VETERANS' DIGITAL ALLY

Digital Literacy and Scam Vulnerability Among Veterans (Colorado vs. National, 2018–2025)

A Literature Review Focusing on Veteran Digital Inclusion and Fraud Risk

April 6, 2025

Contents

Executive Summary

Colorado vs. National Overview: Over the past seven years, veterans in Colorado have mirrored many national trends in digital inclusion and fraud exposure. Around one-quarter of veterans lack broadband internet at home in both Colorado and the U.S. overall American Immigration Council (2022). Colorado veterans slightly outperform national averages in connectivity (about 77% have high-speed internet vs. 73% nationally) American Immigration Council (2022), yet they remain more likely than the general population to be offline (6.5% of Colorado veteran respondents reported no home internet, compared to 4.3% of all Coloradans) Benton Institute for Broadband & Society (2024). Limited digital literacy and access are persistent issues, especially for older veterans.

Older vs. Younger Veterans: Veterans over age 50 exhibit lower digital literacy levels and less internet use, contributing to higher vulnerability to scams. In contrast, veterans under 49 are generally more digitally connected and savvy, but still face frequent scam attempts tailored to the military community. Notably, over half of all U.S. veterans are age 60 or older, meaning any digital divide disproportionately affects this older group Benton Institute for Broadband & Society (2024). Veterans' median fraud losses are significantly higher than those of non-veterans (by approximately 44% in recent data) Hersey (2023), with older veterans often suffering the largest financial impacts.

Key Trends in Digital Literacy: Both Colorado and national data indicate that veteran households have high broadband adoption rates (roughly 85% in recent years) Benton Institute for Broadband & Society (2024), but the digital skills gap is evident. Many veterans, especially older ones, are uncomfortable with or unaccustomed to common online activities. For example, Colorado veterans report far lower usage of social media (59%) compared to the general population (78%) Benton Institute for Broadband & Society (2024), and are less likely to search or apply for jobs online Benton Institute for Broadband & Society (2024). Insufficient digital literacy was identified by the FCC as a major barrier for veterans, alongside perceptions that the internet is not relevant to them Benton Institute for Broadband & Society (2024). Two-thirds of offline veteran households cited lack of interest or need as the primary reason for not using the internet, reflecting both generational attitudes and skill gaps Benton Institute for Broadband & Society (2024).

Key Trends in Scam Vulnerability: Veterans are disproportionately targeted by scams and often at higher risk of financial loss than civilians. A 2021 survey found veteran and military adults are 40% more likely to lose money to fraud than non-veterans Campbell (2024). Over 80% reported being targeted by scams related to their service or VA benefits Campbell (2024). In Colorado and nationally, law enforcement and watchdog agencies have noted a surge in scams aimed at veterans – from fake VA loan offers to benefits buyout schemes. Nearly one in three veterans nationally has lost money to service-related scams, with "benefits buyout" scams (offers to trade pensions for a lump sum) and fraudulent record fees among the most common tactics Campbell (2024). Total fraud losses in the military/veteran community have climbed sharply in recent years (from $267 million in 2021 to $414 million in 2022, a 55% jump) Hersey (2023), underscoring an urgent need for improved digital awareness and fraud prevention.

Factors Influencing Outcomes: Socio-economic and geographic factors deeply influence veterans' digital literacy and scam risk. Rural veterans often face limited broadband availability and are less likely to engage in online services, which can hinder digital skill development Benton Institute for Broadband & Society (2024). Lower-income veterans are less able to afford internet service or devices, and they report cost as a significant barrier to going online Benton Institute for Broadband & Society (2024). Additionally, veterans have a higher incidence of disabilities (over 30% have at least one) Benton Institute for Broadband & Society (2024), which can complicate technology use. These overlapping challenges mean that the most vulnerable subgroups are often older, low-income, disabled, or rural veterans – populations that require targeted support.

Research Gaps and Future Needs: There are notable gaps in the research and data specific to veterans. Few studies disaggregate digital literacy by veteran status and age, making it difficult to pinpoint nuanced needs of younger vs. older veterans. Data on scams against veterans often aggregate all ages or combine active-duty with veterans, obscuring age-specific trends. Colorado-specific data on veteran scam victimization is limited, relying mostly on general older adult fraud surveys. More granular research is needed on how veterans learn digital skills, what scam types different age groups fall victim to, and how effective current interventions are. Addressing these gaps will inform better policy and training programs.

Recommendations: Improving veterans' digital literacy and reducing fraud requires a multi-pronged approach. This includes expanding broadband access in underserved (especially rural) areas, offering veteran-focused digital literacy training (e.g., basic computer skills, online safety, navigating VA websites), and increasing fraud awareness outreach through trusted channels like Veteran Service Organizations (VSOs). Policy measures – such as enforcing bans on unaccredited actors charging veterans for benefit services Campbell (2024) and establishing dedicated fraud prevention units in the VA – are steps in the right direction. The report concludes with detailed recommendations and an FAQ knowledge check for stakeholders and educators.

Veterans 50+ — Digital Literacy Challenges and Scam Vulnerability

Demographics and Digital Access

The majority of U.S. veterans today are over 50, with over 50% age 60 or older Benton Institute for Broadband & Society (2024). This cohort includes Vietnam War-era and older Gulf War veterans who did not grow up with digital technology. Consequently, older veterans tend to have lower digital literacy and less internet engagement than their younger counterparts. Surveys consistently show older veterans lag in internet access: for instance, a Colorado study (2019) found 26.8% of Coloradans over 60 lacked broadband at home American Immigration Council (2022). Nationally, around 27% of veterans (disproportionately seniors) had no high-speed internet in 2019 American Immigration Council (2022). While home broadband adoption has improved in recent years, a significant number of older veterans remain offline or use the internet only minimally. In one study of VA patients, fully 30.8% of veterans aged 80+ and 17.9% of those 65–79 lacked any digital device (smartphone or computer), compared to just 3.4% among veterans under 50 Russell et al. (2024). Similarly, about 25% of veterans 80+ lacked affordable, reliable internet access in that study Russell et al. (2024). These statistics highlight a digital divide by age: many older veterans either cannot access or choose not to engage with online resources.

Digital Literacy and Usage

Beyond access, older veterans often have lower digital skill levels and comfort with technology. They may struggle with tasks like navigating websites, managing online accounts, or recognizing cybersecurity threats. According to the Colorado Health Access Survey, veterans as a group were far less likely than the general population to use the internet for various purposes — a gap largely attributable to older veterans' behavior. Only 59% of Colorado veterans reported using social media, versus 78% of all adults Benton Institute for Broadband & Society (2024). Likewise, just 18.2% of veterans applied for jobs online versus 32.6% of all Coloradans Benton Institute for Broadband & Society (2024). These differences suggest that many older veterans are not taking full advantage of online tools (for social connection, employment, telehealth, etc.), possibly due to lack of digital know-how or confidence. Qualitative feedback supports this: listening sessions in Colorado found some older vets were "struggling financially and personally with health issues that seemed to block their ability to get connected" Benton Institute for Broadband & Society (2024). Some did not know about programs that offer discounted internet, or assumed they were ineligible Benton Institute for Broadband & Society (2024). Nationally, the FCC has reported that among veteran households without internet, insufficient digital literacy and a perception that the internet is not relevant are major factors Benton Institute for Broadband & Society (2024). In fact, two-thirds of offline veteran households said they lacked interest or need for the internet Benton Institute for Broadband & Society (2024) — a mindset more common in older, retired individuals. This highlights an important facet of digital literacy: convincing older veterans why being online is worthwhile (for healthcare access, benefits information, staying in touch) is as necessary as teaching how to use the technology.

Scam Vulnerability

Unfortunately, lower digital literacy and limited online experience can make older veterans particularly vulnerable to fraud and scams. Many scams targeting veterans still occur via phone, mail, or in-person tactics that prey on trust and confusion, and those not regularly online may be less aware of common scam warning signs. The veteran community has been heavily targeted by fraudsters offering fake veterans' benefits services, impostor charities, and investment schemes. One in three veterans (of all ages) has reported losing money to a service-related scam Campbell (2024), and anecdotal evidence suggests older veterans are often the victims in the most costly cases. For example, in late 2023 a 76-year-old Navy veteran with cognitive impairment was defrauded of more than $3.5 million in a wire scheme Hersey (2023). Scammers frequently exploit the "earned benefits" narrative — older vets may be told they qualify for a special pension advance or that they owe money related to their VA benefits Hersey (2023,?). Lacking digital literacy can exacerbate these risks: an older vet who isn't comfortable verifying information online might take such calls or emails at face value. Moreover, many older veterans have significant life savings or fixed pensions, making them attractive targets. The Federal Trade Commission (FTC) warns that veterans and military retirees filed nearly 300,000 fraud reports from 2019–2023, with losses of $842 million Hersey (2023). The median loss for veterans is 44% higher than for other adults Hersey (2023), indicating that when veterans (often older) fall victim, the financial damage tends to be greater. In Colorado, authorities have seen scams ranging from bogus VA loan refinancing offers to impostors threatening elderly veterans with arrest if “fees” aren’t paid. Older veterans who are less digitally savvy may also be less aware of resources to verify or report scams, leading to underreporting and prolonged abuse.

Case Example — Colorado

A recent Colorado case underscores the vulnerability of older veterans. In 2023, a 46-year-old Colorado veteran (not yet senior but an example of limited digital acumen) received calls from someone impersonating law enforcement, claiming he owed money and even spoofing a sheriff’s office number. He ended up transferring over $17,000 via a bitcoin ATM before realizing it was a scam Hersey (2023,?). Local officials noted they were “not surprised” by the scam, as criminals specifically target veterans in Colorado with government impostor frauds. While this victim was middle-aged, such social engineering tactics often disproportionately ensnare older veterans who might be less familiar with cryptocurrency or caller ID spoofing. Colorado’s response has included joint efforts by the Attorney General’s Office and AARP ElderWatch to educate seniors (many of them veterans) about such impersonation scams and fraudulent calls. The prevalence of robocalls and spam also affects older vets: nationally, veterans report receiving more frequent robocalls and suspicious texts than civilians (about 9–10% higher frequency) Service (2021), which increases exposure to scams like tech support fraud or phishing. In summary, veterans over 50 face a dual challenge: bridging the digital literacy gap to participate fully in the online world, and simultaneously fending off a barrage of scams that prey on their age, benefits, and trust. Colorado’s veteran population, which skews older, illustrates these issues vividly. Many older veterans need accessible training and support to build digital skills (for instance, how to use email or patient portals), as well as clear guidance to recognize scams (e.g., “the VA will never ask for your password over the phone” and similar principles) Service (2021,?). Encouragingly, initiatives are emerging to assist them — from VA’s Digital Divide Consult program (providing tablets/internet for telehealth) to local workshops on internet basics. These efforts acknowledge that improving digital literacy among older veterans not only enhances their quality of life and health access, but also provides a critical line of defense against fraud. An informed, connected senior veteran is far less likely to fall victim to scams than an isolated, tech-averse one.

Veterans Under 49 — Digital Engagement and Fraud Risks

Digital Proficiency and Usage

Veterans younger than 49 largely consist of the post-9/11 generation and Gulf War-era veterans, many of whom served in the 2000s or 2010s. This cohort tends to be more digitally native — they entered military service in an era of computers, smartphones, and the internet, and they often continue using technology fluidly in civilian life. As a result, basic digital literacy (internet use, email, social media, etc.) is generally high among younger veterans. Surveys indicate that the vast majority of veterans under 49 have internet access and devices: in VA health system screenings, only about 3–4% of veterans under age 49 lacked a smartphone or computer Russell et al. (2024), and around 15% had issues affording reliable internet (considerably lower than older age groups) Russell et al. (2024). Many younger veterans rely on mobile devices as their primary connection; the FCC noted that veteran households without children (often older veterans) lag in mobile broadband subscriptions, but veteran households with children (which tend to be younger families) actually subscribe at higher rates than their non-veteran counterparts Benton Institute for Broadband & Society (2024). In Colorado, younger veterans likely contribute to the finding that 85% of veteran households had paid home internet by 2019 Benton Institute for Broadband & Society (2024,?). Younger veterans are also more likely to engage in online activities such as job hunting, online education, and social networking — indeed, many transitioning service members use online job boards and veteran networks (like LinkedIn groups for vets) to find employment. Their digital literacy challenges are typically less about basic access and more about refinement of skills (e.g., optimizing privacy settings, understanding online financial tools) and ensuring secure usage.

Online Behavior and Literacy Needs

Despite being comfortable online, younger veterans still have areas where digital literacy can be strengthened. For example, some younger veterans may be mobile-dependent (using smartphones for most tasks) and might lack experience with desktop productivity tools or advanced internet research techniques. In Colorado's digital equity efforts, it was noted that some veterans (likely younger ones looking for jobs) could benefit from training in using technology for employment purposes Benton Institute for Broadband

& Society (2024,?). State survey data showed relatively low percentages of veterans using the internet to search or apply for jobs (24.9% and 18.2% respectively) Benton Institute for Broadband & Society (2024), suggesting possible skill or confidence gaps even among those of working age. It is also noted that some veterans under 49 entered service immediately after high school and may not have had advanced computer training unless their military role provided it. The military experience itself is mixed in terms of digital literacy: some younger veterans left with strong IT skills from tech-heavy fields, while others did not receive much computer training. Interestingly, states like Connecticut have recognized that many veterans received digital training during service, which can be leveraged for civilian careers requiring digital skills Benton Institute for Broadband & Society (2024,?). In other words, younger veterans often have a foundation of technical aptitude (discipline with learning new systems, following security protocols) that can be built upon with the right guidance.

Scam Exposure and Vulnerabilities

Younger veterans face a different scam landscape compared to their older peers. Because they are active online, they are frequently targeted through digital channels: social media scams, phishing emails, fraudulent websites, and text messages. AARP's research highlights that the military/veteran community receives more of these contacts than civilians — for example, about 9% more phishing attempts and 8% more fake prize or lottery offers than the general population Service (2021). Younger veterans are likely a big part of that statistic since they are reachable via technology throughout the day. One growing threat is social media disinformation and impersonation: foreign actors and criminals have been known to create fake veteran profiles or veteran support groups to build trust with servicemembers and younger veterans online Committee (2020,?). These tactics can lead to romance scams or identity theft. The U.S. House Committee in 2020 warned of "Hijacking our Heroes" — spoofing veterans on social media to propagate scams Committee (2020). A younger veteran might connect with someone on Facebook who appears to be a fellow veteran in need or a liaison for a VA program, only to be solicited for money or personal data. While younger individuals tend to be more aware of internet scams in general, veterans under 49 have a specific set of vulnerabilities tied to their military service, such as scams offering to consolidate or forgive VA student loans or GI Bill benefits, or fake job postings promising veteran preference. Notably, active-duty servicemembers (often under 30) and recent veterans reported tens of thousands of fraud cases in recent years — though fewer in number than older veterans, the rate can be high relative to their population. From 2019 to 2023, active-duty members filed about 30,000 fraud reports (with $142 million lost) Hersey (2023). Many younger veterans share risk factors with active-duty personnel: frequent relocations (making them targets for moving or rental scams), reliance on military pay/benefits (targeted by financial scammers), and a culture of trust and camaraderie that scammers abuse. Impostor scams are the top fraud category for the military community Hersey (2023), often involving someone pretending to be a government official or veteran-affiliated agent. A younger veteran might get an email that looks like it's from a "VA Benefits Update Center" asking them to re-verify their direct deposit — a phishing attempt for bank information. If their digital literacy in cybersecurity is lacking, they could be fooled by the official-looking communication. On the other hand, younger veterans may be quicker to report scams when they encounter them, using online complaint tools (e.g., FTC websites), which is a positive sign.

Financial Impact

In aggregate, scams affect older veterans more in total dollars, but younger veterans are far from immune. A 2021 AARP survey found that younger military/veteran adults (age 18–44) were slightly more likely to report encountering service-related scams in the past year than older veterans Campbell (2024). However, they lost smaller amounts on average, possibly due to having less savings or better scam detection. One common scam targeting younger veterans is the "benefits buyout" scheme, where a scammer offers quick cash in exchange for the veteran signing over future disability or pension payments. Nearly half of veterans who lost money to scams fell for these benefit buyouts Campbell (2024). Although one might assume this skews older, some younger veterans with service-connected disability payments have been swindled by such offers when in immediate need of cash. In Colorado, many veterans under 49 are in the workforce or pursuing education and might be targeted with employment scams or fake VA program fees. For example, a scammer might advertise a high-paying security job "for veterans only" but require an upfront training fee. Additionally, instances of fraud related to the PACT Act (which expanded health benefits for burn pit exposure) have been reported nationally — scammers promise to help veterans (often younger Gulf War and War on Terror veterans) apply for new benefits for a fee Hersey (2023). VA and veterans groups have issued warnings: applying for earned benefits is free, and any unsolicited offer to assist for payment is a red flag AARP (2023). In summary, veterans under 49 generally possess stronger digital skills and greater online exposure, which is a double-edged sword: they benefit from connectivity yet face constant scam attempts. Their needs center on cybersecurity education (e.g., how to spot phishing and use two-factor authentication) and trustworthy information about verifying benefits or military records. With the right resources, younger veterans can not only protect themselves but also help educate older veterans through peer mentorship.

Socio-Economic, Geographic, and Demographic Factors Influencing Outcomes

Age and Generation

Age is a major factor: older veterans (many of whom served in Vietnam or earlier) generally face more challenges with digital technology, while younger veterans (Post-9/11 era) are more adept. For example, Vietnam-era veterans are now in their 70s, whereas Iraq/Afghanistan veterans might be in their 30s or 40s. Each generation's exposure to technology during and after service affects their baseline digital literacy. Age also correlates with the type of scams encountered: older veterans are more likely to face phone or mail scams, while younger veterans see more online scams. Additionally, older veterans are more likely to live alone or be retired, increasing isolation and vulnerability, while younger veterans often have more peer and family support.

Income and Education

Veterans span a wide range of socio-economic statuses. In general, veterans have slightly lower poverty rates than non-veterans due to military benefits and training Benton Institute for Broadband & Society (2024). However, veteran poverty is rising Benton Institute for Broadband & Society (2024), and those in lower-income brackets face distinct hurdles. Lower-income veterans often cannot afford broadband or new devices, directly limiting digital access. In Colorado, 23% of veterans lacked high-speed internet in 2019, with many likely in lower-income tiers American Immigration Council (2022). Education also plays a role: veterans with college or technical training (often younger veterans using the GI Bill) may be more comfortable acquiring new digital skills, whereas those with only a high school education might not have had formal computer training. Nevertheless, military technical training can offset some differences. Still, digital literacy programs may need to be tailored, and financial strain can increase scam vulnerability.

Rural vs. Urban Geography

Geographic location critically influences digital experiences. Rural veterans often face limited broadband and isolation. In Colorado, many veterans live in rural mountain or plains communities where broadband options are sparse; rural Coloradans (veterans and non-veterans alike) are about three times more likely to lack home internet than urban residents (10% vs. 3.4%) Benton

Institute for Broadband & Society (2024). Even when broadband is available, rural connectivity may be too slow or unreliable. Rural veterans might have to travel long distances for digital training and are more susceptible to telephone scams. In contrast, urban veterans typically enjoy better internet access and proximity to digital resources.

Disability and Health Status

Veterans experience higher rates of disability than the general population — in 2022, over 30% of veterans reported at least one disability Benton Institute for Broadband & Society (2024). Disabilities (e.g., vision impairment or fine motor issues) can hinder digital literacy. Cognitive impairments (such as traumatic brain injury or age-related dementia) can further reduce the ability to learn new technologies or detect scams. Scammers often target veterans with cognitive issues, as seen in repeated fraud cases among older veterans with dementia Hersey (2023,?). Additionally, mental health conditions (e.g., PTSD, depression) may reduce proactive engagement with technology. Advances in adaptive technology (e.g., screen readers, voice-controlled devices) offer promise, but ensuring access and training remains challenging. The VA and state programs have begun addressing these issues Benton Institute for Broadband & Society (2024).

Race and Ethnicity

Veterans are a racially and ethnically diverse group. Racial minorities among veterans often face compounded disparities, such as lower wealth and reduced broadband adoption. A JAMA study found that Black veterans had a significantly higher prevalence of lacking reliable internet (31.1%) compared to white veterans (19.4%) Russell et al. (2024). Structural inequalities related to income, neighborhood infrastructure, and historical exclusion affect digital access. Additionally, non-native English speakers may have difficulty navigating digital content and scam communications. Culturally competent, multilingual outreach is essential.

Gender and Family Status

The veteran population is predominantly male (approximately 90% nationally), but women are the fastest-growing subgroup. Female veterans, who tend to be younger, generally exhibit digital literacy patterns similar to the younger cohort Russell et al. (2024). Family status is also important: married veterans or those living with family might have support for technology use, while single or widowed veterans, particularly older ones, may lack such support.

Conclusion and Recommendations for Future Action

Conclusion

Veterans in both Colorado and nationwide face a complex interplay of challenges regarding digital literacy and scam vulnerability. Data from the past seven years show a clear generational divide: older veterans often struggle with basic digital access and skills, leaving them vulnerable to fraud, whereas younger veterans are generally tech-proficient but still heavily targeted by sophisticated scams. Colorado's veteran population reflects these national trends, with urban tech hubs contrasted by rural areas where many remain disconnected. The consequences are significant: inadequate digital literacy impedes access to telehealth, benefits, education, and employment, while high scam vulnerability threatens financial security and trust. Although Colorado has made strides (with slightly lower rates of veterans offline and proactive state planning) American Immigration Council (2022,?), broader issues remain that require attention. Ultimately, improving digital literacy and reducing scam risk is not merely a technological challenge — it is about honoring our commitment to veterans' wellbeing.

Future Study Areas

Further research should focus on:

- Longitudinal studies tracking veteran digital skills over time.
- Evaluations of specific interventions (e.g., a 5-week computer course for seniors).
- Examining the psychology behind veteran-targeted scams, including the impact of military training.
- In-depth qualitative studies to understand veterans' attitudes toward technology and fraud.

Policy and Programmatic Recommendations

Based on the literature review, the following recommendations are proposed:

1. **Expand and Fund Digital Literacy Programs:** Develop veteran-centric digital literacy training by adapting curricula with relatable military analogies (e.g., likening cybersecurity to physical security

protocols) Benton Institute for Broadband & Society (2024). Collaborations among libraries, community colleges, nonprofits, the VA, and the Colorado Department of Veterans Affairs are recommended.

2. **Improve Broadband Access and Device Availability:** Expand broadband infrastructure in rural and underserved areas. The Cleland-Dole Veterans Benefits Act of 2022, which aims to enhance rural connectivity, should be fully implemented Benton Institute for Broadband & Society (2024). Programs providing free or low-cost devices and device vouchers should be supported.

3. **Strengthen Scam Prevention and Reporting Mechanisms:** Enhance fraud education and establish a “Veteran Scam Alert” system Campbell (2024). Nonprofits like AARP’s Fraud Watch Network and state agencies such as AARP ElderWatch should coordinate outreach, while legislation should enforce protections for veterans.

4. **Leverage Trusted Networks and Peer Learning:** Utilize the trust within the veteran community by training tech-savvy veterans as mentors or digital ambassadors to help peers.

5. **Integrate Digital Skills into Veteran Services:** Embed digital literacy components into existing veteran services. For instance, VA hospitals could screen for digital needs and refer veterans to programs like Digital Divide Consult Russell et al. (2024); workforce programs should include digital job readiness, and Colorado could integrate these benchmarks into its Veterans Upward Bound program VUB Colorado (2023).

6. **Data Collection and Monitoring:** Improve data collection on veterans’ digital engagement and fraud incidents by refining national surveys and FTC reporting categories.

Collaboration among the VA, state governments, veteran service organizations, libraries, tech companies, consumer protection agencies, and educational institutions is essential to ensure every veteran can safely participate in the digital world.

FAQ and Knowledge Check

Q1: What proportion of veterans lack internet access, and how does Colorado compare to the national average?

A1: As of the late 2010s, roughly one-quarter of U.S. veterans did not have high-speed internet at home. In Colorado, about 23% of veterans lacked broadband access at home versus 27% nationally American Immigration Council (2022). Colorado veterans were slightly more connected than the U.S. average. However, Colorado survey data still showed veterans were more likely to be offline than non-veterans in the state (6.5% of Colorado veterans had no home internet, compared to 4.3% of all residents) Benton Institute for Broadband & Society (2024).

Q2: Why are older veterans generally less digitally active than younger veterans?

A2: Older veterans grew up in a pre-digital era and thus often have less exposure and comfort with technology. Many veterans over 50 (especially 60+) have lower rates of device ownership and internet use Russell et al. (2024). They may feel that going online isn't necessary or is too complicated – indeed, two-thirds of veteran households without internet cited "no interest or need" for it Benton Institute for Broadband & Society (2024). Physical and cognitive challenges with age (e.g. poor eyesight, unfamiliarity with computers) also contribute. In contrast, younger veterans (under 49) served during the internet age and typically use computers and smartphones routinely, so they tend to be far more digitally active. Essentially, it's a generational difference in experience and skills.

Q3: In what ways do digital literacy gaps manifest among veterans?

A3: Digital literacy gaps show up as lower usage of common online services and lower confidence with technology among some veterans. For example, veterans (driven by the older cohort) use social media and job search sites at significantly lower rates than the general public Benton Institute for Broadband & Society (2024). Many are not aware of or comfortable with tasks like managing healthcare appointments online or using email effectively. Another manifestation is veterans having internet access but only using it for very limited purposes (or relying on someone else to help). The FCC found that lack of digital skills and a sense that the internet isn't relevant are big reasons some veterans stay offline Benton Institute for Broadband & Society

(2024). So, gaps include both practical skills (how to use devices, software) and mindset/awareness (understanding the benefits of being online).

Q4: What types of scams are most commonly targeting veterans?

A4: Veterans face a variety of scams, but some of the most common scams exploit their military service or benefits. These include: “benefits buyout” scams – offering a lump sum cash in exchange for signing over VA pension or disability payments (which is always a bad deal and often fraudulent) Campbell (2024); phony VA or government calls – imposters pretending to be from the VA, IRS, or law enforcement demanding payments or personal information Hersey (2023); charity scams – fake veterans’ charities seeking donations; fee scams – charging for records, benefits applications, or COVID/PACT Act benefits that are actually free services AARP (2023); and various identity theft and phishing schemes targeting military/vet info. AARP’s research indicated that 4 out of 5 veterans had been targeted by scams tied to their service/benefits in just one year Campbell (2024). Additionally, like all consumers, vets also get hit by general scams (tech support scams, lottery scams), but the fraudsters often add a military twist (e.g., “veteran discount” offers that are fake) to lure them in.

Q5: Why might veterans be more likely to lose money to scams than civilians?

A5: Statistics show veterans are about 40% more likely to lose money to fraud than non-veterans Campbell (2024). There are a few reasons for this. One is that scammers specifically target veterans – knowing they may have steady military pensions or VA benefits, criminals see “follow the money” opportunities Campbell (2024). Veterans also share a common bond and trust; scammers exploit that by posing as fellow veterans or authority figures from veteran services, making their ploys more believable. Additionally, some veterans, particularly older ones, may be more isolated or less digitally savvy, which can make them easier prey. There’s also the factor of frequency – veterans and military families get bombarded with more scam contacts (robocalls, etc.) than average Service (2021), so statistically they have more “chances” to be defrauded. Lastly, a sense of duty or respect for officialdom ingrained during service might lead some vets to comply when someone impersonating an officer or government agent calls threatening action – a manipulation of their training. All these factors combine to elevate the risk of financial loss.

Q6: What are some barriers veterans face in adopting digital technology?

A6: Key barriers include lack of affordable internet or devices, insufficient digital skills, and attitudinal barriers. For low-income veterans, the cost of monthly broadband or buying a computer can be prohibitive – veterans with the lowest incomes are the most likely not to have home internet Benton Institute for Broadband & Society (2024). In rural areas, the barrier might be simply that high-speed service isn't available or is very slow Benton Institute for Broadband & Society (2024). On the skills side, veterans who haven't had training may find technology intimidating or confusing – for instance, not knowing how to set up a secure Wi-Fi or how to use videoconferencing (which became important for telehealth). Attitudinal barriers are significant: some veterans question the relevance of the internet in their lives Benton Institute for Broadband & Society (2024), or they have privacy/security concerns that deter them from going online. Disabilities (like hearing or vision loss, or mobility issues) can also be barriers if adaptive tech isn't in use. Essentially, barriers range from economic (cost), infrastructure (access), educational (know-how), to personal (mindset).

Q7: How do socio-economic and geographic factors influence a veteran's digital experience?

A7: Socio-economic status (income, education) and geography (urban vs rural) play a huge role. Lower-income veterans often can't afford top-notch internet or the latest devices, and may live in areas with fewer free digital resources (e.g., no nearby library with computers). They might also prioritize other expenses over tech. Education can influence comfort with learning tech – a more educated veteran might pick up new digital skills faster or have been exposed to computers during schooling. Geography is critical: urban veterans usually have better internet options (multiple providers, higher speeds) and likely cell coverage, plus physical access to places like libraries, VA centers, or Apple stores for help. Rural veterans might have only one spotty internet provider or rely on satellite internet, and they might be 50 miles from the nearest digital skills class. Rural vets thus face more hurdles getting online and might have to travel to get tech help. Additionally, rural communities might have tighter social circles – which can be good (word of mouth about scams travels fast locally) or bad (if one scammer hits a small town, they might hit many vets there before word spreads). In Colorado, for example, veterans in Denver have very different digital landscapes than those in a small mountain town. These factors influence how easily a veteran can become digitally literate and how exposed or protected they are from fraud.

Q8: What research or data is still needed to better address veteran digital literacy and fraud?

A8: Experts see a need for more veteran-specific data and tailored studies. For example, regular surveys that track veterans' digital skill levels (like ability to perform certain online tasks) would help measure progress and needs. Data split by age, era of service, and state/region would refine our understanding – e.g., how do Vietnam vets in Colorado compare to Gulf War vets in New York in internet use? We also need more data on scam incidents specifically involving veterans (separated from active-duty) and what the outcomes are. Right now, many stats combine all "military consumers." Another research need is to evaluate what interventions work best: does giving a veteran a free tablet and a training session increase their usage and decrease their likelihood of being scammed? Which educational messages change behavior? There's also interest in qualitative research – hearing directly from veterans about their challenges or why they might distrust technology, to inform more empathetic solutions. In short, more granular data and more outcome-focused research (what actually reduces the digital divide and scam losses) would greatly help practitioners design effective programs.

Q9: What are some recommended actions to improve digital literacy among veterans?

A9: Recommendations include: expanding affordable broadband and device programs for veterans (so cost isn't a barrier), offering veteran-focused digital training (through VA hospitals, vet centers, libraries, and nonprofits) on everything from basic computer use to safe internet practices, and leveraging peer support – for instance, having tech-savvy veterans teach their fellow vets in the community. Tailoring training to resonate with veterans is encouraged (for example, using military terminology or examples in the curriculum) Benton Institute for Broadband & Society (2024). Another action is integrating digital skills assistance into existing veteran services – if a veteran visits a VA clinic, there could be information available about enrolling in an "Internet 101" class or an advisor who can answer tech questions. On a broader scale, making sure that organizations that serve veterans (like the VFW, American Legion halls) are equipped with Wi-Fi and computers for vets to use can provide practice opportunities. Essentially, it's about meeting veterans where they are, both literally (in communities, at

VA facilities) and figuratively (in terms of starting skill level), and providing the resources and encouragement to get them comfortable online.

Q10: How are policymakers and organizations addressing scams against veterans?

A10: In recent years, there's been a notable increase in efforts to protect veterans from fraud. For example, the VA Secretary formed a task force in 2023 specifically to tackle scams targeting veterans, aiming to coordinate prevention and response across agencies Hersey (2023). Laws and bills are being introduced – some states have made it illegal for unaccredited groups to charge veterans for help with benefits (closing a scam loophole) Campbell (2024). The Federal Trade Commission and state attorneys general have been issuing consumer alerts around Veterans Day to highlight common scams. Nonprofit organizations like AARP have initiatives (AARP's Operation Protect Veterans) which send out scam alerts and educational materials to veterans. There are also partnerships forming: for example, the U.S. Postal Inspection Service and AARP released the "Scambush" report to shed light on the issue Campbell (2024). On the ground, many VSOs (Veteran Service Organizations) now include fraud awareness in their newsletters or meetings. In Colorado, the Attorney General's Office partners with AARP ElderWatch to host fraud webinars for older adults, including veterans. So policymakers are responding through legislation, task forces, and support for outreach programs. The consensus is that it requires constant vigilance and updated strategies, since scammers adapt quickly. The hope is that through these combined efforts – law enforcement, regulation, and education – the tide of fraud losses impacting veterans will be stemmed in the coming years.

References

AARP (2023). Veterans are disproportionately targeted by scammers. [Press Release – AARP Alaska].

American Immigration Council (2022). Examining gaps in digital inclusion in colorado. [Fact sheet].

Benton Institute for Broadband & Society (2024). Coloradans at the heart of state's digital access plan. [Blog post].

Campbell, J. (2024). Testimony in support of sb 831 – veterans' benefits services – fees and compensation. Maryland Senate Education, Energy, and Environment Committee. (Citing AARP "Scambush" survey results).

Committee, U. H. (2020). Hijacking our heroes: Social media spoofing of veterans. Report.

Hersey, L. F. (2023). "my savings were drained": Veterans' pensions and benefits are a target for fraud, feds warn. Stars and Stripes.

Russell, L. E., Cornell, P. Y., Halladay, C. W., Kennedy, M. A., and Cohen, A. J. (2024). Sociodemographic and clinical characteristics associated with veterans' digital needs. *JAMA Network Open*, 7(11):e2445327.

Service, A. . U. P. I. (2021). Military veterans battle surprise attacks from scams and fraud – key findings. Washington, DC: AARP. [Summary of survey findings].

VUB Colorado (2023). Veterans upward bound program in colorado. Website.