

VAU.S. Department
of Veterans Affairs

CYBERSECURITY AWARENESS MONTH

Protecting Yourself and Your Benefits from Cyber Scams



VBA IS COMMITTED TO DETERRING SCAMMERS

Have you or a loved one been the victim of an online scam? Are you wondering how you can protect your data and safeguard your benefits?

We are here to help. The Department of Veterans Affairs (VA) is proud to honor Veterans by actively working to identify growing fraud threats and trends. Veterans need to be aware of the criminals' tactics and stay abreast of methods to protect their data and themselves.

A CLASSIC EXAMPLE OF ONLINE SCAMS



An imposter creates a fake profile on a social media application



They connect with the victim and attempt to establish a fast relationship through frequent communication



Once trust is gained, the imposter will ask for money, Personally Identifiable Information (PII), or other compromising information

PREVENTATIVE MEASURES

Cyber scams targeting Veterans are becoming increasingly popular on social media platforms and other websites. Veterans must be cognizant of the risks and vulnerabilities that may leave them susceptible to attacks. The following [tips](#) can help Veterans practice safe online behavior and prevent fraud.

- ✓ **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 the PII 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 slow 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. If you are a victim of ransomware, do not respond to any threat and [report the incident](#) immediately.

Resources:

- If you miss a VA benefits payment, identify a discrepancy in payments, or find suspicious activity with your direct deposit account, contact the VA immediately at 1-800-827-1000.
- File a complaint with the Federal Trade Commission (FTC) by visiting [reportfraud.ftc.gov](https://www.ftc.gov/identity-theft).