
USAA®
THE USAA
EDUCATIONAL
FOUNDATION®
PERSONAL SAFETY
protecting
your identity

our mission

The mission of The USAA Educational Foundation is to help consumers make informed decisions by providing information on financial management, safety concerns and significant life events.

table of contents

identity theft **insight**

Your most valuable possession is:

- **A** Your home.
- **B** Your vehicle.
- **C** Your good name.

The answer is **C**

Your name is as valuable as it is irreplaceable. No matter what tangible items you own, your identity and reputation are assets to retain and protect at every turn.

What you may not know about identity theft is what criminals count on. Even children can fall victim to these often unnoticed practices until it's too late to easily repair the long-term damage to their credit or future livelihood. But you can take steps right now to protect yourself and your family by first knowing exactly what constitutes identity theft and how it can occur. This helpful guide will get you started in the right direction to ensuring your identity holds its value for a lifetime.

Tech terms in brief

Encryption the process of making your data humanly unreadable — and more secure.

Firewall a defense system using software and/or hardware to block unauthorized and unwanted traffic from getting into your computer and devices on your network.

Router Small peripheral device that creates a network — often wireless — among different computers.

SSID Service Set Identifier is the ID that's assigned by the manufacturer of your router.

SSL Secure sockets layers are protocols that provide communication security over the Internet.

URL Universal Resource Locater or the address of a web page.

WEP Wireless Encrypted Privacy, an older protocol for securing wireless networks.

WPA, WPA2 Wi-Fi Protected Access and Wi-Fi Protected Access 2, the security standard for wireless networks.

What is identity theft?

IDENTITY THEFT CAN TAKE MANY FORMS SUCH AS:

- Opening bank or credit card accounts in your name and then using these accounts to make purchases or obtain cash.
- Changing the billing address on your real accounts so you may not be immediately aware of any discrepancies if you rely on paper statements to make your payments.
- Using false or nonexistent addresses in conjunction with opening fraudulent accounts in your name.
- Taking out loans in your or a family member's name, including minor children.
- Giving your name and personal information for employment, medical treatment or other purposes.
- Using your social security number to submit false tax returns to obtain a refund.
- Providing your name when arrested and charged with a crime.

How does identity theft occur?

There are multiple ways criminals can obtain and then use your identity, like:

- Stealing your purse or wallet.
- Taking mail out of unlocked mailboxes or going through your trash bins for documents containing sensitive, personal information.
- Diverting your postal mail to another location with a simple change of address card.
- Posing as an authority figure, such as a bank officer or landlord, in order to request your credit report.
- Observing and capturing your Personal Identification Number (PIN) from a debit card transaction at an Automated Teller Machine (ATM) or retail store.
- Hacking into your computer and/or installing malware (malicious software) designed to steal your user IDs, passwords and more.
- Stealing files, either paper or electronic, from an employer, physician, merchant or other business.
- Using phone, e-mail or web scams — including posting fake employment opportunities — that require you to provide personal information.

How do you know if you've been the victim of identity theft?

- You see withdrawals from your bank account that aren't yours.
- You don't receive your bills or debit or credit cards as expected or requested.
- Merchants refuse your checks.
- Debt collectors contact you about debts that aren't yours.
- You find unfamiliar accounts or charges on your credit report.
- Medical providers bill you for services you didn't use.
- Your health plan rejects your legitimate medical claim because their records show a condition you don't have.
- The IRS notifies you that more than one tax return was filed in your name, or that you have income from an employer you don't work for.
- You receive a notice that your information was compromised by a data breach at a company where you do business or have an account.
- Your child is turned down for government benefits because the benefits are being paid to another account using your child's Social Security number.
- You get a notice from the IRS saying your child didn't pay income taxes, or that your child's Social Security number was used on another tax return.
- You receive collection calls or bills for products or services you didn't receive.

preventing an identity crisis

Be smart about how and where you use or enter financial or personal data, whether you are offline or on the Internet — most of all, stay alert to anything that seems suspicious and report it immediately to your financial institution or credit card companies. This means keeping an eye on your children's credit too! With some extra care and precautions, you can make great strides to avoid becoming a victim of an identity crisis.

According to the Federal Trade Commission (FTC), there are four main ways you can keep your personal information more secure:

- Only share your information with people or businesses you know.
- Store and dispose of sensitive materials securely, especially your Social Security number.
- Ask questions before deciding to share any personal information.
- Maintain updated security measures on your computers and other electronic devices.

reduce your paper trail

Today's mail contained a utility bill, a statement from your insurance company and an unsolicited "pre-approved" offer for a new credit card. Which of these items is the most potentially dangerous source of identity theft?

The credit card account offer — it's a common way thieves steal identities every day. Even if they are not activated, these communications are best shredded and, if possible, stopped altogether by opting out of future mailings. But really, anything you just toss in the trash without first shredding or rendering unreadable could spell trouble.

IMPORTANT REMINDERS:

- Memorize your Social Security number (SSN) and NEVER carry your card.
- Keep important documents like birth certificates or financial papers that display your SSN in a secure location. Consider getting a safe deposit box to store these items as well as your passport and copies of your credit cards should you need to report these as lost or stolen.
- Don't imprint your personal checks with your SSN or driver's license number.
- Lock up your purse or wallet when at work, the gym, or school. If traveling, leave your wallet in the hotel safe deposit box and just take select items like a driver's license and one credit card.
- Only use ATMs that are in familiar and well-lit locations where you feel comfortable. Ideally, use the ATMs at your financial institution — thieves can install card-readers inside unauthorized machines at places like convenience stores that digitally read and steal your information. Other good-sense ATM practices include:
  - Being aware of your surroundings and any other people in the area. Have your card ready to transact your business quickly without stopping to count it out in the open.
  - Never using machines that appear damaged or compromised — be sure to report the ATM's location to the card issuer — Shield account numbers and PINs from view when using credit or debit cards.
- Shred, shred and shred some more! That includes credit applications, insurance forms, bills, old credit or debit cards and similar materials. Check with your financial adviser as to how long you should keep bank or other financial statements. Use a cross-cut shredder for documents, compact discs (CDs) or digital video discs (DVDs) with personal or financial information.
- Get a locked postal mailbox at your home if possible; if you're going to be traveling, have mail held at the post office or arrange for a trusted neighbor to collect it daily.
- Go green and choose paperless statements for bank, credit card, investment or insurance materials.
- Review your monthly financial statements for unauthorized entries or transactions and contact the appropriate institution immediately if you notice anything amiss.
- Peel off the labels from empty prescription containers before tossing these in the trash and shred the accompanying pharmacy instructions that contain personal information.

reduce your e-footprint

The Internet is a wonderful thing — unless someone uses it to gain access to your computer and your personal information. Again, staying aware is key and being proactive makes it harder for identity thieves to take advantage of your good name.

- Use a pop-up blocker with your browser.
- Always log off from your computer.
- Disconnect your computer from the Internet if you are not using it for an extended period of time.
- Protect your home wireless network by hiding the network name (SSID) and using WPA2 (Wi-Fi Protected Access). It is a stronger encryption protocol. Avoid using WEP (Wired Equivalent Privacy). It has been replaced by WPA2. Also, regularly change your encryption key or password.
- Keep your browser updated. The most recent version is generally more secure.
- Set your browser and operating system to automatically download and install security updates.
- Do not share personal information via e-mail or the Internet unless you know and trust the website/recipient. Make sure you are using a secure website. For more information, refer to “How To Recognize A Secured Website.”
- Never reply to e-mail or pop-up messages that ask for personal financial information such as your SSN, date of birth, or mother’s maiden name or call any numbers included in these messages.
- Do not open e-mail attachments or links from unknown individuals or if the sender’s name is familiar but the address or subject line seems unusual. Spoof e-mails use contacts acquired from a real e-mail address to send links to sites, possible viruses and more. If it doesn’t seem right, delete it immediately and let the person know their e-mail account may have been compromised.
- Do not cut and paste a link from a message into your browser; instead, key in the website address yourself.
- Always review your financial accounts and statements for unusual activity.
- When accessing your bank or any credit card accounts online, make sure you log off even if the session expires automatically after a period of idleness — and clear the history from the browser.
- Back up your files, ideally on an external device such as a USB memory stick or thumb drive, at least every six months and store it elsewhere, such as a safe deposit box or in a locked file at a secure location.
- Install a shredder program to completely delete files as you go or use a wipe program to delete all files before discarding an old computer. Another user could reformat the hard drive and ultimately recover the data.

Preventing unauthorized access to your computer

If you're using the Internet, then your computer — with all your data — is potentially a target for identity thieves and malicious activity unless you take these precautions:

- Understand your computer and network settings, at home or at work.
- Install firewalls to monitor the flow of data between your device and the Internet while helping to prevent the installation of malicious software designed to send your information to hackers.
- Install a spyware detection program and be alert to things like: e-mail attachment files ending in .exe or .dll; high volumes of pop-up ads; sudden change in your browser's home page; sluggish performance; new toolbars that randomly appear in your browser; new icons on the system bar at the bottom of your computer screen or on the desktop.
- Install anti-spam and anti-virus software.

When in doubt, disconnect from the Internet and consult a verified tech professional for assistance in cleaning up your computer and ridding it of any potential dangers. If your children use your device, instruct them as to safe surfing procedures.

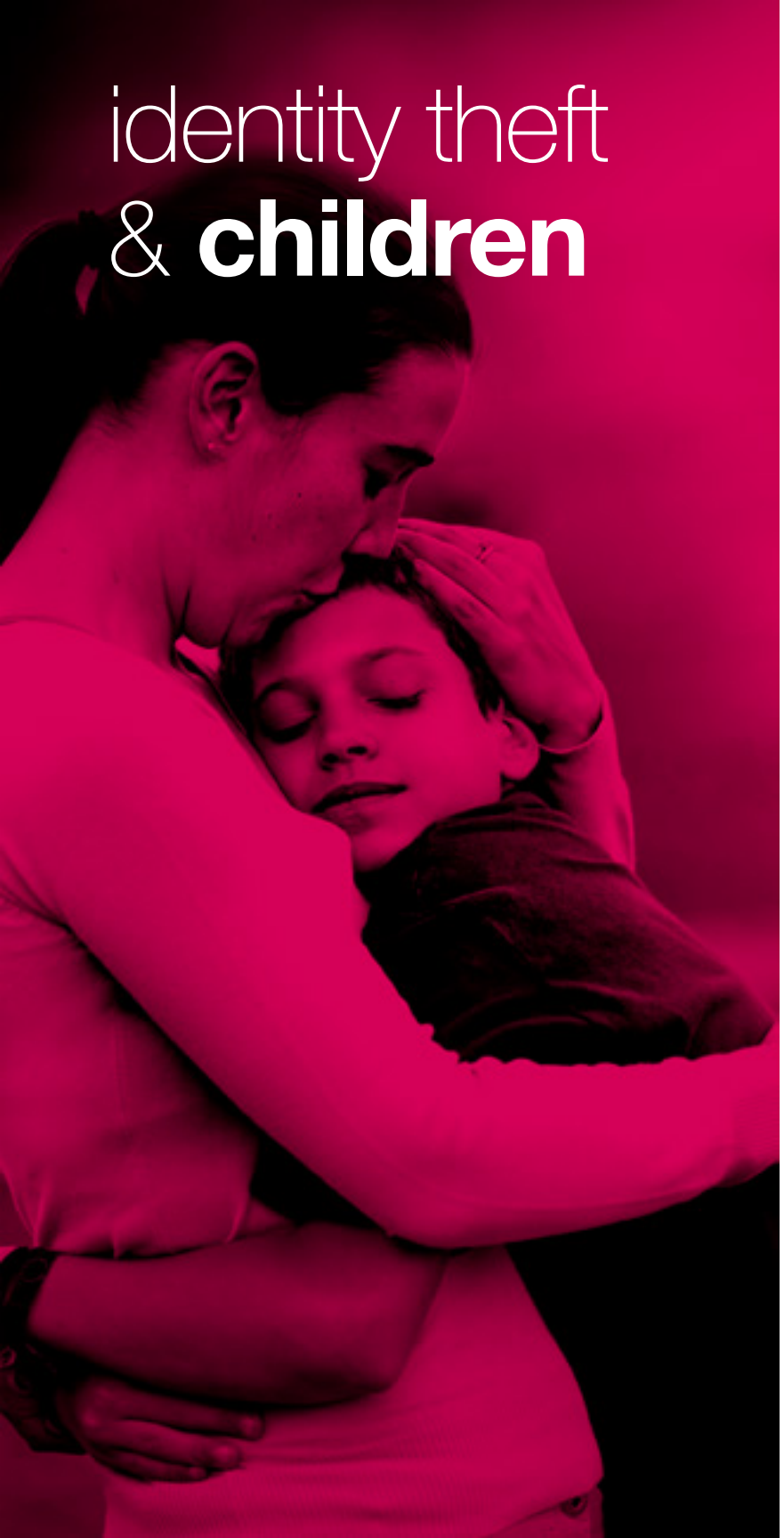
For more information and tips, visit staysafeonline.org

Did you know?

That your smart phone is actually a small computer? Built with a mobile operating system (OS), your smart phone has computing and connectivity capabilities that make it just as vulnerable to hackers and malware as your desktop or laptop machines!

Mobile phone or device apps or e-transactions require extra caution too. Be aware of who uses your phone, never store account numbers or passwords in your contacts, change your mobile banking PIN regularly and keep copies of any reference numbers. Use the pass-code lock option to make it harder to access your phone if lost or stolen. And NEVER give your pass-code or your PIN number to anyone!

identity theft & **children**



Protect the innocent.

Think your kids are immune to identity theft? Unfortunately, because of their pristine credit reports, even infants and young children are potential targets — and it's not just a crime committed by total strangers. There are also concerns originating with "friendly thieves," meaning a family member or close friend, who use the Social Security numbers (SSN) of children to open accounts, apply for loans and more. An unblemished credit history won't stay that way if you are unaware. So when you check your credit, it's a good idea to check your child's credit too and look for any discrepancies or red flags.

IN ADDITION:

- Even government agencies, physician's offices, and similar businesses are subject to security breaches. Before you give your child's social security number, birth certificate, or similar sensitive information to anyone, ask how it may be stored, used, and ultimately destroyed.
- Keep this same type of information in a secure location such as a safe deposit box.
- Never post your child's birth date on social media sites — instruct older children to follow suit.
- Supervise what they do post and encourage them to let you know if anyone asks for their personal data or before they complete any registration forms or open any type of account. Federal laws prohibit the solicitation of information from children under 13 but it doesn't always protect the user if they elect to provide it anyway. Age-appropriate explanations about the dangers of identity theft along with your guidance can help them proceed with caution.
- Visit the Social Security Administration website at *ssa.gov* to view your child's records; this can help alert you to fraudulent use of their SSN.

Your child may be a victim of identity theft if:

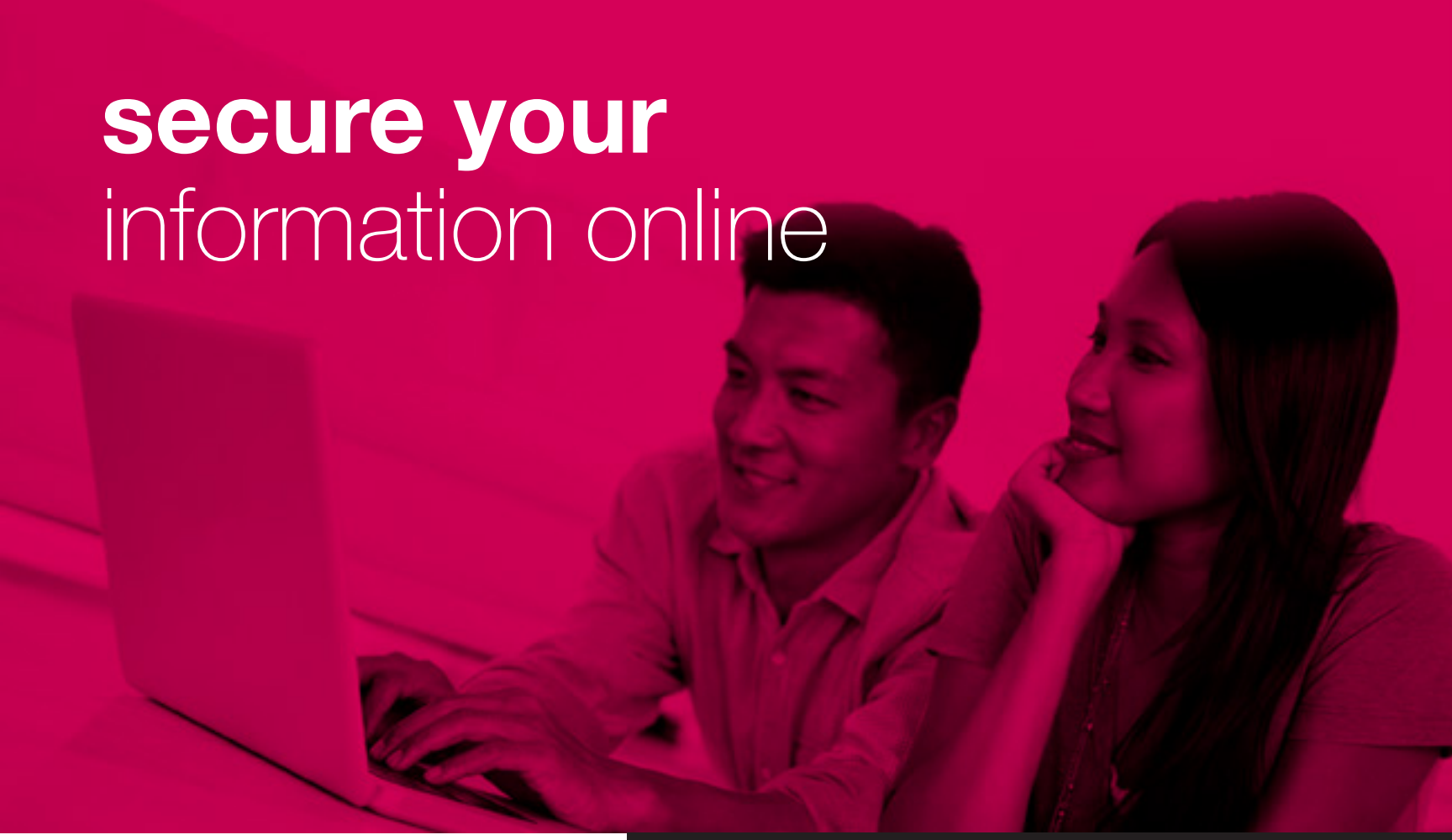
- You receive credit card offers, statements or similar materials in your child's name.
- Agencies such as the IRS contact your child for monies owed or in reference to any activity.
- Collection companies attempt to contact your child for non-payment of bills.

You can create a fraud alert by contacting just one of the three credit reporting bureaus — Experian, TransUnion, Equifax — and that company is required to contact the other two. For up-to-date contact details and more information, see *consumer.ftc.gov* and click on "Privacy and Identity."

If your child's identity has been compromised:

- Immediately notify your financial institution and corresponding credit card companies to close the account in question.
- File a police report.
- The Federal Trade Commission (FTC) suggests you consider filing a fraud report, creating a fraud alert and placing a "freeze" on your child's credit. See state-specific laws regarding freezes at the National Association of Attorneys General, *naag.org*

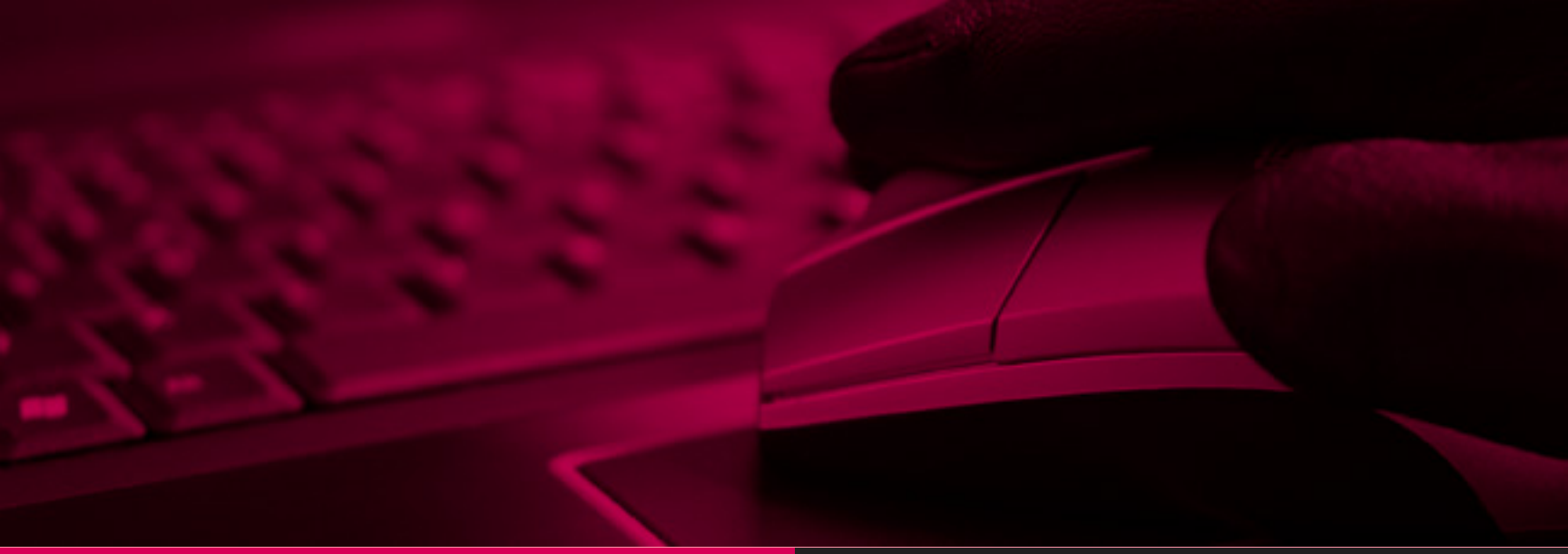
secure your information online



Check the settings on your browser to either surf the web in a privacy mode that never saves your searches or manually clear the history each time you use the Internet. Some search engines also offer an encrypted version now for additional security.

Cookies — to **enable or disable?**

Every time you visit a website, “cookies” are stored on your computer and contain information such as site preferences or log in status. While cookies are not necessarily used for malicious purposes, you can choose to disable these in the privacy settings tab on your web browser. Clearing your history, cache and cookies at the end of each web session will also help delete these from your computer. Regardless of your preferences, surf the web wisely and help protect your identity online.



Password **proficiency**

While many sites requiring registration with a unique user ID and password may have established parameters for how to create a password, there are some universal tips to keep in mind.

NEVER USE: SSNs, birthdates, phone numbers, relatives' names, addresses or anything that an identity thief may easily decipher. Change passwords often and do not save them in your contacts on a mobile or other device. Most important — NEVER OPT FOR THE "SAVE PASSWORDS" feature that may be offered on certain sites. If you think it's a lot of trouble to remember different passwords for different sites, think about how much more trouble it will be to salvage your identity.

Wi-Fi Worldly

Public Wi-Fi or "hotspots" seem like a great concept when you're stuck in an airport or just passing time at the local coffee house. Unfortunately, public Wi-Fi is also a real attraction for identity thieves who can easily hack into your computer if you don't take a few precautions. According to the FTC, most Wi-Fi hotspots don't encrypt the information you send over the Internet and are therefore not secure.

What's more, not every website you access may be encrypted. Look for "https" at the beginning of the web address (the "s" is for secure and you'll also see a padlock icon that means it's secure). Some websites use encryption only on the sign-in page, but if any part of your session isn't encrypted, your entire account could be vulnerable. Look for https on every page you visit, not just when you sign in. Visiting only secure sites, logging off the Internet when done, and never sending personal information in this type of setting is advisable. If you frequently use Wi-Fi hotspots, consider getting your own VPN or Virtual Private Network available through a VPN provider or even some employers who have staff members who frequently travel on business.

responsible businesses, safer transactions

How do you recognize a responsible company that's committed to protecting your information?

Whether you're dealing with a retail store, a credit card issuer or service business, make sure you know:

- The privacy policy that ensures your information is protected and how it will be used and stored. Look for the fine print or disclaimers that state the company doesn't specifically sell your data to other businesses.
- Monitoring and alert processes if unusual account activity is detected.
- Provision of assistance for fraud victims and education for protection methods.

Understanding high-risk transactions

Businesses are required to verify the authenticity of each customer's transaction. The increase of identity theft and fraud make this a regular part of responsible companies' procedures. At times, based on the policy of each business, your transactions may be flagged as potentially "high-risk" and you'll be asked to verify your information. This may seem intrusive or annoying but it's a very necessary tool that can help keep your identity and your credit intact. Ask the companies you deal with how they handle this effort and make sure you understand the details.

Safer online shopping

Your computer and the Internet connect you to thousands of businesses literally all over the world — which can be a great convenience or a huge problem depending on what you know about secure transactions.

HOW TO RECOGNIZE A SECURED WEBSITE

Closed padlock symbol or key: means your information is being sent over an encrypted, or "scrambled," connection for greater security — should an identity thief or hacker attempt to intercept this data stream, the information would be unreadable and unusable.

https:// — Look for these letters and symbols at the beginning of the web page title in the address bar. The "s" means SECURE. Note that newer technology allows search engines to locate the page or site without the full inclusion of these letters — click in the space on the bar at the end of the address or URL and the https:// should appear. If not, don't use the site.

FOR MORE SECURE E-COMMERCE:

- Only shop with companies you know and trust. You can check out reviews and complaints by doing a search of the company name online or see the Better Business Bureau site, *bbb.com*, for more details.
- Never save your password for any site.
- If you must use a shared computer with multiple user accounts, don't access your banking information online.
- Ask your financial institution if it's possible to obtain a one-time credit card number for a single transaction. Keep copies of all transactions and activity and check your statements.
- Decline any requests for additional information or survey responses.
- IMMEDIATELY notify your financial institution or credit card issuer of any discrepancies.

unwanted solicitations

Intrusive at best, dangerous at their worst, solicitations conducted by phone, mail or e-mail may be valid but are often used to scam unsuspecting people to acquire valuable personal information. You can opt out of these activities by contacting these agencies:

CREDIT REPORTING INDUSTRY

OptOutPrescreen.com will remove your name from all mailing lists either permanently or for up to five years, depending on your preference.

DIRECT MARKETING ASSOCIATION

At *dmachoice.org*, you can stop most promotional postal mail as well as e-mail offers and unwanted promotions.

DO NOT CALL REGISTRY

Go to *donotcall.gov* and provide the designated phone numbers to end telemarketing calls.

Remember — not all solicitation may end immediately; it could take up to several weeks for your opt-out requests to be updated. Check with each agency for their individual guidelines as well as any renewal processes.

Charitable acts

Just like any other business, you should first verify the authenticity of any charitable organization requesting donations whether you're contacted by phone or mail. Inquire as to what percentage actually benefits the intended recipients and how much pays for administrative or operating costs before making a contribution. If you're at all unsure, don't donate especially over the phone. Ask for more information to be provided to you and do your homework — *CharityNavigator.org* is an independent evaluation entity that provides detailed information as to how a charity spends its funds. *Guidestar.org* is another good source of financial and other data based on tax filing information.

Keeping Seniors Safe

Every year, more and more elderly individuals fall victim to scams involving fraudulent charitable causes — sometimes even losing life savings that are unrecoverable. Talk to your elderly family members or friends about the importance of screening phone calls and never giving out their personal information to anyone, even if it's someone they know. Assign a trusted relative or financial adviser as the "go-to" person for any help with these kinds of solicitations. While you don't want to imply that your senior isn't capable of making the right decision, it's possible to approach the subject with only having a concern for their safety — so make sure to involve them in choosing the person or persons whom they will ask for help.

3 safety tips

1. Don't pay for any services in advance.
2. Don't be pressured into making any quick decisions regarding purchases or donations.
3. NEVER pay for or provide financial or personal information to claim a prize.

KNOW YOUR TELEMARKETING RIGHTS

- The caller must identify the company name, the nature of the call as an attempt to sell a product or service, and what is being sold.
- Calls cannot take place before 8 a.m. or after 9 p.m.
- Any requests for calls to cease must be honored.

Complaints can be made at *donotcall.gov* or (888) 382-1222.

detecting identity theft

Early detection and proactive measures can help you recognize whether your identity and information has been compromised.

Know your credit rights

The Fair Credit Reporting Act and the Fair and Accurate Credit Transactions (FACT) Act of 2003 require that any consumer reporting agency must ensure that your credit rating is as accurate as possible, by:

- Providing you with a complete and up-to-date report.
- Investigating any identified discrepancies.
- Keeping your information from anyone other than legitimate users of the agency.
- Removing detrimental information from your file after seven years (bankruptcies can be removed after seven to ten years).
- Allowing you to include in your report a personal statement regarding any disputed information as it relates to unresolved investigations of a claim.

recovering from identity theft: for consumers & servicemembers

Remember...

Identity theft is the actual act of someone stealing your identity and using your personal identification to commit fraudulent acts such as purchases, making withdrawals from bank accounts, obtaining more credit cards or even employment.

Generally — and as soon as you become aware of any fraud or loss of your personal identification documents such as a driver's license — notify your bank or credit union, creditors, any appropriate government agencies such as your state's department of motor vehicles and consumer reporting bureaus. If you feel you need additional assistance do not hesitate to consult your family attorney or financial adviser. According to the FTC, your liability may depend in part on how quickly you report the loss or theft of your credit or debit card — so act fast and follow up any telephone conversations with a written letter sent by certified mail.

THE FTC ALSO RECOMMENDS THAT YOU:

Create an identity theft report — This gives you some important rights to help recover from the theft. To create one, file a complaint with the FTC at *consumer.ftc.gov* and print your Identity Theft Affidavit.

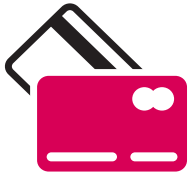
File a police report — Use the above to file a police report and create your identity theft report.

Place a fraud alert — This can make it harder for an identity thief to open more accounts in your name. The alert lasts 90 days but you can renew it.

To place a fraud alert on your credit report

Contact **ONE of the three** main credit reporting agencies — they must notify the other two agencies

For more information, visit *ftc.gov/credit*



To place a freeze on your credit report

A credit security freeze requires that you contact the three major credit bureaus to disallow new creditors from viewing your credit report and score. Because most businesses won't lend without first checking your report, a freeze can deter identity thieves from forming new accounts in your name.

Be aware however — placing a freeze on your credit could involve fees for freezing and unfreezing your credit depending on your state's laws and it won't stop thieves from using existing accounts if you haven't taken the measures to prevent this once fraud has been detected.

Each of the three credit reporting bureaus has a section and form to order a credit security freeze based on the state in which you live. At *experian.com* for example, once you select the state you'll be directed to a page with specific fee and other information regarding freezes.

EQUIFAX®

Equifax Inc. • Atlanta, GA • USA • www.equifax.com

equifax.com
(800) 685-1111

Experian℠

experian.com
(888) 397-3742

TransUnion®

transunion.com
(800) 888-4213

Active Duty Servicemembers

You can place an alert on your credit report for up to one year. At your request prior to the end of that period, you may have the alert removed. While the alert is in effect all creditors must verify your identity prior to issuing any credit in your name — often, servicemembers choose to enable an alert right before deployment. The law allows you to designate a personal representative to place or remove an alert. But be aware — an active duty alert may make it difficult for your spouse to obtain additional credit. For additional information regarding fraud alerts and other concerns specific to your status, you can go to *ftc.gov*.

The Military Sentinel site is specifically designed for your unique needs, whether at home or deployed overseas. Here, you can:

- Set up scam alerts and review a database of servicemember-specific current fraud activity.
- Obtain educational information that helps to better understand credit issues, how to recognize a variety of scams from work-from-home schemes to fraudulent loan offers.
- File secure, online identity theft complaints with the FTC and Department of Defense (DOD) officials.

Be Diligent, Be Prepared to Follow Up

You can't be too careful when it comes to addressing identity theft and getting professional help may forestall some of the ensuing problems. So don't hesitate if you feel you need additional assistance to consult your family attorney or financial adviser.

As for a resolution, be aware that the process takes time. Understand your rights as a victim and as a consumer — the FTC provides a great deal of information regarding this area at *consumer.ftc.gov/topics/repairing-identity-theft*

How can you repair your credit after being the victim of identity theft?

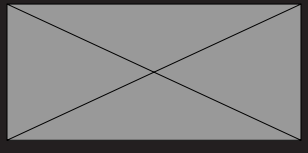
- Order and read your credit reports.
- Look for fraudulent activity on existing accounts or the opening of fraudulent accounts.
- Check all key information: Name, address, SSN, and employers.
- Dispute any errors on the report — such as accounts you didn't open or debts you didn't incur — with both the credit reporting agencies and the fraud departments of the businesses reporting the errors.
- Obtain an identity theft report and ask the credit reporting agencies and businesses to block the disputed information from appearing on your credit reports. Credit reporting agencies must block transactions and accounts if you are a victim of identity theft.
- As you contact businesses to make corrections, ask for copies of any documents the identity thief used to open a new account or make charges in your name.

THE USAA
EDUCATIONAL
FOUNDATION®

FOR MORE INFORMATION PLEASE VISIT:

usaaedfoundation.org

THE USAA EDUCATIONAL FOUNDATION®



PLEASE RECYCLE

70520-1213