AURA

Addressing Cybercrime's Disproportionate Impact on America's Armed Forces

October 2021

Active-duty service members, Veterans and military families at higher risk of digital threats

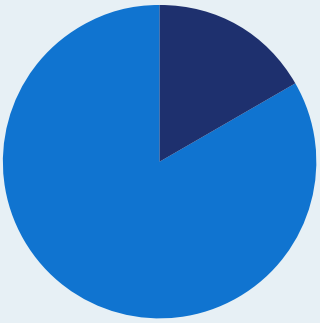
Cyberattacks are the fastest growing crime in the U.S., and are increasing in size, cost & sophistication according to Cybersecurity Ventures.

Active-duty military, Veterans and their families are disproportionately affected by these growing threats.

According to the Federal Trade Commission (FTC), data shows active-duty service members are **76% more likely than other adults to report an identity thief misused an existing account**, such as a bank account or credit card.

The FTC also notes they are nearly **three times more likely to report debit card misuse** or other electronic theft of money directly from bank accounts, and 22% more likely to report that stolen information was misused to open a new account, especially new credit accounts.

Key Fact



Furthermore, **one-fifth** say that they have already experienced two or more types of identity theft.

Source: FTC

Seven Reasons For The Military's Increased Risk Of Digital Threats

01 Service members' and Veterans' personal information has been affected by multiple data breaches.

02 Service members and Veterans are used to sharing their personal information.

03 Members of the military have access to highly sensitive data.

04 Service members and their families relocate often.

05 Active-duty service members spend long periods of time abroad, making it difficult to monitor accounts.

06 Military often use communal wifi or internet wired through a foreign government.

07 Members of the military are often photographed in uniform, which includes their name and/or rank.

01

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

Alert

With only a social security number (SSN), cybercriminals can:

- Secure a loan or credit card in the victim's name
- Drain their bank account
- Use their health insurance
- Claim Social Security
- Identify themselves as the victim to police in the event of an arrest

02

Service members and Veterans are used to sharing their personal information.

The DOD and other organizations have historically relied on SSNs to identify service members and Veterans. This information was previously printed on prescription bottles, dog tags and sensitive documents required to prove military status to secure everything from retail discounts to government benefits. Thankfully, the DOD has moved away from this identification approach and SSNs are no longer included on military ID cards.

03

Members of the military have access to highly sensitive data.

It's no secret that foreign governments increasingly use cybercrime as a way to gain access to government data, confidential information or even to disrupt democracy. Whether authorized or unauthorized, service members have access to extremely sensitive government data, making them a valuable target for cybercriminals. Attackers might gain access to these systems by hacking and infecting software used by the military or government, like in the case of SolarWinds, or engage a service member directly and demanding access to government documents by threatening violence toward a loved one or draining the victim's bank account.

04

Service members and their families relocate often.

Nearly 14% of active-duty service members report a family member or someone they know stole their identity, double the number (7%) of FTC reports by other adults. This often occurs when people find important documents or financial records left behind by a service member after a move or when away on a military assignment.

Key Fact

Active-duty service members report identities being stolen by someone they know **twice as often** as other adults

Source: FTC

Key Takeaway

Whether authorized or unauthorized, service members have access to extremely sensitive government data, making them a valuable target for cybercriminals.

05

Active-duty service members spend long periods of time abroad, making it difficult to monitor accounts.

Service members' tendency to regularly travel large distances can often mean they are unable to readily access a phone or email, making it impossible to monitor their accounts while abroad or to detect a threat until it's too late.

Alert

While the service member's family can monitor accounts while they are away, it can be difficult to know when a charge is legitimate or fraudulent, and is further complicated when cybercriminals take small amounts of money at a time in an attempt to remain undetected — the "salami" method.

Regularly checking credit reports overseas can also be near impossible for many members of the military. Military personnel have protections that allow them to cancel housing contracts, vehicle leases and other accounts before they ship out, but if there is a problem, service members may only learn of the issue if and when they read it on a credit report. Getting a credit bureau error fixed is doable, but can take a long time and can hurt security clearance applications.

Cybercriminals often take further advantage of military travel by calling the service member's family at home, saying, for example, there's an urgent problem with their loved one that requires an immediate wire transfer. They will often threaten a consequence, such as the service member losing access to critical health care, and may intimidate the family member by suggesting they try to validate the threat by trying to reach the service member. In these cases, the criminal may already know the service member is impossible to reach.

Did You Know?

Many cyberattackers will track military personnel, waiting until they are deployed or unavailable to call each relative with the same fraudulent story, in an attempt to steal as much money as possible.

06

Military often use communal wifi or internet wired through a foreign government.

Often, active-duty service members' only access to the internet is through shared computers and wifi at the military base.

Alert

Public, shared wifi or networks hosted through foreign governments can often be less secure and data can be stolen.

The dynamic of shared computers and wifi further complicates protecting yourself online, as monitoring financial and other sensitive accounts in these settings can be risky.

07

Members of the military are often photographed in uniform, which includes their name and/or rank.

Whether shared via news channels, government sites or social media, seemingly innocuous photos of service members can offer just enough information for a cybercriminal to take action. Given the criminal's goal is often to impersonate the victim or a family member, it's important to remember sharing any personal details on social media — from a pet's name to your favorite foods can put the service member — or an average person — at risk.

Key Takeaway

Sharing any personal details on social media can put the service member — or an average person — at risk.

Tips for active-duty military, Veterans and their families to better protect themselves online

Be suspicious.

Service members, Veterans and their family members should practice skepticism. As cyber threats diversify, they are becoming more sophisticated and appear increasingly legitimate.

For example, if a caller requests money, ask for enough information to verify who is calling, from where and why. If they say they're from a phone company:

- Ask which one
- Where they are located
- The name of their supervisor
- How long you've had an account with them, etc.

If you're still suspicious, call the phone number available on your latest bill or on their website to verify — and be sure to check if the website is legitimate. It's not uncommon for cybercriminals to replicate a company's website almost identically, with just a letter off in the domain, for example.

Establish protocol.

Consider creating a way for family members to establish trust when receiving a call from a bank or health insurance provider. For example, decide on a code (a word, number, etc.) that only a service member and their spouse know, tell the company, and use the code as another verification method.

Be protective.

Don't share SSNs, dates of birth or other sensitive personal information over the phone when others are around. Watch the receptionist at your doctor shred the piece of paper on which you wrote your SSN before walking away.

Freeze credit and/or set up an active-duty credit alert.

While it can be inconvenient to freeze credit, it's a great way to prevent cybercriminals from opening credit cards, taking out a mortgage or other loans in your name. While credit freezes do not prevent attackers from stealing your identity, they do prevent the criminal from using it to access and steal credit.

> **One way active-duty military can help prevent credit — related issues, especially when traveling, is by requesting an active-duty credit alert.**

This encourages lenders and creditors to take extra steps to verify your identity, before opening a new credit account or making changes to existing accounts. **An active-duty alert is free and lasts for one year**, and the service member's name is removed from pre-screened credit card or insurance offers for two years. Any of the three national credit bureaus can set up an active-duty alert, and whichever one you contact will notify the other two.

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.** Similar to the process with active-duty alerts, the bureau you contact will notify the two others.

Use strong — and different — passwords for each account.

Use complex and different passwords for each of your online accounts. A secure password uses multiple digits and a mix of upper — and lower — case letters, along with special characters such as @, # and %. Don't use a pet's name, a hometown or a favorite sports team — or anything a stranger could figure out by looking at your social media history or other publicly available information.

Do not write your password down digitally or on paper. If you can't remember your passwords, explore a password manager, which manages different, complex passwords for each account you have across mobile and desktop. However, make sure to create a complex password for the password manager itself, as that will serve as the gatekeeper for all your other passwords.

Read credit reports and all account statements.

The three credit bureaus 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.

Be careful when shopping online.

Only shop on websites that protect your personal and financial information with encryption. If a site has “https” at the beginning of the domain, it’s encrypted — the “s” stands for “secure.” You should still use caution, however, as this encryption doesn’t necessarily mean the site itself is from a trustworthy source — only that your data isn’t available to anyone but you and the site you’re visiting.

Shred documents with sensitive information.

Whenever possible, **don’t leave behind documents with personal information.** In the event of a move or relocation, set up mail forwarding so that credit card offers and other sensitive data reach only you and your immediate family.

Explore a virtual private network (VPN).

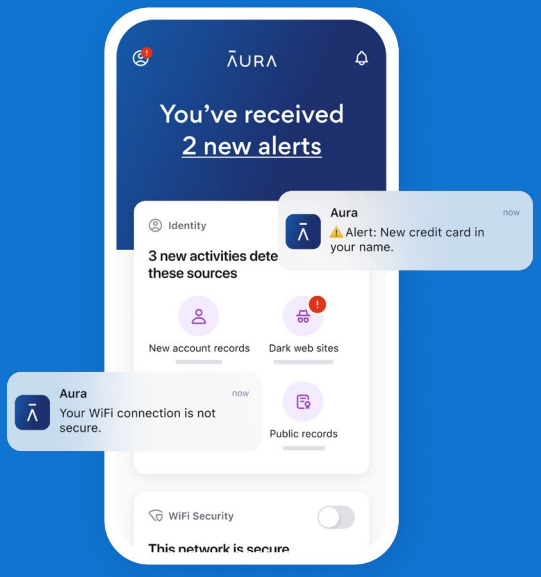
When traveling, deployed or in any situation where you might be using shared internet or devices, consider a VPN service. **There are a number of free VPN services that offer privacy and anonymity** by creating a private connection from a public internet network. **VPNs encrypt your data, hide your IP address and obscure your online identity.**

Take action quickly.

In the event of identity theft or other fraudulent activity, a service member (or a spouse if the service member is deployed) should **alert superiors,** especially if security clearance is in the near future.

Explore digital security solutions.

At Aura, we understand firsthand how daunting it can be to take control of your digital life. That’s why we created easy-to-use, all-in-one digital security protection to keep you and your family’s personal information, devices and finances safe from online threats. It combines everything you need to proactively control your dig-ital lives — credit monitoring, lost wallet recovery, antivirus, VPN, multi — device protection, and monitors 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.



AURA