# 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 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.