Syracuse University
D'Aniello Institute for Veterans & Military Families
JPMorgan Chase & Co., Founding Partner

RESEARCH & ANALYTICS

RESEARCH REPORT | JANUARY 2023

Cybercrime Risk in the Military Community: WHAT DO WE KNOW?

COMCAST

ACKNOWLEDGMENT

This report is published by Syracuse University's D'Aniello Institute for Veterans and Military Families (IVMF). This research is funded by Comcast to conduct a study on the prevalence of cybercrimes on military families. The contents of this publication are solely the responsibility of the authors. Any views expressed in this paper are of the authors only.

ABOUT SYRACUSE UNIVERSITY'S D'ANIELLO INSTITUTE FOR VETERANS AND MILITARY FAMILIES (IVMF)

Syracuse University's D'Aniello Institute for Veterans and Military Families (IVMF) was founded in 2011, as a partnership between Syracuse University and JPMorgan Chase & Co. Headquartered on the campus of Syracuse University and located in the Daniel and Gayle D'Aniello Building at the Syracuse University National Veterans Resource Center, the IVMF was founded as higher-education's first interdisciplinary academic institute singularly focused on advancing the lives of the nation's military, veterans, and their families. The IVMF team designs and delivers class-leading training programs and services to the military-connected community, in support of the transition from military to civilian life and beyond. Each year, more than 20,000 service members, veterans, and family members engage IVMF programs and services, which are provided at no cost to participants. The IVMF's programs are informed by the Institute's sustained and robust data collection, research, and policy analysis team and infrastructure. The D'Aniello Institute's work on behalf of the military-connected community is made possible by gifts and grants from individuals and corporations committed to those who served in America's armed forces and their families. For more information, please visit ivmf.syracuse.edu

ABOUT COMCAST CORPORATION

Comcast Corporation (Nasdaq: CMCSA) is a global media and technology company that connects people to moments that matter. We are principally focused on connectivity, aggregation, and streaming, with 57 million customer relationships across the United States and Europe. We deliver broadband, wireless, and video through our Xfinity, Comcast Business, and Sky brands; create, distribute, and stream leading entertainment, sports, and news through Universal Filmed Entertainment Group, Universal Studio Group, Sky Studios, the NBC and Telemundo broadcast networks, multiple cable networks, Peacock, NBCUniversal News Group, NBC Sports, Sky News, and Sky Sports; and provide memorable experiences at Universal Parks and Resorts in the United States and Asia. Visit www.comcastcorporation.com for more information.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In 2021 alone, military consumers reported losing over $267 million to fraud.[1] That same year, the general population also saw increases in consumer fraud. Cybercriminals continue to exploit vulnerabilities and misuse digital information to commit crimes such as phishing scams, identity fraud, and financial fraud. This is unsurprising given the near universal public reliance on the internet, meager cybercrime awareness, and technology outpacing adoption of widespread prevention and security measures.[2] Furthermore, breaches of personal data are on the rise as sensitive data are more frequently collected, stored, or shared digitally through internet transactions (e.g., names, email addresses, phone numbers, login credentials).[3] Such aggregated, sensitive data become easy and valuable targets for opportunistic criminals to commit identify theft and other lucrative, yet difficult to detect, cybercrimes.[4]

Knowing the full scope of this problem without greater consistency in cybercrime reporting is nearly impossible.[5] For example, the FBI estimates that only 15% of American fraud victims report these crimes to law enforcement.[6] Cybercrimes go unreported often because victims either never recognize they have been victimized, perceive nothing can be done, or do not know what amounts to a crime.[7] Improvements to cybercrime classification, data collection, and reporting are necessary. Also needed is a better understanding of how cybercrimes impact vulnerable groups.

Some data suggest that members of the military community are disproportionately impacted by cybercrime, report more incidents, and incur greater losses.[8] Although the overall rate of cybercrimes has increased in recent years within the U.S. and globally, there are several reasons to speculate on why military-connected persons might be targeted. Like civilians, service members, veterans, and their families rely on the internet to conduct professional and personal business, connect socially, store information, and manage their personal finances.[9] Unlike civilians, however, military members and their families also move frequently, have access to valuable military conferred benefits (e.g., retirement, education, health care), and exhibit more trust of philanthropic organizations, making them easy targets for scammers. Moreover, deployed service members often experience greater difficulty to continuously monitor suspicious activity on their accounts.[10] Finally, military-connected individuals are inevitably required to provide sensitive and personal identifying information for security clearances and to prove eligibility for benefits and resources.[11]

Information and evidence pertaining to military-connected cybercrimes remain limited. While not exhaustive, this paper offers a first step to assess the following:

- what is known about military-specific cybercrimes;
- gaps and limitations of existing data and areas for improvement;
- potential factors that increase cybercrime vulnerability among military-connected individuals and small business owners;
- existing efforts and policy change to improve data and information on military-connected cybercrime; and
- cybercrime prevention resources and services for victims.

Recommendations

Overall, the widespread lack of data impedes effort to control and defeat cybercrime. Congress has passed legislation to enable better data collection, improve government coordination, and ensure a common language that describes cybercrime. Yet, more immediate solutions to educate and protect potential victims are needed. The U.S. government has an obligation to ensure military veterans and their families receive the education, information, and other measures to reduce cybercrime risk and prevent financial losses. Those resources should be targeted to specific subgroups based on status (i.e., active duty vs. veteran) and other risk factors, highlighting prevention measures individuals can take to protect themselves, their data, and their finances.

Additional recommendations for federal leaders and the military community include the following:

- Government agencies, the private sector, and military-connected nonprofits should form stronger partnerships to improve information sharing, coordination, and policy making.
- Government and/or private sector champions should convene key stakeholders to develop and implement new solutions to better inform and address cybercrime threats in the military community (e.g., FTC, DoD, VA, AARP, Cyber Crime Support Network, etc.).
- Senior government leaders should partner with cybersecurity experts to develop and disseminate information that arms the military community with the latest and best practices to reduce vulnerabilities to cybercrime.
- VA should seek opportunities to increase engagement with veterans about how to protect their benefits and avoid phishing schemes and scams.
- DoD should identify critical moments throughout a service member's career journey to increase awareness of cybercrime.
- Tailor cybercrime resources and programs that meet the needs of different groups, including active-duty service members, veterans, and military family members, and considers related demographic, location, and information accessibility factors.
- Include cybersecurity information and resources related to small business.
- Offer opportunities for the military community (including family members) to receive cybersecurity training that emphasizes the risks of cybercrime are underestimated.
- Encourage and enable military-connected reporting to provide a better estimate of the scope of the problem.

Cybercrime in the Military Community:

A SNAPSHOT

RISKS TO MILITARY COMMUNITY

- security clearances
- threat or blackmail exposure
- benefit access and eligibility
- long-term mental, emotional, financial well-being
- reputational harm for individuals and businesses [18]
- lifestyle-specific vulnerabilities (relocations, deployments)

DRIVERS OF CYBERCRIME UNDERREPORTING[19]

- undetected/unrecognized crimes
- shame or embarrassment (e.g., romance scams)
- reputational harm (personal or business)
- low confidence in law enforcement
- perceived barriers to reporting
- lack of awareness on how to report

CYBERCRIMES MAY BE PREVENTABLE BY

- ✓ Helping service members, veterans, and their families understand and anticipate how they might be targeted; [20]
- ✓ Monitoring who is targeted and why to inform and improve prevention and intervention efforts; and
- ✓ Knowing which groups or individual circumstances are at greater risk to attacks to tailor more targeted communications efforts and prevention strategies.

PREVENTION IS KEY TO AVOIDING CYBER-VICTIMIZATION

- ✓ Be informed and take proactive steps to mitigate personal risk
- ✓ Tailor information awareness and prevention strategies to those at greatest risk
- ✓ Strengthen data collection and monitoring to support agency leadership decision making and smart policy to support cybercrime prevention

LEARN ABOUT SOCIAL ENGINEERING TACTICS USED BY CYBERCRIMINALS SO YOU CAN AVOID THEM

Cybercriminals use their social skills to deploy tactics known as social engineering, used to manipulate victims into providing information or access. Social engineering uses social interaction to deceive or convince persons into divulging confidential or personal information that are then used for fraudulent purposes.[21]

For information visit, https://www.cisa.gov/uscert/ncas/tips/ST04-014

Resources are available, but victims may not know about them. For more information, see the Resources section of this paper.

INTRODUCTION

In 2015, the U.S. Office of Personnel Management (OPM) announced a significant data breach involving personnel data for current and former federal employees.[12] This incident revealed publicly the risk and vulnerability that even service members, veterans, and their families face with cybercrime.[13] The OPM data breach included sensitive background investigation records for 21.5 million users: 19.7 million individuals who had applied for a background investigation and 1.8 million spouses or co-habitants of applicants.[14] Among other sensitive information, the stolen records included full names, birth dates, home addresses, and social security numbers as well as details about prospective employees' personal life, mental health information, family members, and other personal contacts.[15]

One outcome of the OPM breach was that it shined a national spotlight on the impact of cybercrime as the DoD, Congress, and others considered how personal data from military-connected persons could be misused through blackmail, damaged credit, or other financial or social harm (e.g., harassment).[16] The OPM breach simultaneously magnified the cybersecurity gaps related to government data and caused more specific concern that military-connected individuals, including veterans and family members, were vulnerable to identity theft, fraud, or worse.[17]

WHAT IS CYBERCRIME?

Cybercrime definitions vary depending on the source, but generally, cybercrime refers to any criminal activity that either targets or uses a computer, computer network, or a networked device to commit other crimes (e.g., through damage or intrusion).[22] Cybercrimes can also be supported through technology and might include the use of computers to conduct illegal activities such as fraud or identity theft, among others. Cybercrime is often preceded by theft or fraud and may take many different forms. It may also involve the commission of multiple crimes simultaneously.[23] For example, a criminal might infiltrate a computer or network, develop malicious software, and use social engineering techniques.[24] Due to overlaps, it may require legal discretion to ascertain or categorize each crime that is committed.[25] Additionally cybercrimes encompass a multitude of crimes, among them theft of data, romance scams, cyberextortion, phishing, cyberstalking, identity theft, and malware attacks.[26]

For information about different types of cybercrimes, how to seek help, and how to report a cybercrime please visit https://fightcybercrime.org/scams/

PREVALENCE OF CYBERCRIME

Internet crime has increased in tandem with pervasive use of email, social media, the internet, online data storage, and increased networked activity. Besides the rise in cybercrime victims overall, cybercrime victims may also incur significant financial consequences if their personal or financial information is misused for criminal purposes.[27]

What's The Difference Between Cybercrime and Fraud?[28]

The rise of cybercrimes has blurred the definition between fraud and cybercrimes, and research on cybercrime often does not distinguish between the two.

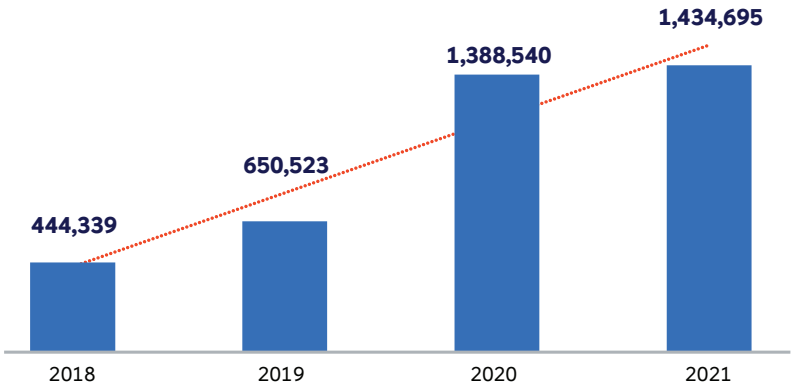
The two crimes overlap, but they are also different. Fraud is committed for financial gain, but cybercrime may be executed for many reasons, including political, passion, opportunism, or to exploit a vulnerability.

There are two additional differences: the skills needed to manage the types of threats and the way each crime is carried out; cybercrimes inherently involve the use of a computer.

Many of the same tools and measures are used to address both types of crime, but detection, manage and control of one crime doesn't necessarily influence the ability to detect, prevent or manage the impact of the other.

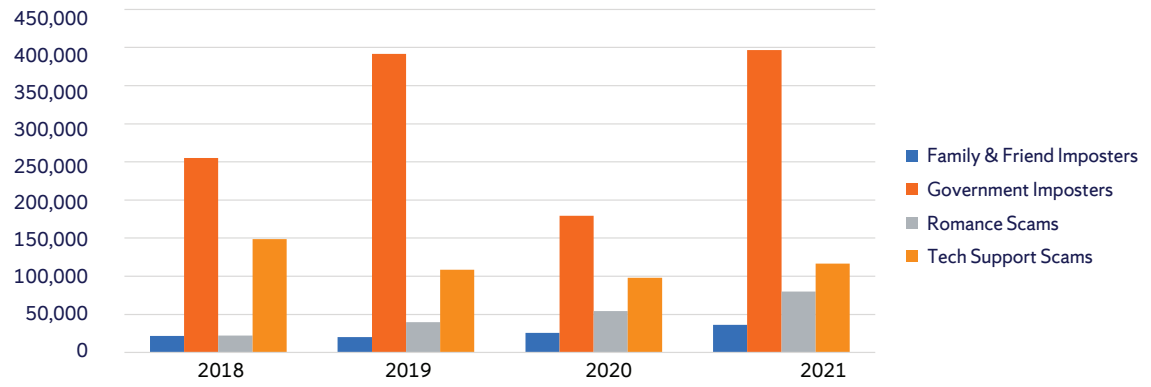
Figure 1: FTC Consumer Reports of Identity Theft (2018-2021)

IDENTITY THEFT INCIDENTS HAVE INCREASED OVER TIME. LARGER INCREASES WERE SEEN IN 2020, COINCIDING WITH THE COVID-19 PANDEMIC.



Note: Total population, number of reports of identity theft
According to the FTC, identity theft is when someone uses your personal or financial information without your permission. They might steal your name and address, credit card or bank account numbers, Social Security number, or medical insurance account numbers.
Source: Adapted from: Federal Trade Commission, The Big View: All Sentinel Reports 2018-2021. Retrieved from https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports

Figure 2: FTC Consumer Reports of Imposter Scams (2018-2021)



Note: Total population, number of imposter scams report
Source: Adapted from: Federal Trade Commission, The Big View: All Sentinel Reports 2018-2021. Retrieved from https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports

Figure 3: FTC Top Identity Theft Types by Number of Consumer Reports (2021)

Note: Total population, number of report by identity theft types
Source: Adapted from: Federal Trade Commission, The Big View: All Sentinel Reports 2021. Retrieved from https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports

IN 2021 THE FTC REPORTED IDENTITY THEFT AS THE TOP FRAUD CATEGORY WITH 1,434,693 TOTAL IDENTITY FRAUD REPORTS. THE TOP TWO TYPES OF IDENTITY THEFT INCLUDE GOVERNMENT DOCUMENTS/BENEFITS FRAUD AND CREDIT CARD FRAUD.

Table 1: FTC Top 10 Fraud Categories, Number of Reports, and Monetary Losses (2021)

	Category	# of Reports	% Reporting $ Loss	Total $ Loss	Median $ Loss
1	Imposter Scams	995,789	17%	$2,399.5M	$1,000
2	Online Shopping and Negative Reviews	410,399	51%	$393.5M	$150
3	Prizes, Sweepstakes and Lotteries	154,785	12%	$263.1M	$980
4	Internet Services	106,246	23%	$222.6M	$500
5	Business and Job Opportunities	104,288	25%	$208.7M	$1,995
6	Telephone and Mobile Services	97,977	11%	$21.5M	$250
7	Investment Related	81,923	72%	$1,770.3M	$3,000
8	Health Care	68,924	12%	$17.6M	$198
9	Travel, Vacations and Timeshare Plans	62,196	21%	$95.8M	$1,111
10	Foreign Money Offers and Fake Check Scam	39,113	26%	$78.1M	$2,000

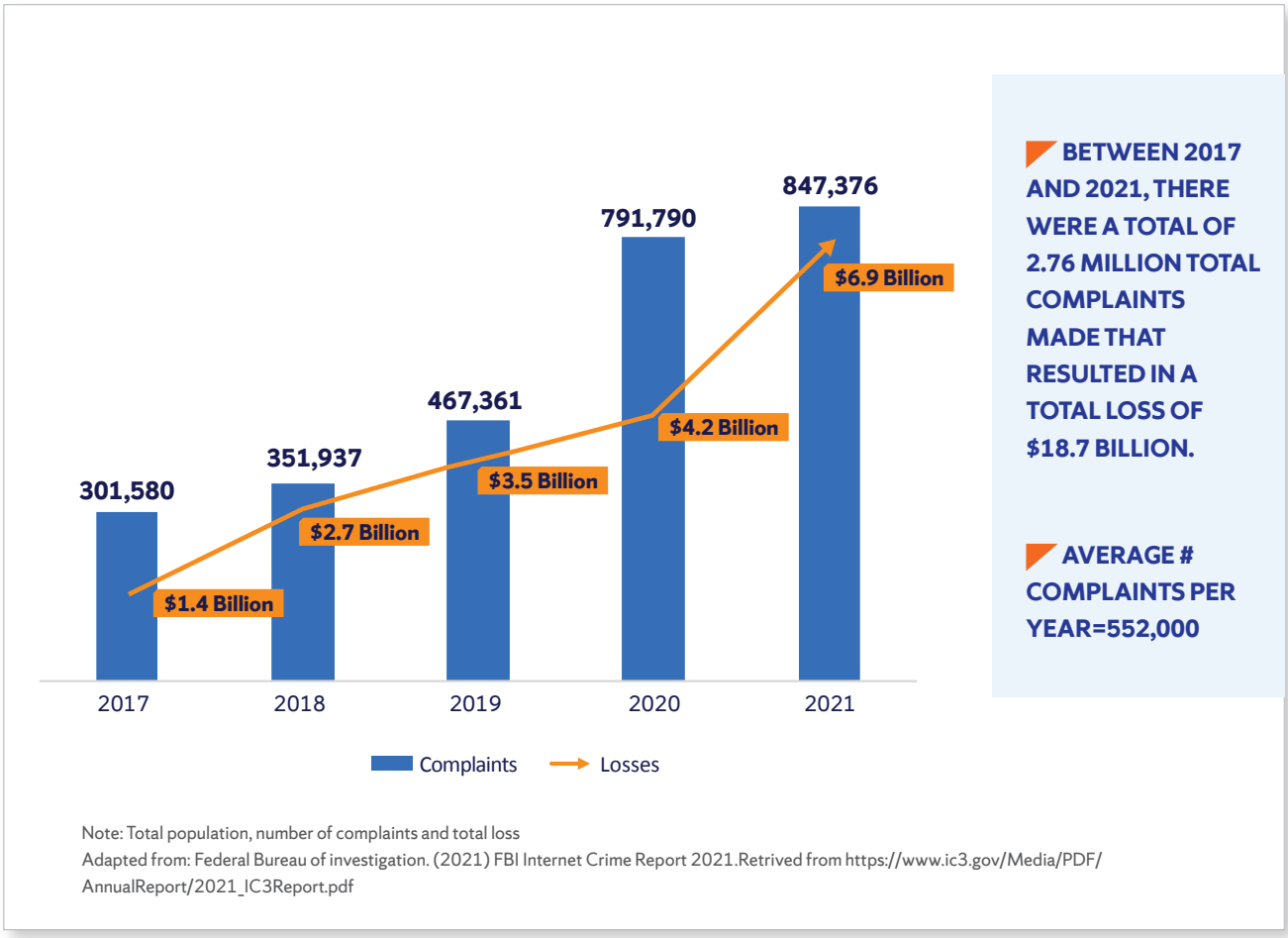
Note: Total population, number of report, percentage reporting a loss based on number of report, total loss, and median loss
Source: Adapted from: Federal Trade Commission, The Big View: All Sentinel Reports 2021. Retrieved from https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports; downloaded October 5th, 2022

Federal Trade Commission Definitions:

- Imposter Scams - Someone pretends to be a trusted person to get consumers to send money or give personal information. Examples include scammers claiming to work for or be affiliated with a government agency; scammers posing as a friend or relative with an emergency need for money; scammers posing as a romantic interest; scammers claiming to be a computer technician offering technical support; and scammers claiming to be affiliated with a private entity (e.g., a charity or company).
- Online Shopping and Negative Reviews - Undisclosed costs, failure to deliver on time, non-delivery, and refusal to honor a guarantee on purchases made online; internet auctions (starting October 22, 2020).
- Investment Related - Investment opportunities in day trading; gold and gems; art; rare coins; other investment products; reports about companies that offer advice or seminars on investments; etc.
- Business and Job Opportunities - Business opportunities (e.g., offers to start a new business); work-at-home plans, (e.g., stuffing envelopes or processing medical claims); multi-level marketing schemes; job scams, job listings, or employment services; inventions or idea promotions.
- Internet Services - Problems with webstite content, including websites that offer content for a fee or advertise products and services; difficulty canceling an ISP or online account; issues with online payment services, social networking services; undisclosed charges; and website design and promotion services.
- Telephone and Mobile Services - Advertising related to mobile plans, rates or coverage areas; problems with mobile applications or downloads; other mobile device problems; charges for calls to “toll-free” numbers; unauthorized charges, such as charges for calls consumers did not make; unauthorized switching of consumers’ phone service provider; misleading pre-paid phone card offers; VoIP service problems; unsolicited faxes; etc.
- Health Care - Fraudulent, misleading or deceptive claims for: dietary supplements; weight loss products or services; impotency treatments; health spas and equipments; infertility services; sunscreens; HIV test kits; as well as complaints about over-the-counter or prescription drugs.
- Travel, Vacations and Timeshare Plans - Deceptive offers for “free” or low-cost vacations; cut-rate student travel packages; misleading timeshare offers; etc.
- Prizes, Sweepstakes and Lotteries - Promotions for “free” prizes for a fee; foreign lotteries and sweepstakes offered through the phone, fax, e-mail or mail; etc.
- Foreign Money Offers and Fake Check Scams - Letters or e-mails promising a percentage of millions of dollars that from a foreign country in return for money, bank account numbers or other identifying information from the victim; fraudulent schemes involving foreign lotteries, mystery shoppers or internet purchases\classified ads in which someone is overpaid with a counterfeit check and asked to wire back the difference immediately after check deposit, leaving the victim responsible for the funds withdrawn; etc.

According to the FBI's Internet Crime Complaint Center (IC3) Annual Report from 2021, there were nearly 52,000 reports of personal data breaches.[29] Phishing (sending intentionally disguised emails to deceive and solicit personal information such as passwords or credit card numbers) and similar fraud were most frequent type of cybercrime reported and impacted approximately 324,000 individuals.[30] Similarly, FTC received 2.8 million fraud reports in 2021.[31] Consumers reported losing more than $5.8 billion, an increase of more than 70% over 2020. Impostor scams have consistently been the most frequently reported reason for fraud loss among FTC consumers, and they reported losing more than $2.3 billion, an increase of $1.2 billion from 2020.[32] In 2021, consumers reported a median loss of $1,000. Impostor scams have remained the top fraud loss among consumers since 2018. The second highest number of fraud reports were related to online shopping. Fifty-one percent of consumers making reports to the FTC reported losing money with a median loss of $150. While there are fewer reports of investment scams, the loss to each consumer is significantly larger than other types of fraud, with a median loss of $3,000 in 2021.[33]

Figure 4: FBI's U.S. Internet Crime Complaint Center (IC3) of Complaints and Losses (2017-2021)



Note: Total population, number of complaints and total loss
Adapted from: Federal Bureau of investigation. (2021) FBI Internet Crime Report 2021.Retrived from https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

IMPROVING DATA AND REPORTING OF CYBERCRIME

The problems with cybercrime data are widely recognized and those issues are not exclusive to the military community. To that end, in 2022 members of Congress passed legislation that became law on May 5. Known as the Better Cybercrime Metrics Act, "this bill establishes various requirements to improve the collection of data related to cybercrime and cyber-enabled crime." Requirements of the legislation include specific tasks for federal organizations to carry out and improve how the government tracks, measures, analyzes, and prosecutes cybercrime.[34]

Better Cybercrime Metrics Act

The law is designed to address some of the concerns related to interagency coordination, cybercrime definitions, and data collection. The law includes provisions that engage the Department of Justice, the National Academy of Sciences, and the Government Accountability Office, among other agencies. Those provisions include the following:

1. The Department of Justice (DOJ) must work with the National Academy of Sciences to develop a taxonomy for categorizing distinct types of cybercrime faced by individuals and businesses.
2. DOJ must establish a category in the National Incident-Based Reporting System for collecting cybercrime reports from federal, state, and local officials.
3. DOJ's Bureau of Justice Statistics and the Bureau of the Census must include questions about cybercrime in the annual National Crime Victimization Survey.
4. The Government Accountability Office (GAO) must assess the effectiveness of reporting mechanisms for cybercrime and disparities in reporting cybercrime data and other types of crime data.

Source: S.2629 - 117th Congress (2021-2022): Better Cybercrime Metrics Act. (n.d.). Retrieved October 5, from https://www.congress.gov/bill/117th-congress/senate-bill/2629.

CYBERCRIME IN THE MILITARY COMMUNITY: WHAT WE KNOW

Information on cybercrime in the military community lies with only two sources: the Federal Trade Commission (FTC) and the AARP. Both have collected data that specifically examine cybercrime and fraud in the military community. Existing data is sparse and subject to interpretation for several reasons.[35] First, the limitations in both FTC and AARP data reflect the challenges of collecting reliable and accurate cybercrime data more broadly. For instance, data on cybercrime is not necessarily representative because it is based on the self-report of victims. Additionally, cyber reporting is decentralized, as victims can potentially report to several different agencies. For example, some crimes are reported to the FTC, while others are reported to the FBI. Data silos create barriers to accurately estimating or interpreting the magnitude of the cybercrime problem. Another challenge is that cybercrime is thought to be underreported, with many victims not reporting at all.[36] The following table outlines some of the challenges related to cybercrime data, definitions, and response.

Table 2: Central Challenges with Cybercrime [37]

CHALLENGE	DESCRIPTION
Reporting	• Decentralized reporting (no single entity for reporting). • Self-report bias (e.g., people might over- or under-report) • 15% of American fraud victims report to law enforcement, thus hard to know the full scope of the problem[38]
Adequate law enforcement capabilities	• Difficult to train and retain investigators, prosecutors, and examiners with the specialized skills needed to address cybercrime • Cyber criminals mask identities and evade detection by law enforcement • Individuals must take responsibility to protect themselves
Jurisdictional issues	• Cybercrime crosses national and state borders and thus legal jurisdictions, further complicating investigation and legal action.
Limited awareness or knowledge of cybersecurity risk	• Despite efforts to raise awareness, organizational and individual information security remain at risk, particularly through the pervasive use of internet transactions containing sensitive data. • Despite some evidence of improving consumer awareness of cybercrime, there is also evidence that consumers do not consistently utilize the tools that could prevent cybercrimes. • One survey showed that over a quarter of adults in the United States use the same password for all their online logins. [39]
No central clearinghouse for reliable resources or best practices	• Many consumer resources are provided by cybersecurity companies selling products, making it hard to determine information reliability or objectivity.
Pace of technological advancement	• Criminal innovation outpaces prevention activities, law enforcement, and policy.
Classifications of crimes	• Poor definitions of cybercrime due to overlap with other types of crime, inconsistency, and self-report data collection.

SOURCES OF MILITARY DATA

Federal Trade Commission Data

The Federal Trade Commission (FTC) is the only federal agency that regularly collects self-report data identifying military-connected cybercrimes, in some cases, distinguishing between demographic categories of veteran, active-duty, active-duty dependents, and Guard and reservists.[40]

AARP has also administered surveys to examine fraud in the military community. Its data focuses on fraud but also includes cybercrime and compares military and civilians.[41] The findings from both sources, despite limitations, share similarities, both suggesting some military-connected individuals may be more vulnerable to cybercrime and in some cases, suffer greater financial losses.

When comparing military-connected individuals with overall cybercrime rates have led to speculation and concerns about whether military-connected persons are unusually vulnerable to cybercrime (e.g., identify theft) compared to the general population.[42] Several researchers have noted, for example, that events intrinsic to the military lifestyle—such as relocations, deployments and accessing valuable government—benefits may increase cybercrime vulnerability. This may be due to less frequent account or credit score monitoring or special circumstances related to the military lifestyle that present opportunities for criminal exploitation (e.g., unemployment, government benefits eligibility, or family or friends serving as financial custodians during deployments).[43]

FTC REPORTS THAT FROM 2018 TO 2021, REPORTS FROM THE MILITARY AND VETERAN COMMUNITY NEARLY DOUBLED (125K TO 206K) AND MONETARY LOSSES REPORTED BY MILITARY CONSUMERS TRIPLED ($81M TO $266M)

Table 3: FTC Military Consumer Reports of Number of Reports and Percentage Reporting Fraud Loss (2018 to 2021)

	Active Duty Service Member		Spouse/Dependent		Military Retiree/Veteran		Reserve/National Guard	
	# of reports	% fraud loss	# of reports	% fraud loss	# of reports	% fraud loss	# of reports	% fraud loss
2018 →	9,064	26%	25,736	14%	84,327	14%	5,907	18%
2019 →	12,052	19%	25,267	12%	79,706	14%	6,356	16%
2020 →	12,523	39%	18,890	25%	114,906	22%	7,658	30%
2021 →	18,564	38%	14,868	34%	162,555	24%	10,915	34%

Note: Military population, number of reports (includes fraud, identity theft, and other report) and percentage fraud loss based on fraud number of reports

Source: Adapted from Federal Trade Commission, Fraud, Identity Theft, and Other Reports by Military Consumers. Top Reports 2021. Retrieved from https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports

FTC's Consumer Sentinel Network

The FTC's Consumer Sentinel Network (also known as Sentinel), considered to be an investigative cybercrime tool, is the mechanism used to collect cybercrime data.[44] Specifically, the FTC receives reports directly from consumers; federal, state, and local law enforcement agencies; the Better Business Bureau; industry members; and nonprofit organizations.[45] The FTC uses the reports to initiate many of its law enforcement investigations and shares these reports with approximately 2,800 federal, state, local, and international law enforcement professionals. These reports are considered a critical aspect of the FTC's law enforcement mission involving consumer protection because they are used to curtail illegal activities or provide refunds to consumers.[46]

Sentinel received more than 5.7 million reports in 2021 and includes data from 25 states.[47] The data collected includes fraud reports, identity theft reports, and complaints related to consumer issues, including issues with credit bureaus, banks, and lenders.[48] In 2021, the FTC received nearly 1.4 million reports of identity theft.[49] From 2018 to 2021, reports to the FTC from the military and veteran community nearly doubled, from 125,000 reports to 206,000 reports.[50] And monetary losses reported by military consumers tripled, from $81 million to $266 million in the same period.[51]

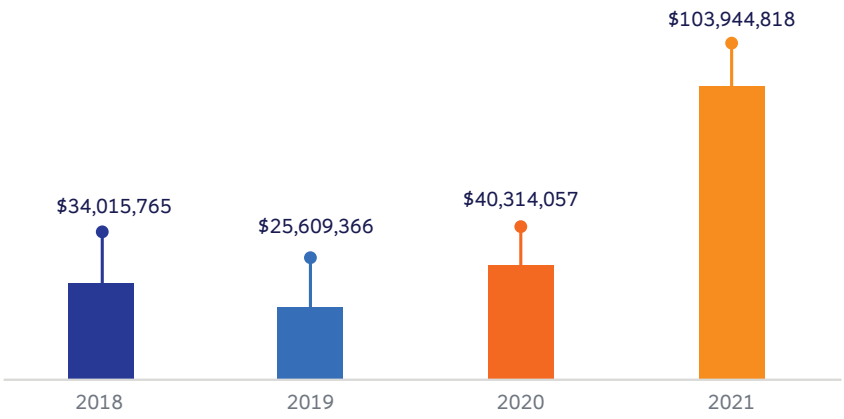
MANY SCAMS ARE ALSO CONSIDERED CYBERCRIMES BECAUSE THEY OCCUR WITH THE AID OF A COMPUTER OR THROUGH THE INTERNET.

According to **Military.com**, some of the most common cyber scams affecting the military community include:

- Sextortion scams - Claim to have explicit photos and threaten to release them unless money is received.
- Romance imposter scams - Fake profiles created on dating websites and used to target service members, veterans, or their families for financial gain.
- Real-estate scams - Fake rental homes that are posted online and demand cash security deposits for rental.
- Family or friend imposter scams - An email that claims to be from a family member or friend who is in trouble and needs money.
- GI Bill scams - Fraudulent schools created to take GI Bill money but do not provide education or present a degree.
- Charity scams - Charities claim to support military- or veteran-related causes but do not.
- Fake job scams - Nonexistent jobs that are offered to military families or veterans and then steal personal information when a person applies for that position.
- DFAS phishing scams - Fake emails supposedly sent from the **Defense Finance and Accounting Service**, which attempt to steal personal or financial information.

Adapted from: Absher, J.(13, April, 2021). *New Partnership Battles Cybercrime Targeting Military and Veterans. Military.com*, https://www.military.com/money/personal-finance/2021/04/13/new-partnership-battles-cybercrime-targeting-military-and-veterans.html; Stouffer, C. (7, November, 2022). *Romance scams in 2023: What you need to know + online dating scam statistics*, https://us.norton.com/internetsecurity-online-scams-romance-scams.html; Alkhalil Z, Hewage C, Nawaf L and Khan I (2021) *Phishing Attacks: A Recent Comprehensive Study and a New Anatomy*. Front. Comput. Sci. 3:563060. doi: 10.3389/fcomp.2021.563060

Figure 5: FTC Military Consumer Total Loss of Imposter Scams (2018-2021)



IMPOSTER SCAMS WERE THE TOP FORM OF FRAUD REPORTED BY MILITARY CONSUMERS, WHO REPORTED LOSSES OF NEARLY $204 MILLION BETWEEN 2018 AND 2021. THIS IS COMPARED TO MORE THAN $5 TRILLION LOST BY ALL CONSUMERS. THE MEDIAN LOSS STEADILY INCREASED FROM $500 IN 2018 TO $1,000 IN 2021.

Note: Military population, total loss of imposter scams
FTC Defines an impostor scam as "Someone pretends to be a trusted person to get consumers to send money or give personal information. Examples include scammers claiming to work for or be affiliated with a government agency; scammers posing as a friend or relative with an emergency need for money; scammers posing as a romantic interest scammer; claiming to be a computer technician offering technical support; and scammers claiming to be affiliated with a private entity e.g., a charity or a company." Adapted from: Federal Trade Commission, The Big View: All Sentinel Reports 2018-2021. Retrieved from https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports

Table 4: FTC Top 10 Military Fraud Categories, Number of Reports, and Monetary Losses (2021)

	Category	# of Reports	% Reporting $ Loss	Total $ Loss	Median $ Loss
1	Imposter Scams	44,040	20%	$103.9M	$1,030
2	Online Shopping and Negative Reviews	18,314	63%	$29.6M	$178
3	Prizes, Sweepstakes and Lotteries	5,201	19%	$23.7M	$2,000
4	Business and Job Opportunities	4,563	22%	$12.9M	$2,395
5	Investment Related	3,089	76%	$49.5M	$3,000
6	Foreign Money Offers and Fake Check Scams	2,447	28%	$7.8M	$2,498
7	Telephone and Mobile Services	2,305	28%	$2.3M	$225
8	Internet Services	1,781	16%	$2.0M	$500
9	Health Care	1,768	11%	$1.9M	$267
10	Mortgage Foreclosure Relief and Debt Management	1,257	24%	$4.6M	$1,120

Note: Military population, number of report, percentage reporting a loss based on number of report, total loss, and median loss
Source: Adapted from: Federal Trade Commission, The Big View: All Sentinel Reports 2021. Retrieved from https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports; downloaded October 5, 2022

See Table 1 for Definitions. In addition, Mortgage Foreclosure Relief and Debt Management - Mortgage lenders, brokers and other entities making false promises to save consumers' homes from foreclosure; mortgage refinancing, mortgage term modifications and debt management issues; credit organizations charging excessive fees, making false promises to provide free services, pay creditors or reduce interest rates.

Table 5: FTC Military Consumer Report by Status (2021)

Status	# of Reports	# of Fraud Reports	% Reporting Fraud Loss Total	Total Fraud Loss	Median Fraud Loss
Active Duty Service Member	**18,564**	**8,670**	**38%**	**$34M**	**$881**
Military Retiree/Veteran	**162,555**	**87,350**	**24%**	**$177M**	**$570**
Reserve/National Guard	**10,915**	**6,015**	**34%**	**$25M**	**$758**
Spouse/Dependent of Active Duty Service Member	**14,868**	**8,799**	**34%**	**$30M**	**$536**

Note: Military population, number of reports, number of fraud reports, percentage reporting fraud loss based on fraud number of reports, total fraud loss, and median fraud loss.
Source: Adapted from Federal Trade Commission, Fraud, Identity Theft, and Other Reports by Military Consumers. Top Reports 2021. Retrieved from https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports; Retrieved October 5, 2022.

Table 6: FTC Military Consumer Report by Branch (2021)

Rank	# of Reports	# of Fraud Reports	% Reporting Fraud Loss	Total Fraud Loss	Median Fraud Loss
Enlisted	**134,049**	**74,355**	**26%**	**$151M**	**$550**
Officer	**32,183**	**18,917**	**23%**	**$54M**	**$676**

Note: Military population, number of reports, number of fraud reports, percentage reporting fraud loss based on fraud number of reports, total fraud loss, and median fraud loss
Source: Adapted from Federal Trade Commission, Fraud, Identity Theft, and Other Reports by Military Consumers. Top Reports 2021. Retrieved from https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports; Retrieved October 5, 2022.

Table 7: FTC Military Consumer Report by Branch (2021)

Branch	# of Reports	# of Fraud Reports	% Reporting Fraud Loss	Total Fraud Loss	Median Fraud Loss
Army	**89,566**	**42,968**	**25%**	**$93M**	**$583**
Navy	**40,206**	**22,128**	**24%**	**$45M**	**$550**
Air Force	**38,465**	**21,354**	**22%**	**$42M**	**$550**
Marine Corps	**18,523**	**9,307**	**27%**	**$21M**	**$545**
Coast Guard	**3,135**	**1,690**	**28%**	**$7M**	**$600**

Note: Military population, number of reports, number of fraud reports, percentage reporting fraud loss based on fraud number of reports, total fraud loss, and median fraud loss

Of the 208,427 total reports from military consumers in 2021, 91% provided military branch information

Source: Adapted from Federal Trade Commission, Fraud, Identity Theft, and Other Reports by Military Consumers. Top Reports 2021. Retrieved from https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports; Retrieved October 5, 2022.

WHAT IS THE FEDERAL TRADE COMMISSION'S CONSUMER SENTINEL NETWORK?

The FTC's Consumer Sentinel Network has access to millions of cybercrime reports. The Consumer Sentinel Network gives law enforcement members access to reports submitted directly to the FTC by consumers, as well as to reports shared by data contributors.

Consumer Sentinel includes reports about:

- Coronavirus scams
- Identity theft
- Do-Not-Call Registry violations
- Computers, internet, and online auctions
- Telemarketing scams
- Advance-fee loans and credit scams
- Immigration services
- Sweepstakes, lotteries, and prizes
- Business opportunities and work-at-home schemes
- Health and weight loss products
- Debt collection, credit reports, and financial matters

Based on data from Consumer Sentinel Network, the FTC has online data visualizations that allow users to examine data from 2018-present and the data is updated quarterly. Data visualizations and downloadable data can be found here, and include reports from active-duty service members, veterans, as well as some military family data.

Military specific data as well as civilian data can be examined in Tableau. Users can download data in Excel, filtering data to examine particular types of crime, years, or subgroups.

Source: *Consumer Sentinel Network*. Federal Trade Commission. https://www.ftc.gov/enforcement/consumer-sentinel-network

Non-Governmental Research

AARP

AARP has led one of the only major studies of military cybercrime to date. The study examined the incidence of fraud within the military population to identify factors that made active-duty military and veterans susceptible and assessed variables such as age, gender, education and ethnicity. AARP's research showed that veterans and service members are 40% more likely to lose money to scams and fraud compared to their civilian peers. The research also found that veterans and service members were targeted more frequently and lost more money than their nonmilitary counterparts. Finally, nearly one third of the military and veteran respondents indicated they had lost money supporting veteran or military-related causes or signing over benefits to the VA.[52] AARP noted: "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."[53]

AARP's research showed that veterans and service members are 40% more likely to lose money to scams and fraud compared to their civilian peers.

"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."

Q&A WITH JOSH SOTO — CYBERSECURITY AND BUSINESS STRATEGIST

Q: Why do you think members of the military community might be more vulnerable to cybercrime?

A: There are several reasons that might potentially make veterans a more susceptible target: One big one that stands out is that veteran's information may, unfortunately, be more accessible. A variety of previous data breaches, including the OPM data breach, have compromised sensitive service member information through a wide range of sources. As members of the military community, we and our families are also a more valuable target for cybercriminals. Service members tend to be more reliable, secure predictable income and retain sensitive clearances and access for longer periods of time, taking the guesswork out of target acquisition for would-be attackers.

Members of the military also tend to be more trusting and charitable as a function of fast paced, dynamic work in organizations of established values and teamwork. Unfortunately, these same values can often lend themselves to social engineering frameworks if adequate training or awareness is not in place.

Q: Are there any aspects of the military lifestyle that increase vulnerability to cybercrime?

A: Some aspects of a military lifestyle may increase the likelihood of coming across malicious actors more frequently. Members of the military community move often, and they rapidly integrate into new communities, which often increases engagement on digital platforms and expands their digital presence.

If you're moving constantly, you're vulnerable to moving and travel scams. If you're away from home, you might be on dating sites where many scams originate. Frequent moving provides an opportunity for housing and rental scams, and if someone is on active duty or deployment, they may not be reachable or aware of bad actors at work. In this case, if a spouse or someone else at home notices fraudulent activity, they may not be able to discuss it, delaying the response time.

Q: Are there any specific techniques that cybercriminals use to target members of the military that you are aware of?

A: Social engineering is a preferred and insidious method of overcoming many defenses: convincing targets that they are dealing with a legitimate entity, such as the government, and preying on the target's own trust and tendencies. A small amount of time gathering facts about someone can make an attack personalized and convincing, even to some of the most experienced security experts.

DO MILITARY DEMOGRAPHICS MATTER?

Cybercrime is a growing problem in the general population. Additionally, cybercrime among special populations is understudied, but the military population might share certain risk factors and the consequences might be greater. Below we examine some of the specific subpopulations in the military community vulnerable to certain cybercrimes and reasons why.

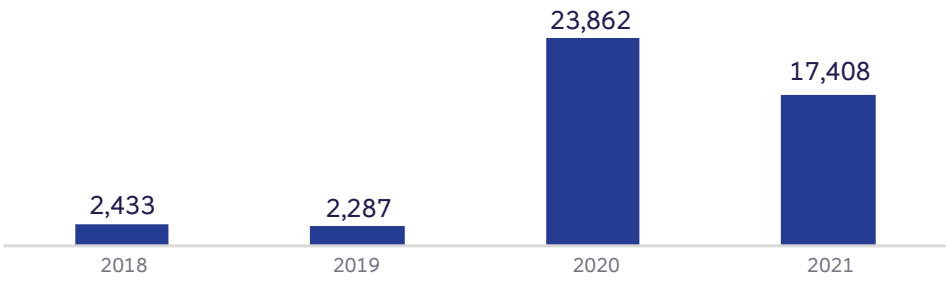
Veterans

According to the U.S. Census, there are just under 18 million veterans in the U.S.[54] Veterans have access to valuable benefits, and this can provide a financial incentive for criminals looking to access account information. The FTC data shows that from 2018 to 2021, veterans and military retirees made 441,949 reports and reported $345 million in total financial losses. In 2021, imposter scams, followed by online shopping scams, were the most reported categories of fraud by veterans.

According to the GAO, the VA does not collect data that could show the prevalence of scams directed at veterans. Such data could help the VA target outreach to veterans or provide information that could inform law enforcement action. Likewise, the VA does not always verify direct deposit information on its applications, which could help prevent payments being stolen. Yet, there are ways to verify such information. The Social Security Administration has set precedent for verifying direct deposit information and uses this process when reviewing individuals' checks or account statements for receipt of benefits.[55]

Prizes, sweepstakes, and lotteries, internet services, and business and job opportunities were the five most highly reported fraud categories.

Figure 6: FTC Military Consumers Reports of Government and Benefits Fraud (2018-2021)



Note: Military population, number of reports for government and benefits fraud
Source: Adapted from Federal Trade Commission, Fraud, Identity Theft, and Other Reports by Military Consumers. Top Reports 2021. Retrieved from https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports; Retrieved October 5, 2022.

ALL MEMBERS OF THE MILITARY COMMUNITY HAVE ACCESS TO GOVERNMENT BENEFITS THAT MAY INCREASE THEIR VENERABILITY TO CYBERCRIME. SIGNIFICANT INCREASES IN GOVERNMENT AND BENEFITS FRAUD WERE SEEN IN 2020.

In 2019 the GAO examined financial exploitation of veterans related to information the VA collected. The GAO noted that, in fiscal year 2018, the VA paid $3.2 billion in total pension benefits to 232,000 recipients. The GAO examined scams that target veterans, which include overcharge for home-based care, charges for services not received, receipt of bad investment advice from financial services organizations, and misdirection of benefit payments. It also noted improvements that the VA could implement, including using VA's applications to warn veterans about exploitation or scams and alerting veterans that they cannot be charged fees for filing claims.[56]

In addition, legislation recently proposed aims to remedy some of these issues. The proposed legislation would require the VA to assess cybercrime vulnerability to veterans and the availability of resources to help protect veterans from cyber-risks. This work would then inform recommendations to the secretary of veterans affairs on how to reduce cyber-risks to veterans and would require a report to Congress containing the results of the study.[57] While the legislation described has not been passed, it offers solutions to many of the issues raised in the GAO report and elsewhere.

HR2326 VETERANS CYBER RISK AWARENESS ACT

EFFORTS TO IMPROVE CYBERCRIME INFORMATION SHARING AT THE VA:

H.R. 2326, introduced April 1, 2021, by Rep. Nancy Mace, R-S.C., would require the Department of Veterans Affairs to conduct an outreach campaign to educate veterans about cyber-risks, such as disinformation, identity theft, scams, or fraud perpetuated through the internet. The bill would:

- Coordinate with federal, state, and other entities that educate the public about cyber- risks;
- promote and disseminate best practices and educational materials regarding cyber-risks to veterans and information about how veterans report cyber-risks to the appropriate law enforcement agency or entity other than the Department of Veterans Affairs; and
- establish and maintain a publicly accessible website of the Department regarding the campaign and includes hyperlinks to websites that include information for veterans on cyber risks.

If passed the legislation would require the VA to report on the campaign's progress of within 60 days. The **Congressional Budget Office** estimates the requirement would cost less than $500,000, based on comparing costs of similar outreach campaigns.

Source: https://www.congress.gov/bill/117th-congress/house-bill/2326/text?r=8&s=1

Service Members

According to 2021 FTC data, active-duty service members are 76% more likely than other adults to report that an identity thief misused one of their existing accounts, such as a bank account or credit card. Most notably, they are nearly three times as likely to report that someone used a debit card or some other electronic means to take money directly from their bank account." [58]

Military Families

Like service members and veterans, military families also may be vulnerable to cyberattacks, but there is little data to show how they are specifically impacted. While service members may routinely receive information from their military commands related to cyberthreats, military families may not receive the same type of information without actively seeking it. For instance, military spouses experience a 22% unemployment rate.[59] Research indicates that many people receive cybersecurity training in their workplace. Unemployed spouses, as well as those who are not in the labor market, may miss out on training opportunities that employed individuals might receive.

As recently as 2019, cybersecurity experts found that Iranian-backed cyberterrorists had placed malware on computers belonging to U.S. military veterans. Some have speculated that hackers may intentionally seek access to personal data from family members to later infiltrate computers belonging to current military members. By using this information, they could potentially gain access to Pentagon networks, allowing them to collect sensitive military information. In one instance, hackers stole personal credit card information from a military family member and eventually used social media to send threats to her family.[60]

WHICH ASPECTS OF MILITARY SERVICE PRESENT AN OPPORTUNITY FOR CYBERCRIMINALS?

Unlike civilians, military members, veterans, and their families move frequently, and they may have access to valuable benefits (e.g., retirement benefits, GI Bill, health care). In addition many regularly interact and are inclined to trust philanthropic organizations related to the military, making them easy targets for scammers, and service members are often deployed, making it difficult for them to consistently monitor suspicious activity on their accounts.[61] Finally, like their civilian counterparts, service members, veterans, and their families rely on the internet to, among other things, conduct professional and personal business, connect socially, store information, and manage their personal finances.

Personal Data Risks

Cybersecurity concerns are magnified because military connected individuals routinely provide substantial sensitive and personally identifying information when applying for security clearances, benefits, or other government resources.[62] Because this information is typically collected over the internet and later compiled, aggregated, and stored on a server or on the cloud, it may become accessible to criminals if improperly secured or if security is breached. In 2015, as was noted, during two separate cybersecurity incidents, data from federal employees, contractors, and others, including active-duty service members and their spouses was inappropriately accessed.[63]

Notably, this aggregated data, when monetized, is especially valuable to opportunistic criminals because it contains significant amounts of conveniently aggregated personal information (e.g., security clearance forms). This stored data, once accessed, delivers a rich environment for enterprising criminals to commit identify theft and other lucrative but difficult to detect cybercrimes at scale. Undetected crimes also go unreported and are often inadvertently accelerated because victims don't realize they have been wronged, believe nothing can be done or do not realize what has happened is considered a crime.[64]

Deployment

During deployment, service members are away from friends and family with limited contact, often leaving their spouse solely responsible for household financial decisions. Many military families find themselves with orders to move from one state or country to another every few years. When it's time for retirement or discharge, service members must rapidly assimilate back into civilian life, often after many years in the military community. [65]

Inconsistent Account Monitoring and Account Access

According to the FTC, among active duty, almost 14% indicate that their identity was stolen by a family member or someone they know. This is compared to 7% of other adults who report similar circumstances.[66] The data suggests that during military assignments or deployments service members may inadvertently or intentionally allow access to documents or important financial records to persons who take advantage, leaving them vulnerable to identity theft.[67]

Social Media Use

Surveys show that military members use social media more than civilians. Social media provides an accessible way to connect with friends, family, and the broader community. Unfortunately, it also provides a venue for cybercriminals to interact with potential victims, gain their trust, and gather information about them. Cybercriminals take advantage of the military community's widespread use of social media.[68] For instance, cybercriminals can leverage social media platforms to obtain sensitive information—including how long someone is deployed, their birthday, their locations, phone numbers, pets' names, and names of family members. Using this information, they can create fake profiles that can be used to implement various scams. [69]

Frequent Career and Life Transitions

The military and veteran community consists of more than 20.9 million Americans.[70] This includes active-duty service members, reservists, guard members, veterans, as well as all their families. Throughout their service and afterward, these individuals experience a variety of transitions which may make them more vulnerable to cybercriminals. Military transition might include deployment, relocations, discharge, and retirement. Each transition provides an opportunity for cybercriminals to exploit these aspects of military life to commit fraud, sometimes stealing hundreds of millions of dollars from the military and veteran community each year. One advocate noted that transitioning veterans may suffer financial losses related to their transition from the military because they may be targeted and vulnerable to job opportunity scams, which totaled $12.9 million in 2021.[71]

The Military-to-Civilian Transition

During their time affiliated with the military, and later when they transition, service members, veterans and their spouses frequently request online records, share documents, and enter personal data to access military specific benefits—such as buying a home with a VA loan, using GI Bill education benefits for themselves or dependents, or managing health care benefits. Each transition creates an opportunity for cybercriminals. These criminals—using fake websites, spoofed phone numbers or fake email addresses—may pose as a representative from a government or military agency (e.g., VA), to steal personally identifiable information.[72] According to the FTC in 2021, among 88,080 military-connected fraud reports to the FTC, imposter scams accounted for the most money lost—$103.9 million—with a median loss of $1,030.[73]

In addition to imposter scams, cybercriminals target members of the military and veteran community for a multitude of other online scams and fraud. Online shopping scams accounted for the second highest dollar amount lost by military consumers in 2021, with $29.6 million in losses reported to the FTC.[74] Financial losses due to job opportunity scams—typically directed at recently retired service members transitioning into civilian life—totaled $12.9 million in 2021.[75]

Small Business Ownership

According to the 2019 Annual Business Survey conducted by the U.S. Census Bureau, almost 6% of businesses are veteran-owned.[77] Small businesses are a frequent target of cybercriminals, particularly via financial attacks such as ransomware or phishing for employee credentials.[78] A major challenge for small businesses is how to stay on top of cybersecurity needs, such as using the latest security technologies, with limited resources. Particularly for veteran-owned businesses, it is critical that their businesses remain compliant with the Cybersecurity Maturity Model Certification program,[79] which can be a precondition of contract awards as a government or Department of Defense subcontractor.

The 2022 National Survey of Military-Affiliated Entrepreneurs (NSMAE)[80] highlights the extent of these cybersecurity challenges for military, military spouse, and veteran business owners. Among these military-affiliated entrepreneurs, around 1 in 5 reported that their business had been the target of a cybercrime (23%). Only two-thirds (66%) of military-affiliated business owners felt like they had adequate information to protect their businesses from cyberattacks, and just over half (54%) said they know where they would seek assistance if they were impacted by cybercrime.

The U.S. Small Business Association supports small businesses with recommendations on cybersecurity best practices and support tools for self-assessment.[81] Best practice recommendations include use of secure payment processing, backing up data, and utilizing technologies like multifactor authentication for business accounts. Participants in the 2022 NSMAE survey reported inconsistent use of these cybersecurity practices, using some of these items more than others. For instance, 92% of military-affiliated business owners "often" or "always" utilized secure payment processing. Only 82% reported they had implemented data backups (a vulnerability for ransomware attacks common targeted to small businesses), 79% "often" or "always" used multifactor authentication, and only around half (49%) had implemented cybersecurity training for employees (both are vulnerabilities to phishing or spyware attacks).[82]

Other Considerations

Research conducted by the Pew Research Center, found some age-related differences and cybersecurity practices. For example, persons under the age of 50 reported using similar online passwords on multiple sites; this was compared to 45% of internet users ages 18 to 49 and 32% of those ages 50 and older. Likewise, a higher percentage of younger adults said they had previously shared their passwords with others, with 56% of 18- to 29-year-old internet users saying they have done so.[83] In addition a 2019 report conducted by the GAO found that elderly veterans are "among the most vulnerable."[84] The Department of Veterans Affairs has acknowledged the issue but also notes that as long as veterans are competent to manage their finances they are free to spend their money as they see fit, including products or services that may be detrimental.[85]

Other research has shown that, contrary to what might be intuitive, younger people may be more vulnerable to cybercrime than older people; however, older people tend to lose more financially.[86] The FTC found similar results, noting that it received significantly more reports of fraud loss among younger consumers but higher fraud losses among older consumers.

VA PENSION POACHING

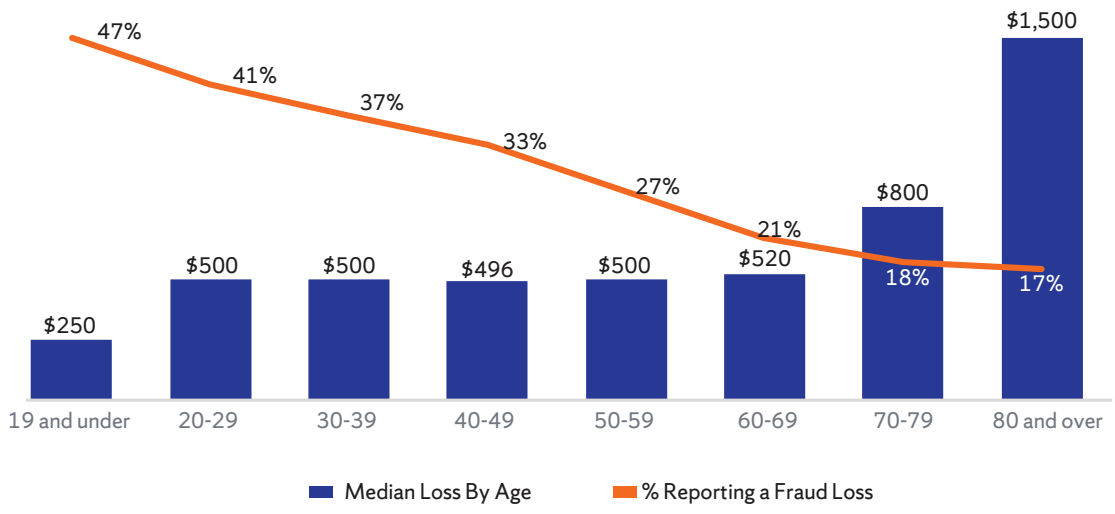
According to the VA, pension poaching is a financial scam that targets VA-eligible beneficiaries, veterans' survivors, and their families. Using this scam, unethical advisors may instruct claimants to hide their assets in various financial products, such as annuities, savings accounts, or investments that lead to profit for the advisor (e.g., through fees).

This can result in the appearance that VA benefits were approved in error when the VA reviews a claim for benefits. If the VA determines that eligibility did not exist, the claimant may be disqualified from receiving needed benefits and will be required to repay these benefits to the government. AARP found that 47% of military/veteran research participants indicated they had been targeted by scams requesting military benefits.[76]

To learn more about VA pension poaching: https://www.benefits.va.gov/BENEFITS/factsheets/limitedincome/pension-poaching.pdf

Figure 7: FTC Consumer Report of Percentage Reporting a Fraud Loss and Median Loss by Age (2021)

A GREATER PERCENTAGE OF YOUNGER CONSUMERS REPORTED LOSSES WHILE OLDER CONSUMERS REPORTED LARGER MONETARY LOSSES



Note: Total population, median loss by age and percentage reporting a fraud loss. Of the 2,878,566 total fraud reports in 2021, 46% included consumer age information.
Source: Adapted from Federal Trade Commission, Percentage Reporting a Fraud Loss and Median Loss by Age. Retrieved from https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts ; Retrieved October 5, 2022.

RESOURCES

Cybercrime Education and Support

- AARP provides a list of **Do's and Don'ts** for veterans. AARP provides a veterans' edition of its **AARP Watchdog Alert Handbook** and offers periodic online training on cybersecurity and tips for preventing fraud.
- The Better Business Bureau offers the **BBB Military Line** to help military families and veterans avoid scams and fraud.
- The **Cybercrime Support Network** offers training and information specific to the military community on preventing cybercrime and fraud as well as peer support groups and information about specific cybercrimes. The network provides information to recognize, report and recover from cybercrime. Cybercrime Support Network is an advocate and partner in protecting online data and privacy crimes.
- **Militaryconsumer.gov** provides information for service members to help keep their financial information secure. The Military Consumer website provides **information to help military personnel avoid scams**. Resources are available to help active-duty service members, veterans, and their families protect themselves and their finances.
  - > ***Credit tools for active-duty military***
  - > ***Identity Theft, Military Personnel & Families: What to know, What to do - by the Federal Trade Commission*** *gives information on the difference between fraud alerts and credit freezes as well as other helpful resources if you become a victim of identity theft.*
- The United States Postal Service provides **Operation Protect Veterans**, which offers tips and prevention against scams and is a partnership between the U.S. Postal Inspection Service and AARP that provides
- **The U.S. Department of Veterans Affairs** provides a website and other resources on identity theft.

Legal Assistance, Training, and Advocacy

- **National Conference of State Legislatures** maintains a list of criminal penalties, restitution, and identity theft passport laws.
- **The National Crime Victim Law** Institute offers the following tools/resources for attorneys and advocates:
  - > ***Legal Advocacy:*** *This is provided in the form of legal technical assistance, legal research, and educational writing as well as trainings to attorneys, advocates, judges, legislatures, and victims.*
  - > ***Education and Training:*** *Training is centered on victims' rights enforcement and is customized per needs and experience level: introductory for those new to victims' rights; advanced for those working in the trenches. Trainings are customizable by audience, length and learning objective, and can be taught in person, using distance-learning technology, or through a combination of methods.*
  - > ***Public Policy:*** *Works with policy partners to secure victims' rights' legislation that guarantees victims substantive rights and the procedural mechanisms to protect those rights.*

Cybercrime Support for Victims

Below is a list of organizations if you need to report a cybercrime or need some support after becoming a victim of one.

- **Cybercrime Support Network (CSN)** serves individuals and small businesses impacted by cybercrime:
  - > ***FightCybercrime.org:*** *website of resources to help cybercrime victims recognize, report, and recover from over 45 types of cybercrime.*
  - > ***Peer Support Program:*** *A 10-week virtual support group for romance scam survivors.*
  - > ***Military & Veteran Program:*** *A program that delivers cyber safety training and education to active-duty service members, veterans and their families at no cost.*
- **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.
- **The National Institute of Corrections** through the U.S. Department of Justice offers a **Victim Resource Map**: This is a tool for victims with links to organizations that provide aid, information, and support directly to victims of crime. Searchable by crime type or location, the map contains links to valuable national and state programs.

- **U.S. Department of Justice, Office for Victims of Crime** offers a **Directory on Crime Victim Services** to locate nonemergency crime victim service agencies within the United States. The search can be customized by location, type of victimization, or service needed.
- **U.S. Department of Veterans Affairs** 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 at 800-MyVA 411 (800-698-2411).

Cybercrime Resources for Small Business

Below is a list of resources for small business owners who have been or suspect that they have been a victim of a cybercrime.

- **Cybersecurity and Infrastructure Security Agency (CISA)** has compiled a **list of free cybersecurity resources**, including services provided by CISA, widely used open-source tools, and free services offered by private and public sector organizations across the cybersecurity community. Use this resource repository to advance your security capabilities. CISA also provides **guidance for small businesses**.
- **CISA** also offers **free cyber hygiene vulnerability scanning** for small businesses. It offers several scanning and testing services to help organizations assess exposure to threats to help secure systems by addressing known vulnerabilities and adjusting configurations.
- Maintain DoD industry partner compliance - Of special relevance to federal contractors and subcontractors is the **Cybersecurity Maturity Model Certification (CMMC) program**. Its purpose is to safeguard controlled unclassified information that is shared by the DoD. CMMC, a framework and assessor certification program, provides a model for contractors to meet a set of cybersecurity standards and requirements. It's based on a three-tiered model (foundational, advanced, expert) that requires companies to implement security measures (and be assessed accordingly), depending on the sensitivity of the information. Rulemaking is in progress, but it is essential for contractors to remain current with requirements, as a certain CMMC level will be required as a condition of contract award.
- The Federal Communications Commission offers a **cybersecurity planning tool** (The Small Biz Cyber Planner 2.0) to help you build a custom strategy and cybersecurity plan based on your business needs.
- Manage information communication technology supply chain risk - Use the **ICT Supply Chain Risk Management Toolkit** to help shield your business information and communications technology from sophisticated supply chain attacks. Developed by CISA, this toolkit includes strategic messaging, social media, videos, and resources, and is designed to help you raise awareness and reduce the impact of supply chain risks.
- **The US Small Business Administration** Cyberattacks are a concern for small businesses. Learn about common cybersecurity threats, why cybersecurity matters, and how to protect yourself and your business.

SUMMARY AND RECOMMENDATIONS

The cybercrime landscape is dynamic, shifting constantly as technology, culture, policy, and the law change. The continued ingenuity of cybercriminals challenges experts, policymakers, and individuals to keep pace. Because of that pace, immediate solutions for many consequences of cybercrime remain elusive. As this paper illustrates, little is known about specific subpopulations and their vulnerability to cybercrime, including the military.

The lack of data impedes the effort to control and defeat cybercrime. Interim solutions that educate and protect potential victims are needed. Some evidence suggests cybercrime may disproportionately impact military consumers, but the problem's scope is unknown without the ability to collect representative data.

The federal government has an obligation to make sure military veterans and their families receive the benefits to which they are entitled, along with education, information, and other measures to reduce risk to the military community and prevent financial losses.

CYBERCRIME MAY DISPROPORTIONATELY IMPACT MILITARY CONSUMERS, BUT THE PROBLEM'S SCOPE IS UNKNOWN WITHOUT THE ABILITY TO COLLECT REPRESENTATIVE DATA.

THE LACK OF DATA IMPEDES THE EFFORT TO CONTROL AND DEFEAT CYBERCRIME. INTERIM SOLUTIONS THAT EDUCATE AND PROTECT POTENTIAL VICTIMS ARE NEEDED

The following recommendations are directed at federal agency leaders and the military community:

- Government agencies, the private sector, and military-connected nonprofits should proactively form stronger partnerships to improve information sharing, coordination, and policy making.
- Government and/or private sector champions should convene key stakeholders to develop and implement new solutions to better inform and address cybercrime threats in the military community (e.g., FTC, DoD, VA, AARP, Cyber Crime Support Network, etc.).
- Senior government leaders should partner with cybersecurity experts to develop and disseminate information that arms the military community with the current and evolving best practices to reduce vulnerabilities to cybercrime.
- VA should seek opportunities to increase engagement with veterans about how to protect their benefits and avoid phishing schemes and other scams.
- DoD should identify critical touchpoints throughout a service member's career journey to increase awareness of cybercrime.
- Tailor cybercrime resources and programs that meet the needs of different groups, including active-duty service members, veterans, and military family members, and considers related demographic, location, and information accessibility factors.
- Include cybersecurity information and resources related to small business.
- Offer opportunities for the military community (including family members) to receive cybersecurity training that emphasizes the high prevalence of cybercrime, provides tips on effective cybersecurity measures, and emphasizes how cybercrimes risks are often underestimated.
- Encourage military-connected reporting of cybercrimes to provide a better estimate of the scope of the problem.

CONCLUSION

Despite questions on the volume and veracity of data on cybercrimes in the U.S., there is enough data to know more can and should be done to protect military consumers. Legislation has been passed that is intended to enable better data collection, improve government coordination, and ensure a common language that describes cybercrime. In the meantime, education, prevention, and resources specific to the military community are needed. Those resources should be targeted to specific subgroups, such as veterans, active-duty service members and military families, highlighting specific cybercrime prevention measures they can take to protect themselves, their data, and their finances.

REFERENCES

[1] Military Consumer Sentinel Network. (October 6, 2022). Military Top Reports The Big View: Sentinel Reports by Federal Trade Commission. Retrieved from : https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports.

[2] FBI. (n.d.). Internet Crime Report 2020. FBI. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[3] Ibid

[4] Lenning, B.J. (25, September, 2022). Personal Communication.

[5] Shinder, D. L., & Tittel, E. (2002). Chapter 1 - Facing the Cybercrime Problem Head On. In *Scene of the Cybercrime: Computer Forensics Handbook*. essay, Syngress Publishing.

[6] US Department of Justice. Financial Fraud Crime Victims. https://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud

[7] Shinder, D. L., & Tittel, E. (2002)

[8] England, Z. Military Members are Disproportionately Affected by Cyber Crime. (10, June 2020). Military Times. https://www.militarytimes.com/2020/06/10/military-members-are-disproportionately-affected-by-cybercrime-heres-why-and-how-to-avoid-it/; Military Consumer Sentinel Network (2022)

[9] Ibid

[10] Sauer. J. (2021). Scambush: Veterans Battle Surprise Attacks from Fraud and Scams. AARP. https://www.aarp.org/research/topics/economics/info-2021/fraud-scams-military-veterans.html

[11] Josh Soto, Personal Communication, 8 June 2022

[12] Kaspersky. (n.d.). What is cybercrime? How to protect yourself from cybercrime. https://usa.kaspersky.com/resource-center/threats/what-is-cybercrime

[13] United Nations Office on Drugs and Crime. (n.d.). E4J University Module Series: Cybercrime Module 5: Reporting Cybercrime. https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/reporting-cybercrime.html

[14] Burda, R. (15, July, 2022). CSN Written Testimony Before The House Committee On Oversight and Reform Subcommittee on National Security. https://fightcybercrime.org/blog/csn-written-testimony-before-the-house-committee-on-oversight-and-reform-subcommittee-on-national-security/

[15] Cybersecurity & Infrastructure Security Agency (2020, August 25). Avoiding Social Engineering and Phishing Attacks. https://www.cisa.gov/uscert/ncas/tips/ST04-014

[16] U.S. Office of Personnel Management. (June 4, 2015). OPM to Notify Employees of Cybersecurity Incident. https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/

[17] Adams, M. (March 11, 2016). Why the OPM Hack Is Far Worse Than You Imagine. Lawfare Blog. https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine

[18] The Office of Personnel Management. Cybersecurity Resource Center https://www.opm.gov/cybersecurity/cybersecurity-incidents/

[19] Adams, M. (March 11, 2016)

[20] Rein. L. (2015, December 14). The Chinese didn't just hack federal employees. Journalists were swept up in the massive breach, too. The Washington Post. https://www.washingtonpost.com/news/federal-eye/wp/2015/12/14/the-chinese-didnt-just-hack-federal-employees-journalists-were-swept-up-in-the-massive-breach-too/

[21] Adams, M. (March 11, 2016).

[22] Ibid

[23] Jarrett, H.M. & Bailie, M. W. (n.d.) Prosecuting Computer Crimes. Computer Crime and Intellectual Property Section Criminal Division. Office of Legal Education Executive Office for United States Attorneys. U.S. Department of Justice. http:// https://www.justice.gov/criminal/file/442156/download

[24] Kaspersky Lab (2022). What is social engineering? https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering

[25] Peters, A., & Garcia, M. (2020, November 12). A Roadmap to Strengthen US Cyber Enforcement: Where Do We Go From Here?. Thirdway. https://www.thirdway.org/report/a-roadmap-to-strengthen-us-cyber-enforcement-where-do-we-go-from-here

[26] Internet Crime Report 2020. Federal Bureau of Investigation (FBI) Internet Crime Complaint Center. Department of Justice (DOJ). Federal Bureau of Investigation (FBI). https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[27] Federal Bureau of investigation Internet Crime Report. (2021). Federal Bureau of Investigation (FBI) Internet Crime Complaint Center. Department of Justice (DOJ). Federal Bureau of Investigation (FBI). https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[28] Hasham, S.; Joshi, S.; and Mikkelsen, D. (2019). Financial crime and fraud in the age of cybersecurity. Mckinsey. Retrieved from https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity

[29] Insurance Information Institute. (n.d.) Facts & Statistics: Identity theft and cybercrime. Insurance Information Institute. Affiliated with The Institutes. https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#:~:text=According%20to%20the%20FBI's%20Internet,7%20percent%20increase%20from%202020.

[30] The Federal Trade Commission. https://www.ftc.gov/news-events/topics/identity-theft/phishing-scams

[31] Federal Trade Commission. Consumer Sentinel Network. Military Top Reports The Big View: Sentinel Reports by Federal Trade Commission. Retrieved October 6, 2022 from https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports.

[32] Ibid

[33] Ibid

[34] Sen. Schatz, B. (D-H). (2021-2022). S.2629 - Better Cybercrime Metrics Act. 117th Congress. Congress.gov. https://www.congress.gov/bill/117th-congress/senate-bill/2629/text

[35] Roseen, D. (2018, March, 20). Improving Cyber Crime Data to Protect Vulnerable Communities. New America. https://www.newamerica.org/millennials/dm/improving-cyber-crime-data-protect-vulnerable-communities/

[36] Sauer. J. (2021, November). Veterans Battle Surprise Attacks from Fraud and Scams. Washington, DC: AARP Research. https://www.aarp.org/research/topics/economics/info-2021/fraud-scams-military-veterans.html

[37] Information in table one was compiled and synthesized from the referenced source as well as a variety of sources referenced in this document; United Nations Office on Drugs and Crime. (n.d.). E4J University Module Series: Cybercrime Module 5: Reporting Cybercrime. https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/reporting-cybercrime.html

[38] Burda, R. (15, July, 2022). CSN Written Testimony Before The House Committee On Oversight and Reform Subcommittee on National Security. https://fightcybercrime.org/blog/csn-written-testimony-before-the-house-committee-on-oversight-and-reform-subcommittee-on-national-security/

[39] Olmstead, K. & Smithby. A. (January 26, 2017). Americans and Cybersecurity. Pew Research Center. Retrieved at https://www.pewresearch.org/internet/2017/01/26/2-password-management-and-mobile-security/

[40] Federal Trade Commission. (2020, July 13). FTC Launches New Online Tool for Exploring Military Consumer Data. FTC Launches New Online Tool for Exploring Military Consumer Data. https://www.ftc.gov/news-events/news/press-releases/2020/07/ftc-launches-new-online-tool-exploring-military-consumer-data

[41] Sauer. J. (2021).

[42] Federal Trade Commission. Consumer Sentinel Network. Military Top Reports The Big View: Sentinel Reports by Federal Trade Commission.

[43] Burda, R. (15, July, 2022)

[44] FTC Sentinel data is downloaded on a quarterly basis; based on date, numbers included in this report may differ from those displayed online.

[45] The Federal Trade Commission. (n.d) Consumer Sentinel Network. Accessed on 3 October 2022 at https://www.ftc.gov/enforcement/consumer-sentinel-network

[46] Consumer Sentinel Network. Military Top Reports The Big View: Sentinel Reports by Federal Trade Commission. (October 6, 2022).

[47] Ibid

[48] Ibid

[49] Consumer Education Council of North America (CECNA.io). (2022, February 23). Imposters Drove Feverish Growth in Scams Last Year. https://cecna.io/imposters-drove-feverish-growth-in-scams-last-year/

[50] Consumer Sentinel Network. Military Top Reports The Big View: Sentinel Reports by Federal Trade Commission. (October 6, 2022).

[51] Ibid

[52] Sauer. J. (2021). Scambush: Veterans Battle Surprise Attacks from Fraud and Scams. AARP. https://www.aarp.org/research/topics/economics/info-2021/fraud-scams-military-veterans.html

[53] The AARP Fraud Watch Network. (n.d.). Watchdog Alert Handbook: VETERANS EDITION Common Scams Targeting Veterans & Military Families — and How to Stay Safe. https://www.aarp.org/content/dam/aarp/home-and-family/voices/veterans/2022/04/watchdog-alert-fraud-handbook-veterans-aarp.pdf (p. 8)

[54] Bureau, U. S. C. (n.d.). Table S2101 VETERAN STATUS (2020: ACS 5-Year Estimates Subject Tables). Explore census data . Retrieved October 5, 2022, from https://data.census.gov/cedsci/table?q=Veterans&tid=ACSST5Y2020.S2101 (Estimated number is 17,935,456 veterans in the U.S.)

[55] U.S. Government Accountability Office (n.d.). Veterans Benefits: Actions VA Could Take to Better Protect Veterans from Financial Exploitation. Retrieved March 28, 2022, from https://www.gao.gov/products/gao-20-109

[56] Ibid

[57] Rep. Mace, N. [R-SC-1]. (2021, April 1) H.R.2326 - Veterans' Cyber Risk Awareness Act. 117th Congress. Congress.gov. https://www.congress.gov/bill/117th-congress/house-bill/2326/text?r=8&s=1

[58] Fletcher. E. (2020), May 21, 2020). Military Data Spotlight: Identity theft and service members. Federal Trade Commission. ttps://consumer.ftc.gov/consumer-alerts/2020/05/military-data-spotlight-identity-theft-and-servicemembers

[59] U.S. Department of Defense, Office of People Analytics. (2020, Dec). 2019 Survey of Active Duty Spouses. https://www.militaryonesource.mil/data-research-and-statistics/survey-findings/2019-spouses-survey/

[60] Kredo. A. (6 February, 2020). U.S. Military Members, Families Hit with Hacks From Russia, Terror Orgs. The Washington Free Beacon. https://freebeacon.com/national-security/u-s-military-members-families-hit-with-hacks-from-russia-terror-orgs/

[61] Burda, R. (15, July, 2022).

[62] Ibid

[63] Cybersecurity Resource Center. Cybersecurity Incidents. OPM.gov. https://www.opm.gov/cybersecurity/cybersecurity-incidents/

[64] Baker, A. (5, February, 2018). An 'Iceberg' of Unseen Crimes: Many Cyber Offenses Go Unreported. The New York Times. https://www.nytimes.com/2018/02/05/nyregion/cyber-crimes-unreported.html

[65] Ibid

[66] Fletcher. E. (2020)

[67] Ibid

[68] Burda, R. (15, July, 2022).

[69] Ibid

[70] Bureau (n.d.). Table S2101 VETERAN STATUS (2020: ACS 5-Year Estimates Subject Tables). Explore census data . Retrieved October 5, 2022, from https://data.census.gov/cedsci/table?q=Veterans&tid=ACSST5Y2020.S2101 (Estimated number is 17,935,456 veterans in the U.S.); U.S. Department of Defense. (2019). 2019 Demographics: Profile of the military community. Washington, D.C. Retrieved from https://www.militaryonesource.mil/data-research-and-statistics/military-community-demographics/2020-demographics-profile/ (Active Duty 1,333,822, Guard/Reserve 802,248, Active Duty Military Spouses 597,737, Guard/Reserve Military Spouses 597,737)

[71] Burda, R. (15, July, 2022).

[72] The FTC defines identity theft as "Someone pretends to be a trusted person to get consumers to send money or give personal information. Examples include scammers claiming to work for or be affiliated with the government agency; scammers posing as a friend or relative with an emergency need for money; scammers posing as a romantic interest; scammers claiming to be a computer technician offering technical support; and scammers claiming to be affiliated with a private entity (e.g., a charity or company)."

[73] Federal Trade Commission: 2021 Consumer Sentinel Network Data Book. 2021. [Accessed: Jul 7 2022]. Available from: https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAll SentinelReports/TopReports.

[74] Federal Trade Commission: 2021; see note 80 on definition of identity theft

[75] Federal Trade Commission: 2021

[76] Sauer. J. (2021).

[77] Annual Business Survey Release Provides Data on Minority-Owned, Veteran-owned and Women-Owned Businesses. (2021, January 28). U.S. Census Bureau. https://www.census.gov/newsroom/press-releases/2021/annual-business-survey.html

[78] Small Businesses Are a Cybercrime Target, and Verizon's DBIR Has the Data to Prove it. (2022, June 27). Fight Cybercrime. https://fightcybercrime.org/blog/small-businesses-are-a-cybercrime-target-and-verizons-dbir-has-the-data-to-prove-it/

[79] Cybersecurity Maturity Model Certification (CMMC 2.0) Acquisition & Sustainment. Office of the Under Secretary of Defense. https://www.acq.osd.mil/cmmc/index.html

[80] Maury, R., Tihic, M., Pritchard, A., McKelvie, A., Euto, L. (2022, Jan). 2021 National Survey of Military-Affiliated Entrepreneurs. Syracuse, NY: Institute for Veterans and Military Families, Syracuse University. https://ivmf.syracuse.edu/wp-content/uploads/2022/05/2021-National-Survey-of-Military-Affiliated-Entrepreneurs-Research-Report-_FINAL-FINAL-ua.pdf

[81] U.S. Small Business Administration (SBA). Strengthen your cybersecurity. Cyberattacks are a concern for small businesses. Learn about cybersecurity threats and how to protect yourself. https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity

[82] Maury, R.; Tihic, M., Pritchard, A. (2022).2022 National Survey of Military-Affiliated Entrepreneurs. Syracuse, NY: D'Aniello Institute for Veterans and Military Families, Syracuse University

[83] Olmstead, K. & Smithby. A. Americans and Cybersecurity. (January 26, 2017). Pew Research Center. Retrieved at https://www.pewresearch.org/internet/2017/01/26/2-password-management-and-mobile-security/

[84] U.S. Government Accountability Office (n.d.). Veterans Benefits: Actions VA Could Take to Better Protect Veterans from Financial Exploitation. Retrieved March 28, 2022, from https://www.gao.gov/products/gao-20-109

[85] Leiber, N. (2021, November 29). 'Pension Poachers' Are Targeting America's Elderly Veterans. Bloomberg. https://www.bloomberg.com/news/features/2021-11-29/elderly-u-s-veterans-are-increasingly-falling-victim-to-pension-poachers

[86] Lifars (2021). Younger People Less Likely to Report, More Likely to Fall Victim to Cyber Crime. https://www.lifars.com/2021/12/younger-people-less-likely-to-report-more-likely-to-fall-victim-to-cyber-crime/#:~:text=A%20recent%20study%20by%20Atlas,from%20the%20US%20and%20UK.

STAY IN TOUCH

p 315.443.0141
f 315.443.0312
e ivmfalumni@syr.edu
w ivmf.syracuse.edu

@IVMFSyracuseU

D'Aniello IVMF