

Protect your VA benefits

Pause. Verify. Protect. Keep this reminder nearby when a benefits-related request arrives.

Before you respond

- ☐ Pause before opening an unexpected link, attachment or QR code.
- ☐ Verify the request using a known website or phone number you found independently.
- ☐ Check the full web address. A logo, caller ID or HTTPS alone does not prove identity.

Protect your sign-in and information

- ☐ Use strong, unique passwords and multifactor authentication.
- ☐ Keep passwords and one-time codes private. Use codes only in a sign-in you started.
- ☐ Keep devices updated. Review direct-deposit and contact-change notices.
- ☐ Keep sensitive records out of public comments and initial consultation messages.

If something looks wrong

- ☐ Stop contact and save the messages. If bank details were exposed, contact your bank.
- ☐ For an exposed account, use the genuine service and follow its recovery instructions.

Official help and reporting

Veteran fraud resources: vsaferesources.va.gov | 833-388-7233

Identity-theft recovery: IdentityTheft.gov

Report fraud: ReportFraud.ftc.gov

Missing VA benefits payment or suspicious direct-deposit change? Contact VA at 800-827-1000. Reporting does not guarantee recovery of money.

Sources reviewed October 19, 2026

[VA identity and benefits protection \(click to open\)](#)

[VA phishing guidance \(click to open\)](#)

[FTC phishing guidance \(click to open\)](#)