How Veterans Can Identify and Report Scams

Veterans, Service Members, and their families are continuously targeted by scammers. In 2021 alone, Veterans had an estimated $177 million stolen from them through scams and benefits fraud, according to the Federal Trade Commission (FTC). But why? Because Veterans and their families have access to special government resources and because of the monetary value associated with their benefits.

Top Scams Veterans Should Look Out for in 2023

Payment Redirect – Payment redirection occurs when a fraudster obtains Veterans' Personal Identifiable Information (PII) and uses that information to unlawfully access and gain control of their accounts (email, banking, etc.). Once compromised, the fraudster redirects the victim's Department of Veterans Affairs (VA) benefits payments to new accounts or to prepaid debit cards, both of which they control. Veterans' PII is vulnerable to phishing attempts and an array of email scams.

Pension Poaching – Pension Poachers profit by falsely helping Veteran claimants artificially qualify for VA pension benefits. Scammers are using Pension Poaching scams to target Veterans age 65 or older, their families, their caregivers, and their survivors. In fact, Pension Poaching is becoming a preferred method to defraud older Veterans. The scheme often involves financial maneuvers like advising Veterans to hide their assets in trusts or annuity products the Pension Poachers present to them.

Romance and Friendship Scams – Scammers typically use fake online profiles to pose as potential romantic or friendly connections. After gaining a victim's trust, they may request PII, monetary payment, or other compromising information. Also, Veterans may be easily identifiable on social media and dating platforms through photos and job titles.

Tips to Avoid Scams

- If you receive a call asking for money or personal information from someone you don't recognize, hang up immediately. Don't click on suspicious or random links or attachments in emails or texts.
- Before you make a payment or provide your personal information to an organization, stop and check it out to make sure the organization is legitimate. Be cautious of companies who claim to be contacting you on behalf of VA or to have a special relationship with VA. Contact VA at 1-800-827-1000 if you are unsure about the authenticity of any message received.
- Do not provide your social security number, medical records, or other personally identifiable information to anyone offering claims assistance before confirming their credentials using the Office of General Counsel Accreditation tool.
- If you are a victim or spot a scam, you should first file a complaint with your State Attorney General's Office.
- Sign up for the FTC's free scam alerts and get the latest tips and advice about scams. You can also report scams to the FTC.

For More Information Contact VA Privacy Service
Privacy Hotline: 202-273-5070 | Email VA Privacy Service

PRIVACY MATTERS

VA

U.S. Department of Veterans Affairs
Office of Information and Technology