**Safeguarding your identity: Keeping your VA benefits safe from identity theft and fraud**

**Image:** Included in toolkit.

**Suggested Alt Text:** Open laptop keyboard with two hands, one reaching into the other’s wallet to steal financial assets.

VA is committed to provide you and your loved ones information on how to safeguard your identity, keeping your VA benefits safe.

In the contemporary digital era, identity theft is a more likely occurrence than home burglary or car theft. As a Veteran, you hold more [**sensitive information**](https://www.research.va.gov/for_veterans/safeguarding_vets.cfm) than an average citizen, necessitating careful protection of your personal accounts, Veteran ID, VA.gov account login, and any benefits you may receive, such as [**disability compensation**](https://www.va.gov/disability/) and [**education benefits**](https://www.va.gov/education/). Veterans are highly susceptible to fraudulent activities, [**online scams**](https://consumer.ftc.gov/consumer-alerts/2023/11/veterans-and-scams) and deceitful individuals.

[**Identity theft**](https://benefits.va.gov/BENEFITS/factsheets/financial-literacy/ID-theft-fraud.pdf) occurs when hackers obtain sensitive Personally Identifiable Information (PII) like credit card details to sell on the dark web or use for their own gain. Identity theft is a difficult crime to prevent, but there are several measures you can take to safeguard yourself and your VA benefits. It’s essential to stay vigilant and familiarize yourself with the following frequently occurring common online scams:

* Direct Deposit/Payment redirection: A bad actor obtains PII to unlawfully access and gain control of Veterans’ and beneficiaries’ accounts.
* [**Phishing**](https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams): A fraudulent practice where an imposter creates a fake online persona to deceive Veterans and their beneficiaries into providing PII.
* Email: A type of scam in which a fraudster sends a fake email, often promoting a contest or reward, to trick a user into clicking on a malware link or obtain sensitive personal information.
* Phone: A scammer may pose as someone you trust and try to obtain your money or personal information to commit identity theft.
* [**Spoofing**](https://www.fcc.gov/spoofing): A caller disguises the information shown on caller ID, giving them the ability to impersonate a specific person from a certain location.
* Wired: A type of fraud that involves the use of some form of telecommunications or the internet.
* Forgery: The act of forging or producing a copy of a document, signature, banknote or work of art.
* Malware: One of the top cyber schemes used by bad actors to infect computers. They may even hold your computer “hostage” with malware until you agree to pay a ransom; this type of malware is also known as “ransomware.”

## How to protect yourself against identity theft

VA is committed to bringing awareness to Veterans and their beneficiaries about trending fraud scams targeting their personal information and benefits to avoid becoming victims of fraudulent acts.

Here are some identity theft prevention tips Veterans can follow to protect themselves:

* Screen emails carefully, and only open emails from senders you know and trust. Delete and block emails from unknown or suspicious senders.
* Be cautious of popups and links on websites, emails and texts that can be used to infect your device with harmful malware.
* Limit PII when you post online, such as your address, date of birth, workplace, or kinship details.
* Delete old social media accounts and limit online presence and available biographical information.
* Maximize privacy settings on all active social media accounts to protect information from unknown users.
* Do not accept friend or connection requests from individuals with only an online presence. Only add friends or connections you know and trust in real life, not those who you have only met online.
* Download strong antivirus software to protect yourself from malware attacks.
* Be aware of signs of a malware infection. If your computer runs unusually slowly or frequently crashes without explanation, it may be an indication it is infected with malware.
* Never send bank information or payment to “online friends” or others. Scammers may threaten to destroy your files or data if you do not send payment or banking information. Be alert! Identity theft is not always committed by strangers.
* Frequently change and maintain strong passwords and never use PII in the password.
* Be cautious of telephone numbers on your caller ID. Scammers can change the telephone number (spoofing) to make a call appear to come from a different person or place.
* Only shop on sites that are validated—go directly where you want to shop. Check the URL for spelling mistakes or errors.
* Use a credit card instead of a debit card. Credit cards typically provide added protection against fraudulent charges.
* Do not sign forms that are not VA generated or are a third-party authorization for someone to provide “behind-the-scenes” claims assistance.

## How to report identity theft and fraud

VA encourages Veterans and their beneficiaries to know the warning signs of the various types of fraud and the best practices to avoid falling victim to a scam.

If a Veteran believes their identity has been stolen, they should contact the [**Federal Trade Commission**](https://reportfraud.ftc.gov/#/) (FTC). Identity theft can be reported to the FTC at [**IdentityTheft@va.gov**](mailto:IdentityTheft@va.gov). If a Veteran has concerns about their VA services being impacted by identity theft, they can call the toll-free VA Identity Theft Helpline at 1-855-578-5492.

In addition, VA has more than 400 VA Privacy Officers (POs) nationwide. Their responsibilities include all matters related to protecting Veteran information, such as receiving and processing privacy complaints, monitoring VA facility compliance with privacy requirements, and promoting privacy training and awareness. Watch this [**VA Privacy Officers video**](https://www.youtube.com/watch?v=Iu4VCdu3-GY&t=124s) to learn more about Privacy Officers and how to identify and contact the one in your area.

VA also has fraud prevention resources for Veterans. If a Veteran believes they’ve experienced health care-related fraud, they can contact the Veterans Health Administration, Office of Integrity, and Compliance Helpline at 1-866-842-4357 (VHAHELP). If a Veteran believes they’ve experienced VA Benefits fraud, they can contact the VA Benefits Hotline at 1-800-827-1000. Veterans can also learn more about fraud prevention by visiting the [**Protecting Veterans from Fraud**](https://www.va.gov/initiatives/protecting-veterans-from-fraud/) webpage.

## Additional Resources

* Request a free copy of your credit report by visiting AnnualCreditReport.com or by calling 877-322-8228.
* [**VA Privacy Homepage**](https://department.va.gov/privacy/)