Cyber and Identity Theft:

Managing Your Family's Risks

CHUBB

Personal Risk Services

Contents

Cyber and Identity Theft:

Managing Your Family's Risks

Kate Norris

AVP, Family Office Practice Leader

Personal Risk Services

Executive Summary

A woman whose purse is stolen is charged two years later with fraudulently buying prescription drugs. A man's credit card is stolen, and the thieves charge thousands of dollars' worth of merchandise on his account. A college student is scammed by a cyber thief who scours social media for personal information.

Your family's cyber and identity theft risks grow more complex each year.

In addition to sifting through your trash bin and watching your mail box, criminals today can also use technology to compromise your identity. Think about your morning routine. If you pre-order from Starbucks, buy a paper on the corner using Apple Pay, or use the free gym wifi to pay your bills online, before lunch you've shared multiple pieces of information that could potentially be accessed by cyber criminals.

According to a report titled, *Victims of Identity Theft: 2014* from U.S. Department of Justice Office of Justice Programs' Bureau of Justice Statistics, 17.6 million Americans age 16 or older were victims of identity theft in 2014. The majority of identity theft victims (86%) experienced the fraudulent use of existing account information, such as credit card or bank account information, and the number of elderly victims of identity theft increased from 2.1 million in 2012 to 2.6 million in 2014.

Criminals will continue to exploit social media and hack into the latest, most popular applications. Security experts continue to familiarize themselves with the latest cyber-exposures, but so do criminals.

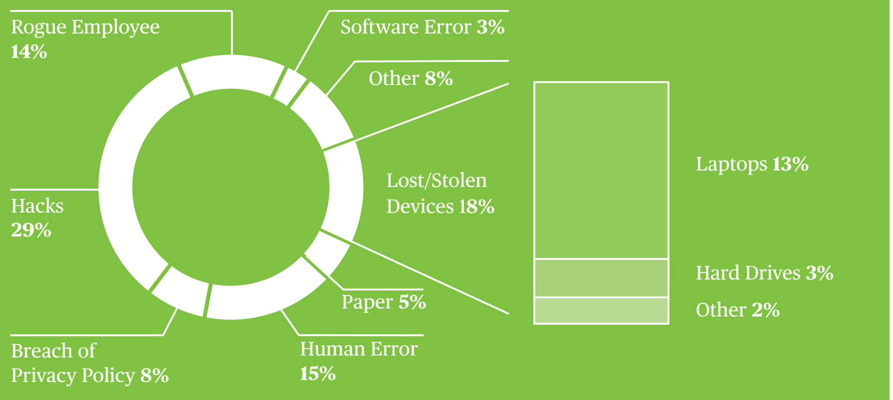
This paper highlights the cyber and identity theft risks families face and how to implement simple steps to reduce them. Before you install your next app, enter a password, or provide private information, invest a few moments to learn more about the potential consequences to your family -- and how to avoid them.

What Types of Cyber Crime and Identity Theft Could Your Family Face?

Criminals can target several types of information:

- **Financial information.** In 2013, 40 million credit and debit card numbers were stolen, according to Forbes. (*The Big Data Breaches of 2014*, by Bill Hardekopf, January 13, 2015) Thieves who gain access to your credit card, bank, brokerage, or even utility information can use your balance sheet as their own.
- **Medical information.** According to a 2015 study by the Ponemon Institute on Medical Identify Theft, as reported by the Coalition Against Insurance Fraud, 2.3 million Americans reported medical insurance theft in 2014 (*By the Numbers: Fraud Statistics*). If your medical insurance information is physically stolen or your hospital group is hacked, criminals can seek treatment using your medical identification.
- Identity information. If an identity thief obtains your name and personal information, he or she can use it if arrested. Victims can end up with convictions on their record they're unaware of, forcing them into legal battles to avoid jail time or problems getting a job.

Sources of Information Theft



Chubb data on claims from corporate clients (2005-2015) reveals that information theft is often preventable.

How Do These Types of Theft Happen?

Cyber criminals use a variety of tactics to access your information:

Network security attack

- **Hacking.** Breaking into a network, computer, device, or file, usually with malicious intent. The thieves are often sophisticated and can exact significant damage. In one of the largest cyber crime filed to date, hackers from Russia and Ukraine targeted organizations including Nasdaq, 7-11, JetBlue and JC Penney. They stole 160 million credit and debit card numbers and breached 800,000 bank accounts, according to Huffington Post (The Nine Biggest Data Breaches of All Time, by Lorenzo Ligato, August 21, 2015).
- **Malware.** Software intended to control or damage a computer system, network, computer, or mobile device.
- **Ransomware.** Software used by hackers to lock down your computer or system; the hackers then demand a ransom to unlock it.
- **Phishing.** An attempt to obtain financial or other confidential information from internet users, often via e-mail. The e-mail looks as if it comes from a legitimate organization, often a financial institution, but links to a fake website.
- **Business partners.** The businesses you work with can also inadvertently pass their cybercrime exposure on to you. According to a recent report released by the Identity Theft Resource Center (ITRC) and sponsored by IDT911™, 781 data breaches were tracked in the United States in 2015 (*ITRC Data Breach Reports*, December 29, 2015). This represents the second-highest year on record since the ITRC began tracking breaches in 2005. The business sector again topped the ITRC 2015 Breach List, with nearly 40 percent of the breaches publicly reported in 2015.

Phones and PDAs hold a treasure trove of personal information.

Lost or stolen devices

- **Laptops.** Lost or stolen laptops accounted for 13% of corporate data breaches according to recent Chubb data (see chart). If they're not password protected, they're easily accessed.
- **Phones and personal digital assistants.** Phones and PDAs also hold a treasure trove of personal information. You likely use them to access your bank account, e-mail, utilities, alarm system, and information on family and friends, and often photos, notes, passwords, and links to other sites.

Human error

- **Passwords.** According to Intel, the average person has more than two dozen accounts requiring passwords (*Password Management - With Intel True Key, You Are Your Password*, by Deb Miller Landau, February 6, 2015). If you're one of them, you may be tempted to create simple passwords or passphrases. That makes it easier for hackers to access your information.
- **Unprotected wireless networks.** Because authentication isn't required to establish a network connection, hackers can use unsecured Wi-Fi to access the same network and then get between you and the connection point. You could end up sending your information to the hacker rather than the hotspot.
- **Social engineering.** Social engineers gain their targets' trust by posing as someone they know. The criminals may get their information from news accounts and other publicly available information or from social medial posts. Armed with these details, the social engineers manipulate their victims into unknowingly giving up additional personal information.
- **Links and apps.** Downloading links and apps, even from sources that look trustworthy, can infect your computers and other devices with malware.

How Can You Protect Yourself and Your Family?

The Ackerman Group, which provides security counsel to corporations and families, has compiled a list of quick tips to help defend against cyber and identity theft:

Maintain current anti-virus protection

- Set up automatic updating to ensure that your anti-virus software is up to date and that your subscription is active.
- Use only one anti-virus system at a time.
- Use the anti-malware features that come with your anti-virus system.

Use firewalls

- Most home Internet service providers (ISPs) come with a gateway with integrated firewall features. Generally, there are some default firewall features turned on. Contact your ISP to ensure that firewall features are turned on. If you purchase a commercial firewall, subscribe to the intrusion detection and intrusion prevention services (IDS/IPS). Make sure the firewall can capably monitor both inbound and outbound traffic.
- Leave your computer's firewall turned on and set it to update automatically.

Block pop-ups

- Use the pop-up blockers in your browser program.
- Do not install third-party pop-up blockers as they may contain malware.

Back up data

- It is crucial in defending against the current wave of ransomware threats to conduct regular system backups, and to store backed up data in offline units stoutly buttressed against infection.

Block and delete unsolicited e-mail and contacts

- Treat any unsolicited e-mail, telephone call, or in-person contact as suspect. For unsolicited e-mails, never open links or attachments. Never provide personally identifiable information, such as your social security number, birthday, account numbers, logon credentials, personal telephone number, etc. In recent years, Posting or sharing personal identifiable information via social media channels can lead criminals into your accounts.

the vast majority of cyberattacks have come in the form of links or attachments in unsolicited e-mails.

Be careful when downloading software

- Be extremely careful when downloading software, especially free software. Even software from legitimate software vendors can, by default, install annoying, unwanted software. If you're a Mac user, be aware that ransomware has been downloaded to Mac computers via legitimate file-sharing applications.
- Before installing a downloaded file, put your mouse pointer over it, right click and select the option to scan for viruses if that option is available.

Avoid advertisements (even on legitimate websites)

- Hackers have begun to taint advertisements on legitimate websites. Avoid selecting advertisements even on legitimate websites such as *The New York Times*.

Use strong passwords or passphrases and update them periodically

- The longer a password is, the more difficult it is to break. Using brute force, hackers can decipher short passwords quickly, but a passphrase of at least 15 characters using a combination of upper and lower case letters, numbers, and punctuation has an exponentially greater chance of defeating those attacks.
- Passphrases are not only long enough to be secure, but are also easy enough to remember. An example of a possible passphrase would be, "IWasBornnIn2016*." It is 16 characters long, contains upper- and lower-case characters, as well as numbers and punctuation. It would be extremely difficult to crack this password using a brute force attack.
- Avoid passwords or passphrases with common words or sequences, such as "football," "baseball," "12345," "qwerty" or predictable letter combinations. Note that "bornn" is misspelled in the password above to defeat hackers searching for common words.
- Update your passwords every 90 days.
- Do not use the same password for all of your accounts. Think of it like having one key for every door or lock in your life. If it fell into the wrong hands, you could put almost every aspect of your life at risk. Remember that on most occasions, when passwords are compromised, it happens without your immediate knowledge. It could be too late before you find out.
- To avoid the hassle of having to remember passwords to all of your different accounts, consider using a *reputable* password manager such as LastPass.
- Even when using a password manager, enable two-factor authentication whenever possible so that even if someone does obtain your master password, it will not be enough to access your account.

Ensure your system is current

- Ensure your computer's operating system automatically installs patches. This will protect you from vulnerabilities that are discovered after an operating system ships. In addition, ensure your web browser and all other programs are always up to date.
- Use web browsers such as Google Chrome or Microsoft Edge that automatically update themselves, and use a "sandboxed" Java to run programs for sites. (Sandboxing is a mechanism for separating running programs.)
- If your computer has the Java client installed separately, remove it for added security. Install the Java client only if the site you need to use will not run without it.

Do not over-share on social media outlets

- Posting or sharing personal identifiable information via social media channels can lead criminals into your accounts. For example, sharing your date of birth, city born, street you live on, and favorite dog's name are often part of the questions you are asked to verify your identity when logging into sites.

- Do not tag your current location or check in to places on social media or picture-sharing apps. Even when your information is set to be shared only with your "friends," there is no way to guarantee that information will not find its way to non-friends or strangers.

Be aware of the risks of connecting in public places

- Whether at the airport, a hotel or a café, using public Wi-Fi has the potential to expose your identity and data. When using public networks, consider using a Virtual Private Network (VPN), which encrypts your traffic and makes it anonymous. Reputable apps like Norton Wi-Fi also include VPN features.
- When not in use, disable your Wi-Fi and Bluetooth, as these can allow attackers in.
- Bring a wall charger instead of connecting to charging stations at airports, since most of the time USB cables that come with your phone also transfer data. Cybercrooks sometimes maliciously modify these to steal your data or load malware onto your device.
- It is also safer to work from a personal computer than use a computer at a hotel business center, as computers accessible to others in public areas also pose a risk.

When Cyber Extortion Gets Personal

Cyber extortion has rocked many businesses, but the problem doesn't stop there. The Internet Crime Complaint Center (IC3), a multi-agency task force, has received many reports from individuals who have received extortion attempts via e-mail related to recent high-profile data thefts (FBI Public Service Announcement, *Extortion E-Mail Schemes Tied To Recent High-Profile Data Breaches*, dated June 1, 2016). The extortionists threaten to reveal the target's name, phone number, credit card information, and other personal details if a ransom is not paid. The recipient is instructed to pay in digital currency such as Bitcoin to lend anonymity to the transactions. Examples of the extortion e-mails include:

"Unfortunately your data was leaked in a recent corporate hack and I now have your information. I have also used your user profile to find your social media accounts. Using this I can now message all of your friends and family members."

"If you would like to prevent me from sharing this information with your friends and family members (and perhaps even your employers too) then you need to send the specified bitcoin payment to the following address."

FBI Tips to Protect Yourself:

- Do not open e-mail or attachments from unknown individuals.
- Monitor your bank account statements regularly, as well and as your credit report at least once a year for any fraudulent activity.
- Do not communicate with the subject.
- Do not store sensitive or embarrassing photos of yourself online or on your mobile devices.
- Use strong passwords and do not use the same password for multiple websites.
- Never provide personal information of any sort via e-mail. Be aware, many e-mails requesting your personal information appear to be legitimate.
- Ensure security settings for social media accounts are turned on and set at the highest level of protection.
- When providing personally identifiable information, credit card information, or other sensitive information to a website, ensure the transmission is secure by verifying the URL prefix includes https, or the status bar displays a "lock" icon.

What Should You Do if You Become a Victim?

- Contact the three credit bureaus, Equifax, Experian, or TransUnion, to place a fraud alert on your credit report.
- File a report with your local police department.
- Call your insurance broker to help identify resources available via your insurance carrier.
- Work with a qualified security advisor who specializes in protecting high-net-worth individuals and families, and offers specific cyber protection advice.
- Assure that you're adequately protected and your insurance carrier can help you and your family to withstand a loss.

How Do You Find an Insurance Carrier that Knows Cyber Risks?

Because cybercrime evolves so quickly, look for an insurer that offers specific cyber-protection policies for individuals and families.

Ask your independent insurance agent about providers that not only offer high-limit personal excess policies, but actually specialize in high-net-worth personal insurance. Some excess policies include crisis management endorsements that can pay for a public relations agency to help restore your reputation in the event of a high-profile incident.

Choose an insurance company that understands your lifestyle and offers a cyber family safety service that addresses your unique needs. Some carriers offer an in-home safety consultation or can recommend an international personal security firm with expertise in protecting wealthy individuals and families.

What Resources Are Available to Help Combat Cyber Risk?

Many resources are available to help you manage your family's cyber safety. The resources below can get you off to a strong start:

Visit any of the three credit bureaus, **Equifax**, **Experian**, or **TransUnion**, to check your credit information or to place a fraud alert on your credit report.

The Ackerman Group counsels corporations and families on a variety of security issues, with an emphasis on prevention.

IDT911 provides identity management and protection solutions.

Chubb Personal Risk Services offers complimentary proactive services and identity theft resolution services to homeowner and automobile policyholders.

Independent agents can advise you on cyber safety, additional information resources, and knowledgeable insurance carriers.

Chubb. Insured.℠

Chubb is the marketing name used to refer to subsidiaries of Chubb Limited providing insurance and related services. For a list of these subsidiaries, please visit our website at new.chubb.com. Insurance provided by U.S. based Chubb underwriting companies. All products may not be available in all states. Coverage is subject to the language of the policies as actually issued. Surplus lines insurance sold only through licensed surplus lines producers. This information is advisory in nature and is for informational purposes only. No warranties or representations of any kind are made to any party and no liability is assumed by reason of the information in this presentation. The information provided should not be relied upon as legal advice. For such advice, a listener or reader should consult their own legal counsel. Chubb Personal Risk Services, P.O. Box 1600, Whitehouse Station, NJ 08889-1600. This presentation is copyrighted and is the property of Chubb. Any use of this presentation without Chubb's prior, written consent is prohibited.
Form 02-01-0712 (Ed. 10/16)