**Protect Your Benefits: Combatting Payment Redirection Fraud**

Take control of your benefits security

**Image:** Included in toolkit.

**Alt Text:** A Veteran interacting with a mobile device.

With the largest expansion of benefits currently underway with the Sergeant First Class Heath Robinson Honoring our Promise to Address Comprehensive Toxics Act (PACT Act), it’s important to stay on high alert for criminals who want to take advantage of you.

Online scams can take a variety of forms, with scammers constantly devising new ways to trick people into giving them sensitive information to steal money and identities. Payment Redirection Fraud is a key example of this crime, which involves criminals impersonating others and using or diverting payments to bank accounts under their own control.

**Payment Redirection Fraud Puts Your Veteran Benefits at Risk**

Payment redirection occurs when a bad actor obtains Veterans’ Personal Identifiable Information (PII) and uses the information to unlawfully access and gain control of your personal information (email or bank accounts, va.gov, etc.). Once your information is compromised, the scammer redirects the victim’s VA benefits payments to accounts or prepaid debit cards the scammer controls. Veterans’ personal information is vulnerable to phishing attempts and an array of email scams.

Bad actors are leveraging publicly available information from internet sources, social media, dark web, etc., to gather PII:

* With enough demographic information, they can call the National Contact Center and change Veterans’ bank accounts to redirect their payments.
* With stolen passwords and credentials, they can access Veterans’ information through VA.gov.

When a fraudulent payment redirect case is reported or suspected, Veteran Benefits Administration’s (VBA) Benefits Delivery Protection and Remediation (BDP&R) team investigates the incident and confirms the fraudulent activity by:

* Determining the necessary actions to protect the Veteran’s benefits.
* Reporting those responsible for the alleged fraud.
* Immediately reinstating the Veteran’s benefits, making the Veteran whole again.
* Diligently working to serve America’s Veterans and remaining committed to protecting all Veterans and beneficiaries, specifically the most vulnerable, from fraud and abuse.

**Protect Yourself**

You are the front line against threats to your personal information. Follow these tips to take control of your online safety.

What Not to Do:

* Do not share your personal information (date of birth, military entrance or discharge information, branch of service, banking, or credit card information, etc.), or other VA sign in credentials (e.g., VA.gov), with anyone
* Do not sign a blank form to be filled out later without seeing the contents
* Do not share your VA National Contact Center personal identification number (PIN) with anyone – including family, friends, or any entity who makes contact via mobile communication
* Do not give out PII via text – VA will never text to confirm or request PII for benefits or federal payments
* Do not deposit VA benefits directly into a family member or caregiver’s bank account unless the person is court appointed or a VA-accredited fiduciary

Take Action:

* Be alert! Identity theft is not always committed by strangers
* Frequently change and maintain strong passwords and never use PII in the password
* Verify your identity - obtain a VA Security PIN to secure direct deposit accounts from theft and protect PII
* Be cautious of companies claiming to contact you on behalf of the Department of Veterans Affairs (VA) or presenting itself as having an affiliation with VA
* Contact VA immediately at 1-800-827-1000 if you find a payment discrepancy or suspicious activity within your direct deposit account

Veterans and your dependents are the targets of many types of fraud, including mail, telephone, and online fraud. VA is actively working to prevent these incidents, but you are the best line of defense against this criminal activity. **Bookmark** and visit [Cybersecurity Spot](https://digital.va.gov/cyber/) regularly for tips to enhance your online security.

If you suspect fraudulent activity, visit the [Department of Justice fraud webpage](https://www.justice.gov/criminal-fraud/report-fraud) and report it to the proper authority.