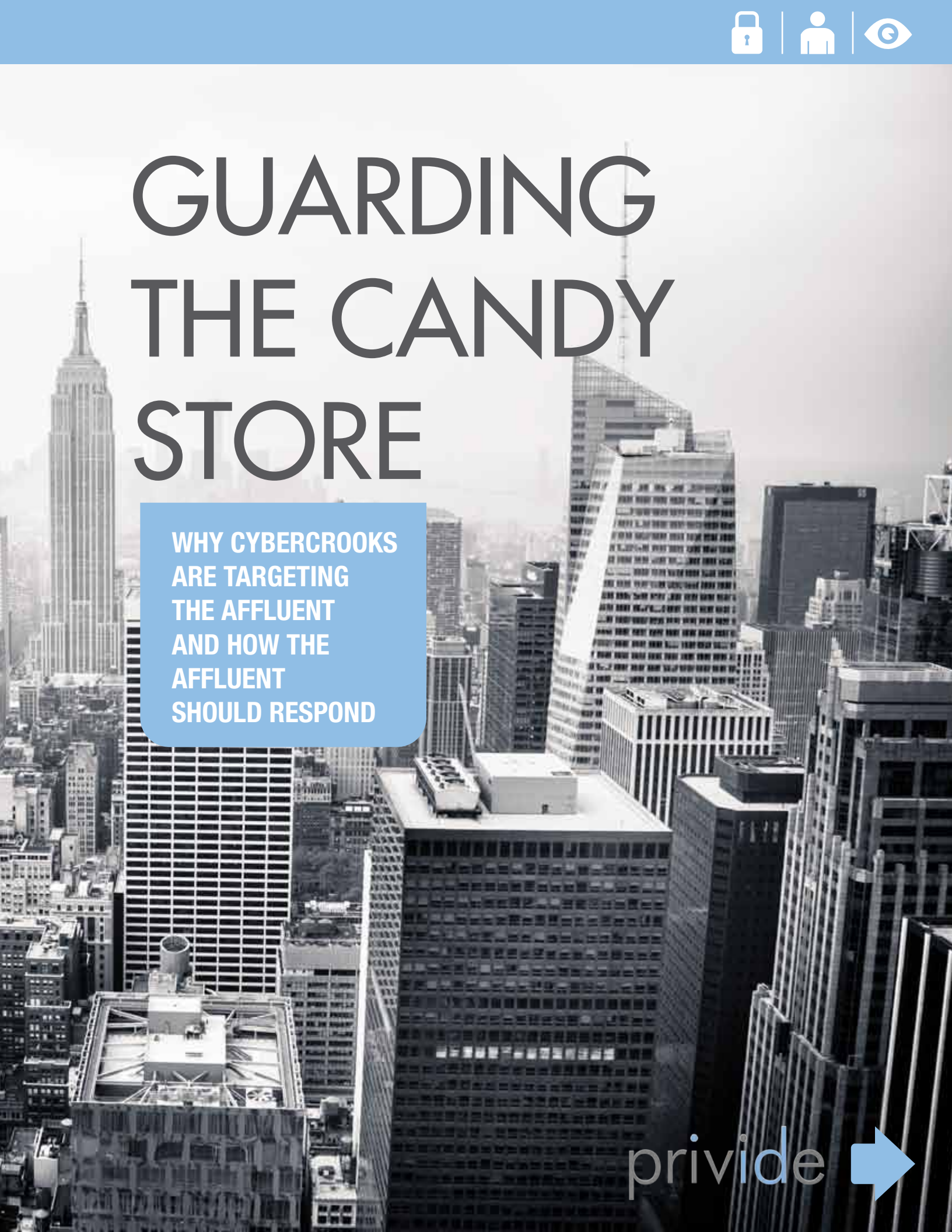


GUARDING THE CANDY STORE

WHY CYBERCROOKS ARE TARGETING THE AFFLUENT AND HOW THE AFFLUENT SHOULD RESPOND

privide

CYBERCROOKS, IDENTITY THIEVES, AND THE AFFLUENT

NOT ALL CONSUMERS ARE CREATED EQUAL. AT LEAST IN THE EYES OF HACKERS AND IDENTITY THIEVES. PROFESSIONAL AND HIGHLY SKILLED CYBERCROOKS ARE NOW FOCUSING THEIR ATTENTION ON THE TARGETS THAT PROVIDE THE BIGGEST PAYOFF WITH THE LOWEST RISK. CROOKS CALL THEM "CANDY STORES."

Candy Stores are the most affluent personal targets - higher net worth families, professional advisors, and successful small business owners who not only offer the best payoff to hackers and identity thieves but also provide a gateway to endless other assets.

The crooks are after more than money. Data is the currency of cybercrime, and Candy Stores provide access to a wealth of valuable information that includes personal and corporate secrets, business and social contacts, customer and employee files, and financial and investment information.

For the affluent consumer the worry is also about reputation, retirement, public embarrassment, family, bucket list, partners and business associates, legacy, wasted time, private secrets, business deals.

And while the business of cybercrime is evolving rapidly, almost daily, for the last decade consumer security has changed little. For most consumers, options are limited to a cookie-cutter identity protection service and some antivirus software. That's it. For the more affluent consumers, who are targeted by the more sophisticated attackers, these defenses offer little resistance.

Written by one of the world´s top consumer security experts, this free guide will explain who's targeting these individuals and businesses, what their motivations are, and how they're doing it.

The guide will also explain how to spot and avoid some of the advanced threats you may be targeted with, as well as a variety of free tools that can help protect your money, your credit, your computers, devices, information, and secrets.

CONTENTS

ABOUT THE AUTHOR

This guide was created by Neal O'Farrell, widely considered the most experienced consumer security expert on the planet. He earned that reputation fighting cybercrime and identity theft around the world for more than three decades. Today Neal leads Privide Inc., the only company to provide advanced cyber, identity, and privacy protection to higher net worth individuals, families, and businesses.

By the time he was 25 Neal was considered one of the world's youngest computer security experts, developing advanced encryption systems to protect sensitive communications systems for governments, the military, and the financial industry. Many of the technologies we take for granted today, to protect our computers, our information, and our banking, Neal was working on more than a quarter of a century ago.

As Executive Director of the Identity Theft Council, an award winning non-profit victim support network, he has personally helped thousands of victims of identity theft. The Council is a national partnership that includes the Council of Better Business Bureaus, the Community Bankers of America, the Online Trust Alliance, the Identity Theft Resource Center, and the Elder Financial Protection Network. In 2011 Neal's work was recognized by the security industry when the Council was the first non-profit to win the prestigious SC Magazine Editor's Choice Award, presented at the RSA Security Conference in San Francisco. Previous winners of the award include the SANS Institute and the NSA.

Neal was the only security expert to be appointed Senior Advisor to the Stock Act panel, the Congressionally-mandated study into the security, privacy, and other implications of the Stock Act, signed into law in 2013. Neal has authored more than 150 articles on security and has appeared in numerous publications around the world including CNN Money, BusinessWeek, USA Today, SmartMoney, CNET, Information Week, the National Law Journal, Today.com, NBC, CBS, CNBC, Fox Business, and the South China Morning Post.

He is the author of "Double Trouble - Protecting Your Identity in an Age of Cybercrime," used as an education tool by numerous organizations including three of the top five U.S. banks as well as Costco and the NFL Player's Association. He was a member of the Federal Communications Commission's Cybersecurity Roundtable Working Group, and Technical Editor for the "Hack Proofing" series of security guides from Elsevier Publishing.

ABOUT PRIVIDE

Privide is the first firm to provide advanced cyber, identity, and privacy protection to high net worth consumers, professional advisors, and growing small businesses. For more information please visit **www.privide.com**, or contact Neal O'Farrell, founder and CEO of Privide, directly at **neal@privide.com**

1

SO WHY TARGET CANDY STORES?

A CANDY STORE (THEIR TERM, NOT OURS) HAS TO FIT A NUMBER OF CRITERIA.

- THEY HAVE TO BE EITHER WEALTHY OR AT LEAST MORE AFFLUENT THAN THE AVERAGE CONSUMER.
- THEY SHOULD IDEALLY HAVE INFORMATION AND CONNECTIONS THAT THEY WOULDN'T WANT EXPOSED OR OTHERS TO HAVE ACCESS TO.
- THEY SHOULD HAVE SUBSTANTIAL BANK ACCOUNTS, IDEALLY INVESTMENT AND BUSINESS.
- THEY SHOULD BE CONNECTED TO OTHER SIMILAR INDIVIDUALS, THROUGH THEIR FRIENDS, NEIGHBORS, WORK, CHARITIES, POLITICAL ACTIVITIES ETC.
- A GOOD SUBSTITUTE WOULD BE A PROFESSIONAL, LIKE A LAWYER OR PHYSICIAN, WHO HAS ACCESS TO CLIENT AND PATIENT RECORDS.

"NEARLY **$5 BILLION**
WAS STOLEN FROM CONSUMER BANK ACCOUNTS IN THE U.S. IN 2012 BY HACKERS INFECTING COMPUTERS WITH MALWARE"
JAVELIN STRATEGY AND RESEARCH.

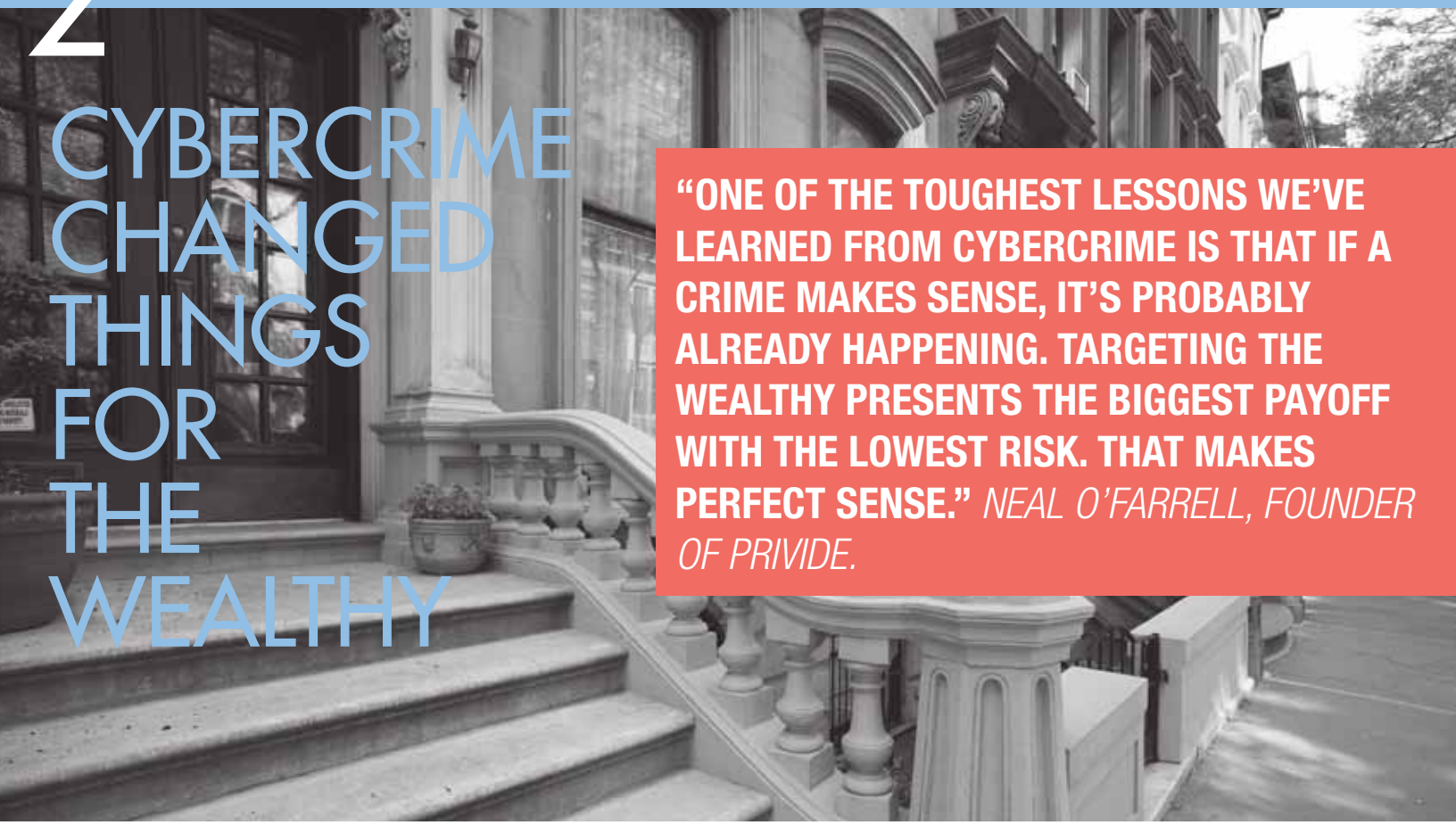
CANDY STORES CAN INCLUDE SUCCESSFUL SMALL BUSINESS OWNERS AND PROFESSIONALS, PHYSICIANS, LAWYERS AND LAW FIRMS, FINANCIAL ADVISORS, WEALTH MANAGERS, BROKERS, INSURANCE AGENTS AND MANY OTHER PROFESSIONS.

THERE ARE A NUMBER OF REASONS CYBERCROOKS WANT TO TARGET SUCH INDIVIDUALS:

- THEY TEND TO HAVE MORE MONEY TO STEAL AND BETTER CREDIT TO EXPLOIT.
- THEY HAVE MORE ACCOUNTS TO PROTECT, FROM INVESTMENT ACCOUNTS TO TRUST ACCOUNTS, AND OFTEN DON'T PROTECT THEM VERY WELL.
- THEY TEND TO HAVE MORE WEAK LINKS AROUND THEM, FROM ADVISORS TO EMPLOYEES, WHO CAN BE USED AS A BACK DOOR.
- THEY HAVE INFORMATION THAT COULD BE OF HIGH VALUE ON THE BLACK MARKET, INCLUDING PERSONAL AND CORPORATE SECRETS, BUSINESS AND SOCIAL CONTACTS, INVESTMENT INFORMATION, AND EVEN CLIENT AND PATIENT RECORDS.
- THEY CAN OFFER A STEPPING-STONE TO MANY OTHER "CANDY STORES" THROUGH THEIR BUSINESS AND SOCIAL CONNECTIONS.
- THEY CAN PROVIDE A BACK DOOR TO THEIR OWN CORPORATE INFORMATION, ESPECIALLY CUSTOMER AND EMPLOYEE DATA.
- THEY'RE TYPICALLY MUCH HARDER TO PROTECT AND OFTEN TOO BUSY TO FOCUS ON SECURITY.
- THESE VICTIMS RARELY REPORT THE CRIME FOR FEAR OF EMBARRASSMENT OR HARMING THEIR REPUTATION.

2

CYBERCRIME CHANGED THINGS FOR THE WEALTHY



"ONE OF THE TOUGHEST LESSONS WE'VE LEARNED FROM CYBERCRIME IS THAT IF A CRIME MAKES SENSE, IT'S PROBABLY ALREADY HAPPENING. TARGETING THE WEALTHY PRESENTS THE BIGGEST PAYOFF WITH THE LOWEST RISK. THAT MAKES PERFECT SENSE." *NEAL O'FARRELL, FOUNDER OF PRIVIDE.*

Who knew that cybercrime would become the great equalizer? It sounds counter intuitive but wealthy neighborhoods are not the preferred pickings of the thieving class, because rich is rarely worth the risk. Wealthier neighborhoods are usually better protected, gated, and guarded. And you're probably not going to blend in very well when you're cruising the neighborhood in that old panel van with the Penske decal still visible under the single coat of emulsion. Even if you're staying under the speed limit.

Then there are all those extra eyes to avoid. Landscapers, perhaps a nanny or two, or maybe a housekeeper. And if you're lucky to slip past all the human surveillance, you're still not home free. The homes of the wealthy tend to be harder to breach: sophisticated intruder alarms with rapid-response remote monitoring; maybe a video surveillance system and security lights; and almost definitely high quality doors and windows with security locks that don't seem to agree that resistance is futile.

For most crooks, the reward is just not worth the risk. But cybercrime has changed all that. Cybercrime has allowed the most sophisticated crooks to reach out and touch their victims, any victims, from the next neighborhood over or from the other side of the world. They're now free to pick any victims they want, the reward potential has skyrocketed, and the risk is now so low it's barely even a factor. It's like a video game, where the gamer not only has all the control and options, but knows all the cheats needed to guarantee the highest score every time.

The attacks are also far more advanced and persistent than ever before, often making conventional credit monitoring of limited value. Symantec recently told the story of how a CEO was targeted by an endless series of sophisticated hacking attacks that went on for nearly a year. In one month alone the victim was targeted 24 times – that's nearly once a day.

Privide handled a case of a wealthy family where both parents and both teenage kids were the subject of a persistent and very successful series of identity attacks that also went on for nearly a year. And a Silicon Valley entrepreneur whose personal information was pilfered from a wealth management company had to suffer through more than 300 harassing and threatening phone calls in just one month, often starting at five in the morning, and coming from dozens of payday lenders from the U.S. and beyond and all claiming he owed them money.

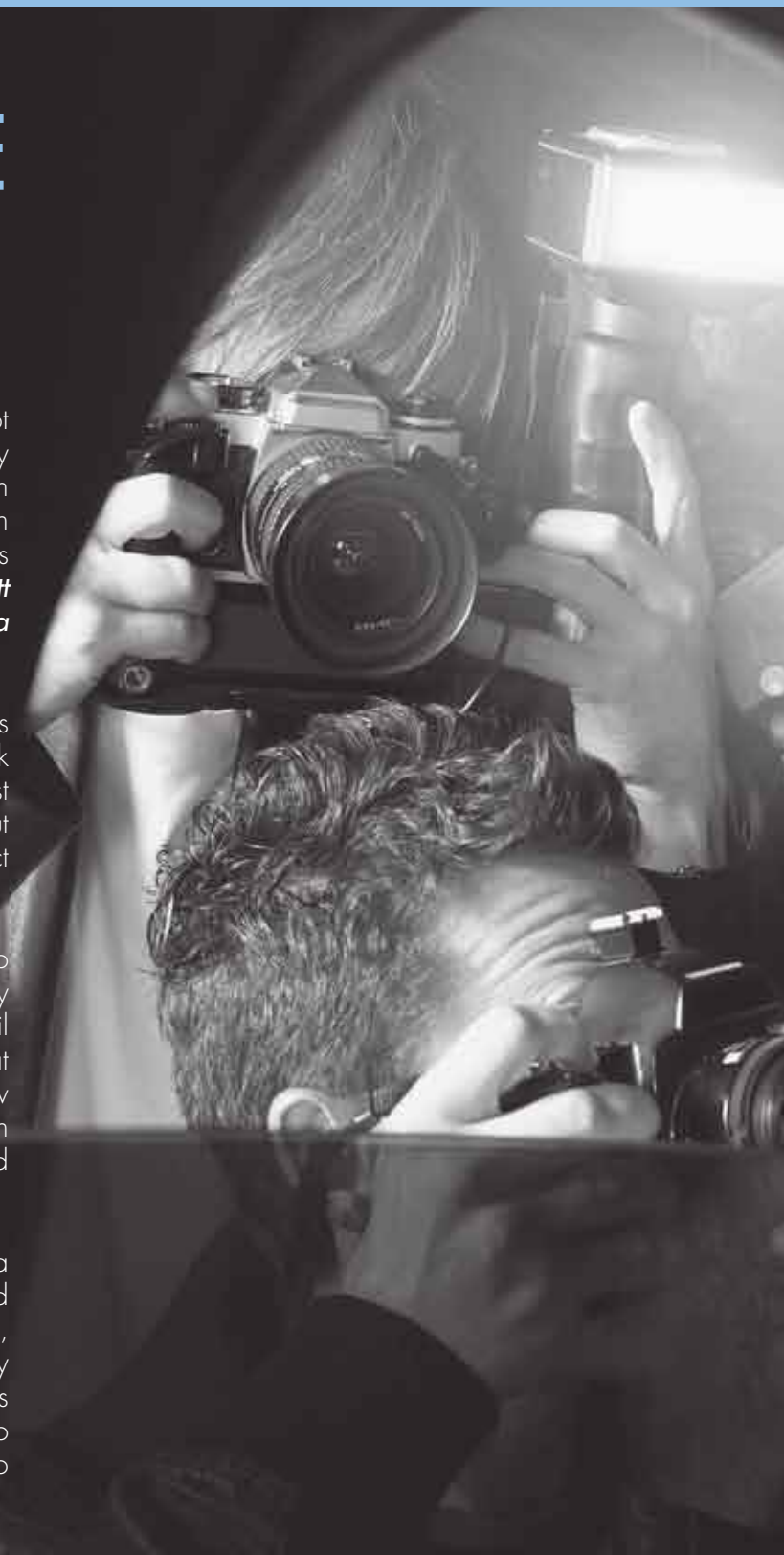
CELEBRITIES ARE NO EXCEPTION

Success and fame can attract all kinds of miscreants, and not just hackers for profit. An internet user with a grudge can very easily become a relentless stalker that may never be caught. In 2012, an amateur hacker was sentenced to ten years in prison when he was convicted of hacking more than 50 celebrities and Hollywood entertainment executives including ***Scarlett Johansson, Mila Kunis, Christina Aguilera, and Vanessa Hudgens.***

According to reports, Chaney got access to the email accounts of the celebrities using a very popular trick – targeting a weak link. In this case the weak link appeared to be a personal stylist who boasted about her celebrity clientele. Once he figured out the stylist's email password, he was able to access her contact list and private email discussions.

In interviews, Mr. Chaney said it was easy to get access to many of the email accounts. He started by assuming that many of the celebrities used Gmail accounts, and that their email addresses used their first and last names. He then used that information to contact Gmail and reset their passwords. How did he answer Gmail's security questions, like mother's maiden name or first school? It was all available in public records and easily searchable.

Once he got access to email accounts, Mr. Chaney stole a variety of personal information including personal and sometimes nude photographs, business contracts, letters, scripts, driver's license information and Social Security Numbers. He also sent emails from the compromised accounts requesting more photos, and used his victim's contact lists to reach other targets. Some of the nude photos were also released to and published by a number of gossip websites.



"I JUST REALLY HOPE THIS DOESN'T HAPPEN TO SOMEONE ELSE. YOU CAN LOSE EVERYTHING BECAUSE OF THE ACTIONS OF A STRANGER."

*ACTRESS **RENEE OLSTEAD** AT THE TRIAL OF CELEBRITY HACKER CHRISTOPHER CHANEY, DECEMBER 2012*

THE LIST OF CELEBRITIES TARGETED BY HACKERS AND IDENTITY THIEVES READ'S LIKE AN A-LIST, AND INCLUDES:

- STEVEN SPIELBERG
- SCARLETT JOHANSSON
- MILA KUNIS
- CHRISTINA AGUILERA
- TIGER WOODS
- RICKY JERVAIS
- 50 CENT
- PAUL ALLEN
- BEYONCE

OTHER CELEBRITY VICTIMS INCLUDE PARIS HILTON, KIM KARDASHIAN, MEL GIBSON, ASHTON KUTCHER, BILL GATES, KRIS JENNER AND MANY OTHERS.

"THAT FEELING OF SECURITY CAN NEVER BE GIVEN BACK AND THERE IS NO COMPENSATION THAT CAN RESTORE THE FEELING ONE HAS FROM SUCH A LARGE INVASION OF PRIVACY."

*SINGER **CHRISTINA AGUILERA** AT THE TRIAL OF CELEBRITY HACKER CHRISTOPHER CHANEY, DECEMBER 2012*

4

THIEVES FOCUS ON THE WEAKEST LINK

THE TARGET STORES BREACH IN 2014 THAT EXPOSED NEARLY 100 MILLION RECORDS WAS TRIGGERED BY A HACKER WHO USED A PHISHING EMAIL TO TRICK AN EMPLOYEE AT A SMALL HVAC CONTRACTOR.

A common ploy by crooks who want to get closer to their chosen target is to exploit one of the many weak links around them. Affluent identities can be much more vulnerable to those around them who may provide easier access – secretaries, admin assistants, portfolio managers, investment managers, financial and legal advisors, and even family and friends.

Thieves often target these individuals with spear phishing and social engineering attacks as a weak link or back door to the real target. One of the ways cyber crooks might try to target your wealth is through your wealth managers or advisors. In December 2013 global security firm Kroll issued an alert that it is seeing significant growth in sophisticated attacks against wealth management firms. Attacks that have resulted in millions of dollars in financial losses.

THE MAY 2014 DATA BREACH AT EBAY THAT EXPOSED INFORMATION ON 145 MILLION USERS WAS AS A RESULT OF A HACKER SENDING PHISHING EMAILS TO A HANDFUL OF EBAY EMPLOYEES.

In the recent case of celebrity hacker Christopher Chaney, who managed to break into the email accounts of celebrities like Scarlett Johanssen and Mila Kunis by figuring out the answers to the secret questions that protected their email passwords, the only way he was able to find the addresses of the dozens of stars he targeted was because he focused on the email account of one celebrity hairstylist these victims confided in. And exchanged emails with.

And in the highly publicized attack on Target Stores, that resulted in one of the biggest data breaches in history and exposed more than 110 million customer records, the attack was started by targeting a low-level employee at a Target vendor using nothing more than a phishing email laced with malware.

And also in 2014, Russian hackers targeting energy companies knew they would have greater difficulty penetrating the security of those corporations. Instead, they found out the favorite restaurants of key employees, hacked those websites, and infected online menus with malware that would be secretly downloaded by employees.

"CYBER CRIMINALS ARE ACTIVELY SEEKING OUT UNPREPARED SOFT TARGETS, AND ASSET MANAGERS' LACK OF CYBER SOPHISTICATION MAKES THEM IDEAL TARGETS."
PRICEWATERHOUSE COOPERS, 2014

5

WHY PROFESSIONAL ADVISORS ARE A TARGET TOO

Nearly fifteen years ago, speaking at the 25th Annual Conference of the State Bar of California's Intellectual Property Section, Privide founder Neal O'Farrell warned of the likelihood that law firms will be targeted as a path to their clients.

In February of 2013, the FBI announced at LegalTech New York that it is seeing hundreds of law firms fall victim to hackers. A few months later the American Bar Association warned its members that "You have been or will be hacked. It is a matter of "when," not "if."

Successful professionals who have access to high net worth clients also meet the definition of Candy Stores. Professional cybercrooks now have a vast array of advanced tools they can use to launch remote, automated, and undetectable attacks against these individuals and their firms. Attacks like spear phishing, social engineering, keyloggers, and website exploits are usually undetectable. And a single security failure by an advisory firm can inflict serious damage on its clients.

"WHAT'S GOING ON IN THE INDUSTRY TODAY IS FULL-SCALE WAR ON FINANCIAL SERVICE COMPANIES AND INSTITUTIONS ALL OVER THE WORLD."

WEALTH MANAGEMENT MAGAZINE, 2013

Such is the concern for the financial sector and particularly for personal advisors that the SEC has introduced cybersecurity as part of its annual testing for broker/dealers.

SO WHY TARGET THESE FIRMS?

- THEIR OWNERS AND PARTNERS ARE OFTEN INDIVIDUALLY HIGH NET WORTH AND WORTH TARGETING.
- THEY PROVIDE AN OFTEN TOO-EASY BACK DOOR TO THEIR CLIENTS AND ACCOUNTS.
- THEY HAVE DETAILED CUSTOMER FILES AND SOMETIMES ACCOUNT CREDENTIALS AND OTHER INSIDE INFORMATION.
- THEY'RE SUSCEPTIBLE TO EXTORTION BECAUSE OF THE IMPORTANCE OF MAINTAINING ABSOLUTE CLIENT TRUST AND BUSINESS REPUTATION.

"HACKERS ARE DEPLOYING SOME OF THE MOST SOPHISTICATED ATTACKS EVER SEEN, AND LAW FIRMS ARE A PRIMARY TARGET. LAW FIRMS ARE STOREHOUSES OF VALUABLE INFORMATION, OF INTEREST TO EVERYONE FROM ORGANIZED CRIME TO SPOUSES IN MARITAL DISPUTES."
FIRMEX, APRIL 2013

In March 2014, southern California wealth management firm Silverage Advisors revealed to clients that in spite of backing up important client data to removable drives and then storing those drives in a safe in the home of one of the partners, it didn't do any good.

Burglars broke into the home, forced open the safe, and disappeared with the tapes. According to the LA Times the tapes contained the financial records of hundreds of the firm's affluent clients including names, addresses, Social Security and driver's license numbers, and account information. And as usual, unencrypted.

A few weeks later, wealth management firm Sterne Agee announced that thieves had stolen a laptop from the car of an employee, a laptop that contained the personal information of an unspecified number of private clients. The data included account information and Social Security Numbers.

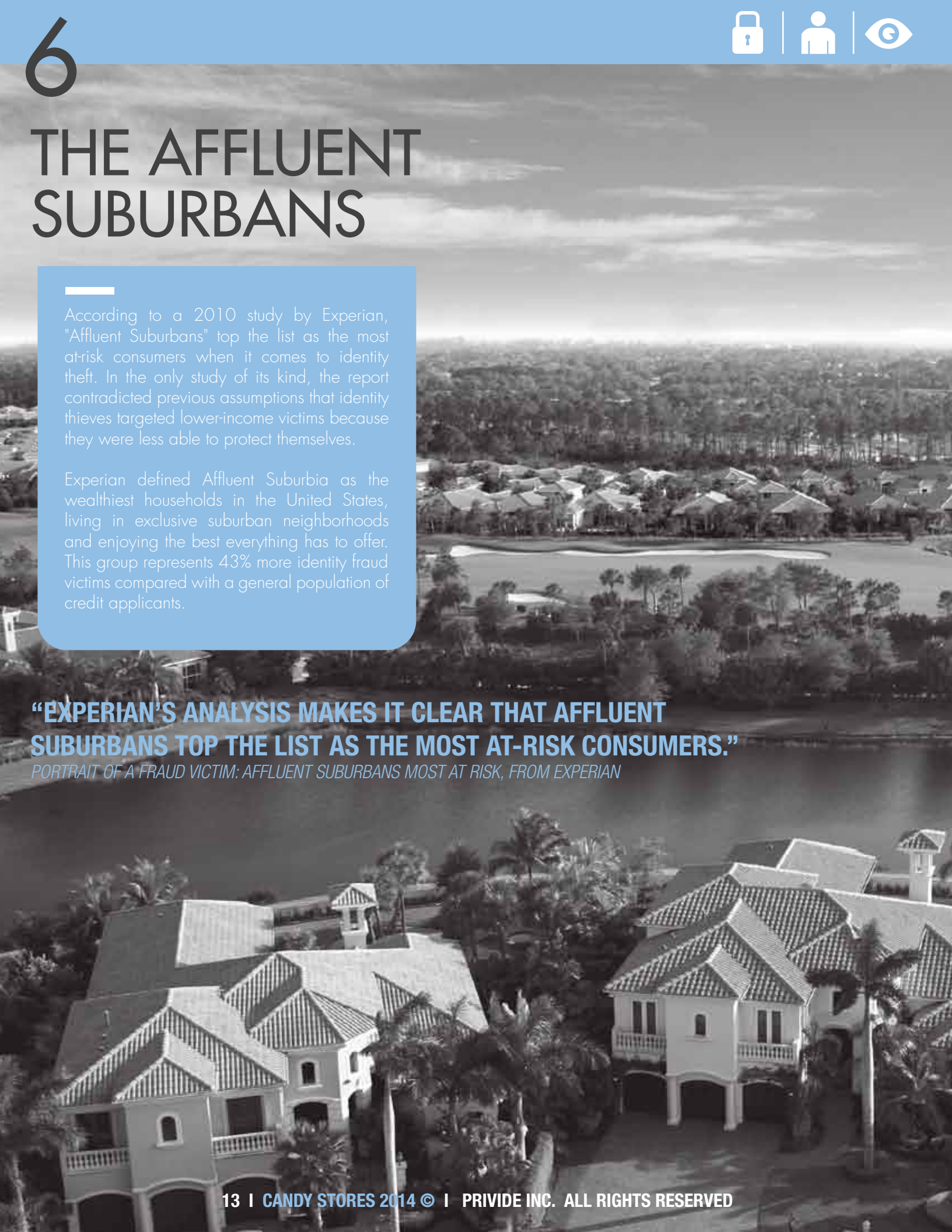
The company has more than $23 billion under management. And once again the data was unencrypted.

6

THE AFFLUENT SUBURBANS

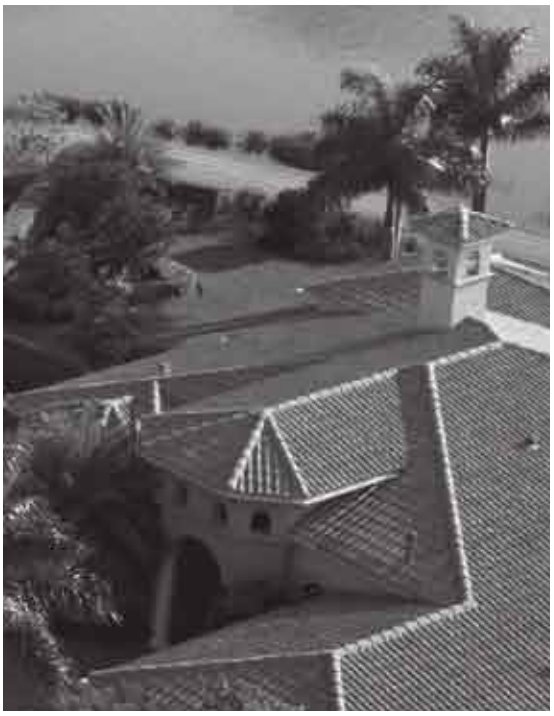
According to a 2010 study by Experian, "Affluent Suburbans" top the list as the most at-risk consumers when it comes to identity theft. In the only study of its kind, the report contradicted previous assumptions that identity thieves targeted lower-income victims because they were less able to protect themselves.

Experian defined Affluent Suburbia as the wealthiest households in the United States, living in exclusive suburban neighborhoods and enjoying the best everything has to offer. This group represents 43% more identity fraud victims compared with a general population of credit applicants.



"EXPERIAN'S ANALYSIS MAKES IT CLEAR THAT AFFLUENT SUBURBANS TOP THE LIST AS THE MOST AT-RISK CONSUMERS."

PORTRAIT OF A FRAUD VICTIM: AFFLUENT SUBURBANS MOST AT RISK, FROM EXPERIAN



THE REPORT ALSO FOUND THAT YOU HAVE AN INCREASED CHANCE OF FALLING VICTIM TO IDENTITY THEFT IF:

- YOUR INCOME IS HIGHER THAN THE MEDIAN.
- YOU DRIVE NEW OR LUXURY VEHICLES.
- YOU'RE A HOMEOWNER.
- YOU'RE COLLEGE EDUCATED.
- YOU PLAY TENNIS OR SKI.
- YOU TRAVEL FREQUENTLY, ESPECIALLY FOR LEISURE.
- YOU'RE INVOLVED IN POLITICS.
- YOU TAKE PART IN CHARITABLE ENDEAVORS AND CULTURE AND THE ARTS.

And it's apparent that the wealthy are worried. A survey in June 2011 by Chief Executive Magazine of 5,000 CEOs found that identity theft was the biggest fear for CEOs after third party lawsuits. 57% of participants ranked concern over personal identity theft as high or very high. The authors of the study commented that "While most CEOs have put enormous effort and energy into building the value of their businesses, we are concerned that many CEOs haven't put nearly enough focus into protecting their wealth."

A STUDY BY CHIEF EXECUTIVE MAGAZINE FOUND THAT IDENTITY THEFT AND THIRD-PARTY LAWSUITS WERE THE TOP CONCERNS FOR EXECUTIVES.

According to the 2012 study "U.S. Trust Insights on Wealth and Worth - Survey of High Net Worth and Ultra High Net Worth Americans," security and privacy were a major concern.

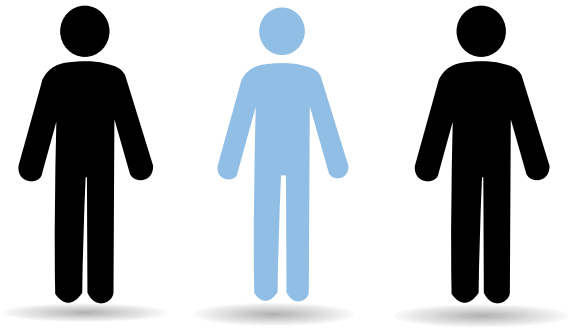
· THOSE AGE 18 - 46 WORRIED ABOUT INTRUSION ON PRIVACY (60%) AND FINANCIAL ID THEFT (52%)

· WEALTHY BABY BOOMERS, THOSE AGED 50+, WORRIED ABOUT FINANCIAL ID THEFT (60%), ONLINE THEFT (59%), INFORMATION SECURITY BREACH (57%), AND INTRUSION ON PRIVACY (52%)

· AND THOSE AGED 67 AND OLDER WORRIED ABOUT FINANCIAL ID THEFT (92%), INTRUSION ON PRIVACY (91%), INFORMATION SECURITY BREACH (86%) AND ONLINE THEFT (82%)

The study also found that the youngest generation is more likely to take advanced, actionable steps to protect privacy/security such as analyzing their online presence/information, increasing physical security, and conducting background checks. By comparison, those in older generations are primarily focused on strengthening online passwords and access controls. And twenty-eight percent of respondents across all generations have purchased additional insurance, e.g., liability and ID theft.

THE EPIDEMIC OF IDENTITY THEFT



1 IN 3 CONSUMERS WHO RECEIVE A DATA BREACH NOTIFICATION WILL FALL VICTIM TO FRAUD.

Identity Theft is the single biggest crime spree in America, fuelled by everything from cybercrime and hacking to data breaches, mail theft, and the drug trade. And as the crime quickly evolves, it has become more professional. Much of the world of identity theft is controlled by international crime rings that are able to commit massive identity frauds with little risk of being caught.

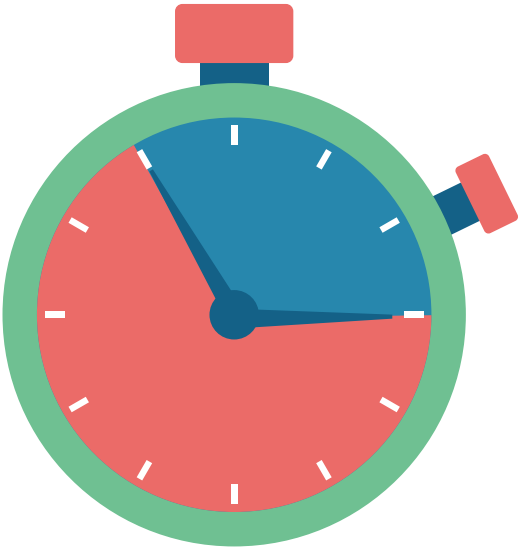
Many of these criminals are ignoring the low reward high risk crimes like credit card fraud, and instead targeting more affluent consumers who promise a much bigger payoff at a much lower risk. And the crimes go far beyond simply opening up new store cards and going on shopping sprees.

The crooks are committing real estate fraud, tax fraud, criminal identity theft, and targeting poorly protected bank accounts. And of course, they're targeting personal and business data, the currency of cybercrime.

There were an estimated 16.6 million victims of identity theft in the U.S. in 2013. That works out to an average of more than one million new victims every 30 days. Or one every two seconds. That might help explain why identity theft has been the Number 1 consumer complaint to the Federal Trade Commission every year for the last thirteen years.

To put those numbers in perspective, there are more victims of identity theft each year than there are reported murders, attempted murders, assaults, burglaries, attempted burglaries, arsons, vehicle thefts, purse snatchings, pickpocketings, check fraud, and shoplifting, combined.

But if you're a victim, don't expect much help. Because law enforcement is so overwhelmed by identity theft cases, most police departments now investigate less than 1% of reported identity theft cases. That's an unprecedented investigation level and the lowest for any crime in the history of modern law enforcement.



1 NEW IDENTITY THEFT VICTIM EVERY 2 SECONDS.

EXTORTION A GROWING THREAT

Cybercrooks understand that for many professionals, business owners, and high net worth consumers, their reputation is of enormous value. And they're willing to pay a high price to protect it. Cybercrooks also know that the wealthy have many secrets they may want to protect at all costs – from their neighbors, from the media, from the Government, from the IRS, from their competitors, even from their spouses.

Poorly protected computers, phones, laptops, emails, and text messages are a great source of secrets and very easy to tap into. In Aril 2014 the Harley Medical Group in the U.K. revealed that not only had hackers managed to steal personal information on nearly 500,000 of its cosmetic surgery clients, the thieves attempted to use the information to extort money from the medical group.

This was exactly the type of attack cybercriminals love. High value, big payoff, and low risk. The business can be extorted to pay up or be humiliated. Its patients could also be targeted for extortion, and especially if they're famous or had private or potentially embarrassing procedures performed. The stolen information could also make its way to other criminals who can use the records in countless ways – including selling or leaking it to media outlets. And while a financial identity can sell on the black market for less than $5, a medical identity can fetch upwards of $300.

This is typical of a Candy Store crime. Not only is the target of the crime of high value, exploiting them gives the criminals access to thousands of other potential targets. Many of whom are in turn of high value and who may be willing to pay a high price to keep their nip tuck secrets secret. It's a high value crime with a big and pretty endless potential return and with low risks. Victims like this are usually the last to report such a crime for fear of public humiliation and a further invasion of their privacy.

Harley's website boasts a survey which claims that "98% of our patients surveyed would recommend us to their friends and family." They may think differently now.

Theft is not the only risk. In January 2014 the offices of Charlotte, N.C.-based lawyer Paul Goodson reported that all their files, thousands of them, had been encrypted and lost forever after a type of malware known as ransomware made its way into the firm when an employee clicked on an infected email.

In a similar attack, also in 2014, a small town in New Hampshire admitted that it lost more than 8 years of files to the same malware.

$27 MILLION.

THAT'S HOW MUCH ONE SMALL GANG MADE IN DECEMBER 2013 BY INFECTING COMPUTERS WITH CRYPTOLOCKER RANSOMWARE THAT DEMANDED RANSOMS FOR HIJACKED INFORMATION.

8

YOUR CURRENT SECURITY IS PROBABLY A HACKER'S GIFT

When it comes to security, you can probably forget what you're currently doing and start over. Some consumers have become sufficiently paranoid and savvy about security that they've done the right thing and layered themselves and their families with effective security.

But the vast majority of consumers rely on three predictable defenses that hackers rely on in a different way – antivirus software, an identity protection service, and hope. None of which actually work very well.

Let's start with antivirus software. In May 2014 security giant Symantec, the world's biggest consumer antivirus company, announced that "antivirus is dead." They were referring to the widely-accepted truth that consumer antivirus software probably offers little defense to the latest generation of sophisticated malware and hackers.

Research backs it up. In repeated tests, the University of Alabama found that consumer antivirus software can detect only around 19% of viruses and other malware, and in some cases as little as 10%.

30 MILLION NEW TYPES OF COMPUTER VIRUSES AND MALWARE WERE DISCOVERED IN 2013 ALONE, AN AVERAGE OF 82,000 EVERY DAY. NEARLY 80% OF THOSE WERE TROJANS, THE MOST DANGEROUS.

A THIRD OF THE WORLD'S COMPUTERS ARE INFECTED WITH MALWARE, ACCORDING TO ANTIVIRUS FIRM PANDA.

IN THE 2012 ATTACK ON THE NEW YORK TIMES BY CHINESE HACKERS, ONLY ONE OF 44 DIFFERENT TYPES OF MALWARE USED BY THE HACKERS WAS EVER DETECTED.

IN 2014 IT WAS DISCOVERED THAT RUSSIAN HACKERS HAD TARGETED HUNDREDS OF ENERGY COMPANIES BY PLANTING MALWARE IN THE ONLINE MENUS OF RESTAURANTS FAVORED BY EMPLOYEES OF THOSE COMPANIES.

"MORE THAN 740 MILLION PERSONAL RECORDS WERE EXPOSED IN DATA BREACHES IN 2013."

THE ONLINE TRUST ALLIANCE, JANUARY 2014

In December 2013, security firm OPSWAT installed a very basic keylogger on a test computer. Keyloggers are a type of malware and much favored by hackers as a way to infect computers, steal personal information, and hijack bank accounts.

Over a three-week period the company tested 45 of the most popular antivirus programs to see if they could detect this very basic keylogger. Only one could. Which probably explains why in January 2013 the New York Times was hacked by Chinese hackers who targeted 44 different types of malware at the company's very substantial defenses. Only one was ever detected.

Antivirus software traditionally works by detecting malware it already knows and recognizes, and usually only the most basic predictable kind. It doesn't usually do so well against anything more sophisticated. And that's the key. The professionals are using very sophisticated malware that they test on real antivirus software first so they know it will bypass any defenses before they launch it.

As for identity protection services, they're only focused on a very small subset of threats, like a thief opening new credit accounts, and only warn users after the fact. They don't actually stop any type of identity theft.

Which is why some of these firms have been fined millions of dollars for misleading claims about the effectiveness of their services. Credit and identity monitoring services are of some value but should never be used in isolation from other security measures. And their only focus is on identity theft, offering no protection against cyber and privacy risks.

And as for the last defense, you're free to rely on the hope that you can hide in the crowd and the hackers will never find you. But you might be out of luck. The cybercrime industry is very wealthy and successful too, and are big into automation when scouring the internet and world for vulnerable targets. In the U.S. alone there are an estimated 10,000 active identity theft rings. Chances are there's one operating near you.

THE THREATS TO BANK AND BUSINESS ACCOUNTS

Your bank and investment accounts are a hot target for cybercrooks, and they have all the tools to break in from the other side of the world without setting of any alarms. Until it's too late. Research firm Javelin Strategy and Research estimated that in 2012, nearly $5 billion was stolen from U.S. bank accounts by hackers using malware.

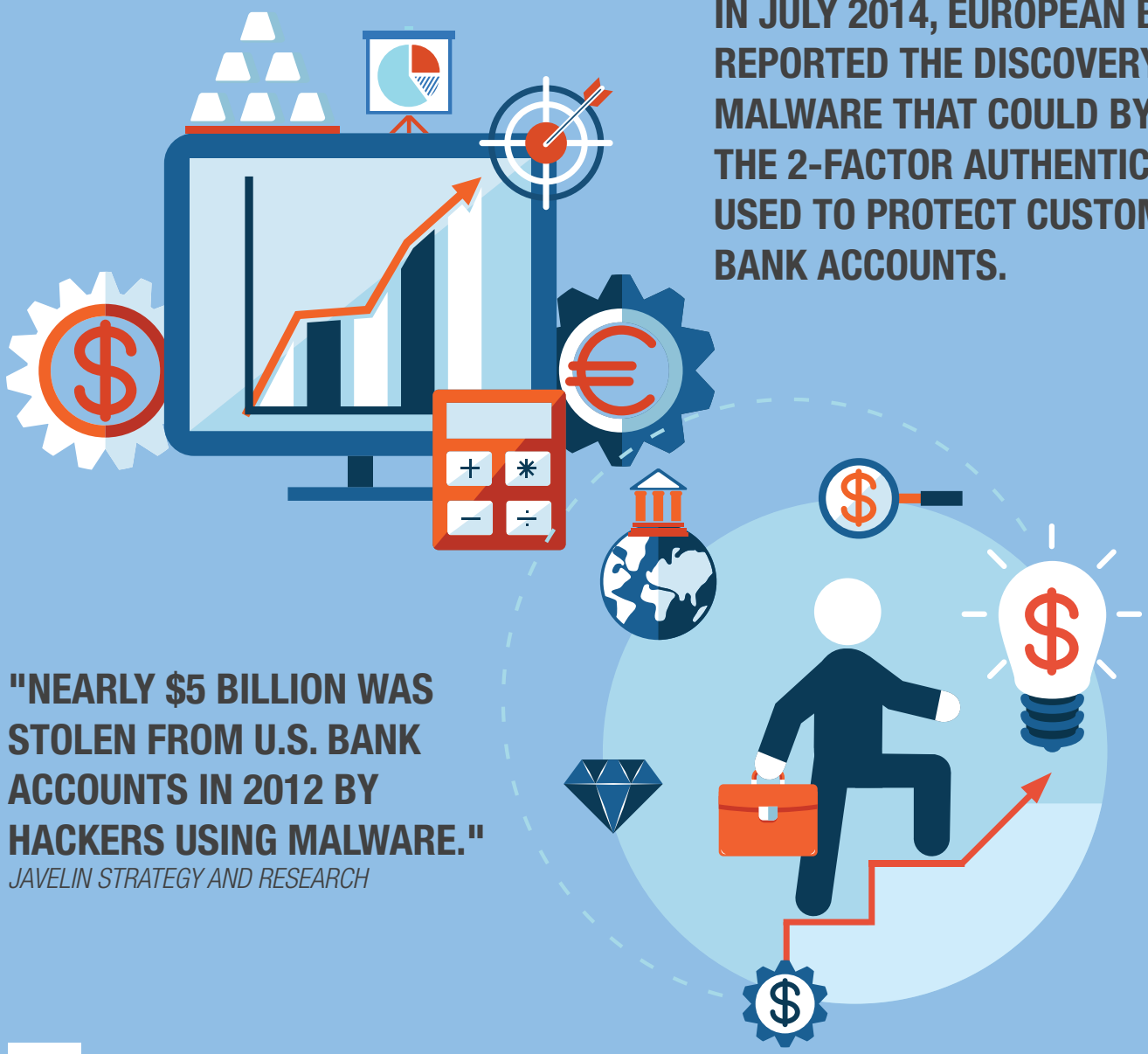
The favorite tool for this kind of cyber heist is a piece of malware specifically created for the task, called a banking Trojan. The Trojan is considered so dangerous, one of the first experts to discover this class of cyber weapon admitted it scared him because he had no answer for it.

Banking Trojans are able to sneak on to a computer even if it has antivirus software installed. They can detect what kind of antivirus software is running on the computer, disable it, then mimic it so that the user sees nothing suspicious.

The Trojan will usually contain a keylogger that can steal anything typed into the computer, especially bank logins and passwords.

And don't think about using a touchscreen device to get around keyloggers, because they usually include screen scrapers capable of copying anything that's on your screen too.

Once inside a bank account, banking malware will start surveying the landscape – what kinds of balances you have, how low you let them go, what kinds of transaction and security alerts you have set up and what phone number or email address those alerts go to.



IN JULY 2014, EUROPEAN BANKS REPORTED THE DISCOVERY OF NEW MALWARE THAT COULD BYPASS THE 2-FACTOR AUTHENTICATION USED TO PROTECT CUSTOMER BANK ACCOUNTS.

"NEARLY $5 BILLION WAS STOLEN FROM U.S. BANK ACCOUNTS IN 2012 BY HACKERS USING MALWARE."
JAVELIN STRATEGY AND RESEARCH

The malware can then begin transferring your money to other accounts, making sure that any alerts to you are either blocked or diverted. So you'll never know until it's too late. And victims are not difficult to find. In 2013, an escrow firm in Huntington Beach California quickly went out of business when a Trojan accessed their bank account and emptied it of $1.5 million. It all started when an employee simply opened a phishing email.

The money was stolen in just three large transfers – one to hackers in Russia and the other two to hackers in China. No arrests were ever made or the culprits ever identified. And because a Trojan can often leave no trace and appear to log in at the same time as a legitimate user, the bank initially blamed the company's employees for embezzlement.

Most consumers are aware of zero liability, as well as federal laws that ensure consumers are not held liable for funds stolen from their bank accounts by hackers. What most consumers don't know is that those same protections don't exist for commercial accounts.

What that means is that if you have any money currently in business accounts and the security of that account is breached by hackers, the bank is not liable. Whatever you lose stays lost. And many business owners have found this out the hard way.

10

SPEAR PHISHING IS THE MOST POPULAR ATTACK

There are many tricks and tools available to hackers to reach out and infiltrate the world of almost any target. But one of the most popular and effective tactics is spear phishing.

AN ATTACK WILL OFTEN GO SOMETHING LIKE THIS:

ONE OR A SMALL GROUP OF PROFESSIONAL CROOKS WILL IDENTIFY LARGE GROUPS OF POTENTIAL TARGETS AND START DOING THEIR RESEARCH – ABOUT THEIR PERSONAL LIVES AND FAMILY, FRIENDS AND SOCIAL NETWORKS, CHARITIES AND CAUSES THEY'RE INVOLVED IN, BUSINESSES THEY'RE A PART OF, WHO THEIR FINANCIAL AND LEGAL ADVISORS ARE, WHO THEIR KEY EMPLOYEES ARE.

A TARGET OR GROUP OF TARGETS WILL BE IDENTIFIED – EITHER THE FINAL TARGET OR SOMEONE CLOSE TO THEM.

THE MOST LIKELY ATTACK WILL BE A SPEAR PHISHING EMAIL – AN EMAIL BASED ON WHAT THE CROOKS HAVE LEARNED ABOUT THE TARGET AND DESIGNED TO LOOK LIKE IT COMES FROM SOMEONE THE TARGET KNOWS.

A COMMON PLOY IS TO IMPERSONATE A FINANCIAL ADVISOR, LAWYER OR ACCOUNTANT, A FAMILY MEMBER, AN EMPLOYEE, THE IRS, OR EVEN A PERSONAL TRAINER OR HAIR STYLIST; SENDING AN EMAIL USING THAT PERSON'S REAL EMAIL ADDRESS; AND USING A TOPIC THAT WON'T AROUSE THE SUSPICIONS OF THE TARGET.

THE EMAIL IS LIKELY TO INCLUDE EITHER AN ATTACHMENT OR A LINK TO A WEBSITE, AND CLICKING ON THAT LINK OR OPENING THAT ATTACHMENT WILL LAUNCH A PIECE OF MALWARE THE TARGET'S ANTIVIRUS SOFTWARE CAN'T DETECT.

MORE THAN 80% OF NEW MALWARE IS TROJANS, THE MOST DANGEROUS KIND.

Why won't the malware be detected? Cybercrooks buy malware kits on the black market, and use another black market service called crypting to make sure the malware can't be detected. Crypting is a service where hackers test a piece of malware against all the most commonly used antivirus software, like Norton, McAfee, and AVG. What they're trying to determine is which if any of the antivirus programs can detect the malware. If they can detect it, the malware is constantly tweaked until it can pass the most common antivirus programs.

The malware is increasingly likely to be a banking Trojan or a RAT. A RAT is a Remote Access Trojan capable of taking complete control of the infected computer. Some RATs can even control the computer's webcam and microphone.

In most cases the malware will make it past the antivirus software and take full control of the computer. It will be able to view and copy anything that's on the hard drive, monitor and infect email communications, record all keystrokes, steal passwords and logins, access bank accounts, and make copies of everything on the screen. The malware will also open a secret communication channel back to the hackers, where they can siphon the information from the computer, constantly update the malware, encrypt the communications so it can't be detected, and take over or disable any security software on the computer.

11

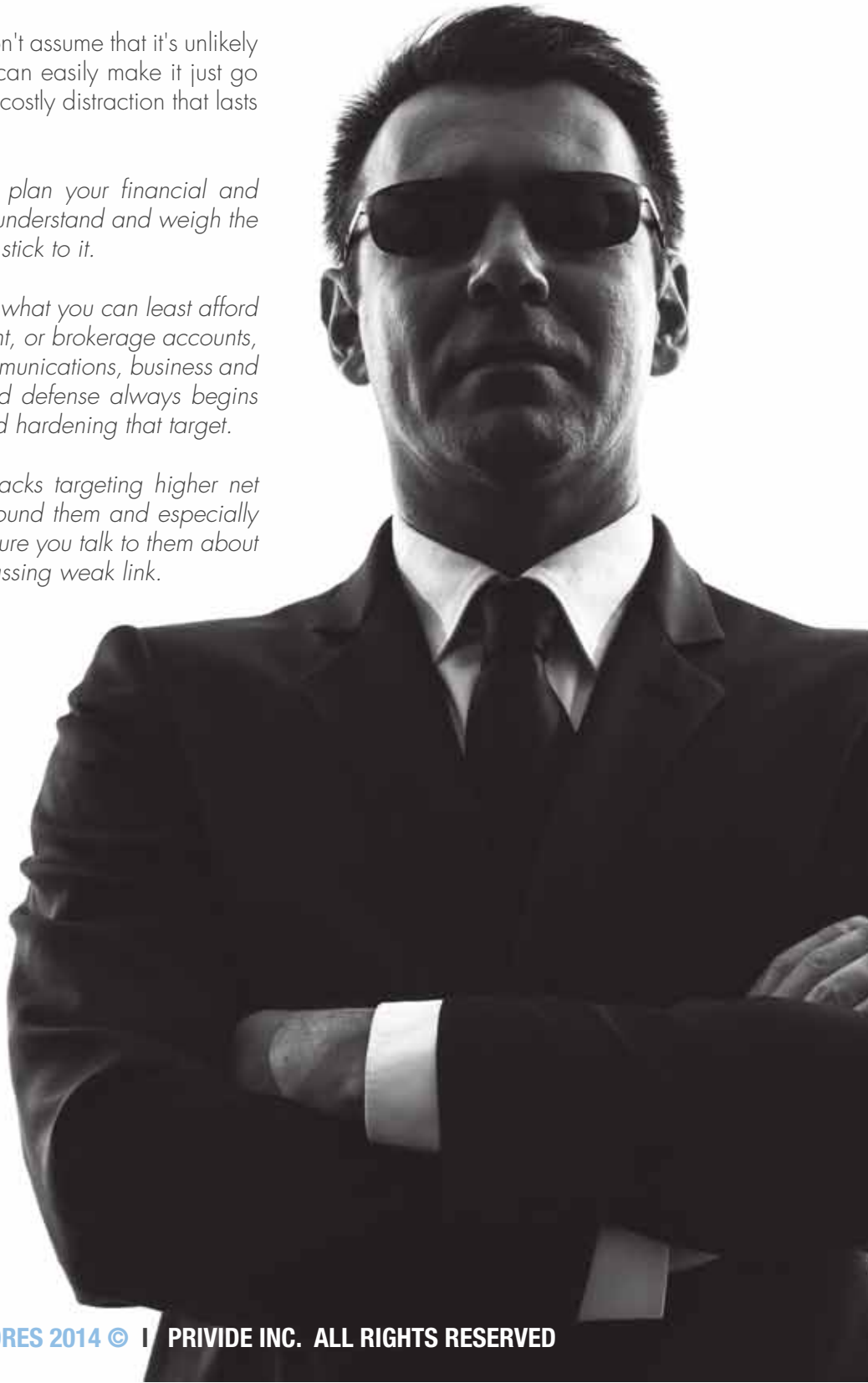
SO HOW CAN YOU PROTECT YOURSELF?

Take the threat seriously and personally. Don't assume that it's unlikely to ever happen to you, or if it does, you can easily make it just go away. One single incident can become a costly distraction that lasts for years.

* *Plan your protection just like you would plan your financial and wealth management. Use a professional, understand and weigh the risks, create a personal security plan, and stick to it.*

* *Think about what the thieves want most or what you can least afford to lose. Is it access to your bank, investment, or brokerage accounts, access to your private discussions and communications, business and investment plans, your reputation? A good defense always begins with knowing what the attacker is after and hardening that target.*

* *Think about those around you. Many attacks targeting higher net worth victims begin by targeting those around them and especially family, friends, and employees. So make sure you talk to them about the risks so they don't become an embarrassing weak link.*



APPROXIMATELY 30,000 NEW WEBSITES ARE COMPROMISED EVERY DAY BY HACKERS LOOKING TO DISTRIBUTE THEIR MALWARE TO SURFERS.

* *If you have employees, make security awareness training a regular event so they know what to look for and what to avoid. Good security vigilance is great for them and their families too.*

* *Protect your accounts in multiple layers of security. That includes strong and frequently changed passwords, account activity alerts, multi-factor authentication, lots of malware protection on any computers or devices you use to access these accounts, and keylogger protection to defend against banking Trojans.*

* *Think about using a separate and dedicated computer for access to your most sensitive accounts. Don't use that computer for surfing, email, or anything else that could let in malware. A cheap $200 computer is a small price to pay for the security it can bring.*

* *Be especially vigilant for spear phishing attacks, and make sure family members and employees are aware too. Spear phishing usually manifests as a legitimate and convincing email, from a partner, advisor, friend, or even the IRS, inviting you to click on an urgent link or attachment. That link or attachment typically leads to a malware downloaded to your computer. It's one of the most effective techniques hackers have and vigilance is your only defense.*

* *Use encryption. For personal and even small business use, there are a number of free and easy-to-use encryption programs that will protect your most sensitive data from the most determined hacker. You can even protect phone calls, emails, text messages, photos, and videos.*

* *If your phone calls, text messages, and emails are sensitive, use one of the growing number of free apps, like RedPhone and Wickr, that will encrypt all these messages to military grade, destroy them after a pre-set time, and hide any trace they were ever even sent.*

* *If you spend a lot of time online, use a safe surfing tool like McAfee Secure. The majority of malware is now being delivered through compromised websites which in turn infect any computers visiting those sites. It's estimated that more than 30,000 new websites every day are compromised by hackers looking to distribute their malware.*

* *Focus on your advisors. They can sometimes be the weakest link and the first stop for hackers trying to get to you. Ask them what their security procedures are, what they know about spear phishing, how they protect your information (and especially accounts), how often they train their employees, how they verify requests from their clients. Don't be general, get specific.*

* *Manage your passwords. Your passwords may be the only thing that's standing between hackers and things like your bank accounts and email. A smart password regime should make those passwords harder to guess, crack, or steal. Password managers like LastPass and Dashlane will help you manage multiple passwords.*

* *Protect your privacy by leaving no traces when you surf. It's safe to assume that every site you visit, everything you download, and everything you search for is being recorded by someone. Products like Cocoon and ZenMate can help ensure your privacy and anonymity when surfing.*

* *If you're planning to use one of the many cloud storage services, think twice before using these services to store and share sensitive information. More secure options like nCrypted Cloud will make sure your data is encrypted before it makes it to the cloud.*

* *Guard your bank and investment accounts, and especially from banking Trojans and keyloggers. Using a separate computer for accessing bank account helps, and keylogger protection like Trusteer and keyscrambler can offer enhanced protection against keylogging software. And be especially careful about business accounts. They're not protected by zero liability.*

12

PROTECT YOUR FAMILY

Hackers are heartless, and there's nothing and no one they won't exploit to achieve their goals. And that includes your family.

Whether it's using what your kids post of Facebook or Twitter to learn something more about you, or tricking family members into clicking on infected links or downloading infected files, cybercrooks have a wealth of tools that can be very effective in exploiting any weak link.

IN JUNE 2014 FACEBOOK ANNOUNCED THE DISCOVERY OF A BOTNET THAT HAD INFECTED MORE THAN 50,000 FACEBOOK ACCOUNTS AND MORE THAN 250,000 COMPUTERS, AS A WAY TO DELIVER MALWARE TO IT USERS.

THERE ARE A NUMBER OF PRECAUTIONS YOU CAN TAKE TO MINIMIZE THE RISKS:

Talk to your family, educate them about the risks, and make sure they're always aware and vigilant. You don't have to mention that you think they could be the target for hackers – it's simply common sense behavior for all kids.

Be their security mentor. Make sure that the devices they use have all the required security tools, that they're using good passwords, and that their devices don't provide access to others. For example, your kids should never be allowed to use your personal computer or tablet for things like homework, surfing, or talking to their friends. Privide can help you create such a plan.

Talk to them about the risks of posting too much personal and sensitive information on sites like Facebook, Instagram, and Twitter. Set up rules for use and make sure you follow through if the rules are broken.

Think about monitoring what your kids do and say on social media. Tools like Minor Monitor and Social Shield will alert you if your kids say or post things they shouldn't or connect with strangers.

Need to know where your kids are? Tools like Life360 and Mama Bear will allow you to use their phones to find out where they are, and even alert you if they're not where they're supposed to be or travel outside permitted zones.

13

PROTECT YOUR BUSINESS

- MAKE CYBERSECURITY A PRIORITY AND NOT AN AFTERTHOUGHT. IF YOU MAKE SECURITY AS IMPORTANT AND PASSIONATE A PRIORITY AS PROFIT, YOU'LL NOTICE THE DIFFERENCE. AND SO WILL YOUR CLIENTS. AND YOU'LL ALSO BUY YOURSELF SOME RELIEF IF AFTER EVERYTHING YOU'VE DONE YOU STILL EXPERIENCE A BREACH.
- LAYER YOUR BUSINESS OR PRACTICE IN SECURITY – THAT INCLUDES PRODUCTS, PROCESSES, RULES, AND BEHAVIOR.
- FOCUS ON EMPLOYEES AND THEIR AWARENESS AND VIGILANCE. THEY'RE THE MOST LIKELY TO BE TARGETED AS A WEAK LINK. SECURITY AWARENESS MUST BE A CULTURE. THEY MUST BE TAUGHT TO TRUST BUT VERIFY. ALWAYS SUSPECT AND QUESTION BEFORE DECIDING, TO THINK SECURITY FIRST.
- FOCUS ON EMAIL BECAUSE THE MOST DANGEROUS THREATS ARE LIKELY TO COME IN THE FORM OF MALWARE-LADEN PHISHING EMAILS.
- ENCRYPT, ENCRYPT, ENCRYPT. IF ALL ELSE FAILS BUT YOU'RE USING GOOD ENCRYPTION TO PROTECT SENSITIVE INFORMATION, THEN NOTHING'S REALLY FAILED. YOU CAN EASILY ENCRYPT ENTIRE HARD DRIVES OR JUST SPECIFIC FOLDERS OR FILES AS WELL AS LAPTOPS AND TABLETS.
- PROTECT YOUR PERSONAL COMMUNICATIONS WITH CLIENTS AND PARTNERS. THERE ARE SOME GREAT AND FREE APPS THAT WILL PROTECT ALL YOUR SENSITIVE PHONE CONVERSATIONS, TEXT MESSAGES AND EMAILS, DESTROY THEM LATER, AND LEAVE NO TRACE.
- HAVE A CLEAR, WRITTEN, TOUGH, AND CONSTANTLY UPDATED PASSWORD POLICY IN PLACE. AND MAKE SURE YOU AND YOUR EMPLOYEES STICK TO IT. DON'T RELY ON PASSWORDS ALONE. THEY SHOULD ALWAYS BE BOLSTERED BY SOME ADDITIONAL TYPE OF AUTHENTICATION.
- HAVE A RESPONSE PLAN IN PLACE. LET'S FACE IT, A BREACH IS A MATTER OF WHEN AND NOT IF. SO ASSUME YOU'RE GOING TO HAVE SOME KIND OF BREACH AND PLAN ACCORDINGLY.
- CLASSIFY YOUR DATA AND CONTROL ACCESS TO IT. HACKERS HAVE PRIORITIES WHEN IT COMES TO THE KIND OF DATA THEY'RE AFTER. CLIENT ACCOUNTS AND PASSWORDS ARE HOT, SO TOO ARE CLIENT INFORMATION AND COMMUNICATIONS. YOUR PERSONAL INFORMATION AND WEALTH ARE OF VALUE TOO. IDENTIFY WHAT THE THIEVES WANT MOST AND STRICTLY CONTROL ACCESS TO IT. EVEN FOR EMPLOYEES.

14

GREAT FREE TOOLS THAT PROTECT YOU

THERE ARE HUNDREDS OF FREE TOOLS AVAILABLE TO HELP PROTECT YOU, YOUR FAMILY, AND YOUR BUSINESS FROM ALL KINDS OF SIMPLE AND ADVANCED THREATS. MOST ARE EASY TO INSTALL AND USE AND WORK AUTOMATICALLY AND IN THE BACKGROUND. SO NO NEED TO HEAD BACK TO SCHOOL TO LEARN HOW TO PROTECT YOURSELF.

PROTECT AGAINST MALWARE

Did you know that there are more than 40 different types of antivirus software programs available for consumers? And you've probably never heard of the biggest and best. How about Avira, or Avast? Those brands are usually amongst the top three of all antivirus brands in the world and some of the best are free.

Free antivirus software is available from brands like AVG, Avast, Avira, Microsoft Security Essentials, ZoneAlarm, and Panda Security. And in some cases, you can use more than one antivirus program on the same computer.

If you use a Mac, which is great from a security perspective, then you should consider installing the free Sophos antivirus.

In addition to your resident antivirus software, you should also do regular scans with additional tools like MalwareBytes. They can provide an extra layer of security and a valuable second opinion.

And don't forget to protect your mobile devices too. There's been a surge in malware targeting mobile devices, and especially Android phones and tablets.

MOBILE SECURITY

With hundreds of millions of mobile devices in use, especially smartphones and tablets, it's hardly surprising that there are also millions of different types of malware now chasing those products. They're either looking for personal and corporate data, or they want to trick the phones into making premium calls to faraway places that make a lot of money for scammers.

As if that wasn't enough, device theft is on the rise, with brazen crooks going to great lengths to steal iPhones, iPads and any mobile device not tied down. For example, in 2013 the San Francisco Police Department announced that more than 50% of all street robberies in the city involved smartphones or tablets. It's been dubbed Apple Picking

And hacking isn't just about malware. If you use public Wi-Fi hotspots, there's a very good chance that a hacker or snoop is somewhere nearby listening in and hoping to glean some valuable information. Luckily there are plenty of great free security tools to help – tools that will protect your device from malware, secure your hotspot surfing, and even wipe and track a lost or stolen phone.

One of the best and most popular is made by San Francisco security startup Lookout. This free software will protect your phones and tablets from malware, find them if you lose them (or they're stolen), wipe them, backup and restore your information etc. Other free mobile security products include Avast, AVG, Norton, and Prey.

SECURITY ON SOCIAL NETWORKING

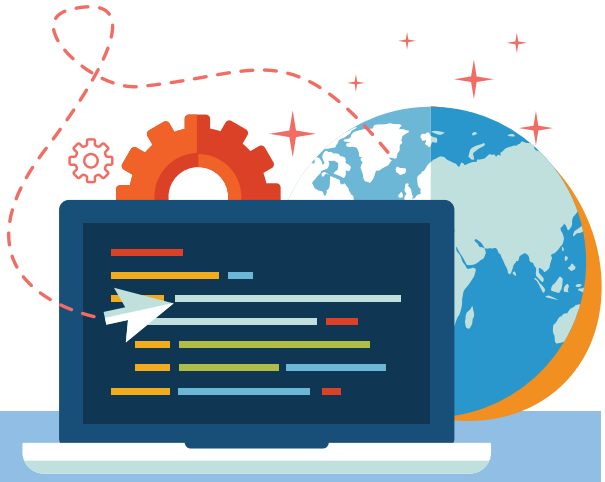
With more than a billion users around the world on social networking sites like Facebook, Twitter, Instagram, Pinterest, Tumblr, Flickr, and LinkedIn, these sites have become a magnet for hackers, scammers, and identity thieves. But there are tools available to help protect you, your family, and if you own a business, your employees.

For example, Safego from Bitdefender are popular Facebook security apps that will monitor your Facebook page for scams and malicious posts and instantly send you an alert if they find anything suspicious.

They will also allow you to automatically publish warnings about scams on your own Facebook page as a way to alert your friends of possible dangers.

And if they find a malicious link or scam on a friend's page, they can also alert them too. So you're not just protecting yourself, you're also protecting your entire network of friends. And they will keep a record of all the malicious links they find and even who posted them to your page. They can also protect your Twitter account.

And if you have kids on Facebook, Twitter, or Google+, you should sign up for free services like MinorMonitor or Social Shield that will help you monitor what your kids say and do on social networks, and who they "friend."



FOR EXAMPLE:

- THERE ARE APPS THAT WILL ALLOW YOU TO MAKE COMPLETELY SECURE CALLS ON YOUR SMARTPHONE TO ANYONE ELSE WHO HAS THE SAME APP INSTALLED.
- THERE ARE APPS, PLUGINS, AND SERVICES THAT WILL ALLOW YOU TO SEND SECURE AND PRIVATE EMAILS TO ANYONE YOU WANT, EVEN IF THEY DON'T USE SECURE EMAIL.
- THERE ARE APPS THAT WILL ENCRYPT AND PROTECT YOUR TEXT MESSAGES SO NO ONE CAN READ THEM, EVEN IF THEY HAVE ACCESS TO YOUR PHONE AND PASSWORD.
- THERE ARE APPS AND TOOLS THAT WILL AUTOMATICALLY ERASE EMAILS AND TEXTS AFTER A SPECIFIED LENGTH OF TIME.
- THERE ARE APPS THAT WILL CREATE A SECURE COMPARTMENT ON YOUR SMARTPHONE THAT WILL HIDE WHO YOU CALL AND WHEN.
- THERE ARE APPS THAT WILL CREATE SECURE VAULTS ON YOUR SMARTPHONE OR TABLET WHERE YOU CAN SAFELY STORE MESSAGES, PHOTOS, NOTES, PASSWORDS ETC.

You have a right, and in many instances an obligation, to keep your secrets secret. Whether they're business secrets or your personal business, now you have the tools and they're free. We recommend free security apps like Redphone and Wickr.

PROTECTING YOUR SECRETS

The ongoing scandal over eavesdropping on American citizens by everyone from the NSA to Google, Facebook, and even the phone companies is a reminder to us all that nothing we ever say, text, or email is safe from eavesdropping. Unless you protect those communications.

And while nothing is absolutely secure, there are plenty of free and easy-to-use tools that will protect you from the most advanced hackers and eavesdroppers.