Identity theft prevention guide

What is identity theft? It's when someone steals a piece of your personal information in order to impersonate you. Most times the theft is committed for financial reasons such as accessing bank and credit card accounts.

Popular ways thieves obtain your personal information

- Stealing a wallet or bag that contains personal identification and credit cards
- Stealing or diverting mail by falsifying a change of address form
- Going through the trash
- Stealing information from the workplace
- Data breaches
- Fraudulent emails and phone calls that trick the recipient into providing personal information

Download our identity theft prevention guide as a PDF

Helpful tips to fight identity theft and fraud

Elder fraud tips

- Stay connected with older loved ones through regular phone calls, visits or emails.
- Ensure they are set up for direct deposit of checks so others don't have to cash them.
- Help your older loved ones sign up for the National Do Not Call registry to prevent telemarketer calls and reduce the possibility of elder fraud.
- Advise your older loved ones to not sign any documents they don't understand.
- Regularly check on their financial situation. Discuss or review financial transactions, bills and emails with them.
- Let them know they should always check with you or another trusted person before giving any personal or financial information to anyone.
- Watch for unusual recent changes in the person's accounts, including atypical withdrawals, new person(s) added, or sudden use of a senior's ATM or credit card.
- Check on your older loved one's appearance/mental health. Do they suddenly appear confused, unkempt, and afraid.
- Review utility, rent, mortgage, medical, or other essential bills to see if they are unpaid despite adequate income.
- If there is a caregiver, make sure they do not allow others access to your older loved one without your consent.
- There are piled up sweepstakes mailings, magazine subscriptions, or "free gifts," which means they may be on "sucker lists."

Social Security Number tips

- Try to memorize your Social Security Number.
- Don't carry your Social Security card.
- Don't add your Social Security Number to checks.
- Be cautious when providing your Social Security Number; ask the requestor if another form of identification is acceptable.
- Changing your Social Security Number is not recommended. Your original SSN is attached to many documents, including credit reports, and a new number could look suspicious to creditors and employers. Plus, a new number would have an absence of any credit history and could make it very difficult to apply for jobs, bank accounts, or credit cards.

Shredding tips

- Always a good idea to shred documents that include any personal information that could be used for identity theft.
- Look for a shredder that cuts both lengthwise and crosswise.
- Many business like Staples and the UPS Store offer shredding services; check online for coupons.
- Check your local city/town calendar; sometimes free shredding is offered as a special event.

Computer and mobile device tips

- Be selective with the automatic log-in feature that can prefill user names and passwords.
- Always sign out or off when you are done.
- Utilize any face or fingertip recognition features.
- Use secure browsers that can encrypt (scramble) your information; look for a picture of a lock on the status bar.
- Clear your cache/browser history often.
- Backup all files on a regular basis.
- Update virus protection and operating system software; if possible, also add a firewall.
- Be cautious when using your computer/mobile device in public; be aware of "shoulder surfing."

Password and PIN tips

- Never use your Social Security or phone number or consecutive numbers like "1234."
- Do not use "password."
- Do not use familiar dates such as birthdays or anniversaries.
- Use a combination of upper/lowercase letters, numbers, and special characters.
- Try to memorize your password or PIN. If you need to write it down, do not place in a common spot like taped to a computer or under a keyboard and do not write your PIN down on the card it's associated with.
- Never share your password or PIN.

ATM tips

General

- Be aware of the surroundings/location of machine; have card and all paperwork ready. If you are in an isolated area, have your phone out and preset to "911."
- Consider cancelling your transaction and immediately pocketing your card if you notice anything suspicious.
- When making a withdrawal, do not count your cash at the machine.
- Always take your receipt. If you don't want it, dispose of it safely (shred) and do not use the trash receptacle at the ATM.

Walk-up ATM

- Choose a well-lit location; preferably not isolated from other buildings.
- Park close and do not leave keys in ignition or car running.
- If ATM is enclosed and locked (such as in a lobby), do not enter if someone else is using the machine. Do not let anyone in, if possible, while you are conducting your transaction.
- Be cautious of anyone who stands close and/or tries to engage you in conversation during your transaction.
- Stand squarely in front of the machine to keep your transaction as confidential as possible.

Drive-up ATM

- Keep car running, doors locked, and only open the driver's window.
- Make sure you can reach machine comfortably through the window; avoid opening car door and leaning out to access ATM.

Banking account tips

- Reconcile your monthly statements in a timely manner. Be familiar with statement cycles; if you don't receive your monthly bill, contact your bank. Your statement may have been diverted.
- Consider eDelivery over paper statements (Webster Bank offers eDelivery).
- Check statements carefully; make sure all deposits, charges, checks, and withdrawals are verified.
- When depositing a check, include "for deposit only" on the back with your signature. This way if you lose the check or it's stolen, it can't be cashed by anyone else.
- Immediately let the bank know if any checks have been stolen.
- Do not add your Social Security or driver's license number to checks.
- Use online banking and bill pay over paper checks.
- When you close a checking account, shred all leftover checks.

Credit card tips

- Report a lost or stolen card as soon as possible.
- Always sign the back of your card.
- Keep the number of credit cards you carry to a minimum.
- Cancel old cards.
- Immediately destroy (shred) any pre-approved credit applications; identity thieves can use them to open accounts in your name.
- If a child age 16 or younger receives a pre-approved credit application, it could be a red flag that identity theft has occurred; contact the credit reporting agencies to open an investigation.
- Immediately contact your issuer if you don't receive a physical card for an account you've been approved for.
- Take your credit card receipt with you from any transaction; destroy on your own.
- Stay on top of your cards' expiration dates; contact your issuer if you don't receive a new card prior to expiration.

U.S. Post Office tips

- Install a lockable mailbox to reduce theft.
- Consider a P.O. Box.
- Promptly remove incoming mail.
- Use the "hold mail" feature or have someone regularly pick up mail when away for an extended period of time.
- Fraudsters are targeting the blue U.S. mail boxes – they like the fact that a lot of mail sits in those boxes for hours. Check the label on the box for pick-up times and deposit mail as close to pick-up as possible.
- Give outgoing mail either directly to mail carrier or bring to post office.
- If you have a mailbox with a flag on it to indicate outgoing mail, try not to use it for bill payments; most statements have the kind of personal information fraudsters are looking for.

Webster Security Hotline

If you ever suspect your Webster account(s) contain fraudulent activity, please contact our Security Hotline immediately. Our specialists are available anytime.

800-966-0256

You're a victim of identity theft? We'll walk you through the next steps.

Your resources

More ways to prevent identity theft

- Ways to spot fraud
- Consumer alerts
- Online banking security