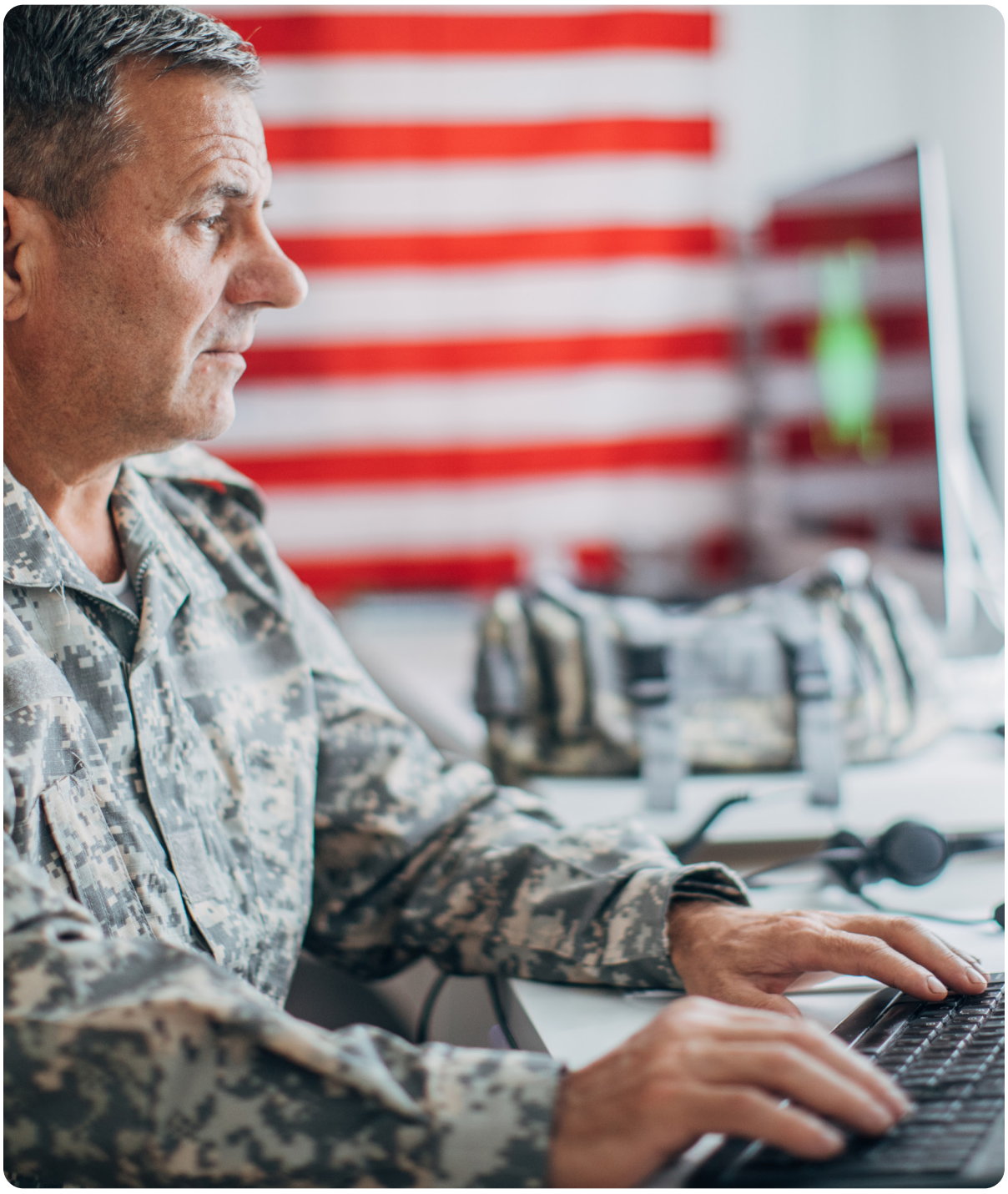
ĀURA

# The Veteran Cybercrime Crisis

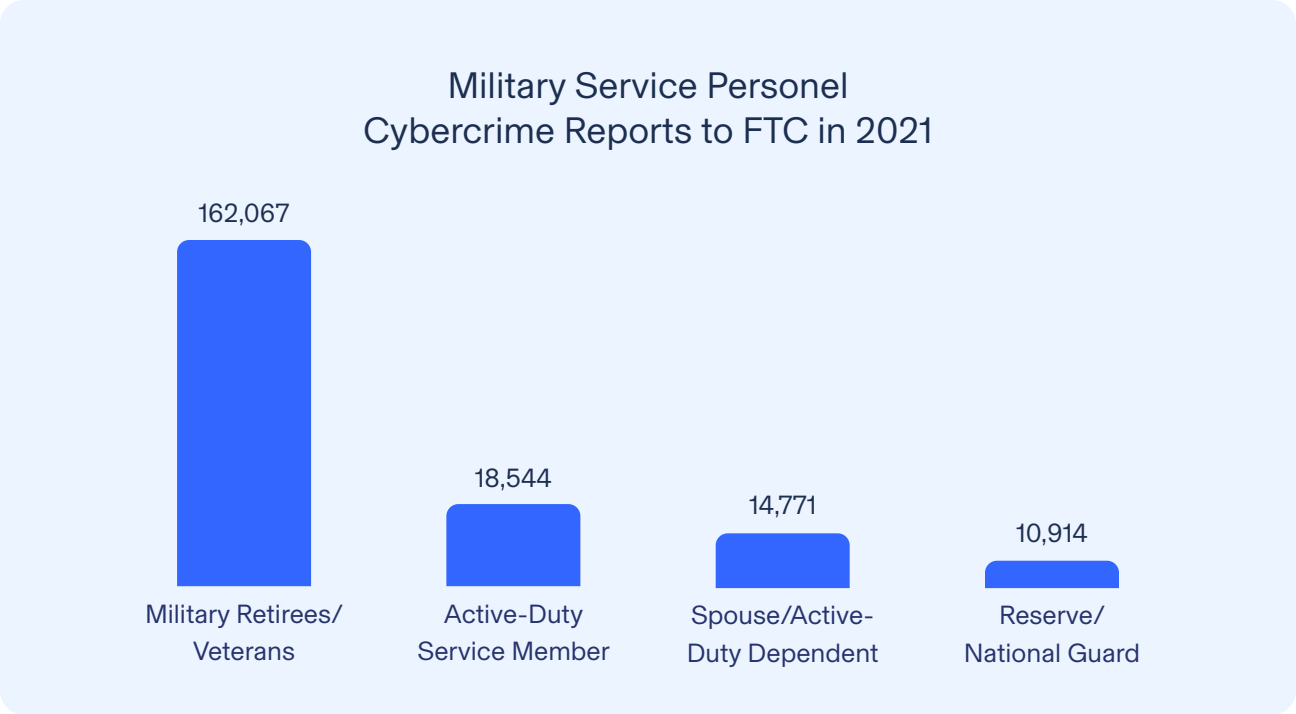


November 2022

# Veterans represent more than three-quarters of fraud, identity theft and other reports by the military community.

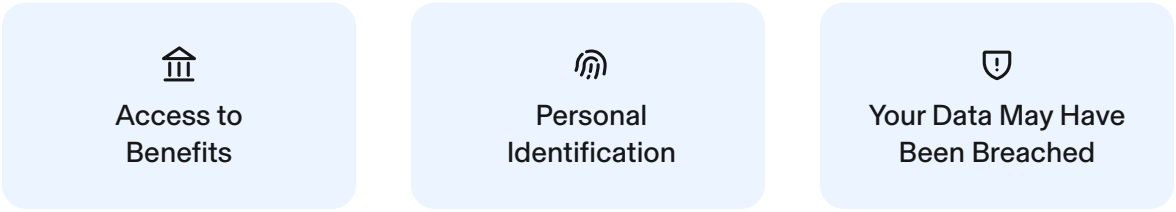
It's no secret that military families are at higher than average risk of cybercrime. But within this community, there's one specific group that data shows is especially vulnerable: Veterans. Of more than 200,000 reports to the FTC in 2021, over 78 percent were made by military retirees and Veterans.[1]

AARP surveys have also found that Veterans and their families are targeted more often by fraudsters, and that one third of those who have been targeted by service-related scams, have lost money, as a result.[2]



# Why are Veterans at Higher Risk?

There are a few reasons Veterans may be at higher risk of cybercrime than civilians and their active-duty counterparts.




## Access to Benefits

Government-provided benefits have always been attractive to fraudsters. From Medicare and disability, to Social Security and other benefits, scammers increasingly impersonate government agencies, conning victims into sharing enough information to steal their benefits. Just recently, during the COVID-19 pandemic, the government saw a massive rise in fraudulent Paycheck Protection Program (PPP) loans and unemployment claims, leading the White House to launch an effort designed to combat fraud related to pandemic relief programs.[3]

Military-specific benefits are no exception. The GI Bill, for example, is known to provide American service members with free or reduced-cost education to those who qualify, offering support as they return to civilian life. One fraudulent education scheme scammed thousands of victims out of these benefits, stealing more than $20 million from deserving Veterans, according to the FBI.[4]

Earlier this year, President Biden signed the PACT Act of 2022 into law, which supports Veterans exposed to burn pits and other toxic substances— and their families—with the care and benefits they've earned and deserve. Scammers are using phishing emails, texts and social media scams targeting Veterans to access their PACT Act benefits or file fraudulent claims on their behalf.

These are just a few examples of government-benefits related schemes.

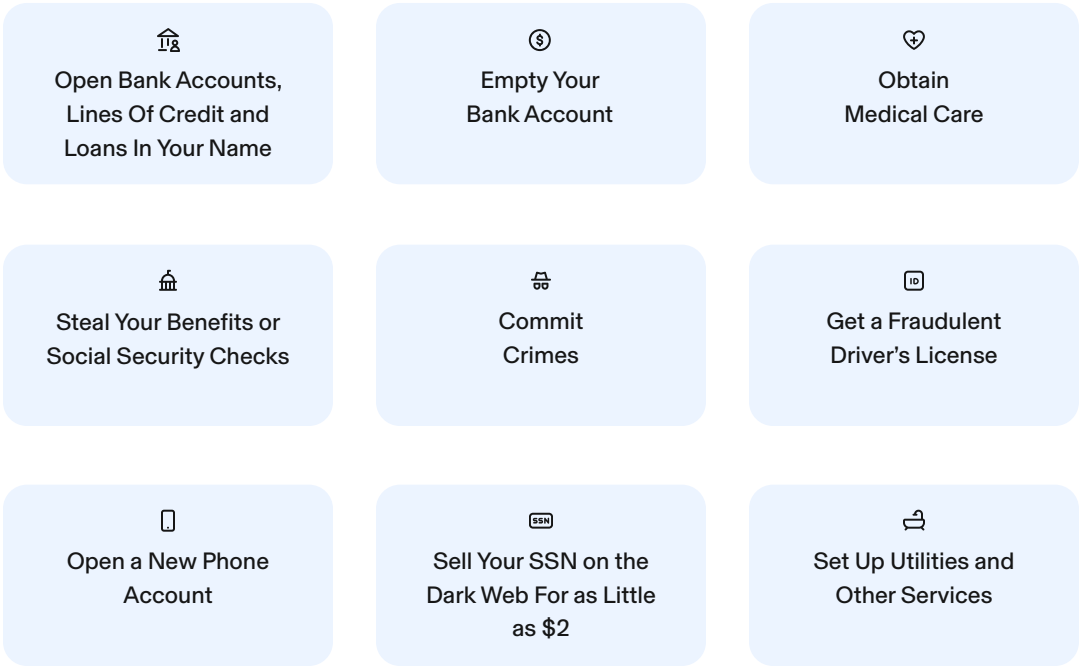
**Pro Tip**

A good rule of thumb is that anytime there are monetary benefits involved — even those requiring you file a claim or request — there's potential for them to be the target of a scam. Remember that caller ID and websites can be faked, and that government agencies will never call you — unless you've asked them to.

## Personal Identification

While the Federal Government began to move away from using Social Security numbers (SSN) on military ID cards more than a decade ago, it continues to be used as a form of identification for service members and their families. And for Veterans who retired from military service before then, they may still have ID cards, dog tags or other forms of identification containing a SSN. Furthermore, you may rely on older DD214 forms that display your SSN to claim military discounts in stores or restaurants, sharing your sensitive personal information with potentially in-intentioned or dishonest individuals.

With just an SSN, a hacker can:




## Your Data May Have Been Breached

Service members' and Veterans' personal information has been affected by multiple data breaches. According to the Identity Theft Resource Center, the military and U.S. government were affected by 99 data breaches in 2018 alone, exposing more than 18 million records.[5]

In 2014, for example, the U.S. Office of Personnel Management (OPM) exposed the social security numbers and security clearance information of more than 20 million active-duty and former military personnel.[6] Three years prior, the U.S. Department of Defense (DOD)'s healthcare system, TRICARE, reported a data breach affecting 4.9 million patients.[7]

# Defend Against Fraud

Take the following proactive measures to defend you and your family against cybercriminals looking to exploit your Veteran status.

## Be suspicious

If you receive a call, email or text message you weren't expecting that demands action, be skeptical. Remember that caller ID, email addresses and websites can be faked to look like the real thing.

If you receive a call from someone claiming to be from the Social Security Administration or your bank, for example, hang up, look up the phone number on the official website, and call directly. Be suspicious of text messages urging you to click a link, reschedule a package delivery or take immediate action on a government benefit. Instead of clicking the link, contact the organization directly. Be suspicious of emails with attachments or links you weren't expecting, and read email addresses carefully. Frauders may have created an email address that is similar to that of one you trust, but is off by one letter or uses .net instead of .com, for example.

## Be protective

Don't share your or your family's SSNs, dates of birth or other personal information over the phone or when others are around. Before sharing this information with a doctor, employer or anyone else— ask if it's completely necessary. And if it is, ask how they secure your data. Watch the receptionist at your doctor shred the piece of paper on which you wrote your SSN before walking away. Consider making a copy of military identification forms with SSN and other sensitive information blacked out for discounts at stores and restaurants.

## Freeze your credit

If you've already experienced identity theft or had issues with fraud, consider freezing your credit. While a credit freeze doesn't prevent your identity from being stolen, it does prevent a criminal from using it to steal your credit.

## Explore fraud alerts

In the case of a lost wallet, for example, you might be suspicious that identity theft will occur — even if it hasn't, yet. Contact one of the three credit bureaus and ask them to set up a free fraud alert. The bureau you contact should notify the two others.

## Monitor your credit and read account statements

The three credit bureaus (Equifax, Experian and TransUnion) offer free credit reports once a year. Consider requesting a credit report from one every four months, rather than all three at one time. Read financial, medical and other account statements. If you see something that doesn't make sense or is a mistake, call the business directly.

## Shred sensitive documents, or keep them safe

Be protective of sensitive documents containing personal identifiable information, like tax forms, birth certificates, Social Security cards, bank account statements, military benefit forms and more. Shred those you no longer need before throwing them away, and safely secure those you do.

# Know the Signs of Identity Theft

There are many types of identity theft. Be aware of the warning signs listed below:

- Unfamiliar Charges on Your Bank Statement
- Unfamiliar Credit Card Charges
- New Credit Cards or Loans in Your Name
- Calls from Debt Collectors
- You're Denied Credit
- Bounced Checks
- Drop in Credit Score
- Hard Inquiries on Your Credit Report
- Calls Verifying Unfamiliar Purchases
- Maxing Out Your Health Insurance Benefits Limit
- Unfamiliar Medical Bills
- Inaccurate Health Conditions in Your Medical Files
- Someone Stole Your Income Tax Refund
- There's a Warrant Out for Your Arrest
- Reported Income That's Not Yours
- Mail Theft
- Your Utilities Are Suddenly Shut Off
- Your ID is Lost or Stolen
- Unfamiliar Bills or Packages Arrive at Your Home
- An Account Looks Different When You Log In
- Suspicious Login Attempts to Your Social Media Accounts
- Authentication Messages for Accounts You Don't Recognize
- You Can't Sign Into an Account
- Email Alerting You of a Data Breach
- You Receive a Fraud Alert
- Your information is found on the dark web

# Get Help

Here at Aura, we believe you've sacrificed more than enough for your country, and want to thank you for your service by helping to keep you and your family's personal information, devices and finances safe from cyberthreats.

Visit aura.com/military for up to 50% off all protection plans for active-duty service members, Veterans and their families, and for more resources designed for military families.

Aura's easy-to-use, all-in-one digital security platform combines everything you need to proactively control your digital lives. It monitors your credit, financial transactions, bank accounts, SSN, the dark web, home and title use, and criminal and court records to keep your finances and your identity safe and secure. And in the event of an issue, Aura's U.S.-based customer service team is available to help you resolve problems 24/7. This is all backed by a $1 million dollar identity theft insurance policy for eligible losses for every Aura customer.[8]

## Citations

[1] FTC Consumer Sentinel Network Data Book 2021

[2] 2021 AARP survey

[3] Fact Sheet: President Biden to Announce New Steps to Combat Criminal Fraud and Identity Theft in Pandemic Relief Programs - The White House

[4] GI Bill Fraud Scheme — FBI

[5] Identity Theft Resource Center 2018 End of Year Data Breach Report

[6] 3 Reasons Veterans Are More Likely to be Victims of Identity Theft | Military.com

[7] Tricare reports data breach affecting 4.9 million patients | Modern Healthcare

[8] Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc.. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

No one can prevent all identity theft or monitor all transactions effectively.