**Empowering Veterans Against Smishing Threats**

**Image:** Included in toolkit.

**Alt Text:** A credit card and mobile device in which a person is entering their credit card number onscreen and surrounding content that says: “Beware of Smishing.”

You may be familiar with phishing as a common cyber scam, but have you heard of smishing? Smishing, which is a term that combines Short Message Service (SMS) and phishing, is one of the biggest cyber scams you need to watch out for because scammers try to steal your personal and banking information through unsolicited text messages on your mobile devices. Veterans may be targeted because of their service to this nation, as scammers impersonate government officials and agencies.

The [Department of Veterans Affairs (VA) Privacy Service](https://department.va.gov/privacy/) encourages Veterans to use the following tactics to spot, prevent, and report a smishing scam.

How to Spot a Smishing Scam

You should be cautious of unsolicited messages, especially if they come from unknown numbers or sources. Sometimes these scammers will use your local area code to appear familiar. Scammers may impersonate local officials, family, or friends. Look out for urgent or threatening language in messages, as scammers often try to create panic and pressure you into immediate action. VA, and other legitimate organizations, will never request sensitive information like passwords or financial details through text messages, so be skeptical of such requests. Watch for misspellings and grammatical errors, as professional organizations usually send well-written communications. If you receive unexpected prize or gift notifications instructing you to provide personal information, exercise caution, as these are also likely scams.

How to Prevent a Smishing Scam

Veterans, you can take steps to protect yourselves from potential scams and fraudulent activities.

* Confirm the legitimacy of message senders by cross-checking information using official channels like the official website or documents; avoid replying directly to texts.
* Be cautious of clicking on links in messages, as smishing often involves deceptive links that may lead to malware.
* Keep your smartphones secure by installing and regularly updating security software to detect and block smishing attempts.
* Ensure your phone settings are on automatic updates for the latest patches and fixes.
* Strengthen your account security by enabling two-factor authentication whenever possible, adding an extra layer of protection.
* Your vigilance is key to keeping your personal information safe.

How to Report a Smishing Scam

Mobile carriers have mechanisms in place to handle reports of phishing and smishing attempts. You should forward any suspicious messages to your mobile carrier’s designated reporting number, which you can find on their official website or by reaching out to customer support. If the smishing scam falsely claims to be from VA or another government agency, do not interact with the scam and report it immediately. All mobile carriers have the option to report suspicious texts by forwarding them to 7726 (SPAM).

If the smishing scam suggests criminal activity like identity theft or fraud, consider reaching out to your local law enforcement agency, providing them with detailed information, including screenshots and any other relevant data. If you’re in the United States, filing a complaint with the FBI through the [Internet Crime Complaint Center (IC3)](https://www.ic3.gov/) is an option, ensuring you include comprehensive details about the smishing incident. The [Federal Trade Commission (FTC)](https://consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages) provides helpful information on identifying scam text messages as well.

**For additional information about smishing**

* [VEText](https://www.va.gov/resources/vetext-for-va-health-care-reminders-and-updates/)
* [VANotify](https://news.va.gov/85891/veterans-get-updates-through-new-digital-notification-feature/)
* [Smish, Smish! Don’t get phished.](https://digital.va.gov/cyber-spot/smish-smish-dont-get-phished/)
* [How to Recognize and Report Spam Text Messages](https://consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages)
* [Hook, line, and sinker: How to up your phishing game](https://news.va.gov/100177/hook-line-and-sinker-how-to-up-your-phishing-game/)
* [Phishing – without rods](https://news.va.gov/125048/phishing-without-rods/)
* [Online scammers are looking to steal your information](https://news.va.gov/110281/online-scammers-steal-information/)