

PROTECTING YOURSELF FROM ROMANCE AND FRIENDSHIP SCAMS

Fraud Prevention Tips for Veterans

VBA IS COMMITTED TO DETERRING FRAUDSTERS

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

We are here to help. Veterans Benefits Administration (VBA) is proud to honor Veterans by actively working to identify growing fraud threats and trends. Veterans need to be aware of the fraudster's tactics and stay abreast of methods to protect their data and themselves.

PREVENTATIVE MEASURES

Romance and friendship scams are becoming increasingly popular on online platforms. Veterans must be cognizant of the risks and vulnerabilities that may leave them susceptible to attack. **The following tips and behaviors can help Veterans practice safe online behavior and prevent fraud.**

- ✓ **Trust your instincts.** Fraudsters may be overly flattering to befriend individuals or attempt to quickly establish a relationship or friendship. If your online interactions with a user seem too good to be true or feel disingenuous, cease communication immediately.
- ✓ **Request a phone or video chat early.** With online friends or love interests, ask to schedule a call after connecting to confirm they match their profile.
- ✓ **Check for evidence of suspicious activity.** Check for evidence of suspicious activity and perform a Google search with the name of the organization or person plus the words "scam", "review" and "complaint".
- ✓ **Conduct a [reverse-image search](#).** This process can help confirm if profile photos are legitimate.
- ✓ **Never send bank information or payment to "online friends" or others.** Fraudsters may request monetary assistance for financial woes or threaten to release or destroy your private photos or conversations if you fail to comply and send payment or banking information. If you are being blackmailed, do not respond, and [report the incident](#) immediately.
- ✓ **Never share your VA login credentials and regularly change your passwords.** Keep all personal VA information (e.g., VA.GOV, eBenefits logins) private, never share personally identifiable information (PII) with "online friends" and do not use PII in your passwords.

\$956 million

The total losses from scams involving fake online identities reported to the Internet Crime Compliant Center (IC3) in 2021.



HOW ROMANCE AND FRIENDSHIP SCAMS HAPPEN



A fraudster creates a fake profile on a social media or dating app



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



Once trust is gained, the fraudster will ask for money, PII, or other compromising information

REPORTING FRAUD

- 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 by visiting reportfraud.ftc.gov.
- Visit the [Cybercrime Support Network](#) for additional [resources](#) to help Veterans.