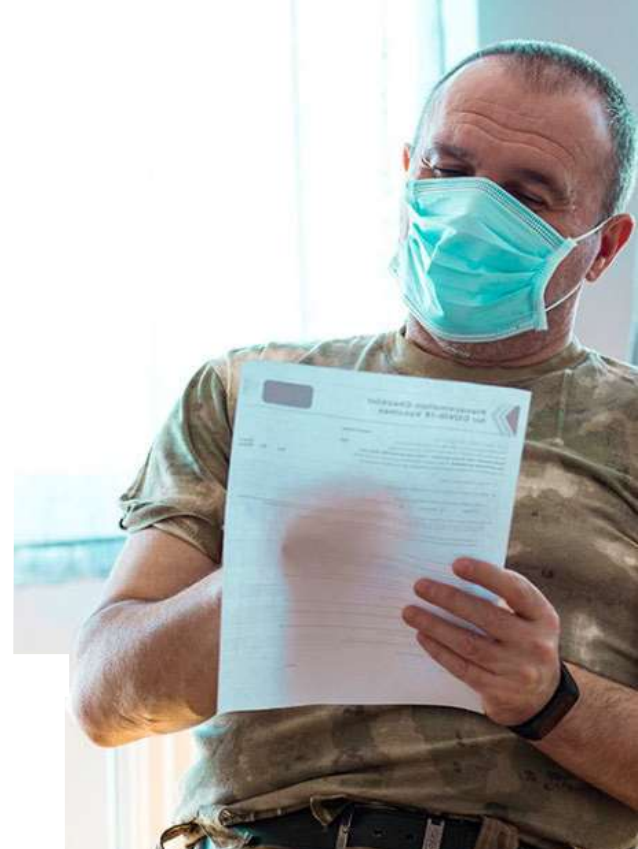




AARP[®]



Scambush: Military Veterans Battle Surprise Attacks from Scams & Fraud

Report Prepared by: Jennifer Sauer, AARP Research and Pete Jeffries, AARP Veterans and Military Families Initiative







AARP.ORG/RESEARCH
© 2021 AARP ALL RIGHTS RESERVED

AARP RESEARCH

<https://doi.org/10.26419/res.00502.001>

Table of Contents

	Executive Summary	3
	Detailed Findings	9
	Scam Prevention Tips and Resources	23
	Study Methodology	24

EXECUTIVE SUMMARY

Executive Summary

In 2017, AARP found that veterans, active-duty service members and their families were more often targeted by con-artists than their civilian counterparts.¹ Since then, AARP has provided the military community with relevant information and resources on how to spot, prevent and report fraud attacks. This year, AARP returned to the field to measure the number of scams, fraud and identity theft schemes threatening service members and veterans.

More importantly, this new research:

- Compares the military community to the civilian population;
- Provides further insights into best practices and tools to prevent a potential attack from the start; and,
- Builds the knowledge base to arm those who served against falling victim to fraud.

AARP's latest survey, "***Scambush: Military Veterans Battle Surprise Attacks from Scams and Fraud***" finds veterans, military, and their families continue to be significantly targeted more by con-artists and are losing money more than non-military/non-veterans when approached by similar scams or schemes. In addition, among those military and veteran respondents to the survey who received service-related scam attempts, nearly a third reported that they lost money supporting fake veteran or military charities or causes, or updating their military records, and nearly half erroneously signed over their U.S. Department of Veterans Affairs (VA) pension or disability benefits.

¹2017 AARP, *Under Fire: Military Veterans and Consumer Fraud in the United States*
<https://www.aarp.org/research/topics/economics/info-2017/military-vet-consumer-fraud.html>

These findings corroborate public reports by the Federal Trade Commission (FTC) Consumer Sentinel Network, which received nearly 66,000 fraud complaints and more than 55,000 identity theft complaints from military consumers in 2020 contributing to a total loss of \$122 million.² And we know scams are significantly under-reported so the losses are likely far higher.

Among the top ten fraud complaints filed with the FTC by veteran and military consumers were impostor scams, prizes/sweepstakes/lottery scams, travel/vacation/ timeshare, mortgage foreclosure relief and debt management scams. Among the seven categories of identity-theft complaints were government documents or benefits fraud, credit card fraud, and employment and tax-related fraud.



²2021 Federal Trade Commission Consumer Sentinel https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf



The following are key findings from the 2021 AARP survey:

- **Military/veteran and civilian adults alike are plagued by robocalls, spam or junk email, and suspicious-looking text or instant messages**—a common way in which scammers attempt to connect with consumers. Survey data shows that significantly more military/veterans than civilians are getting 10 or more robocalls (47% and 38%, respectively) or suspicious-looking texts or instant messages (28% and 18%, respectively) in a typical week and three-quarters of each group report finding 10 or more spam emails in their inbox each week (74% and 73%, respectively).
- **Military/veterans report getting more scam attempts than civilians overall** and in particular, are more likely to receive scam solicitations or offers related to technology support or repair (67% and 58%, respectively), travel or vacation package deals (58% and 51%, respectively), lottery or prize winnings (54% and 46%), special status discounts (48% and 31%), phishing for account information (48% and 39%) to name some.
- **Significantly more military/veteran adults than civilians lost money to at least one of the fraudulent solicitations** or offers ever or recently received (35% and 25%, respectively). The grandparent impostor scam, technology support scam, IRS impostor scam, offers to fix a low credit rating or lower a credit card interest rate, and phishing are ones in which military/veteran adults lost money more than civilians.

- **Roughly one in ten military/veteran and civilian adults received either of the COVID-19 scams mentioned in the survey**—an offer for testing and treatments and an offer to deposit or deliver a stimulus check. While similar numbers of these respondents lost money to the stimulus check scam (23% and 24%, respectively), a greater number of military/veterans than civilians lost money to the testing and treatment scam (30% and 22%, respectively).
- **One in three military/veteran adults who received a service-related scam solicitation or offer at some point, lost money to at least one of those offers.** In particular, many military/veterans lost money to a fraudulent request for a donation to a veteran-specific charity (32%), to update their military record (32%), or sign over their veterans or disability benefits (47%).

The findings suggest that opportunity exists for military/veteran and civilian adults to lower their risk for being targeted and/or losing money or personal information to a scam. Specifically:

- **Continued and targeted prevention tips and resources for military and veterans (and their families) is crucial.** While both Military/Veterans and civilians are targeted by similar scams, military/veterans are actually losing money to the scams more than civilians. Also, though small in actual numbers, the data reveal that both military/veterans and civilians are losing money they can likely never recover by paying a scammer with gift cards, cash or through a P2P payment platform like Zelle or Venmo.
- **Continued efforts to inform military/veterans and their family on the specific differences between a legitimate offer and a fake offer are needed** because too many military/veterans are losing money to con artists pretending to offer a service already provided for free by the government. In particular, an offer to a military member or veteran to update their military record by providing personal identifying information can seem routine and legitimate to any service member but any request for sensitive information should send up a big red flag.

- **Both military/veterans and civilians will benefit from greater information on certain protections that may reduce their risk of being targeted by scammers and losing money to them.** Too many respondents in both groups are not taking advantage of robocall blocking service (49% and 46%, respectively), not registering their phone(s) on the federal Do-Not-Call list (27% and 34%, respectively), or not placing a security freeze on their credit reports at each of the three major credit bureaus (81% and 85%, respectively).
- **Both military/veterans and civilians may need more information on where to check the legitimacy of a charity or cause as well as how to ask a fundraiser about the distribution of a donation.** Well over half of both groups indicate they have not inquired how their donation would be dispersed (how much goes to the charity or cause itself and how much goes to the fundraiser) before making their donation.

Given the preponderance of criminal scammers preying on those who served, AARP's Fraud Watch Network (FWN) has been working with the United States Postal Inspection Service (USPIS) on "**Operation Protect Veterans**"—a public awareness initiative to help veterans and military families fight back and protect themselves and their loved ones by raising visibility to the most current scams, frauds, and identity theft schemes. Whether it's using specific military jargon or veteran-related information, like calling out the need for a "DD Form 214" to receive benefits, Daniel Brubaker, USPIS Inspector in Charge and U.S. Marine Corps veteran notes, "*Scammers know that veterans share a special bond of service. They also know that veterans and military families get special benefits, and thus, they know how to craft a scam to be as effective as possible to get veterans to let their guard down and open their wallets. That's why it's extremely important that veterans, their family, and friends get informed about these scams and spread the word to protect other veterans.*"³

These 2021 AARP survey findings indicate a strong need for additional media and public attention to keep veterans, military, and their families informed, so they can more easily detect and fend off a "scambush"—surprise attacks from scams and fraud.

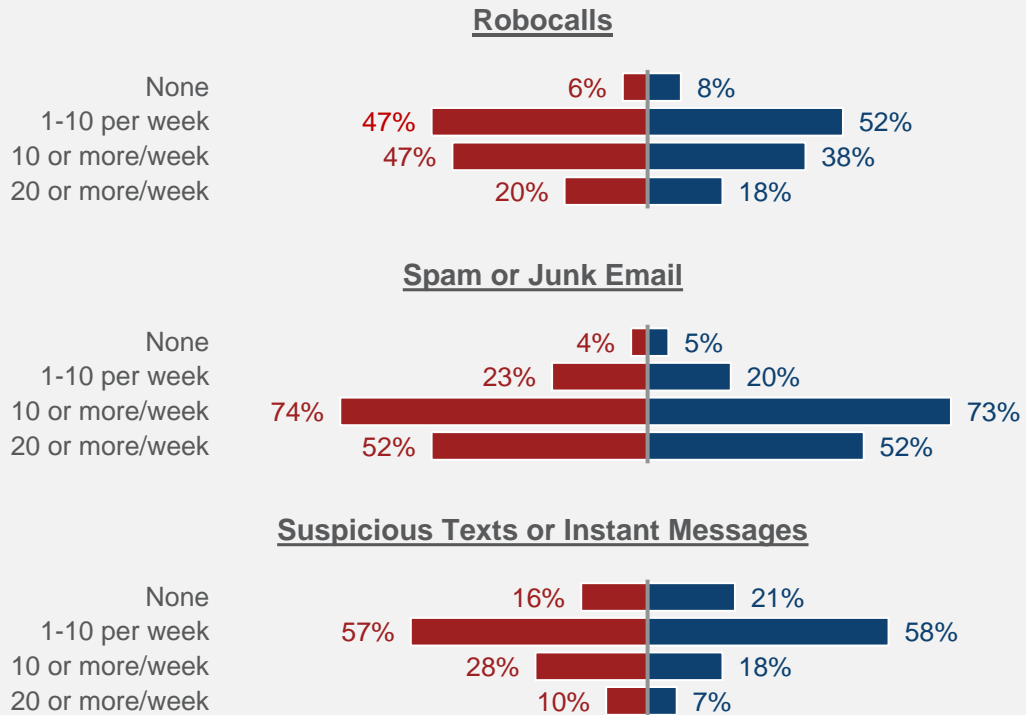


DETAILED FINDINGS

Military/Veterans Report Significantly More Robocalls And Suspicious Texts Per Week Than Civilians

Scammers are savvy and skilled users of technology as ways to target, connect with, and steal from customers. The Federal Communications Commission reports that robocalls are their top consumer complaint.⁴ Indeed, respondents from this survey are getting bombarded with robocalls, spam emails, and suspicious texts or instant messages with significantly more military/veterans than civilians getting more robocalls and texts in a typical week.

Type and number of solicitation contact attempts received in a typical week
Among **military or veteran (n=851)** and **non-military or civilian (n=809)**



Q22. A robocall is a phone call that uses a computer to dial your phone to deliver a pre-recorded message that may share telemarketing offers, public service announcements, or political campaign messages. In a typical week, about how many robocalls would you estimate you get on either your cell phone or landline, whether you answer them or not?

Q25. About how many spam (junk) emails would you say you receive in a typical week?

Q26. About how many suspicious looking text messages or instant messages would you say you receive in a typical week?

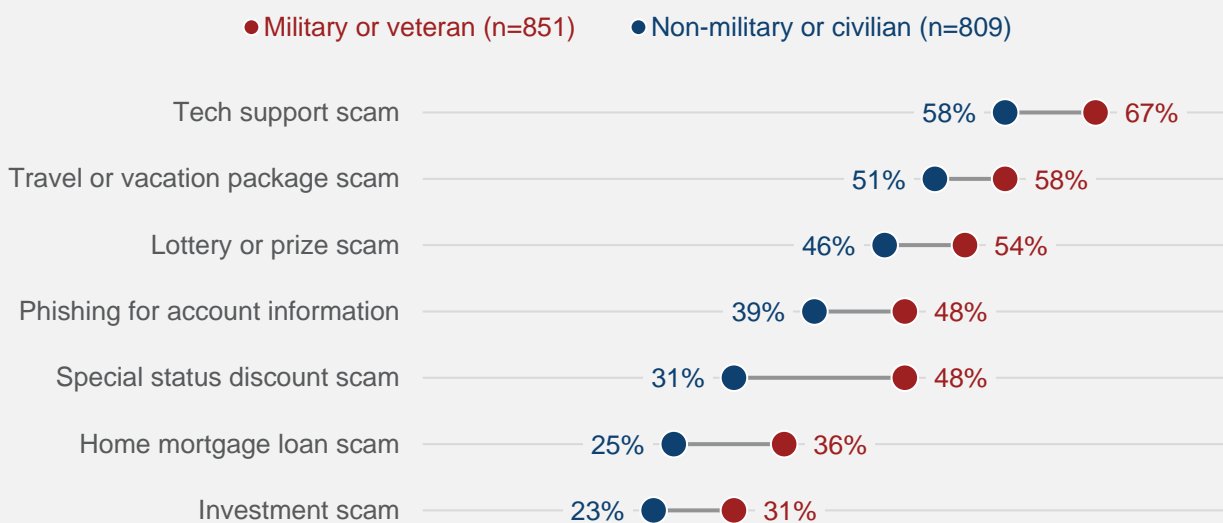
⁴<https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts>

Military/Veterans Report a Higher Volume of Scam Offers Overall, And More Tech Repair, Travel, Lottery, Special Status, and Phishing Scams in Particular

Most military/veteran and civilian adults ages 18 and older report that they have received at least one of the fraudulent solicitations or offers tested in the survey at some point (93% and 92%). However, significantly more military/veteran than civilian adults indicate having ever received at least half (8 or more) of the scam solicitations (49% or 39%).⁵ More specifically, military/veteran adults are significantly more likely than their counterparts to encounter a scam attempt related to technology repair, travel or vacation discounts or packages, winning the lottery or a prize, special status discounts, home mortgage loans, and investment scams.

Percent who ever received scam offers

Types of scams received more by military than civilians



Q1. After reading each type of solicitation below, please indicate if you've ever personally received it – whether exactly or somewhat as described - through a phone call, text, email, social media instant messaging, a screen pop-up, in-person, or a letter in the mail even if you didn't respond to it.

⁵Calculated count of 17 solicitations listed in question 1.

Both Military/Veteran and Civilian Adults Have Been Targeted In Past Year⁶

In fact, among those who indicate having ever encountered any of the 17 solicitations probed in the survey, most military/veterans and civilians encountered at least one of them in the past 12 months (90% and 90%).⁷ The most common were the tech support scam (53% and 46%, respectively) or Social Security impostor scam (45% and 48%, respectively), followed by a phishing (32% and 28%) or special status discount scam (33% and 22%, respectively).



⁶Q1_YEAR. Among the solicitations you have encountered, which, if any in the past 12 months, (or since August 2020 – from a phone call, text, email, social media instant messaging, a screen pop-up, or a letter in the mail) even if you didn't respond to it?

⁷Calculated count of Q1_YEAR

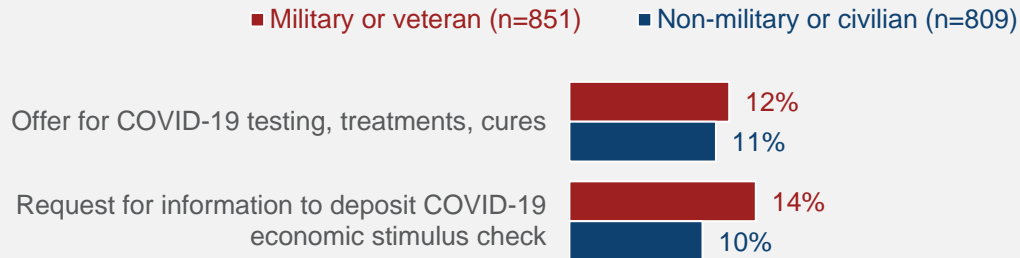
More Military/Veterans Than Civilians Lost Money On A COVID-19 Testing/Treatment Scam

The COVID-19 pandemic proved to be another opportunity for scammers to entice consumers into paying for phony products or services or even a government check. Data from this survey show that among respondents who ever or recently encountered the potential COVID-19 scam solicitations tested in the survey, more military/veterans than civilians spent money as result of receiving an offer for COVID-19-related testing, treatments, or cures for the Coronavirus that did not come from a health care provider known to them. Almost a quarter of respondents in both samples report they lost money because of a call or message from someone saying they are from the government and require bank account information to deposit an economic stimulus payment or to deliver it quickly.



Percent who have encountered COVID-19 scam offers

In the past 16 months



Percent who lost money on...

COVID-19 testing, treatment, and cures scam

Among those who encountered the scam



COVID-19 economic stimulus check scam

Among those who encountered the scam

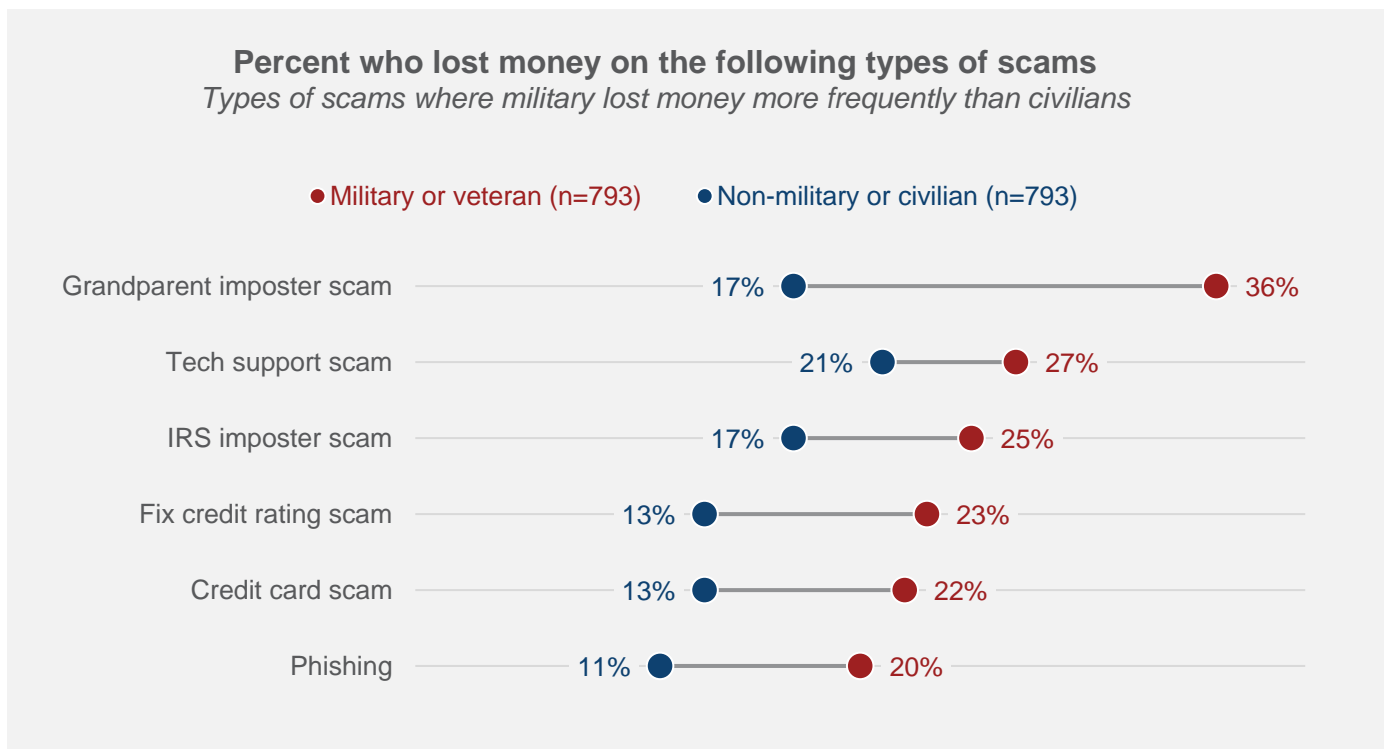


Q2. Now, thinking of the past 16 months, or since about March of 2020, which of the following situations have you encountered....?

Q3. Below is the list of solicitations or offers you indicate you have ever encountered. Please tell us if you spent any money as a result of the offer (paid for the product or service, provided relevant account information, paid an upfront fee or installment etc.) and how you paid for it.

Military/Veterans Are More Likely Than Civilians To Lose Money On Scam Offers

Recent Federal Trade Commission data showed from 2015 and 2019, the median monetary loss for veterans and active-duty members was higher than for civilians.⁸ Data from this survey also indicate more financial loss for military/veteran adults than civilians across the scam solicitations received. As a result of the scam attempts that military and civilians ever or recently received, military/veterans are more likely than civilians to indicate they lost money on at least one scam (35% vs 25%). In particular, significantly more military/veteran respondents than civilians lost money to the grandparent, tech repair, IRS impostor, credit rating repair, credit card, and phishing scam solicitations.



Q3. Below is the list of solicitations or offers you indicate you have ever encountered. Please tell us if you spent any money as a result of the offer (paid for the product or service, provided relevant account information, paid an upfront fee or installment etc.) and how you paid for it

⁸Veterans, service members, and fraud: by the numbers <https://www.consumer.ftc.gov/blog/2019/11/veterans-servicemembers-and-fraud-numbers>

1 in 3 Military/Veteran Adults Lost Money On At Least One Service-related Scam

Scammers often target veterans and those who serve in the military with offers already available to them for free. Data from this survey show that most (78%) military/veterans have encountered at least one of the 14 service-related scam attempts listed in the survey at some point in time, and most of them (86%) received at least one of these offers in the past 12 months. Being contacted by someone offering thousands of dollars in increased benefits, lowering home mortgage rates , and requesting a donation to a veterans-in-need charity are among the top six scam attempts received by military/veterans.

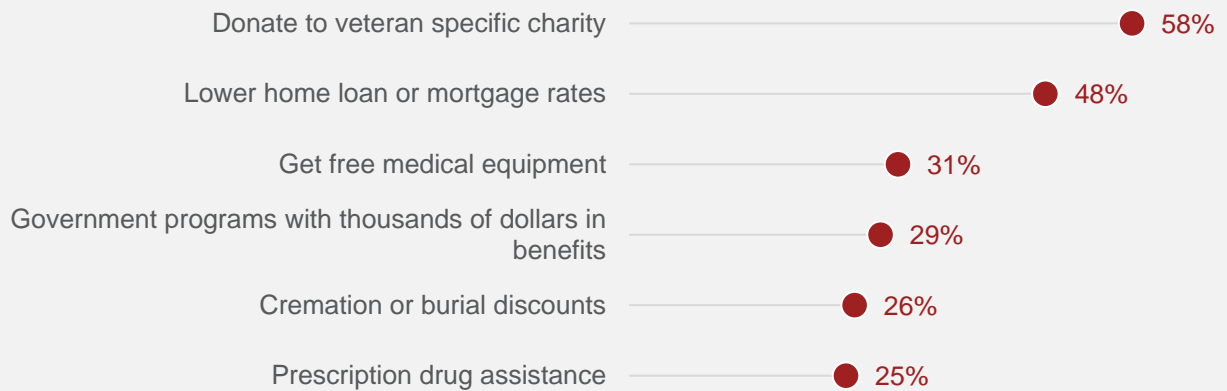
One third of military/veterans lost money to at least one of these service-related scams and more specifically, nearly half reported they lost money to an offer promising a lump-sum payment for signing over their Veterans or disability benefits. About another third lost money on offers to update their military record or a request to donate to veteran-specific charity.



⁹Q12. Among the solicitations or offers you have received, which of the following have you've experienced in the past 12 months...?

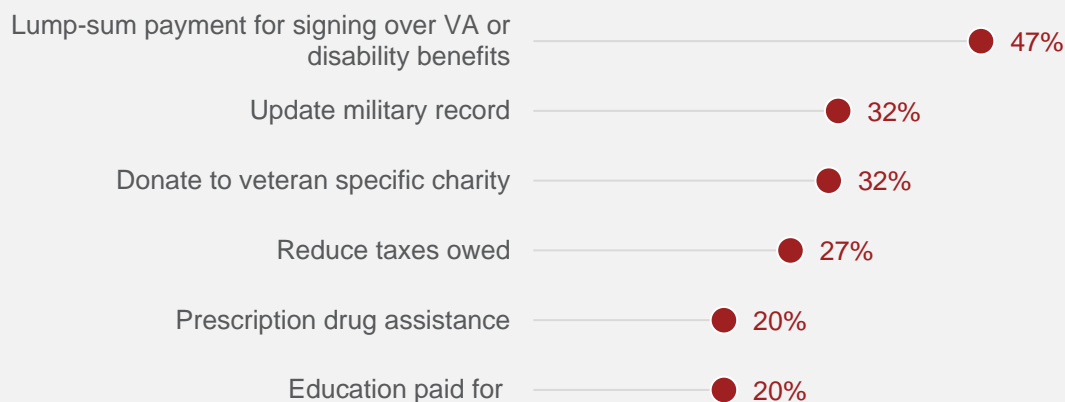
Percent receiving the following service-specific scam offers

Among military or veterans (n=851)



Percent losing money to the following service-specific scam offers

Among military or veterans who lost money to scams (n=669)



Q11. Below are some solicitations you might have received because of your military service from someone not likely to be associated with a military related office. Please indicate which of these requests, if any, you have ever received.

Q13. Below is the list of solicitations or offers you indicate that you have ever received due to your status as a veteran or active military. Please tell us if you spent any money as a result of the contact or offer, and then how you paid for it.

While Credit Cards and Personal Checks were used by many Military/Veterans and Civilians who Paid for the Fraudulent Offer, a few used Gift Cards

Gift card payment scams are increasingly common – where a scammer convinces a target they owe money for some obligation and the quickest way is to purchase gift cards and share the activation numbers off the back. Once the numbers are shared, the scammer drains the funds. Paying for any of the solicitations listed in the general or service-related survey questions with a gift card is a clear indication of a scam. Analysis of how respondents paid for the fraudulent offer shows that a few military/veteran adults and civilians used a gift card to pay for any of the service-related scams while more indicated using a personal check or credit card to pay for the scam offer.

Payment Type Used to Pay for at least one of 17 Scam Offers*

Payment Type	Military/ Veterans (280 adults 18+)	Civilians (187 adults 18+)
Credit card	47% (n=132)	39% (n=73)
Gift Card	20% (n=56)	20% (n=36)
Direct withdrawal from account	17% (n=47)	17% (n=32)
Cash	12% (n=34)	12% (n=21)
Personal check	6% (n=18)	11% (n=20)
P2P payment service	6% (n=17)	5% (n=8)
Other	26% (n=72)	29% (n=54)

Payment Type Used to Pay for at least one of 14 Service-Related Scam Offers*

Payment Type	Military/ Veterans (227 adults 18+)
Credit card	31% (n=70)
Gift Card	10% (n=22)
Personal check	39% (n=89)
Direct withdrawal from account	6% (n=14)
Cash	12% (n=28)
P2P payment service	6% (n=28)
Other	18% (n=40)

**No statistically significant differences between groups. Caution should be used in generalizing the results to the populations because some cell counts are less than 100 respondents.*

Q4A. How did you pay for the solicitation or offer below?

Q13. How did you pay for the solicitation or offer below?

More Military/Veterans And Civilians Need To Take Key Measures To Prevent Scam Attempts

Being vigilant about taking protective measures to protect your personal identification and financial account information can help reduce the risk of being targeted by a scammer or losing valuable personal information and money.

There are a number of services and apps available today to block spoof and illegal robocalls. Yet, data from this survey show that half of military/veterans and under half of civilians are not using a robocall blocking service and at least one in four in either group have not registered their phone(s) on the Federal Do-Not-Call list..

Use a Robocall Blocking Service

	Military/ Veterans (851 adults 18+)	Civilians (809 adults 18+)
Yes, cell phone	27%	31%
Yes, landline	5%	2%
Yes, both	6%	3%
No	49%	46%
Never heard of (VOL)	12%	17%

Registered on the Federal Do-Not-Call list

	Military/ Veterans (851 adults 18+)	Civilians (809 adults 18+)
Yes, cell phone	30%	27%
Yes, landline	14%	11%
Yes, both	23%	16%
No	27%	34%
Never heard of (VOL)	5%	10%

Q23. Do you currently use a robocall blocking service on your cell phone or your landline phone?

Q24. Have you ever registered either your cell phone or your landline on the federal government's Do-Not- Call list?

Likewise, installing and updating protective software on all electronic devices helps protect those devices from criminal intrusion. A security freeze placed on the credit reports at each major credit bureau makes it virtually impossible for someone to use another’s identity illegally to open new accounts. While most respondents in both samples have installed protective software on their electronics, nearly one in five haven’t, thus significantly elevating the risk of criminal intrusion. And most have not place a security freeze on any or each of their credit reports with the three major credit bureaus

Installed Protective Software Devices and Computers

	Military/ Veterans (851 adults 18+)	Civilians (809 adults 18+)
Yes, on all	48%	40%
Yes, on some	30%	31%
No	19%	25%
Never heard of (VOL)	2%	3%

Identity Theft Protection: Security Freeze Placed w/Three Major Credit Bureaus

	Military/ Veterans (851 adults 18+)	Civilians (809 adults 18+)
Yes, w/all three	11%	7%
Yes, not all	7%	6%
No	81%	85%
Never heard of (VOL)	1%	1%

Q23. Do you currently use a robocall blocking service on your cell phone or your landline phone?

Q24. Have you ever registered either your cell phone or your landline on the federal government’s Do-Not- Call list?

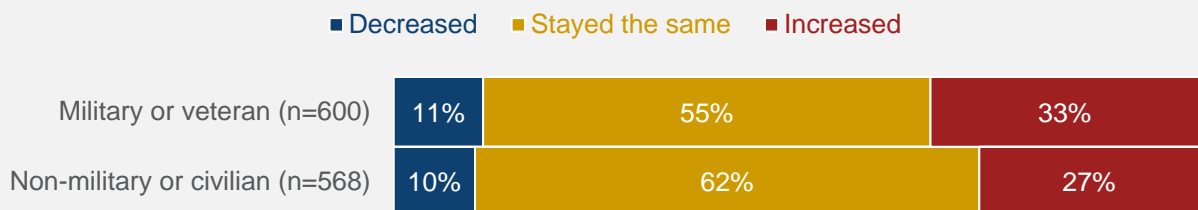
Verifying A Charity Will Help More Military/Veteran and Civilian Adults Avoid Bogus Donation Requests

Fraudulent charities not only steal money from donors; they divert needed support away from legitimate charitable causes. Both military/veterans and civilians report they have been asked at some point to donate money to a charity or cause (70% and 68%, respectively), and many of them say that the number of charitable requests they've received in the past twelve months has increased.



Change in number of charity requests

In the past 12 months



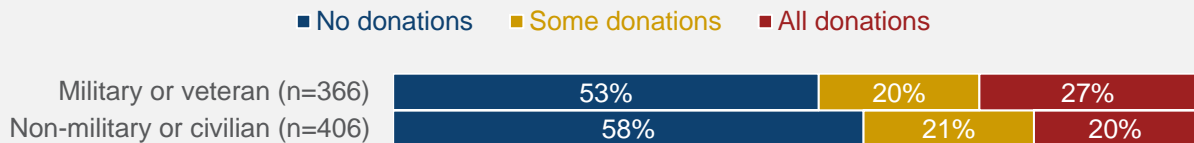
Q14. Have you ever been contacted by someone ...asking you to donate money to a charitable organization or cause such as....?

Q18. [if yes to Q14] In the past 12 months, would you say the number of requests from charities for donations from you has increased, stayed the same, or decrease?

At least two in five military/veteran and civilian adults have made a monetary donation to a charity or cause in just the past twelve months. Yet, it's hard to be sure donations are truly going to the cause, and if so, how much is going to the cause if the giver doesn't do a little research first. For example, when asked how many of their donations were made *after* asking how much would go to the cause and how much would go to the fundraiser, more than half of both military and civilian adults have never asked this question.

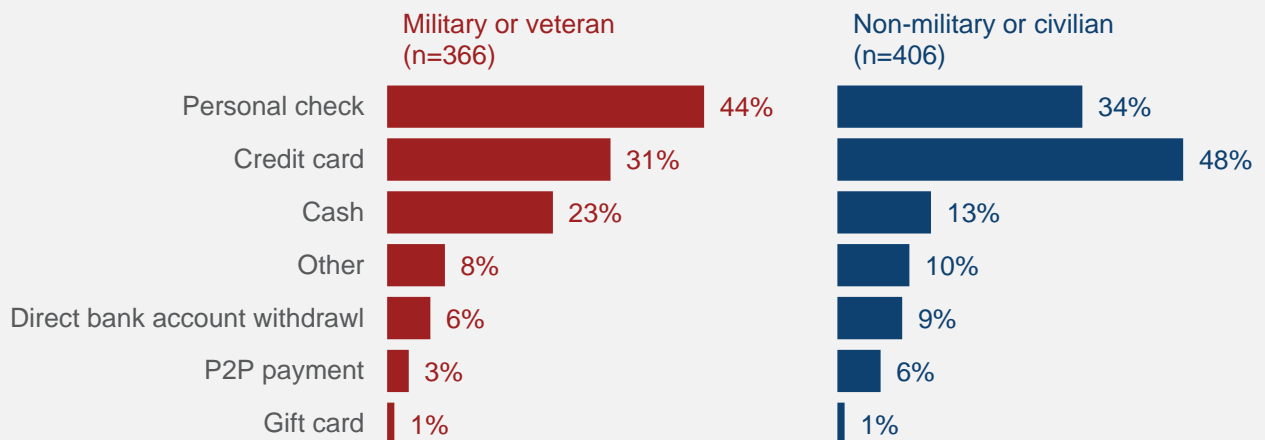
Made donation *after* asking how it would be distributed

Among those who made donations



How donations were paid for

Among those who made donations



Scammers know veterans remain true to the men and women who serve. They will make up fake charities that have the word “veteran” in them or they’ll use a name that closely resembles a real charity. Before donating to a charitable cause, check out the organization. There are several ways to do that online, including Give.org, [Charitywatch.org](https://www.charitywatch.org) and [Charitynavigator.org](https://www.charitynavigator.org)

Q16. And how did you make your donation?

Q17. Thinking again about those donations you made during the past 12 months, how many of them would you say were made after you asked how much of your donation would go to the fundraiser and how much would go to the charity itself?



SCAM PREVENTION TIPS AND RESOURCES

Stay vigilant and fight back!

Knowledge gives you power over scams. The AARP Fraud Watch Network equips you with reliable, up-to-date insights, alerts and [fraud prevention resources](#) to help you spot and avoid scams and protect your loved ones. If you've been targeted by scams or fraud, you are not alone. Our trained fraud specialists provide support and guidance on what to do next and how to avoid scams in the future. The [AARP Fraud Helpline](#), 877-908-3360, is free and available to anyone. We also offer [online support sessions](#) for further emotional support.

Veterans never have to pay for their own service records, if told otherwise, it's a fraud or scam!

The U.S. Department of Veterans Affairs (VA) and Federal Trade Commission (FTC) offer these 7 tips about being contacted about your government or military-service benefits:

- Look out for unsolicited call offers to help you increase your benefits or access little-known government programs. **These are likely scams!**
- Don't **pay for copies of your military records**. You can get them for free through VA.
- VA may check in with you by phone or email. If you are unsure about the caller, hang up and call the agency directly at **1-800-MyVA411** (1-800-698-2411).
- VA representatives will also not 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!**
- Be cautious of telephone numbers on your caller ID. Scammers can change the telephone number (**ID spoofing**) to make a call appear to come from a different person or place, or someone you know.
- VA **does not threaten claimants** with jail or lawsuits.
- Use **VA-accredited representatives** to help you with any benefits issues. The VA maintains a [searchable database](#) of attorneys, claims agents and veterans service organizations (VSOs).

Source: AARP Fraud Watch [Resource Center](#), The U.S. Department of Veterans Affairs, and the Federal Trade Commission

A photograph of a middle-aged Black man with a goatee, wearing a light blue button-down shirt, sitting at a desk. He is looking off to the side with a thoughtful expression. A laptop is open in front of him, and his hands are resting on the keyboard. In the background, there is a mannequin wearing a patterned jacket, and a window with light coming through. A white horizontal bar is overlaid on the bottom half of the image, containing the text 'STUDY METHODOLOGY' in red.

STUDY METHODOLOGY

Study Methodology

AARP commissioned NORC AmeriSpeak to conduct an online survey of active and former U.S. military and non-military (civilian) adults ages 18 and older in August 2021. The sample was drawn from NORC's AmeriSpeak Panel. In total, NORC collected 1660 interviews: 1546 by web mode and 114 by phone mode. The final data was weighted via a raking ratio method separately to non-military age 18+ population totals, and current and former military totals associated using the following variables: age, gender, education, race/Hispanic ethnicity, and Census Division. Due to rounding, percentages may not always sum to 100%. The final sample of 851 Veteran and active military respondents yielded a margin of error of 3.76 percent and the final sample of 809 not-veteran or civilian respondents yielded a margin of error of 4.40 percent at the 95% confidence level.

For brevity in describing the findings for active-duty military and veterans, this report uses 'military/veterans' or 'military/veteran adults' as an abbreviated label as the sample for this group consists of both active and veteran military adults.



For more information about this survey or the methodology, please contact Jennifer Sauer at jsauer@aarp.org

For media inquiries, please contact Emily James, AARP External Relations, at media@aarp.org

<http://www.aarp.org/veterans>