Watchdog Alert Handbook:

VETERANS EDITION

Common Scams Targeting Veterans & Military Families — and How to Stay Safe

aarp.org/VetsFraudCenter

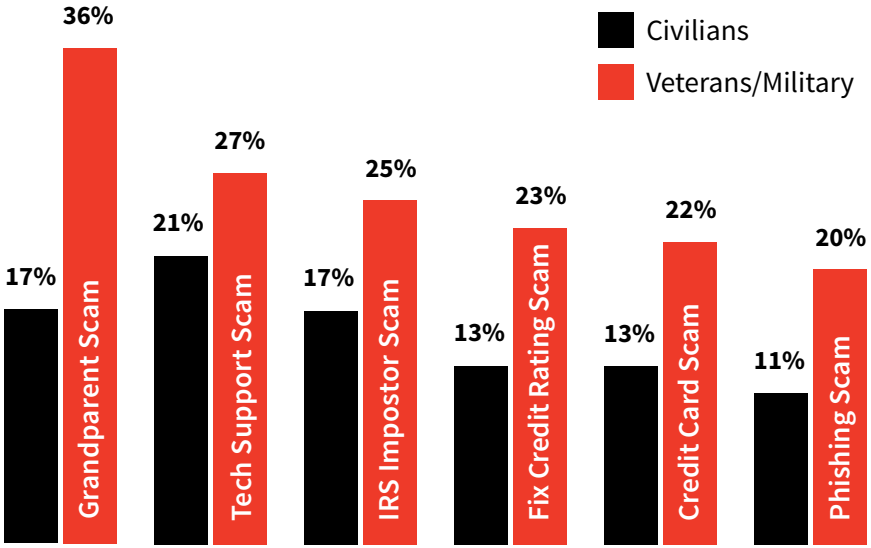
From the AARP Fraud Watch Network

1 in 3 current or former military personnel have been targeted by disability-benefit scams.

Introduction

Despite their service to our country, United States military veterans, active-duty service members and their families are targeted by con artists significantly more than civilians, and are 40% more likely to lose money than their civilian counterparts when hit by similar scams and schemes, according to the 2021 AARP survey *Scambush: Military Veterans Battle Surprise Attacks From Scams and Fraud*.[1]

MILITARY VETERANS ARE MORE LIKELY THAN CIVILIANS TO LOSE MONEY ON SCAM OFFERS[2]



1 aarp.org/home-family/voices/veterans/info-2021/scams-report.html

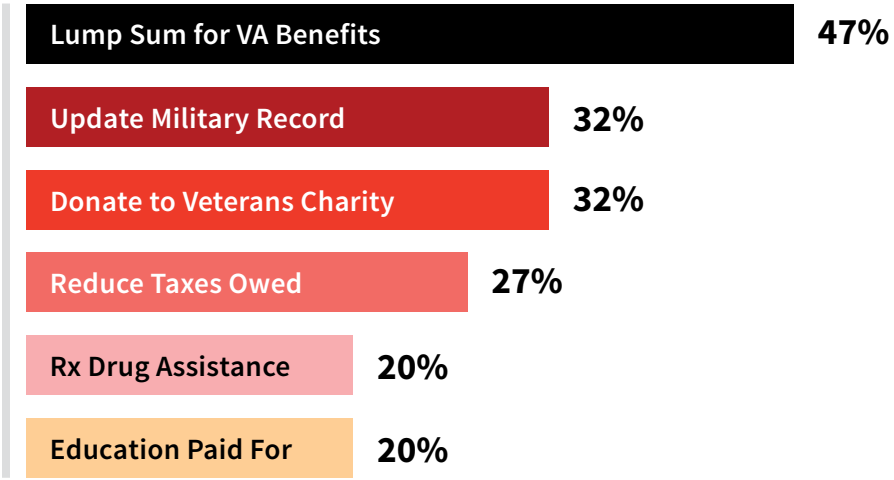
2 According to the 2021 AARP survey *Scambush: Military Veterans Battle Surprise Attacks From Scams and Fraud*

These losses have taken a heavy toll on the military community. Veterans, active-duty military and reservists have reported nearly 500,000 instances of fraud and identity theft over the past five years, according to 2021 Federal Trade Commission (FTC) data. **Veterans and military losses more than doubled in one year to $267 million in 2021 from $102 million in 2020. Their median fraud loss per incident was $600 in 2021 — $100 higher per scam than all consumers.**

Why target veterans and military families? Scammers follow the money — active-duty service members get a steady paycheck from Uncle Sam, while veterans can receive regular benefit payments.

This handbook has intel on the latest scams targeting the military community, tips to spot scammers, and resources to use to protect veterans and military families. **Learn more at aarp.org/VetsFraudCenter.**

PERCENT OF MILITARY OR VETERANS WHO LOST MONEY TO SERVICE SCAMS [3]



3 According to the 2021 AARP survey *Scambush: Military Veterans Battle Surprise Attacks From Scams and Fraud*

Common Scams Targeting Veterans

Criminals who target veterans and service members often use military jargon and specific government guidelines to craft an effective pitch to steal money. See below for common scams directed at veterans, current military and their families.

BENEFITS SCAMS

Pension Poaching

Pension poaching is a financial scam targeting veterans, perpetrated by shady advisers who promise to help former service members grow their retirement funds or obtain extra benefits from the VA. This type of scam is often directed toward people who do not actually qualify for VA pensions. Victims could be required to repay these benefits to the government.

Tip: Be cautious if someone offers to move around your assets to qualify for a VA pension. Check the **VA's searchable database**[1] or call **855-578-5492** to see whether an attorney or financial professional is VA-accredited and has the required training to complete and submit claims.

Benefits Buyout

Scammers offer a payment in exchange for military disability or pension payments. A lump-sum payment never materializes, or the offer is a fraction of the value of the benefits.

Tip: Apply directly to the VA if you believe you're eligible for the agency's Aid and Attendance benefits. There's no cost for forms and no fees to apply.

1 va.gov/ogc/apps/accreditation

Records Scheme

A scammer attempts to charge for access to or to update your DD Form 214. These are free by law.

Tip: The VA will never ask for personal data by phone, text or email. If an unsolicited call purporting to be from the VA requests personal information like your Social Security number, hang up and call the agency directly at **800-MyVA 411** (**800-698-2411**).

HEALTH CARE SCAMS

Medical Equipment

Scammers call to offer "free" or discounted braces, wheelchairs or other devices. The goods may or may not arrive, but scammers get your info to steal your identity or rip off the VA with excess charges.

Tip: Don't order medical equipment over the phone unless advised to do so by your physician and hang up on any unsolicited calls offering you a device that will be billed to Medicare. Call Medicare (**800-633-4227**) or your insurance company if you see claims for supplies you don't recognize.

GI BILL EDUCATION MARKETING SCAM

Veterans seeking to take advantage of the GI Bill for college courses may be targets of deceptive marketing tactics that provide false information and encourage them to attend expensive for-profit educational institutions.

Tip: The VA offers a comparison tool to help you locate a school and determine your benefits. Visit VA.gov/education.

Rx Drug Assistance

Scammers offer deep discounts on prescriptions. Ultimately, no medications come, but the criminals have your personal information to use your identity.

Tip: When purchasing online, look for sites with a ".pharmacy" domain, which reflects proper review and accreditation. Also know your meds. If you notice anything different or unusual in the appearance, packaging, smell, taste or texture of drugs you bought online, consult your pharmacist.

IMPOSTOR SCAMS

VA Phishing

Scammers contact veterans claiming they work for the VA, asking for personal information to update their records.

Tip: The VA rarely calls individuals for record updates. If you're unsure, hang up and call the VA at **800-MyVA 411** (**800-698-2411**).

Tricare Scams

Crooks pretending to be from Tricare, the health care program for military personnel, retirees and their families, contact beneficiaries offering them services. It's another ploy to steal personal or financial data.

Tip: Don't hesitate to say "no" if an adviser pressures you to act fast, and call Tricare's toll-free Fraud Hotline at 877-968-7455.

Employment Scams

Con artists post bogus job offers to recruit veterans on various online job boards. The scammer may use or sell personal information provided in the job application.

Tip: It's a scam if you must pay to get the job, you need to supply credit card or banking information, or the ad is for "previously undisclosed" federal government jobs.

Identity Theft

Beyond stealing your money, some criminals specialize in stealing identities. Most of us have been notified that our sensitive information has been exposed to a data breach, a common means of identity theft. Identity theft can also involve stealing incoming or outgoing mail, rifling through garbage cans and recycling bins, or impersonating someone you would trust.

Identity theft becomes identity fraud when someone uses your identity for financial gain, such as opening new accounts in your name, filing for government benefits in your name, filing false tax returns — or even taking over your accounts. This fraud can be committed by the criminal who stole your data or by the criminal who bought your data.

Tip: Identity theft can come from many sources. Here are steps you can take to block and spot attempts to steal your identity:

- To protect yourself now against future identity fraud, **add a fraud alert to your credit reports**, which requires a lender to contact you before opening a new account in your name.
- **Freeze your credit.** A freeze blocks lenders from opening new accounts in your name. You can freeze and unfreeze your reports at no cost, but you need to do it with each of the three bureaus.
- **Use strong and unique passwords for all online accounts.** A password manager is a great tool to set and safely store passwords; options include Bitwarden, LastPass, Dashlane, or others.
- **Set up electronic access to all financial accounts.** You can set alerts to text you with each transaction, so you can track activity, as well as other alerts. If app access is available, it has more encryption. Bonus: You don't have to wait a month or a quarter to review your account activity.

MORE SERVICE-SPECIFIC SCAMS

Fake Military Charities

Scam artists use fake veterans charities or causes, allegedly to collect money for veterans and military families experiencing hardship. Not only do the scammers pocket the money, but they also divert donations away from legitimate charities that actually serve veterans.

Tip: Look up an organization before donating. Check out **CharityWatch.org** or **CharityNavigator.org**.

Other 'Special' Military Deals

Legitimate discounts honoring the service of military and veterans abound. Scammers, sometimes posing as soon-to-be-deployed service members, offer special deals for veterans on cars, electronics and other products. They often ask for payment by wire. Once you've paid, the seller disappears, and the goods never arrive.

Tip: Don't send money to someone you don't know or someone you've only met online or over the phone. Also, don't rely on caller ID to determine if a call is legitimate. Scammers use spoofing tools to make it appear they are calling from a genuine government or business number.

Rental or Moving Scams

A scammer posts a fake rental property on a classified ad website offering discounts for active-duty military and veterans. They ask for a wire transfer of a security deposit to the landlord, only there's no rental property, and the security deposit is gone.

Tip: Be sure to research sale properties or rentals offering veterans and military families a discount online at MilitaryByOwner.com. Also, check online property records to verify ownership and don't make any payments until you've signed a contract.

Con artists specifically target veterans with false claims of military service brotherhood. They know patriotism among vets can be an open door into hearts and wallets.

Other Scams to Watch For

AARP research shows veterans are also targeted significantly more and lose more money than civilians to general consumer fraud. These swindles range from grandparent-impostor scams and financial phishing schemes to tech support fraud, IRS impostors and bogus claims to fix credit ratings or credit card interest rates.

Grandparent Scam

Someone claiming to be your grandchild, or representing your grandchild, calls claiming an urgent need for help: They've caused an accident and they've hurt someone badly; they were pulled over and the police found drugs in the car, or some similar scenario. They need you to send money right away with promises you won't tell their parents. They may ask for gift cards, wire transfer or cash.

Tip: As hard as it may be, hang up on a call like this. Contact your grandchild or a family member who can confirm their whereabouts. The criminal will count on you staying on the phone to convince you of their lie.

Business Impostor Scam

Contact from your bank, a shipping company, a retailer, tech support, utility or other entity claiming there is a problem. They may also claim that your auto warranty is about to expire or that they can help you resolve your debt. Options might include: press 1 to be connected to a representative, call back a certain number or click on a link to access your account.

Tip: Do not press 1, do not call back a number given to you, and do not click on a link. If you think the call could be legitimate, find a number you know to be correct and call to inquire. And beware of searching online for a customer service number — you may end up calling a scammer directly.

Online Romance Scam

You meet someone on a dating site, simply playing an online game, or perusing your social media feed. This person takes a quick interest in you, suggests you move to another platform to talk, and turns on the charm. They will flatter you, ingratiate themselves, and convince you that you belong together. Only you never meet in person — he's serving a tour abroad. Eventually, they will start asking for money. The requests for money turn into demands, and they are relentless.

The older the target, the heavier the financial toll. The median individual loss from a romance scam for people 70 and over was $9,000 in 2021, according to the FTC, compared to $2,400 across all age groups.

Tip: Never send money to someone you know online whom you've never met in person.

How Scammers Operate

In Person

Crooked companies and scammers knock on doors to steal people's money or even to case your home for a later attempt at burglary. Criminals may claim to be from your utility provider or alarm service, or say they're selling subscriptions or seeking charitable donations.

Tip: Commit to not opening your door to strangers. If you do engage with someone, be wary of pressure to make a quick decision or pay cash up front for work, and thoroughly read any contracts before signing.

Phone

Despite — and maybe because of — technological advances, the telephone remains a hot method of contact for today's scammers. Phone scams often begin with a recorded robocall about some urgent matter that instructs you to stay on the line or press a button to speak to a representative.

Tip: Add your numbers to the National Do Not Call Registry at donotcall.gov or 888-382-1222. This will cut down on legitimate telemarketing calls, making it more likely that calls that do get through are scams. And when in doubt, let your answering machine or voicemail screen your calls.

Email

These days, it's easy for criminals to send authentic-looking emails or texts that appear like they are coming from an entity you do business with. The goal is for the message to instill urgency, to get you to take an action (click a link, call a phone number) without considering whether the message is fraudulent.

Tip: Skip the click! Call or type in the web address directly of who you think is trying contact you.

On the Web

Beware of online ads. A click on a scam ad could send you to a perfect copy of a legitimate site or could download malicious software intended to steal your credentials. Stick with retailers you have already done business with or that you trust.

Tip: If you have the business' app, log in to see if the discount is legitimate, or go directly to the website.

Social Media

Every social media platform is swarming with scammers looking to score money or sensitive information. Keep your distance on social media and set your account to only be open to friends and family. Avoid accepting friend requests from strangers and know that accounts are easily hacked, so a message from a friend encouraging you to click a link for a free grant may be a criminal who has hacked your friend's account.

Tip: Lock down your social media accounts to access only by friends and family. Follow the advice our parents gave us — don't talk to strangers, including those who reach out by phone.

Text

Text messaging is one of the fastest-growing contact methods for today's scammers. As with phone calls and emails, the scammer impersonates a familiar or trusted source to get you to act immediately to address some urgent matter.

Tip: Avoid clicking on links in emails or texts. Instead, go to the website by typing the address into your browser, use the app for the sender (if you have one), or call them using a number you know to be legitimate (e.g., from a statement).

Protect Yourself

Fortify Your Devices

Make sure your devices' operating systems are up to date and set updates to occur automatically. Often, updates are to patch a known pathway for criminal activity. Keep your protective software up to date as well, such as firewalls and antivirus tools. If you use your device in public, do not connect to free public Wi-Fi unless you enable a virtual private network (VPN). Options include ExpressVPN, NordVPN or Surfshark.

Pay Safely

Consider any request for an unusual payment a red flag. These include money transfer apps, gift cards, cryptocurrency and wire transfers. The safest way to pay for something is with credit cards because they offer consumer protections. Debit cards have similar protections, but if yours is compromised and money leaves your account, you have no access to that money until — and unless — the card issuer confirms fraud did occur.

SAFEGUARD YOUR SOCIAL SECURITY NUMBER (SSN) AND PERSONAL INFORMATION

- Don't carry your Social Security card in your wallet.
- Don't print your SSN or driver's license number on your checks.
- Shred sensitive information.
- Limit the number of credit cards you carry.
- Keep copies of credit cards (front and back) in a safe place in case a card is lost or stolen.

Gift Cards

Gift cards are not a legitimate form of payment. Anyone who directs you to pay for some obligation by purchasing gift cards and sharing the numbers off the back is lying to you.

Con artists have latched onto gift cards as a convenient form of payment in their scams. The reasons are several: Gift cards can be purchased just about anywhere, they are virtually untraceable, and criminals can drain the cards quickly.

Visit aarp.org/giftcards to learn more.

AARP RESOURCES

AARP Fraud Watch Network
aarp.org/fraudwatchnetwork

Get the latest news and information on scams, sign up for biweekly Watchdog Alerts, review more than 70 quick tip sheets on common scams, or report a scam on our scam-tracking map.

AARP Fraud Watch Network Helpline
877-908-3360

AARP's Fraud Watch Network Helpline is a free resource for AARP members and nonmembers alike. Trained fraud specialists and volunteers field thousands of calls each month. Report a scam or get guidance you can trust, free of judgment.

AARP VOA ReST Victim Support Program
aarp.org/fraudsupport

ReST stands for Resilience, Strength and Time. AARP has joined with the Volunteers of America to bring this helpful resource to victims of fraud and their families. This peer-led virtual session hosts up to five people and exists to address the emotional impact of your fraud experience.

OPERATION PROTECT VETERANS

Operation Protect Veterans is a joint program of AARP's Fraud Watch Network and the U.S. Postal Inspection Service (USPIS). The initiative provides free resources and community programs to proactively spot scams and delivers helpful guidance from fraud specialists to help veterans, military and families who have been targeted.

To learn more, visit uspis.gov/veterans.

COMMUNITY RESOURCES

Charity Rating Sites
Charity Navigator: charitynavigator.org
Give.org: give.org

Check websites that provide ratings and reviews of charities so that you can know if they are legitimate before you donate, including Charity Navigator and the Better Business Bureau's Wise Giving Alliance.

Consumer Finance Protection Bureau (CFPB)
consumerfinance.gov

Download free financial scam awareness resources at **consumerfinance.gov/blog** by searching keyword "Service Members."

Credit Bureau Contact Information
Experion: experian.com | 888-397-3742
Transunion: transunion.com | 888-909-8872
Equifax: equifax.com | 800-685-1111 (in N.Y., 800-349-9960)
Annual Credit Report (order free credit reports):
annualcreditreport.com

Customer Service Numbers of Commonly Impersonated Organizations
IRS (Treasury Inspector General): 800-366-4484
Medicare (HHS Office of Inspector General): 800-447-8477
Social Security Administration: 800-772-1213

Federal Trade Commission (FTC)
877-FTC-HELP (**877-382-4357**) | **reportfraud.ftc.gov**

Call the Federal Trade Commission to file a complaint if you feel you have been defrauded.

Military Consumer
MilitaryConsumer.gov/protect

Learn more about spotting scams and safeguarding your identity at **MilitaryConsumer.gov/protect**, a website run by the FTC, the Department of Defense and the Consumer Financial Protection Bureau.

National Do Not Call Registry
Register your numbers: 888-382-1222 | donotcall.gov

To help cut down on robocalls, add all your numbers to the National Do Not Call Registry, operated by the FTC. It won't stop fraudulent calls, but it will make them easier to spot because most legitimate telemarketers won't call numbers on the registry.

U.S. Department of Veterans Affairs (VA)
va.gov | 800-MyVA 411 (800-698-2411)

To learn more about protecting yourself from fraud, and how to report it, go to **va.gov** and search "Office of Inspector General." If you receive an unsolicited call from some claiming to be from VA, hang up and call the agency directly at 800-MyVA 411 (800-698-2411).

U.S. Postal Inspection Service
uspis.gov

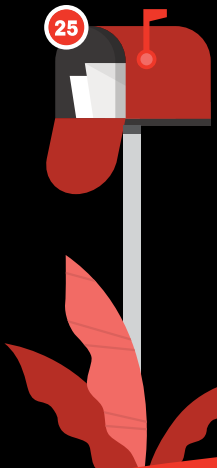
The U.S. Postal Inspection Service has information about how to protect yourself from mail fraud and how to identify when you've been targeted.

You Fought for Us. We're Fighting for You.

AARP's team of fraud fighters has real-world tips and tools to protect U.S. veterans, service members and their families.

» If you or a loved one has been targeted by a scam or fraud, you are not alone. Fraud specialists at the **AARP Fraud Watch Network Helpline** provide free support and guidance on what to do next. **Call 877-908-3360.**

» If you've experienced fraud and are struggling in its aftermath, visit **aarp.org/fraudsupport** to learn about free, peer-led online sessions aimed at helping fraud victims begin healing emotionally.



AARP®

601 E St. NW
Washington, DC 20049

aarp.org/Veterans

D20774 (0422)