



# Protecting Yourself Against Identity Theft and Fraud

In today's digital world, you are more likely to have your identity stolen than your car stolen or your home burglarized. As a Veteran, you have more to protect than the average citizen. Along with your personal accounts, you also have to protect your Veteran ID, [VA.gov](https://www.va.gov) account login and any benefits you may receive, such as disability compensation and education benefits.

VA has a number of protections in place to keep your personally identifiable information (PII) safe, including using highly trained VA employees to handle sensitive material and employing a team of network security experts to monitor and safeguard systems and databases. VA is also working to reduce the collection of Social Security Numbers (SSNs) as the department's primary identifier.

While it is hard to prevent identity theft, it's important to remember several guidelines to protect yourself and your VA benefits from identity theft and fraud.

## Learn to identify and avoid scams

**PHISHING EMAILS** These scam emails have gotten very sophisticated, even using bank and other company logos and official-sounding language to trick the targeted recipient into providing them with personal information. If you receive this type of email, don't click on it – call your bank, credit card company or other organization directly and verify that they sent the message. In all cases, if you don't recognize the sender, it's best to delete the email without even opening it.

**EMAIL SPECIAL OFFERS** Email "special offers" and "amazing deals" can sometimes be what's known as "click bait," meaning the message is intended to get you to click on it. This can introduce a virus on your computer or give outside users access to your computer files without your knowledge.

**TELEPHONE SPECIAL OFFERS** Be aware of telephone scams. There is an increase in calls where identity thieves will say anything to cheat people out of money and/or information. Signs of a scam include when the person on the other line says: "You've been specially selected for an offer" or "You'll get a free bonus if you buy our product" or "You've won one of five valuable prizes."

**PHONE CALLS ASKING FOR PERSONAL INFORMATION** If you are asked for personal information on a website or over the phone, be cautious with what you provide. Remember, agencies such as the IRS, banks and credit accounts will not call you and ask for your personal information such as your social security number, date of birth or passwords.

**SILENT CALLS** Be aware of initial "silent calls" – that is, when you pick up and hear silence on the other end of the line. They are trying to see if you are a human answering and will call back later.

**TELEPHONE VOICE RECORDING** If an unknown person calls and asks you to respond to a series of questions that get you to say "yes" or your full name, be aware. They may be recording your voice to authorize fake charges on one of your accounts. This may include the "Can you hear me?" question that uses your response of "yes" or asks you to state your full name.



# Protecting Yourself Against Identity Theft and Fraud

## Pay attention to scams targeting older Americans

Financial scams targeting seniors have grown over the years, but often are underreported. These scams can cause serious financial and other devastating results, so it's important to be extra cautious when sharing information. Scams include:

- A thief acting as a family member or "on behalf of a family member" asks you to wire money to help a relative, usually saying they are injured or in legal trouble.
- A thief, often posing as a lawyer or banker, tells a person that he or she has found a large sum of money and is willing to split it if the person makes a "good faith" payment by withdrawing funds from his or her bank account.

## What to do if you suspect your information is compromised

If you suspect you have been affected by identity theft, contact the Department of Veterans Affairs (VA) Identity Safety Service through its toll-free Identity Theft helpline at 1-855-578-5492 or by email at [vaidtheft@va.gov](mailto:vaidtheft@va.gov).

## Safeguard your information

In addition to fraud detection services, there are steps that you can take to protect your information, including your VA accounts.

- Passwords:
  - » Set a strong password when you create an account by using uppercase letters, lowercase letters, numbers and symbols.
  - » Regularly change your password and do not use the same password for multiple accounts.
  - » If you create a reminder for your password, use a hint rather than the actual password.
- Do not save the login and password to your web browser or cell phone.
- Review and respond to security alerts notifying you when changes are made to an account.
- Shred sensitive VA documents such as old benefits documents, bills, etc.
- Regularly check to ensure the names and information of your beneficiaries are correct.
- Sign out of accounts when you are finished with the session.
- Share less, including on social media, when the information you post could give identity thieves clues to your birthplace, date of birth and other data that could be used to steal your identity.
- Be aware of public Wi-Fi. With the right tools, identity thieves can monitor what you do, even if it's password protected. Not only can criminals see which websites you visit, they can also capture your credentials as you log in to bank, credit card and VA accounts.

## Protect your finances

Pay attention to key financial documents to ensure you are receiving everything on time from the proper source, including:

- Make sure there are no odd charges on your bills or changes to your accounts.
- Be mindful and careful if you receive credit cards in the mail that you did not apply for.
- Check your credit score at least annually – there are a number of websites you can use for free.
- Ensure you receive your tax return on time and call the IRS directly if you do not.

Also, be sure to call the necessary organization or company direct, not necessarily a number in a suspicious email or letter (e.g., call the IRS, not a credit agency claiming they will work on your behalf).