

ID PROTECTION TOOLKIT



ID WISE

Brought to you by the Center for Identity
at The University of Texas at Austin

CONTENTS

2 Information and Documents to Protect

- 2 Name
- 2 Birth date
- 2 Mother's maiden name
- 2 Social Security number
- 2 Mailing and home address
- 3 Email address
- 3 Telephone number
- 3 Place of birth
- 3 Vehicle registration or plate number
- 3 Driver's license number
- 4 Biometric attributes
- 4 Credit card number(s)
- 4 Bank account number(s)
- 4 Medical insurance information

5 Actions to Take Online

- 5 Avoid email scams.
- 5 Use strong passwords.
- 5 Consider two-factor authentication.
- 5 Make security questions difficult.
- 6 Update your computer.
- 6 Use Wi-Fi carefully.
- 6 Choose secure websites.
- 6 Read privacy policies.
- 7 Destroy digital data.

8 Actions to Take in the Physical World

- 8 Monitor your surroundings.
- 8 Guard your Social Security number.
- 8 Invest in a safe.
- 8 Use your shredder.
- 8 Be careful with checks.
- 9 Use a locked mailbox.
- 9 Read your financial statements.
- 9 Read your medical statements.
- 9 Use photo ID.

INFORMATION AND DOCUMENTS TO PROTECT

Name

Your name as it appears on your birth certificate, or a common nickname, is the most commonly requested information in any identifying situation. You may be asked to provide your name in a countless number of scenarios, from registering for a passport to casual conversation.

Your full name, or known nickname, may be used by a criminal to falsely identify himself or herself to gain access to private information.

Birth date

This is the day you were born, according to your birth certificate.

Your birth date may appear on your driver's license, passport, tax forms, insurance information, credit cards, and online accounts. It is one of the commonly used pieces of identifying information by companies.

Paired with your name and other information, a thief may access existing accounts.

Mother's maiden name

This is your mother's last name before she was married.

This piece of information is the most popular security question asked by accounts. With this piece of information, thieves can reset passwords and access secure accounts.

Social Security number

A nine-digit number issued to United States citizens, permanent residents, and temporary residents by the government. This is the primary identifying factor used by government agencies and financial institutions.

This is your most important piece of personal information. If compromised, criminals can access private information and create fraudulent accounts.

Mailing and home address

Your address identifies where you live.

Your address may appear on your driver's license, ID card, credit card billing information, tax forms, and work documents.

Spam mail in the form of phony bills, sweepstakes scams, or other phishing attempts may be sent to your home.

Email address

An email address is a unique account for online mail.

You may be asked for your email at local and national stores, by friends, and by government agencies. Email addresses are also commonly used by websites as a username to login.

Phishing scams are the main concern with email accounts. False, authentic-looking emails may capture your personal information or infect your computer with malware. Paired with other information, thieves may use your email to access private online information.

Telephone number

This is a unique ten-digit number tied to a cell phone or landline.

Your telephone number may be requested by businesses, government agencies, work documents, and friends as a way to reach you.

Automated callers and scammers may impersonate institutions or even family members with elaborate hoax calls used to extract other revealing information.

Place of birth

Your place of birth is the city and state where you were born. This information appears on your birth certificate.

Your place of birth can be used to trace the first three digits of your Social Security number, and the information is often asked as a security question for accounts.

Paired with other information, a criminal could use this to access secure information.

Vehicle registration or plate number

These are state-issued documents identifying your motor vehicle.

You may be asked to provide this information at state departments such as the DMV or your local apartment complex or university.

Your license plate can be traced back to your home address and provide criminals with additional information.

Driver's license number

Your driver's license is the unique, identifying number that appears on your driving permit.

You are often asked to provide this number with checks, work information, and for background checks.

This number can be used to access accounts and other information.

Biometric attributes

Biometrics are identifying human characteristics and traits, including fingerprints, face recognition, DNA, hand geometry, iris recognition, retina and odor/scent. Behavioral characteristics can include typing rhythm, gait, and voice.

Biometrics can be used to access your smart phone or computer, to access secure areas of the workplace, and even to grant you access into Disney World.

By studying and mimicking your walk, voice, or fingerprints, a cyber criminal may gain access to secure places.

Credit card number(s)

Your credit card number is the numbers that tie back to a specific bank or financial account.

You are usually asked to provide this information when making a purchase in person or online.

Thieves can use the information to rack up huge amounts of debt and abuse your finances.

Bank account number(s)

These are the numbers associated with your savings or checking accounts at a financial institution.

Credit card companies, utility accounts, and human resource services often request this information.

This is the secure information criminals are most often seeking. Phishing attempts and phone scams are in place to extract this secure information.

Medical insurance information

Your health insurance information is often found on your Medicare card and on medical documents.

This information will be requested at pharmacies and doctor's offices.

Thieves may use this information to abuse insurance information and seek treatment for ailments under your name.

ACTIONS TO TAKE ONLINE

Avoid email scams.

Email scams, often referred to as “phishing,” are designed to steal money and infect your computer with malware. Typically, the scams involve an email that appears to be from a trusted source. The scams may be enticing—asking you to claim money that belongs to you—or alarming—indicating that there is a problem with your account.

Legitimate businesses will rarely make requests for personal information via email. If you get such a request, you should assume it is a scam until you are able to confirm otherwise. Call the institution that made the request using the customer service number found on their website.

Don't click links, or download or open attachments, unless you know the sender and are certain they are safe.

Use strong passwords.

A good password is often your first line of defense against an identity thief. In general, longer is better, and you should avoid predictable words, phrases, or short series of digits.

A combination of letters and numbers combined with random punctuation is encouraged. Be sure to vary your passwords across websites and services. If a password is stolen in one businesses' breach, it can easily be used to access your other accounts.

Consider two-factor authentication.

Two-factor authentication adds an extra step to the login procedures for many common web-based services, creating an additional layer of security. Two-factor authentication generally requires two of the following three types of credentials before you can access your account:

- » Something you **know**, like a password or PIN
- » Something you **have**, like an ATM card or your phone
- » Something you **are**, like a fingerprint or voice print

Make security questions difficult.

Many websites use security questions like “What is your mother's maiden name?” or “On what street did you grow up?” to help verify account ownership for password recovery. In order to prevent an identity thief from gaining access to your account via password recovery, it helps to make the answers to those questions more difficult.

- » A good answer is consistent. Don't choose a question like "What is the name of your pet?"
- » A good answer is safe. It should not be something that is easily guessed or can be searched.

Update your computer.

Make sure your computer is protected by anti-virus software, along with anti-spyware software and a firewall. Anti-virus software detects, prevents, and removes malicious computer viruses.

Anti-spyware software prevents hackers from gaining access to your system and gathering personal information from it. A firewall provides an additional line of defense against hackers, viruses, and other malicious computer attacks.

Keep anti-virus software, as well as your operating system, browsers, and security, up-to-date. This helps prevent identity thieves from gaining access to your computer and the personal information you store or share on it.

Use Wi-Fi carefully.

When connecting to a network, be aware if the network is private or public. Never share any personal information over a public network. Be sure your home network is password protected, using a strong password different than the factory default that came with your router.

Choose secure websites.

Even if you are shopping from home, you should check that the sites you are using collect your private information via a secure connection. Different web browsers use different icons to show a site is secure, so familiarize yourself with your browser settings. A good rule to keep in mind is that secure sites will have "https" at the beginning of their URL, instead of the standard "http."

Read privacy policies.

Privacy policies are long, boring, and easy to ignore, but they contain all the information about what data a website is collecting from you and how they will use it. It is a good idea to understand these details before you begin sharing your personal information online, especially for sites that you use often or that collect much of your personal information. Keep the following questions in mind when reviewing privacy policies.

When deciding which question to choose, or which answer to give, keep in mind the following characteristics of good questions and answers.

- » A good answer is memorable. If you can't remember the answer, the question is of no help to you.
- » A good answer is consistent. Don't choose a question and answer that may change over time, like "What is the name of your pet?"
- » A good answer is safe. It should not be something that is easily guessed or can be re-searched.

Update your computer.

Make sure your computer is protected by anti-virus software, along with anti-spyware software and a firewall. Anti-virus software detects, prevents, and removes malicious computer viruses. Anti-spyware software prevents hackers from gaining access to your system and gathering personal information from it. A firewall provides an additional line of defense against hackers, viruses, and other malicious computer attacks.

Keep anti-virus software, as well as your operating system, browsers, and security, up-to-date. This helps prevent identity thieves from gaining access to your computer and the personal information you store or share on it.

Use Wi-Fi carefully.

When connecting to a network, be aware if the network is private or public. Never share any personal information over a public network. Be sure your home network is password protected, using a strong password different than the factory default that came with your router.

Choose secure websites.

Even if you are shopping from home, you should check that the sites you are using collect your private information via a secure connection. Different web browsers use different icons to show a site is secure, so familiarize yourself with your browser settings. A good rule to keep in mind is that secure sites will have "https" at the beginning of their URL, instead of the standard "http."

Read privacy policies.

Privacy policies are long, boring, and easy to ignore, but they contain all the information about what data a website is collecting from you and how they will use it. It is a good idea to understand these details before you begin sharing your personal information online, especially for sites that you use often or that collect much of your personal information. Keep the following questions in mind when reviewing privacy policies.

- » What information is collected?
- » How is that information collected? Does the site use cookies or other tracking technology?
- » Why is the information collected?
- » How will the information be used?
- » Who will have access to the information?
- » Can I opt out of providing this information?
- » How do I review, change, or update my information?
- » How is my information protected?
- » How long will the policy be honored?
- » Who can I contact with questions or concerns?

Destroy digital data.

If you are getting rid of a computer, tablet, cell phone, hard drive, or digital storage device, you must ensure that all personal information has been removed first. Deleting data and reformatting hardware is not enough to keep a thief from recovering your info. There are data removal products available if you need them. Many big box electronic retailers offer this as a service. CDs, DVDs, and other storage media should be physically destroyed once you are done with them.

ACTIONS TO TAKE IN THE PHYSICAL WORLD

Monitor your surroundings.

We can give away our identity information without even realizing it. Be cautious of those around you when providing personal information. Keep an eye out when entering a PIN or credit card number to be sure no one is looking over your shoulder to collect that information.

Guard your Social Security number.

Your Social Security number is your most valuable piece of identity information and should be carefully guarded. Situations will arise when someone asks for it, and you should be prepared. If someone asks for your SSN, check to see if it is absolutely necessary that you share the number. There may be another identifier that can be used instead.

If someone insists that they need your SSN, be sure you understand the following before sharing your private information.

- » Why is the information required?
- » How will the information be used?
- » Who will have access to the information?
- » What happens if you don't provide the information?
- » How will the data be stored and protected?

Invest in a safe.

Birth certificates, passports, Social Security cards, and any other personal identifying information should be stored in a secure place in your home—a safe is the best bet. Never carry your Social Security card with you.

Use your shredder.

Identity thieves are not above diving into your trash can to steal your valuable information. Don't provide them easy access to your receipts, credit card statements, credit card applications, health insurance information, and other personal information by throwing it away. Use a micro-cut shredder to shred any documents that you no longer need to keep if they contain your valuable data.

Be careful with checks.

Checkbooks are easy to steal and use, and it can be costly and time consuming to stop payment