MarshMcLennan
Agency

Private Client Services

Personal cyber risks: Protect your family and lifestyle

Make Extraordinary Possible.SM

A business of Marsh McLennan

Contents

01 Introduction

02 Identity theft — a top cyber threat

03 Social networks — a cyber playground

04 New technology

05 Protect your children

06 Products designed to protect you

Introduction

News reports show large-scale data breaches are on the rise and affecting every sector of business from Microsoft to Facebook, even banks and hotels. But we don't hear many reports about consumers falling victim to cybercrime, even though individuals — especially the affluent — are also frequently targeted, and this real threat is on the rise.

Cybercrime is defined as any criminal act that involves computers and networks. In addition, it includes traditional crimes conducted through the internet. Today, cybercrime is a greater risk than ever before because of the copious amount of time people spend online and the increasing number of devices joining the Internet of Things (IoT). It's a rapidly evolving landscape that demands attention.

There are numerous categories of cybercrime, but the ones that affect the most victims include identity theft, credit card fraud, and social networking scams. Review the information presented in this report to learn how to better protect yourself, your family, and your lifestyle from cybercrime and its long-lasting effects.

Identity theft — a top cyber threat

Because of the amount of personal information stored and shared on electronic devices, identity theft is one of the largest cybercrime threats today. In 2021, 42 million U.S. consumers were victims of identity fraud.[1] The best way to protect yourself is to be aware of your activity when using smartphones, tablets, and other devices that store personal information digitally.

According to the Insurance Information Institute, identity theft is the act of taking someone's personal information and using it to impersonate them, steal from bank accounts, establish phony insurance policies, open unauthorized credit cards, or obtain unauthorized bank loans. In more elaborate schemes, criminals use the stolen personal information to get a job, rent a home, or take out a mortgage in the victim's name.

Close to half of identity theft cases are the result of a lost or stolen wallet, checkbook, credit card, or other physical document. Because of the popularity of online shopping, it too can pose as a serious identity theft risk.

Victims of identity theft are often left with lower credit scores and spend months or even years getting credit records corrected. They frequently have difficulty getting new credit, obtaining loans, and even finding employment. Victims of identity theft fraud often travel a long and frustrating road to recovery; depending on the severity of the identity theft fraud damage, the recovery process can take anywhere from a few weeks to several years.[2]

Tips for avoiding identity theft

Reduce your chances of becoming a victim of identity theft by practicing the following tips developed by the Insurance Information Institute:

Keep the amount of personal information you carry to the bare minimum. Avoid bringing additional credit cards, your social security card, or passport in your purse or wallet unless absolutely necessary.

Do not give out personal information. Whether on the phone, through the mail, or over the internet; don't give out any personal information unless you have initiated the contact or are sure you know who you are dealing with and that they have a secure line.

Shred any documents containing personal information. Avoid putting documents with credit card numbers, bank statements, charge receipts, or credit card applications, before disposing of them.

Be aware of phishing and pharming scams. In these scams, criminals use fake emails and websites to impersonate legitimate organizations. Exercise caution when opening emails and instant messages from unknown sources and never give out personal, financial, or password-related information via email.

Maintain strong, unique passwords on your credit card, bank, and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, any part of your Social Security number or phone number, or any series of consecutive numbers. If you suspect a problem with any account, change your password. Update your passwords regularly, and use a password manager program to help you keep track.

Guard your credit or debit card when making purchases or withdrawing cash. Shield your hand when typing your pin in an ATM or register key pad. Don't fall prey to "shoulder surfers" who may be nearby.

Be aware of credit card skimmers. Criminals place skimming devices over the factory-installed card reader on ATMs or gas pumps. When you swipe your card, the skimmer captures the information from your card's magnetic strip and a keypad overlay will record your pin. Examine the machine for anything suspicious before swiping your card.

Always take credit card or ATM receipts. Don't throw them into public trash containers, leave them on the counter, or put them in your shopping bag where they can easily fall out or get stolen.

Proceed with caution when shopping online. Use only authenticated websites to conduct business online. Before submitting personal or financial information through a website, check for the locked padlock image on your browser's status bar or look for "https://" (rather than http://) in your browser window. If you have any concerns about the authenticity of a web page, contact the owner of the site to confirm the URL.

Monitor your accounts. Don't rely on your credit card company or bank to alert you of suspicious activity. Carefully monitor your bank and credit card statements to make sure all transactions are accurate. If you suspect a problem, contact your credit card company or bank immediately.

In order to make it more difficult for identity thieves to open accounts in your name, you can also contact the fraud department of any of the three credit reporting agencies to place a fraud alert on your credit report — by law, the agency you contact is required to contact the other two agencies. The fraud alert tells creditors to contact you before opening any new accounts or making any changes to your existing accounts. The three major credit bureaus are Equifax, TransUnion, and Experian.

In 2021, 42 million U.S. consumers were victims of identity fraud.[1]

Be cautious about sending personal information online when connected to a public wireless network.

Use more secure passwords with your laptop, credit, bank, and other accounts by incorporating upper- and lower-case letters, numbers, and special characters.

If you suspect you're a victim of credit card fraud or identity theft, act quickly to protect yourself.

What to do if your identiy has been stolen

It can take several steps to recover from identity theft. If you do become a victim of identity theft, the Federal Trade Commission (FTC) recommends taking these steps immediately to help limit the damage:

- Call one of the three credit reporting agencies and ask them to put an initial fraud alert on your credit report.
- Order a copy of your credit report from each of the three credit reporting agencies. Your credit report generally includes facts about your identity, where you work and live, and your credit history.
- Create an Identity Theft Report:
  - Submit a complaint to the FTC and print a copy of the report, called an Identity Theft Affidavit.
  - File a report with your local police department and ask for a copy of the police report.
  - Attach the FTC Identity Theft Affidavit to the police report to make your Identity Theft Report.
- Call the businesses where you know fraud occurred, explain that your identity has been stolen, and ask them to close or freeze your accounts.
- Review your credit reports and dispute errors (accounts you didn't open or debts you didn't authorize) with the credit reporting companies and the businesses where the fraud occurred. Mail them a copy of your Identity Theft Report and ask them to stop reporting the inaccurate information and block the disputed information from appearing on your credit report.
- Ask for copies of the documents the identity thief used to open new accounts or make changes in your name. These documents can help prove the identity theft.
- If you have identity theft coverage, contact your insurance advisor to report the claim. Coverage typically provides funds for services and expenses associated with restoring your compromised identity.

The federal government's website **IdentityTheft.gov** provides detailed advice on how to fix problems caused by identity theft. The site will guide you through a personal recovery plan, track your progress, and provide helpful resources such as printable checklists and pre-filled letters and forms.

Act quickly if you suspect credit card fraud

As mentioned in the introduction, use of stolen credit card numbers is one of the most common forms of identity theft and it no longer happens primarily from failure to shred paper documents.

Another way cybercriminals get credit card numbers is through radio-frequency identification (RFID) chips that credit card issuers are placing on cards now instead of magnetic strips. The advantage of RFID chips is quicker transactions at retail outlets like fast-food restaurants and convenience stores. The problem is, radio frequency identification makes it possible for identity thieves to use a simple electronic device to capture the information.

Some effective was to stay on top of credit card fraud include:

- Follow your credit card billing cycles closely.
- Keep a list of account numbers, expiration dates, and credit issuers telephone numbers on hand.
- Sign up for a credit monitoring service.
- Clear online passwords and logins.

If you suspect you're a victim of credit card fraud or identity theft, act quickly to protect yourself. Work with your credit monitoring service or contact the issuers directly to verify if fraud has occurred and remove fraudulent charges if necessary.

> “ If you suspect you're a victim of credit card fraud or identity theft, act quickly to protect yourself.

Social networks — a constant cyber playground

Social networks including sites like Facebook, Twitter, Instagram, LinkedIn, Pinterest, and even Match.com have become a part of many people's daily lives. It's a great way to stay connected, but it's important to be aware of how much personal information you give out, who you connect with, and what links you click on. The Federal Bureau of Investigation (FBI) has identified a number of scams to be cautious of when using social networking sites.

Social engineering

It's no surprise that cybercriminals can fake everything about themselves online, including their names and business affiliations, gender, age, and location. The FBI is continuously investigating investment fraud schemes happening online. Cyber-criminals carry out identity theft crimes by misidentifying themselves on social networking sites and then tricking victims into giving them their account names and passwords, as well as other personally identifiable information.

Fraud schemes

Cybercriminals are quite creative when it comes to online fraud schemes. The FBI reports recent fraud schemes involving cybercriminals gaining access to a victim's social networking or email account. The criminals claim to be the victim and send messages to the victim's friends. In the messages, the criminal claims he or she is traveling and has been robbed of their credit cards, passport, money, and mobile device and is in need of money immediately. Without realizing that the message is from a criminal, the friends wire money to an overseas account and become victims.

Phishing scams

Phishing scams are used by cybercriminals to make potential victims think they are receiving messages from a trusted source. According to the FBI, phishing schemes on social networking sites are cleverly packaged and may include: messages from strangers or compromised friends' accounts, links or videos claiming to lead to something harmless, or messages that claim to be from the social networking site itself. Social networking users fall victim to the schemes because of the high level of trust associated with social networking sites. Users often accept invites to connect with people they don't actually know or don't adjust profile privacy settings appropriately. This gives cybercriminals an upper hand to send messages containing software designed to give the criminal control over the victim's entire computer. Once the malware infection is discovered, it is often too late to protect personal data from compromise.

> “Be aware of how much personal information you give out on social networks, who you connect with, and what links you click on.

Data mining

Cybercriminals use data mining techniques to obtain information from victims through social networking. A cybercriminal may send out a “get to know you” questionnaire to potential users asking them questions that sound like they are coming from a financial institution. The answers to the questionnaire can provide the cybercriminal with the information they need to enter the victim’s bank account, email account, or credit card and do severe financial damage.

Online dating

Millions of people use online services to meet potential partners and start successful relationships. Unfortunately, scammers also use these sites to set up fake accounts, often claiming to be from the US, but are traveling or working out of the country. Their goal is to entice people into relationships, gain their trust, and eventually ask for money. Never wire money to someone you met online to cover travel, medical emergencies, or hospital bills. Never make an online purchase for them, allow them to use your address to receive packages, or forward a package to another country.

> Avoid posting personal information that could put you or your family at risk.

Social networking best practices

Educate yourself and your family members about the risks of posting information on social networks that an identity thief could use for malicious purposes. Learn how to spot potential internet scams and what to do to protect your sensitive information from cybercrime.

Follow these guidelines to keep your information secure when using social networks:

- Avoid posting any personal information about you or your family, including your name or contact information that could put you at risk of identity theft.
- Never send personal information through a message or click on a link in a suspicious message.
- Keep in mind that information posted on social media sites can be seen by anyone; even if you use security settings, hackers can still access this data.
- Set appropriate privacy and security defaults.
- Regularly check your privacy settings on social media sites to learn if your friends and followers receive your updates.
- Use strong password management strategies.
- Never post about upcoming vacations, especially specific details like dates of travel.
- Opt out of Facebook and Twitter functions that automatically tag posts with a location. If a site asks to “use your location” reply “no.”
- Be cautious about installing third-party applications. Do not install applications from sources you do not know.
- Only accept friend requests from people you know directly.
- Be careful what you post—consider everything you post as public.

New technology can bring new risks

Technology is constantly emerging, with early adopters eager to try out the latest trends. It is important to be cautious about diving into new technology, as security for these systems often lags behind the schemes of hackers and scammers.

Bitcoin and virtual currency

Virtual currencies, like bitcoin, can be a fast and inexpensive way to pay for goods and services. This type of money is completely digital, can be used across the globe, and is not regulated by a central authority or bank. Bitcoin users keep their funds in a digital “wallet” stored on a computer, smartphone, or through an online service. If your bitcoin wallet files are accidentally deleted, tampered with, or stolen, your funds could be gone, as virtual currency is not insured by the FDIC. If the company behind your digital wallet fails or is hacked, you could lose your funds. Payments made with virtual currency are irreversible and extremely hard to trace back to the wallet owner. Once you hit send, you can’t get your money back unless the original recipient agrees. Because of this, virtual currency has quickly become popular with hackers, as it allows them to demand and receive payments while keeping their identity hidden.

Non-Fungible Tokens (NFTs)

NFTs are unique digital assets representing ownership of real-world items like art, video clips, music, and more. You've likely seen one as someone's personal social media avatar or even displayed electronically in a home. Recently, NFTs have gained popularity and opened up a new investment opportunity for early adopters. But just like every online transaction poses security risks, there are some NFT cyber risks to consider.

According to Greg Adams, Digital Asset Specialist at Advisor at The Fine Art Group, phishing attempts, malicious contracts, and rug pulls are top risks to watch for when purchasing an NFT. There's been an uptick in exploits when people sign contracts through digital wallets. Before connecting your wallet to make a purchase, ensure the website is valid by checking the URL. Oftentimes, phishing attempts and fraudulent contract schemes are sent through social media messages. Rug pulls happen when a creator sells you an NFT with the promise of building a brand on the IP and never follows through. To avoid rug pulls, only purchase from reputable companies.

Malware

Beware of free downloads. Hackers will often bundle malware in with these popular links. Malware contains viruses and other unwanted software installed on your computer without your knowledge. The hackers then have access to monitor your online activity or control your accounts, giving them the ability to steal personal information, send spam, or commit fraud. If you think there may be malware on your computer stop shopping, banking, and other online activities; update your security software and scan for viruses; and get tech support if necessary.

Ransomware

Ransomware is a type of malware that holds your data hostage by encrypting it. The hackers will then demand payment before removing the encryption and giving back access to your files. They often demand payment in bitcoins or other virtual currency because it is harder to trace. Law enforcement doesn't recommend paying the ransom, because there is no guarantee you will get access back to your files. The best way to defend against ransomware is to use anti-virus software and keep it up to date. Also, make sure to back up your important files and make it part of your routine to do so often. If you have backed up your data, you may be able to restore your computer after the ransomware is removed.

> “Make sure you are running the latest version of software and always install updates on your devices.

Keeping pace with the Internet of Things

The Internet of Things (IoT) refers to the connection of electronic devices and sensors to the internet. They can send, receive, and collect data with or without a person operating them, often using that data to learn your habits and become “smart” in how they interact with you. This technology even allows appliances and gadgets to talk to each other directly. Imagine setting an appointment in your calendar and when you’re ready to leave your car already has the directions ready in the GPS. Or when your alarm clock goes off it signals the coffee maker to turn on. Perhaps you’ve even adapted some of these new technologies already.

With the use of sensors, any inanimate object has the potential to be connected to the IoT. However, by building the technology into devices, manufacturers have made it easier for consumers to interact with the IoT. Household appliances are the fastest-growing category with an increasing number of household systems operating remotely, including furnaces, air conditioners, fire detectors, security systems, appliances, and lights.

While these advancements will likely make life easier, keep in mind that you might not be the only person interacting with your devices. Many times the manufacturer is receiving data as well. These systems have also become targets for hackers who can take over the webcam in your smart TV and monitor your home or control traffic lights and cause gridlock in major cities.

“ Always change the default username and password on your devices.

When you shop for smart devices, make sure to ask some questions. Learn how a device works and what support the manufacturer provides. Know the product's security features; because an online security breach of one device could expose your entire home network.

The FTC offers more tips as you add to the number of smart devices in your home:[3]

- Find out if the product will work with devices you already own or with other companies' devices.
- Ask how you will get security and other product updates.
- Take time during the initial set up of each device to familiarize yourself with any dashboards and widgets that you will use to control the device remotely.
- Don't just accept default settings. Turn on security features and re-evaluate only after you are familiar with the device.
- Consider if you will be able to keep using the device if the manufacturer stops providing updates and other support.

Top five types of identity theft[3]

Types of identity theft	Number of reports	Percent of total top five
Government benefits applied for/received	385,264	31.0%
Credit card fraud—new accounts	363,092	29.2%
Miscellaneous identity theft	300,244	24.1%
Business/personal loan	105,711	8.5%
Tax fraud	89,649	7.2%
Total, top five	**1,243,950**	**100.0%**

Protect your data in the cloud

Cloud services, such as Dropbox, Google Docs, and iCloud, transmit and store users' data across the internet. Companies developing devices on the IoT also use cloud servers to store the data those devices collect. All of these types of connections are susceptible to monitoring and interception.

This type of computing is growing in popularity because it allows users access to files from any connected device, but cybersecurity problems are increasing at the same time.

There are some steps you can take to protect your data from getting into the wrong hands when using cloud services:

- Be aware of what you're storing in cloud services.
- Use different passwords for all your cloud services accounts, and change them all frequently.
- Don't use answers to security questions about yourself that may be available publicly.
- Take advantage of the two-step identification process that most services offer.
- Use a third-party data encryption service.
- Unlink devices you don't use.
- Enable email settings to alert you when new devices gain access to your accounts.

Keep your devices secure

Many people have more than one mobile device. Follow these recommended best practices from the Federal Trade Commission to keep all your devices safe from cybercrime risk:

Use security software

Install anti-virus software, anti-spyware software, and a firewall. Set your preference to update these protections often. Protect against intrusions and infections that can compromise your computer files or passwords by installing security patches for your operating system and other software programs.

Safely dispose of personal information

Before you dispose of a computer, get rid of all the personal information it stores. Use a wipe utility program to overwrite the entire hard drive.

When disposing of a mobile device, first check your owner's manual, the service provider's website, or the device manufacturer's website for information on how to delete information permanently, and how to save or transfer information to a new device. Remove the memory or subscriber identity module (SIM) card from a mobile device. Remove the phone book, lists of calls made and received, voicemails, messages sent and received, organizer folders, web search history, and photos.

Lock your laptop

Keep financial information on your laptop only when necessary. Don't use an automatic login feature that saves your user name and password, and always log off when you're finished. That way, if your laptop is stolen, it will be harder for a thief to get at your personal information.

Encrypt your data

Keep your browser secure. To guard your online transactions, use encryption software that scrambles information you send over the internet. A "lock" icon on the status bar of your internet browser means your information will be safe when it's transmitted. Look for the lock before you send personal or financial information online.

Read privacy policies

Yes, they can be long and complex, but they tell you how the site maintains accuracy, access, security, and control of the personal information it collects; how it uses the information, and whether it provides information to third parties. If you don't see or understand a site's privacy policy, consider doing business elsewhere.

Be smart about Wi-Fi

Before you send personal information over your laptop or smartphone on a public wireless network in a coffee shop, library, airport, hotel, or other public place, see if your information will be protected. If you use an encrypted website, it protects only the information you send to and from that site. Use a secure wireless connection for protection.

Keep passwords private

Use strong passwords with your laptop, credit, bank, and other accounts. Be creative: think of a special phrase and use the first letter of each word as your password. Substitute numbers for some words or letters. For example, "I want to see the pacific ocean" could become 1w2ctpo. For lengthy passwords, consider utilizing a password manager to help you maintain password security and login credentials.

Protect your children

Children are just as susceptible to cyber risks as their parents, but with generally less knowledge on how to protect themselves. Parents can implement the following tips to help provide a safer online experience for their family.

- Talk to your child about computer security, keeping their personal information private, and the importance of using strong passwords and not sharing them.
- Consider using parental controls to limit what your child might see on the internet. These tools can limit access to certain sites, words, or images; prevent a child from sharing personal information; limit their time online; or alert you to online activity.
- Know what child safety features are available for mobile devices. Some devices are made specifically for children, designed to be easy to use, and have features to limit internet access, manage minutes, limit texting, and provide emergency buttons. Remember that filters installed on a home computer won't limit what children can do on a mobile device.
- When downloading apps to a mobile device or social network, children – and adults – should check the privacy policy and privacy settings. By downloading apps, you may be giving the developers access to personal information, which they can then share with third parties.

- Many mobile devices include GPS technology that allows parents to pinpoint where their child is. But this also allows children to map their friends – and be pinpointed by others. Make sure your child knows to only use these features with people they know and trust.
- Encourage your child to think about privacy and the privacy of others before sharing photos and videos. Get permission of the people in the shot before posting it.
- Sending or forwarding sexually explicit photos, videos or message from a mobile device is called “sexting.” Make sure your child knows they could be breaking the law if they create, forward, or even save these types of messages.
- Get to know the sites and apps your child is using. Parents like to know who their kids are friends with offline, but it’s just as important to know who they’re talking to online.

COPPA gives parents tools to protect children online

The Children’s Online Privacy Protection Act (COPPA) was enacted to protect children’s personal information on websites, services, and apps that are specifically directed to children under the age of 13. It also applies to general audience sites that collect personal information regarding children under this age.

COPPA requires these sites, services, and apps to notify parents directly and get parental permission before collecting, using, or disclosing a child’s personal information. COPPA defines personal information as:

- Name
- Address
- Phone number
- Email address
- Physical whereabouts
- Photos, videos, and audio recordings of the child

If you do agree to allow a site, service, or app to collect your child’s personal information, it has a legal obligation to keep the information secure.

Products designed to protect you

A number of insurance carriers offer personal identity products to help protect you from cybercrime threats, such as identity theft. Some carriers include coverage for identity theft and restoration services as part of their homeowners insurance policies. Other companies sell more comprehensive coverage as a stand-alone policy or as an endorsement to a homeowners insurance policy.

Identity theft insurance provides reimbursement to crime victims for the cost of restoring their identity and repairing credit reports. It generally covers expenses such as phone bills, lost wages, notary and certified mailing costs, fees when reapplying for loans, grants or other credit instruments, and sometimes attorney fees (with the prior consent of the insurer).

Some companies also offer restoration or resolution services to guide you through the process of recovering your identity, which can include working with credit card companies, credit bureaus, creditors, and businesses on your behalf to correct any covered identify fraud issues. Identity theft insurance will reimburse a policyholder for expenses incurred to restore his or her identity, up to the limits stated in the policy.

In addition to products and services related to identity theft, some insurers are now offering products to protect NFTs and digital assets so you can protect your investments and your financial future.

Talk to a trusted MMA PCS Personal Risk Advisor about identity theft protection and other cyber risks. With the proper coverage in place, you can avoid a major upset to your financial wellbeing after a cybercrime event.

Visit mmapcs.com to learn more or contact us.

MarshMcLennan Agency

Private Client Services

References

[1] Javelin Strategy & Research
[2] Insurance Information Institute
[3] Federal Trade Commission

About Marsh McLennan Agency Private Client Services

At Marsh McLennan Agency Private Client Services, we serve clients whose lives are anything but ordinary. That's why we design insurance solutions that are just as unique – with the expertise, personal approach, and in-depth industry knowledge necessary to protect our clients' wealth, safeguard the things and people they love, and keep making extraordinary possible.

This document is not intended to be taken as advice regarding any individual situation and should not be relied upon as such. Marsh & McLennan Agency LLC shall have no obligation to update this publication and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting or legal matters are based solely on our experience as consultants and are not to be relied upon as actuarial, accounting, tax or legal advice, for which you should consult your own professional advisors. Any modeling analytics or projections are subject to inherent uncertainty and the analysis could be materially affected if any underlying assumptions, conditions, information or factors are inaccurate or incomplete or should change. d/b/a in California as Marsh & McLennan Insurance Agency LLC; CA Insurance Lic: 0H18131.

Make Extraordinary Possible.SM