Protecting Your Benefits Data From Fraudsters

(From www.news.va.gov, January 30, 2025)

VA is sharing guidance on how Veterans and their beneficiaries can protect their data, especially Personally Identifiable Information (PII). It's crucial to recognize that fraudsters often target Veterans through various scams to gain access to personal data, resulting in identity theft.

Understanding Identity Theft

Identity theft occurs when someone steals personal information—such as Social Security Numbers (SSNs), bank account details, medical records and account numbers, or credit card information to commit fraud. This can lead to unauthorized purchases, drained bank accounts, and even fraudulent claims for benefits in your name. Identity theft can have severe consequences, impacting not only financial stability but also access to VA benefits.

Types of scams targeting personal data

- Generative Artificial Intelligence (AI) Scams: Fraudsters can use AI to create fake identities or impersonate real people, businesses or charities to access secure information and file claims for benefits. They may develop convincing voice or video messages for social engineering attacks to trick people into giving money to fraudsters.
- QR Code Scams: With the rise of contactless payment and information sharing, fraudsters use QR codes as a quick scam. These codes may appear in emails, social media, flyers, websites or public places like parking meters, and direct users to phishing sites intended to steal personal data or request payment under false pretenses.
- Phishing: Phishing, also known as clickbait scams, comes in many forms, such as emails, phone calls, text messages, fake websites and advertisements, and social media videos. Clicking on links can lead Veterans to phishing sites designed to steal personal information, infect devices with malware, or request payment for nonexistent services. Veterans should be constantly vigilant, alert and skeptical to stay safe online. Veterans who share military service or employment information online put themselves at risk of phishing scams.
- Romance & Friendship Scams: Fraudsters create fake profiles on dating apps and social media platforms to befriend individuals. Once a connection is established, they gather personal details to later pressure potential victims with blackmail to gain PII, account numbers and passwords, or financial payment.

How you can secure your data

- 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 which can be used to infect your device with harmful malware.
- Limit the PII you post online, such as your address, date of birth, workplace or kinship details. The less information scammers can find about you online the safer you will be.

- Maximize privacy settings on all active social media accounts to protect information from unknown users and prevent unauthorized access to sensitive information.
- 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 you have only met online.
- Download strong antivirus software to protect yourself from malware attacks. If your computer runs unusually slowly or frequently crashes without explanation, it may indicate it is infected with malware.
- Never send bank information or payment to "online only" friends or unverified entities. Fraudsters create an emergency, threatening to destroy your files or data, or lock your account if you do not send payment. If you experience ransomware, do not respond to any threat, and report the incident immediately.
- Only scan QR codes from trusted sources. Always verify the code's authenticity by visiting the organization's website or contacting them directly.
- Contact your VA Privacy Officer. Veterans can contact their local Privacy Officerto file a complaint regarding an alleged VA privacy violation or for general privacy questions and concerns. The VA Privacy website contains VA privacy guidance and resources, including information on how to:
    - File a Privacy Complaint.
    - Access and download information sheets about protecting Veteran's identity and privacy.

Taking proactive measures to secure personal data is one of the most effective ways to prevent identity theft and other types of fraud. During Data Privacy Week, and every day, VA is here to help ensure Veterans keep their personal information and benefits safe from harm. For more information on fraud impacting Veterans' benefits, visit Protecting Veterans From Fraud | Veterans Affairs. Veterans who suspect they have experienced fraud can find resources to file a report with the appropriate agency by visiting www.vsafe.gov or calling 833-38V-SAFE.