits. Contact the U.S. Social Security Administration when any misuse is discovered.

INCOME TAXES If a person thinks someone has misused their Social Security number to get a job or tax refund – or the IRS sends a notice indicating a problem – contact the IRS immediately.

MEDICAL IDENTITY THEFT If a person suspects an identity thief has used their medical information, get copies of all medical records. Under federal law, individuals have a right to know what is in their medical files. Contact each doctor, clinic, hospital, pharmacy, laboratory, health plan and anywhere a thief could have used the information. For example, if a thief got a prescription in a false name, ask for the record from the pharmacy that filled the prescription and the health care provider who wrote the prescription. There may be a fee to get these copies.

CHILD IDENTITY THEFT Child identity theft happens when someone uses a child's personal information to commit fraud. A thief may steal and use a child's information to get a job, government benefits, medical care, utilities, car loans or even a mortgage. To get a minor child's credit report, a parent or guardian must contact the credit reporting companies and provide proof of identity and other documents.

CRIMINAL VIOLATIONS If an identity thief uses someone's name, date of birth, Social Security number or other personal information during an investigation or arrest, the information will be added to that state's criminal database. Contact the agency that made the arrest, the court that convicted the identity thief, and the state Attorney General's office to get documents that will help prove innocence.

GATHER THE EVIDENCE

Regardless of the type of theft, a cyber crime victim will want to use these three tools to unravel the clues.

Start an identity theft report This will help you get fraudulent information removed from a credit report, stop debt collection resulting from identity theft or from selling the debt to another company for collection, place an extended fraud alert on your credit report and get information from companies about accounts the identity thief opened or misused.

Review your credit reports If an identity thief tampered with your account, order a copy of your credit report. Read the report to see whether other fraudulent transactions or accounts are listed as well. Report any errors to the credit reporting companies and appropriate businesses.

Get copies of documents the identity thief used Ask for copies of any documents the identity thief used to open a new account or make charges in your name. These documents can help prove the identity theft occurred.

Post-cyber breach checklist:

- ○ Contact your bank immediately to report a theft of an ATM and debit card or paper checks
- ○ Report a credit card breach within 60 days of receiving a fraudulent charge notification
- ○ Call the local U.S. Trustee if a false bankruptcy was filed in your name
- ○ Contact the Social Security Administration for Social Security number theft
- ○ Report Social Security number misuse to the IRS
- ○ Get copies of your medical records immediately if you suspect medical identity theft
- ○ Contact credit reporting companies if you suspect child identity theft and ask for a credit report

Safeguard your Family and Assets Now

Most cyber crimes aren't carried out by masterminds, but are successful because the average consumer isn't as careful as he could be.

It has never been more important to minimize an individual's digital footprint in order to safeguard assets and keep families safe.

"The fear is out there that a cyber-initiated event will result in a physical theft or actual kidnapping for ransom. This is happening more and more," said Brown. "Again, the answer is to reduce our digital footprint as much as we can and minimize the potential for people to access our data. I believe the high net worth individual has the tools to do so at their fingertips – and the time is now."

SOURCES:

1. 2015 Identity Fraud Study. Javelin Strategy & Research. https://www.javelinstrategy.com/brochure/347
2. http://www.antifraudcentre-centreantifraude.ca/reports-rapports/2014/ann-ann-eng.htm#a28
3. http://cyberelitesuite.com
4. http://www.forbes.com/sites/johnrampton/2014/04/29/connecting-with-high-net-worth-individuals-through-social-media/
5. http://www.idtheftcenter.org/images/surveys_studies/FacebookSurveyFinding.pdf
6. 2015 Trustwave Global Security Report. https://www.trustwave.com/Resources/Security-Stats/
7. http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/

Looking out for you.

Looking ahead for you.

HUB International Personal Insurance, a specialized practice within HUB International, is dedicated exclusively to serving the insurance and risk management needs of individuals. As one of the largest privately-held personal insurance practice in North America, we provide detailed guidance to help protect the people and possessions that are important to you.

hubinternational.com