



Identity Theft

HOW TO PROTECT YOURSELF: THE BASICS

The Federal Trade Commission estimates that as many as 9 million Americans have their identities stolen each year.

What can you do to protect your good name and ensure that no one steals your personal information—such as your Social Security number or credit card—and uses it to damage your credit and commit fraud or other crimes?

Keep your information private. It's the most basic rule of protecting yourself from identity theft.

DO practice these good habits:

Remember to take your ATM and debit transaction slips and receipts with you after every transaction.

Routinely reconcile your checking account statement with your receipts to ensure that all transactions are legitimate and that no one else has access to your account.

Keep your ATM/debit cards and Personal Identification Numbers (PINs) secure. Store your ATM/debit cards in a wallet that stays with you when you're out, and in a safe place at home. Never keep PINs in your wallet or bag.

Call your bank immediately if your cards have been lost or stolen. Call and put your card "on hold" if you're not sure.

At an ATM, use your body as a shield to protect your account information.

Pick a PIN that is difficult for someone to guess.

Keep your passwords, ATM and debit card code, Social Security number, account numbers and personal identification numbers private.

Shred all sensitive documents—such as bank statements, credit card statements, credit card offers and investment account information—prior to throwing them away.

Secure your mail. While it may be convenient to place your outgoing mail in an unsecured mailbox at your home, such documents are easy pickings for identity thieves who "happen" to be driving or walking by. So, whenever possible, visit your local post office or use a secured U.S. Postal Service mailbox to send your outgoing mail.

Keep the security settings and virus protection software programs on your computer up to date.

DON'T ever do this, even once:

Give your ATM/debit card or PIN to your friends.

Leave your card unattended on a table or desk.

Leave your wallet, debit card or financial information or bills in your car—in case it is towed, broken into or stolen.

Keep your wallet, backpack or purse by a window or door at home. It encourages break-ins. If you have roommates, don't keep your wallet or mail in communal spaces.

Use machines out of your bank's service provider network if you can help it. The machine you use should have options and logos that you recognize. The reason? Anyone can own an ATM. ATMs are not regulated or controlled by the financial industry.

Give out your account information, passwords, or Social Security number. While many businesses—such as doctors' offices and energy companies—will frequently ask for your Social Security number when setting up a new account, in most instances, there is no business reason for them to do so. Ask to be assigned an alternative account number.

Use an ATM on which others can see you enter your PIN. If someone won't allow you any privacy, walk away—that's a sign that trouble is brewing.

Use your birth date, phone numbers, initials or your name as your PIN.

Write your PIN on your card or carry it with you on your person. Don't store PINs in your phone.





Form good online habits. Don't leave a data trail that identity thieves can follow.

DO practice these good habits:

Banking Safety: Use your own computer to conduct financial transactions. Make bank transactions via phone if you must, but never use a public computer. Formally "log out" of the system and close your session completely after you have completed an online banking transaction. Simply minimizing your computer screen or clicking on the X in the upper right-hand of your Internet browser leaves accounts vulnerable. **IMPORTANT: Check bank balances daily and handle any problems IMMEDIATELY.**

Stay away from ridiculous offers. Con artists prey on the vulnerable and come up with all kinds of creative ways to get their hands on your personal information. Common tactics are to offer prizes, super-low insurance or loan rates, or heavy discounts on products. Remember, if something sounds too good to be true, it probably is.

Keep your e-mail address to yourself as much as possible. Request online newsletters or offers only if you really want them. Don't use your e-mail address as a user name. Check privacy policies before giving out your e-mail address; even if a company never sells your name, it may give it away.

Download files or open e-mails ONLY from organizations or people you know. Keep an eye out for suspicious activity occurring on your computer. Make regular backups. Unplug your backup drive so viruses can't get at it.

Get to know a company before purchasing online. If the company's website offers no phone number or physical address, beware. The Better Business Bureau (www.bbb.org) can help you determine if a business is legitimate.

Always erase and reformat old computers before you sell or get rid of them. It's best to reformat the hard drive, remove it from the computer, destroy it, then recycle it.

DON'T ever do this, even once:

Reply to phony e-mail messages. "Phishing," also known as "brand spoofing" or "carding," is a trick Internet scammers use to "fish" for consumers' financial information and password data using fake company e-mails and websites. The phony e-mail messages create the impression that there is an urgent need for the consumer to take immediate action to update personal information to avoid some threat or risk to the consumer's personal accounts.

If you receive an e-mail (or phone call or piece of mail) informing you that you have won a huge sum of money and asking you to supply personal information or cash to an organization or person you don't know, don't respond. This is a classic phishing technique. Thieves want your e-mail address or to verify information they already have on you, or they think you'll send money if they simply ask.

To protect yourself against "phishing":

- Be aware that the "From" e-mail address can be easily forged, so the sender listed may not be the real sender.
- Avoid providing or filling out forms via e-mail because the data are not secure.
- Realize that Internet scammers can create realistic forgeries of websites, so avoid clicking on links in an unsolicited e-mail message. Type the company URL in by hand and go directly to the company's website and fill out information there.
- Ensure that a website is secure by checking to see whether there is an "s" after the http in the address (for example: <https://somewebsite.com>) and that there is a "lock icon" at the bottom of the screen. Both are indicators that the site is secure.

Banking Boot Camp

This program was developed to teach basic banking skills and distribute relevant financial information to teens, young adults and their parents. To obtain other Banking Boot Camp brochures, check with your banker or visit our bank's website and click on the Banking Boot Camp icon.