NEW AMERICA

September 2025

Digital Gaps, Cyber Threats: Designing Policies to Keep People Safe Online

Nina-Simone Edwards

Future Security
Last edited on September 09, 2025 at 8:56 a.m. EDT

Acknowledgments

I would like to thank Bridget Chan for her consistent efforts and patience throughout the writing and publication process, Stephanie Weiner and Ayan Islam for the excellent advice and feedback, and Alex Briñas for the beautiful graphics.

Editorial disclosure: The views expressed in this report are solely those of the author(s) and do not reflect the views of New America, its staff, fellows, funders, or board of directors.

About the Author

Nina-Simone Edwards is a 2025 #ShareTheMicInCyber Fellow.

About New America

We are dedicated to renewing the promise of America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Future Security

Future Security is a partnership between New America and Arizona State University. It reconceptualizes U.S. security policy towards a holistic engagement with current and future challenges including domestic terrorism, armed drones, climate change, pandemics, rising authoritarianism, and new and emerging technologies.

About #ShareTheMicInCyber Fellowship

The #ShareTheMicInCyber Fellowship invests, grows, and platforms emerging cybersecurity and technology leaders from traditionally underrepresented backgrounds in support of strengthening our nation's resilience to digital threats.

Contents

Introduction

Despite increasing digital risks, existing policies fail to adequately protect internet users. Digital divide policy—encompassing policy and strategies aimed at reducing digital inequalities—often focuses on access, yet fails to address the real cybersecurity risks that users face online. Cybersecurity policy has understandably centered on technical defenses and expert-driven solutions. These two domains are tackling different dimensions of the same underlying problem: vulnerability in digital environments. Without integrating both perspectives, users—especially those navigating limited digital environments—remain disproportionately vulnerable. A more effective approach requires these policy areas to inform one another, ensuring that a lack of digital access, skills, or literacy does not lead to a cybersecurity risk.

Typically, the response to a cybersecurity risk is to eliminate that risk through system-level safeguards, secure design, and vulnerability mitigation. Cybersecurity policy and related frameworks like those developed by the **National Institute of Standards and Technology** and the **nonprofit research organization RAND** have naturally followed this structure. However, these frameworks have an underemphasized but important recognition: users themselves need more information and support to understand their vulnerabilities. Without a stronger effort to equip individuals, current frameworks risk protecting the infrastructure while leaving users exposed to malicious online threats.

This report aims to challenge assumptions behind both cybersecurity and digital divide policy by highlighting how human vulnerabilities—such as lack of access to secure infrastructure, low digital literacy, and insufficient digital skills—directly contribute to cybersecurity risks. While scams, fraud, and exploitative tactics are often framed as cybersecurity awareness issues, this perspective can overlook deeper, root causes that shape how individuals experience and respond to risk in an increasingly connected world. When we understand that human vulnerabilities are inseparable from cybersecurity risks, the path toward effective, integrated solutions becomes clearer.

The report begins by first defining what is meant by cybersecurity vulnerabilities and homing in on an important but underappreciated subset of these vulnerabilities—human vulnerabilities. The report then examines and critiques traditional narratives and assumptions that have hindered the recognition of human vulnerabilities in understanding cybersecurity risks, which in turn have limited the formulation of effective responses. Next, the report discusses a potential convergence in policymaking designed to bridge the digital divide and cybersecurity policymaking. The report concludes by discussing concrete policy solutions, informed by the groundwork laid by previous efforts related to addressing the digital divide, while underscoring

the urgent need for more effective, equity-driven approaches. At the intersection of human and cybersecurity vulnerabilities lies the opportunity to build a more equitable digital future—one where all users are empowered to engage securely and confidently.

I. Defining Vulnerability

Cybersecurity Vulnerabilities

Cybersecurity refers to the system of practices, technologies, and policies used to protect data, devices, and users against **threats, risks, vulnerabilities**, and other cyber harms. A cybersecurity "vulnerability" is a weakness or gap that can be exploited; a cybersecurity "threat" refers to malicious actors attempting to gain unauthorized access by exploiting a vulnerability; and a "risk" is the potential loss or damage that results from a threat exploiting a vulnerability. A threat may be due to malware or to the "human factor" (the general understanding that people will make mistakes).[1] According to a 2025 Verizon report, 60 percent of all security breaches include some sort of human error (such as weak passwords, privilege misuse, or social engineering).[2] Threats or risks may also be due to social engineering (tricking someone to reveal information), phishing attempts (fake emails or messages that contain malware), or viruses.

For the purposes of this report, human vulnerabilities in the context of cybersecurity should be more precisely defined as a subcategory of cybersecurity vulnerabilities that is not limited to technical systems or networks. These human-centered weaknesses (beyond being prone to mistakes or errors) are often the very entry points that are exploited. Accordingly, this report will highlight this subcategory when referring to the phrase "cybersecurity vulnerabilities," but will retain the two different phrases ("human vulnerabilities" and "cybersecurity vulnerabilities") to clearly articulate the bridge being built in this report between digital divide and cybersecurity policy.

Human Vulnerabilities

Although there are disciplines that study the impact of technology on people, or how someone who is vulnerable may be susceptible to certain risks, the definition of vulnerability used here is grounded in feminist and feminist legal theories.[3] This choice is intentional: Feminist approaches treat vulnerability not as personal weakness but as a universal and structurally produced condition. By adopting this lens, the analysis shifts from individual blame and instead focuses on how systems create and perpetuate unequal exposures to harm. The result is a more critical examination of the vulnerabilities digital users face, and keener insights into how they might be addressed and eventually eliminated.

Martha Fineman, a leading scholar on critical legal and feminist legal theories and philosophies, describes vulnerability as both universal and situational.[4] Essentially, everyone is vulnerable in some way, but their particular vulnerability hinges on the specific circumstances they face. This perspective shifts the concept of vulnerability from a given status or identity. Fineman's definition instead emphasizes the relationship between individuals and the state, which she believes has a responsibility to protect those rendered vulnerable by specific conditions. This report agrees with Fineman: There is a particular role that the government should play for those who are made vulnerable in digital circumstances.

The digital circumstances most relevant to this report are related to digital access, digital literacy, and digital skills. "Digital access" refers simply to access to the internet and other digital tools or systems. For some communities, access is limited not just by infrastructure, but by affordability, language, or cultural barriers. For example, if an artificial intelligence (AI) tool that individuals must use in order to access government-administered services does not provide translation services in the language they are comfortable speaking, that individual cannot be said to have access to that system, even if they have internet access.

Digital access, skills, and literacy are components of what is commonly referred to as the digital divide. In the late 1990s, the digital divide was used to describe the digital "haves and have-nots."[5] This understanding of the digital divide guided policy efforts that persist to this day. In 1999, the National Telecommunications and Information Administration published *Falling Through the Net*, a report that defined the digital divide and provided data on the levels of access in the United States.[6] Today, despite so many lacking the ability to adequately use technology (that is, those lacking literacy and skills), the term "digital divide" is still primarily used to refer to broadband access.[7] When this report uses the term, it is referring not just to access, but to digital skills and literacy as well. All three dimensions of the digital divide are framed here as human vulnerabilities, as they increase the risk of exposure to cybersecurity threats. Further, each dimension represents a distinct but interconnected barrier that can increase an individual's exposure to digital risk.

Digital literacy and skills are often used interchangeably, but there is an important distinction. "Digital literacy" refers to one's ability to effectively understand, navigate, and evaluate digital outputs. Outputs can be anything from the text of a website to an AI-generated image. As the American Library Association notes, digital literacy includes not just the ability to evaluate digital tools but also critical thinking and the ability to use, interpret, and locate information.[8]

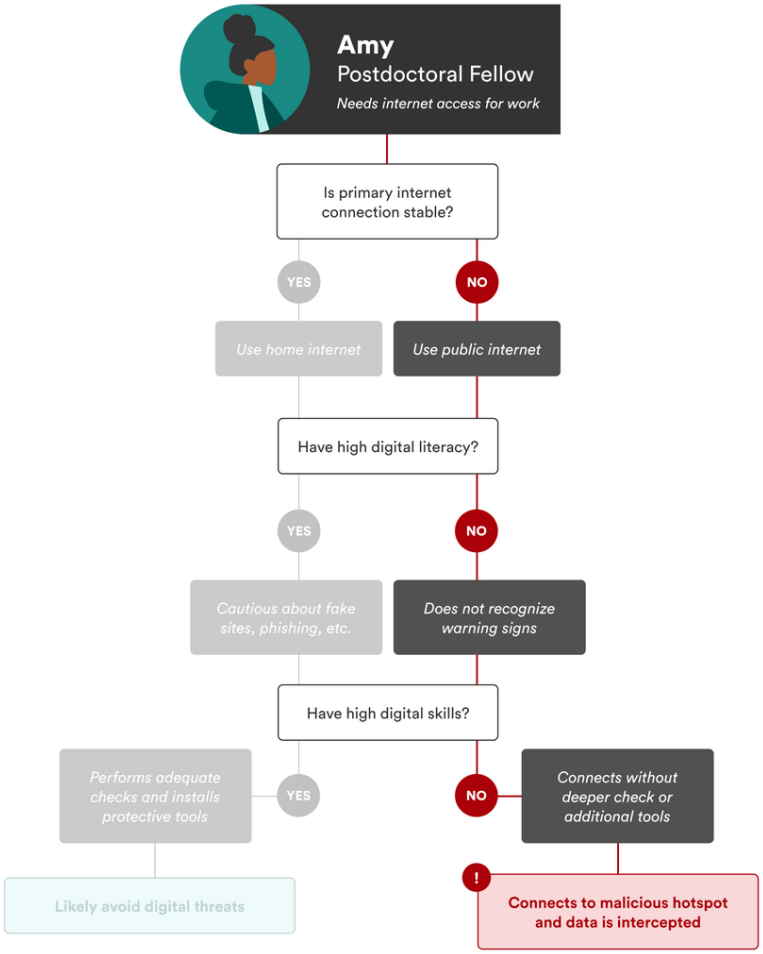
Relatedly, "digital skills" refer to the practical abilities one has to effectively engage with and use digital tools and systems. To differentiate between

literacy and skills, consider a hypothetical student named Amy. Amy is a postdoctoral fellow living in affordable but poorly connected student housing. Her underground unit offers only spotty internet, forcing her to spend time at a café across the street to reliably access the internet. Last week, Amy connected to what she thought was the café's Wi-Fi hotspot. After entering the usual password, she was taken to a screen she did not recognize. It claimed she was "logged in," so she closed the screen. Unbeknownst to her, Amy had connected to a malicious hotspot with the same name as the café network. Her data was quickly intercepted.

In this scenario, as illustrated in Figure 1 below, digital literacy might have helped her recognize something was amiss. International research indicates that individuals with stronger digital literacy tend to be more aware of security risks and engage in proactive behaviors to mitigate them.[9] However, recognizing a risk does not automatically translate into action: Amy needed both digital literacy *and* skills. Digital skills would have enabled her to proactively investigate the network, adjust her security settings, and even install additional protections on her computer.

Thus, lacking sufficient digital literacy or skills, Amy became vulnerable to cybersecurity risks. In fact, her vulnerability began due to her lack of access: She would not have gone to the café if she had had a reliable connection in her home.

Figure 1 | Limited Digital Access, Literacy, and Skills Lead to Data Interception



Source: Alex Briñas/New America

Moving Away from Simplistic Labels

When discussing these vulnerabilities, it is important to move beyond surface-level labels and consider how structural conditions shape individual experiences. It may be easy to say that Amy was "vulnerable" simply because she lacked digital access. More accurately, she was rendered vulnerable because of her situation, which is a critical distinction from labeling her as inherently or permanently vulnerable. Vulnerability is context dependent.

In an early comment on digital divide policy, digital librarian Steve Cisler cautioned against labeling people as digital haves or have-nots because it

creates overly simplistic binary categories.[10] At any given moment, one could be rendered vulnerable and become a digital have-not due to a specific situation, like a sudden lack of internet access or the inability to navigate a specific system, highlighting the fluidity of vulnerability. The label matters less than understanding the conditions that produced the vulnerability.

This critique of oversimplified labels highlights the importance of understanding feminist theories of vulnerabilities, such as Florencia Luna's concept of layered vulnerability. Luna argued that vulnerabilities should not be thought of as static traits but as layers that accumulate in specific contexts.[11] This layered approach ultimately enables a more nuanced analysis.

Here, each situation that renders someone vulnerable adds a new layer that compounds risk or increases exposure. In Amy's case, her situation became more precarious not just because she lacked digital access (which could be considered her first layer of vulnerability), but because she also lacked digital literacy and skills (the second and third layers). Thus, affixing the label of "vulnerable" to someone without access, literacy, or skills is not as useful as understanding vulnerability as a universal, context-dependent layered concept. It should be further noted how language is limiting in this situation: While it does make sense, here, to identify Amy as vulnerable due to her lack of access, skills, and literacy, policymakers should explore the hows and the whys of her specific vulnerabilities (in other words, the situation and the context), which can lead to more sophisticated, diverse solutions to addressing them.

Instead of saying, "Amy is digitally vulnerable. She needs X," policymakers should explore how Amy is vulnerable and try to understand what she needs to address each layer of vulnerability, because "X" alone may not be adequate. If "X" were reliable internet connectivity (either in or outside her home), Amy would have digital access—but she still might lack digital literacy and skills to identify malicious or suspicious activity. In this case, "X"—internet connectivity—would only postpone her exposure to digital risk, not eliminate it. The push for understanding layers of vulnerability is important for this more thorough analysis.

II. Challenging Traditional Narratives

Before examining the link between human and cybersecurity vulnerabilities, there are a few narratives and assumptions that must be addressed. These narratives have shaped how policymakers and the public understand digital risk, often obscuring the structural and human factors that may make people vulnerable. Challenging these narratives is essential to building policy that adequately addresses the full scope of today's cybersecurity landscape. This section outlines these narratives and illustrates how they influence public perception and policy responses to cybersecurity threats.

It Could Never Be Me!

"I never thought I was the kind of person to fall for a scam," said Charlotte Cowles, a financial advice columnist.[12] She was the victim of an elaborate scam that ended with her handing over $50,000 in a taped-up shoe box. She described herself as the opposite of what many would consider "easy" victims of scams: rational, economically secure, with high financial literacy, and a vibrant social life. Yet, she still lost tens of thousands of dollars in one day. Cowles's case does not directly address the human vulnerabilities discussed in this report, but she exemplifies a mindset shared by many—that it could never happen to me.

According to the Federal Trade Commission (FTC), there was a 25 percent increase in consumer losses from 2023 to 2024 due to fraudulent activity, including scams.[13] Scams, defined as a "type of fraud where a victim is deceived into willingly sending money or sharing personal information," have found a home on social media, which has become the most popular method used by scammers to contact their victims, according to reports from January 2021 to June 2023.[14] During this period, $2.7 billion was reported lost to fraud originating on social media, outpacing websites and apps, which accounted for $2 billion in reported losses.

These scams will continue to occur only if everyone believes they are the exception. Many people like Charlotte Cowles believe that they could never become a victim of a scam. The FTC's figures—which notably include only reported losses, meaning there are more losses that go unreported—reveal a disturbing truth, however, that no one is exempt.

A Focus on the Technical, Even in Policy

While the cybersecurity industry emphasizes technical solutions for identifying, analyzing, and mitigating system vulnerabilities, this focus alone is not sufficient for effective cybersecurity policy that protects all. The prevailing logic centers on securing a company's system—which is a necessary undertaking, and one that understandably shapes policymakers' cybersecurity priorities. However, technical solutions can overlook a critical component briefly highlighted in the 2016 RAND *Framework for Exploring Cybersecurity Policy Options*: the user and their vulnerabilities.[15] While the RAND framework was developed to help policymakers draft cybersecurity policy, it also recognizes that users must be better informed about the vulnerabilities that affect them. In the nearly 10 years since the framework was devised, however, this recognition has not translated into sufficient policy action. Policymakers should understand human vulnerabilities when developing frameworks and policies to ensure people are adequately protected.

The User Is the Problem

"The user is the problem" is a narrative that places the victim at fault. "You should have known!" or "Why would you trust that?" are phrases commonly heard by those who have fallen victim to a scam or other form of fraud.[16] This is problematic because, while there are protective measures one can take, it is impossible to predict and counter every single cybercrime. This narrative is unproductive in a world that does not currently provide adequate education about how to protect oneself online. In the United States, laws and relevant frameworks have only slowly addressed online risks, such as data privacy or cyber incident reporting, which means that there are still only a few protections (and protectors) for scams and frauds perpetrated online. The FTC helps enforce in the area of consumer protection, but when harm is not easily quantified or defined, the FTC can only do so much.

Only Certain People Get Scammed

The idea that only certain people get scammed, perhaps the most prevalent assumption about cybercrimes, is related to the assumption that "it could never be me!"[17] The difference is that policies have been shaped by assumptions that only certain groups, such as the elderly or those who do not have active digital lives, fall prey to digital scams. Yet these assumptions are not true: Younger adults, according to FTC data, were found to be 34 percent more likely to report having lost money to fraud than the elderly.[18] Scams cut across every political, demographic, and cultural line and affect people from all walks of life.

The increased use of artificial intelligence (AI) makes this assumption even more harmful. For example, despite internet users' increasing exposure to AI tools like ChatGPT and AI-generated content, people remain extremely susceptible to AI-enabled scams. There have been a slew of recent high-profile cases in which individuals believed they were chatting with **celebrities** when they were actually interacting with AI chatbots. During the 2024 U.S. presidential election, thousands of individuals in **New Hampshire** were discouraged from voting after receiving phone calls they believed to be from President Joe Biden but were really AI-generated robocalls. Not only is the assumption that only certain people get scammed untrue when related to the use of AI, hackers and others with malicious intent are increasingly using AI-generated content to scam. AI, and other digital tools and systems, only **exacerbate** the issue and further highlight the flawed belief that those with a high propensity to be scammed meet a certain profile.

Most Individuals Have High Digital Skills and Literacy

Given the prevalence of individuals online, there is also an assumption that many people already have high degrees of digital literacy and skills. However, one-third of Americans lack the basic digital skills that are needed to engage successfully in the modern economy.[19] A 2023 Pew Research study found that less than 60 percent of U.S. adults answered digital literacy questions correctly.[20] Even further, as a 2025 report by the Harvard Business School noted, "At a time when AI is expected to streamline business operations and render some functions obsolete, inexperience with digital technology could limit people's careers."[21] The shift toward AI is only heightening the urgency of expanding digital skills.

This lack of digital skills, literacy, and access could lead to hypothetical situations like Amy's or real-world situations like Charlotte Cowles's. Amy lacked digital access—but equally important, she lacked the digital literacy that could have allowed her to detect the threat and the digital skills to take appropriate precautions.

III. The Policy Imperative: Understanding the Link Between Human and Cybersecurity Vulnerabilities

When policymakers and standards developers design cybersecurity frameworks, they focus on the needs and perspectives of industry professionals. The National Institute of Standards and Technology (NIST) cybersecurity framework serves as a useful example.[22] The NIST framework is a widely used but voluntary guide for cybersecurity activities and practices within organizations. Frameworks such as this are useful for guiding organizational cybersecurity protocols, but they largely overlook the human and systemic factors that could also lead to cybersecurity risks.

Scholars have studied the "human factor" and the human vulnerabilities (typically understood as mistakes or a lack of training) that lead to cybersecurity risks within companies, but this research is not prevalent in, nor meaningfully integrated into, policy frameworks. This report is not advocating for replacing technical approaches with human-centered ones; rather, it proposes adapting the risk management mindset that underpins frameworks like NIST's to better address the human vulnerabilities this report has defined: limited digital access, skills, and literacy.

The RAND framework takes a step in that direction by recognizing the role of government and considering the interconnected concerns of various cybersecurity stakeholders. Developed in consultation with a variety of industry professionals and experts, the framework is intended to guide policymakers, and it is instructive. It identifies users as stakeholders and emphasizes "the need to provide information to users about their vulnerabilities and risks."[23] It also highlights the necessity of educating consumers on cybersecurity best practices and managing privacy. RAND acknowledged that more research is needed for cyber education and awareness in its framework—a gap this report seeks to fill, particularly by integrating insights from digital divide policy.

Instead of broad focuses on cyber education and awareness, policymakers can channel the existing body of research and literature from digital divide policy. Both the Broadband Equity Access and Deployment Program (BEAD) and the Digital Equity Act (DEA) of 2021 take aim at the digital divide: BEAD by (primarily) seeking to expand access, and the DEA by seeking to increase digital literacy and skills.[24] Although BEAD and the DEA have both faced devastating funding cuts in the early months of the second Trump administration, their creation reflected a bipartisan commitment to closing the digital divide.[25] Tackling the digital divide, which is increasingly framed as a rural economic issue, remains a concern across party lines despite shifts in federal priorities that have disrupted national momentum toward broader digital inclusion.[26]

However, what is missing in both programs is a recognition of the link between the human vulnerabilities of the digital divide and cybersecurity vulnerabilities. In today's increasingly digital world, it is more important than ever to explore, understand, and find solutions for the human vulnerabilities that serve as entry points for cybersecurity vulnerabilities. Understanding this connection will enable more effective, inclusive, and preventative cybersecurity policies for the public.

Policymakers should apply the risk management approach used in organizational cybersecurity policy to address human vulnerabilities related to limited digital access, skills, and literacy. Just as organizations identify, assess, and mitigate technical threats in their systems, policymakers should systematically evaluate how human vulnerabilities create cybersecurity vulnerabilities and develop proactive safeguards to reduce harm at the human level. In Amy's case, the likelihood of a cybersecurity incident was heightened precisely because of her human vulnerabilities. Even more, the likelihood increased due to her layered exposure: She was rendered vulnerable due to both systemic (access) and individual (skills and literacy) factors. To better protect individuals like Amy, cybersecurity and digital divide policies must be strategically aligned: bridging technical risk management understandings with the human-centered prioritization of digital divide policies.

What the Data Show

To understand how human vulnerabilities contribute to cybersecurity vulnerabilities, this report draws on both testimonial and governmental data sources. First, 50 testimonial cases of online scams were identified and analyzed, drawn from news stories and user-submitted experiences. These cases were chosen to explore the intersection between human and cybersecurity vulnerabilities. While hypothetical cases like Amy's illustrate how human vulnerabilities can lead to a cybersecurity breach, many people are

rendered vulnerable through scams such as phishing, social engineering, and other tactics employed by malicious actors. These scams exploit gaps in digital literacy, skills, and access, making them a practical lens through which to examine the real-world consequences of human vulnerabilities.

In addition to these qualitative accounts, Federal Trade Commission (FTC) data on the types of scams, frequency, demographic patterns, and other characteristics of reported scams were reviewed. These data provide a more comprehensive, national-level picture of cybersecurity threats as experienced by the public. Taken together, the two sources capture individual experiences and how they map onto larger trends. They also serve as a foundation for identifying common conditions that render people vulnerable and for proposing policy responses grounded in lived experience.

Testimonial Evidence

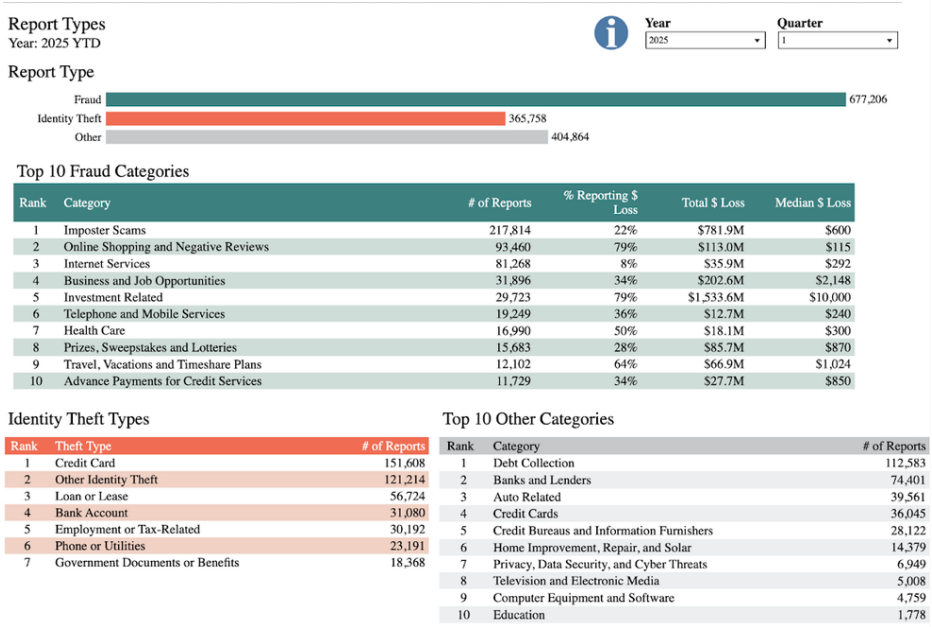
Although online scams are not a new phenomenon, viral news reports have circulated of AI-generated images of a **hospitalized Brad Pitt** or the **AI-generated voice recordings** of President Biden. A Johnny Depp impersonator **"swindled"** as many as 26 elderly people out of money. **"Kevin Costner"** also entered the mix, with scammers demanding money for entry into his fan club, and **Truth Social** has been the site of a variety of scams. All of these scams—and many others not noted here—share one common factor that has not been directly connected to scam analysis: While there are a variety of sources that may attribute the rise of these scams **solely** to age (which we know is **not true**), each of the individuals scammed was rendered vulnerable because of their lack of digital literacy or skills.

And while fewer people may fall for a scam once it has received media attention, the data illustrate how many people are affected by the human vulnerabilities that this report focuses on. Analysis of the 50 cases reveals a common pattern: Victims often lacked digital literacy to recognize potential risks and the digital skills to investigate suspicious activity or implement protective measures.

Federal Trade Commission Data

As shown in Figure 2, the FTC tallied 677, 206 reported cases of online fraud and 365,758 reported cases of identity theft in just the first three months of 2025.

Figure 2 | 2025 Federal Trade Commission Reported Frauds Data



Top 10 Fraud Categories

Rank	Category	# of Reports	% Reporting $ Loss	Total $ Loss	Median $ Loss
1	Imposter Scams	217,814	22%	$781.9M	$600
2	Online Shopping and Negative Reviews	93,460	79%	$113.0M	$115
3	Internet Services	81,268	8%	$35.9M	$292
4	Business and Job Opportunities	31,896	34%	$202.6M	$2,148
5	Investment Related	29,723	79%	$1,533.6M	$10,000
6	Telephone and Mobile Services	19,249	36%	$12.7M	$240
7	Health Care	16,990	50%	$18.1M	$300
8	Prizes, Sweepstakes and Lotteries	15,683	28%	$85.7M	$870
9	Travel, Vacations and Timeshare Plans	12,102	64%	$66.9M	$1,024
10	Advance Payments for Credit Services	11,729	34%	$27.7M	$850

Identity Theft Types

Rank	Theft Type	# of Reports
1	Credit Card	151,608
2	Other Identity Theft	121,214
3	Loan or Lease	56,724
4	Bank Account	31,080
5	Employment or Tax-Related	30,192
6	Phone or Utilities	23,191
7	Government Documents or Benefits	18,368

Top 10 Other Categories

Rank	Category	# of Reports
1	Debt Collection	112,583
2	Banks and Lenders	74,401
3	Auto Related	39,561
4	Credit Cards	36,045
5	Credit Bureaus and Information Furnishers	28,122
6	Home Improvement, Repair, and Solar	14,379
7	Privacy, Data Security, and Cyber Threats	6,949
8	Television and Electronic Media	5,008
9	Computer Equipment and Software	4,759
10	Education	1,778

Source: Screenshot of "The Big View: All Sentinel Reports," Federal Trade Commission, August 12, 2025, https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports.

There were almost 300,000 reports of individuals falling victim to scams of the categories of fraud most relevant to this report: imposter scams; business and job opportunities; investment-related fraud; and scams related to prizes, sweepstakes, and lotteries. The testimonial evidence described above also falls into these categories: the imposter scams involving the likenesses of Brad Pitt and Johnny Depp[27] as well as scams involving fraudulent job opportunities, investments, and prizes and sweepstakes that are particularly prevalent on Truth Social. Although the aggregated FTC data lacks the specificity of the testimonial evidence on victims' experiences, the data overwhelmingly illustrate the prevalence of these scams on the national level, as well as other scams that could potentially evolve and exploit human vulnerabilities.

As seen in the hypothetical case of Amy, digital access can also be an entry point for a cybersecurity vulnerability. Amy lacked digital access and then proceeded to make decisions that led to her data being exposed. Further, this scenario, and the data shared in this section, underscore the importance of understanding how human vulnerabilities are layered. Some of the individuals scammed on Truth Social or by an imposter had digital access in order to communicate with scammers and imposters, but they did not have digital literacy or skills to navigate away from the scams they became victims of. Unfortunately, they were unable to recognize risks or check for potential malicious activity.

Although many of the scams mentioned here used AI-generated content, the scams themselves are increasingly being automated through AI. That is, scamming operations that once featured real people using AI to create images or text are now using AI tools to handle the communication itself. According to Data & Society, "Generative AI serves as a force multiplier for existing scam tactics." Data & Society describes a scenario similar to the testimonial evidence outlined in this report but with AI as the primary tool: "Workers in the [scam] compound use AI-powered translation tools to communicate fluently with targets around the world, AI-generated deepfakes to pose as good-looking romantic prospects, and large language models (LLMs) to tailor messages to each victim's interests and emotional triggers. The phone, scripts, and app interfaces are all provided by the criminal syndicate running the compound."[28] Scams are thus being elevated in terms of scale, speed, and efficiency—trends that only emphasize the need for policy solutions that understand the connection between human and cybersecurity vulnerabilities.

While this report draws on equity-based frameworks to analyze digital risks, it is important to recall the erroneous assumption that only certain people get scammed. Scams, and other cybersecurity vulnerabilities, affect people across political and social identities: This is a universal issue, not a partisan one.

IV. From Risk to Resilience: Policy and Public Awareness Pathways

As discussed elsewhere in this report, traditional narratives often frame cyber threats as issues affecting specific individuals or companies. Everyday individuals may underestimate their own human vulnerabilities, and particularly those that lead to cybersecurity vulnerabilities. This section thus divides the individual from systemic solutions, in line with the human vulnerabilities discussed throughout this report, which are both individual (literacy and skills) and systemic (access).

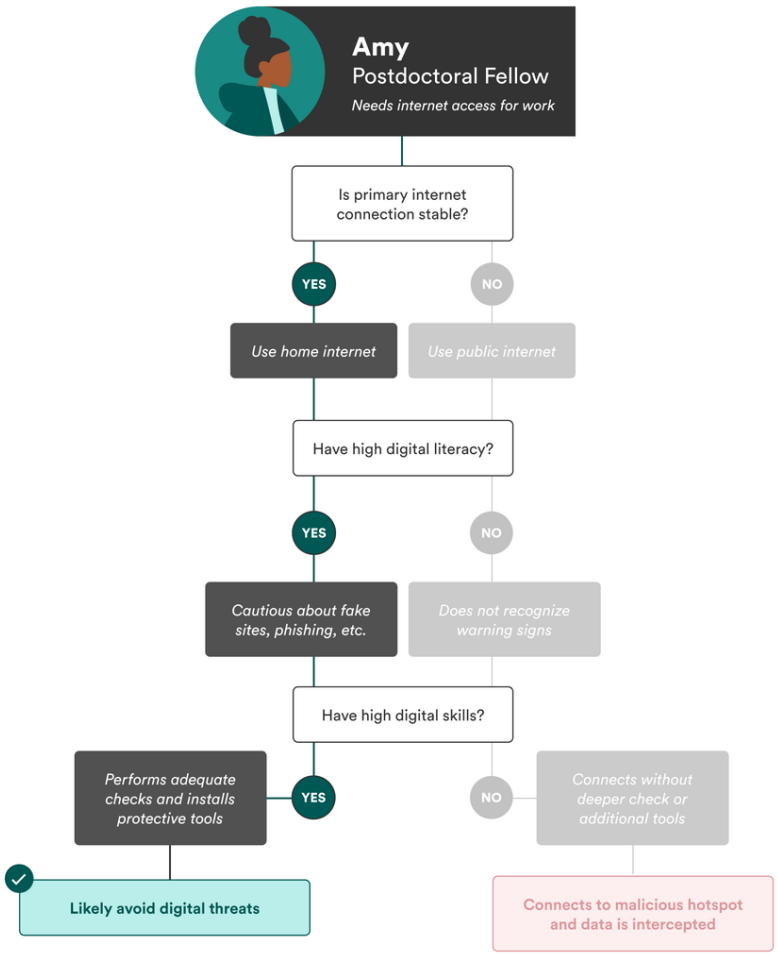
Support and Scale Individual Awareness

Policies and systemic protections are vital to reducing cybersecurity risks, but individual awareness remains a critical frontline defense, especially in light of persistent assumptions about who is truly at risk. Due to these assumptions, there is a dangerous gap between risk and perceived threat. To close this gap, individuals must first be made aware of their human vulnerabilities that may lead to cybersecurity vulnerabilities. Further, digital literacy and skills must become standard knowledge for all users, not just information technology professionals or industry experts.

Although there are human factors that can contribute to cybersecurity vulnerabilities, education increases an individual's ability and opportunity to proactively respond.[29] Cyber education and awareness must be targeted toward the understanding that gaps in digital skills, literacy, and access may produce cybersecurity vulnerabilities. These human vulnerabilities are not just isolated personal shortcomings but often reflect broader systemic inequities, and recognizing the connection between human and cyber vulnerabilities will help increase awareness and hopefully lead to proactive behavior.

If Amy had been aware of her own vulnerabilities, she might have been more cautious about connecting to the café's Wi-FI hotspot. Even if she lacked the technical skills or literacy to detect the risk outright, simply understanding her limitations, as illustrated by the steps in Figure 3, could have prompted her to seek safer alternatives or to ask for help, thereby reducing her exposure to cyber threats.

Figure 3 | Digital Access, Literacy, and Skills Enable Digital Threat Avoidance



Source: Alex Briñas/New America

However, awareness about potential threats is not enough; people must be equipped with digital literacy and skills to recognize and respond to threats effectively. Resources are increasingly available to help individuals build digital resilience, and policymakers must support these initiatives—if not through specific mandated programming or national campaigns, then through funding.

Public libraries, for example, have become valuable community hubs for digital education.[30] While libraries have always functioned as a "third place," a welcoming atmosphere other than home and work or school for community, interaction, and learning, they played a key role in closing the digital divide during the COVID-19 pandemic.[31] The Federal Communications

Commission's Digital Empowerment and Inclusion Working Group produced a report in 2021 describing congressional funding that enabled libraries to increase digital literacy and access.[32] In Illinois, for example, Evanston Public Library provided "Ready-to-Work Starter Kits" to help patrons build basic computer and literacy skills.[33]

Nonprofit organizations like the **National Digital Inclusion Alliance** (NDIA) advance digital equity by "supporting community programs and equipping policymakers to act." Through its Digital Inclusion Program Model, which provides guidance for digital inclusion programs, and its Digital Navigator Model, a replicable framework to help volunteers or staff provide digital skills and access, NDIA provides comprehensive tools to support local communities in closing the digital divide.[34]

Although the 2025 federal funding cuts have severely impacted many programs' ability to provide digital literacy and skills training and classes, NDIA and a few other local organizations are still providing help that individuals need to be better equipped to recognize cybersecurity threats.[35] To fill this gap, policy initiatives must prioritize sustainable funding for digital literacy and cybersecurity education at organizations like the NDIA. Equally important, these initiatives must explicitly address the link between human and cybersecurity vulnerabilities in order to create more comprehensive and resilient digital safety strategies. This could involve expanding NDIA's Digital Navigator Model to include awareness of human vulnerabilities specific to the communities they serve, or adapting NDIA's Digital Inclusion Program Model to emphasize partnerships between digital literacy programs and cybersecurity educators.

Design Vulnerability-Aware Cyber Policy

Attributing errors solely to individual failings reflects a narrow perspective that overlooks the critical role of institutional and systemic design in shaping human behavior. Effective cybersecurity policy must go beyond these traditional narratives, including the understanding that cybersecurity solutions are only technical in nature, and recognize that there are many different structures that create or exacerbate vulnerability.

Build on BEAD and the DEA to Address Cyber Risks

Policymakers should deepen their investment in existing frameworks—namely, the Broadband Equity Access and Deployment Program (BEAD) and the now-terminated Digital Equity Act (DEA)—to create and ensure long-term, systemic integration of human-centered approaches to cybersecurity.

BEAD acknowledges structural exclusions in internet infrastructure, but it does not go far enough in addressing the digital divide's implications for cybersecurity. Notably, the program authorized funds for non-deployment uses, which could include cybersecurity and digital skills.[36] However, on June 6, 2025, the Commerce Department paused all funding for non-deployment projects pending further guidance, casting uncertainty over the future of BEAD funding for these purposes.[37] Millions still remain in broadband deserts, and others navigate the digital world without adequate literacy or skills—all of which increases susceptibility to cyber threats.[38] Despite the important work that BEAD supports, there remains no clear mechanism that addresses the connection between human and cybersecurity vulnerabilities. The groundwork laid by digital divide policies like BEAD to expand digital access, skills, and literacy must be strengthened to directly address how lower levels of these factors can increase vulnerability to cybersecurity threats.

To achieve this, policy must center long-term investments in digital skills and literacy training aimed at the relationship between human and cybersecurity vulnerabilities. The DEA, created to help fund digital skills training, was a promising step in that direction. Its authorizing statute also mandated states' digital equity plans to include ways to document and promote "awareness of, and the use of, measures to secure the online privacy of, and cybersecurity with respect to, an individual."[39] Nonetheless, digital divide and cybersecurity policy have yet to converge in a meaningful way. While state plans were mandated to include cybersecurity awareness, many other programs funded by the statute (those by non-state entities) did not include such a focus,[40] and "cybersecurity awareness" has failed to fully address the human vulnerabilities described in this report. There may have been an opportunity to build on the initial progress of the DEA, but in May 2025, the **Commerce Department** announced that it would not move forward with DEA programming because of the statute's requirement that funded programs serve marginalized populations. As a result, all grants are now terminated under the DEA.

Despite the discontinuation, the DEA—together with programs like BEAD—provides a valuable foundation for advancing a more human-centered cybersecurity strategy. Programs that solely focus on the digital divide should be expanded to support cybersecurity education, community-based training programs, and digital literacy outreach, with a specific emphasis on the connection between human and cybersecurity vulnerabilities. These policy efforts should complement, rather than replace, existing, more technical cybersecurity policies.

If we want effective and equitable cybersecurity policy, statutes like the DEA should be reestablished and redesigned around the recognition that human vulnerabilities often stem from inadequate systemic support and inequitable access to knowledge. The DEA had the capacity to fund programs related to

digital skills and literacy, but future initiatives must go further: There must be an explicit acknowledgement and commitment toward the intersection between human and cybersecurity vulnerabilities, and there must be deeper investment in human-centered cybersecurity policies. Any future version of statutes like the DEA should explicitly require grantees to demonstrate how they are addressing human and cybersecurity vulnerabilities. By redeveloping programs like BEAD and the DEA, which already prioritize the human vulnerabilities this report describes, policymakers can begin to address the human factors at the heart of cybersecurity.

Maintaining, reviving, enhancing, and creating programs and statutes like BEAD and the DEA—rather than building entirely new structures—offers a practical path forward because the groundwork is already there. Nonetheless, shifts in federal policy and funding may curtail these efforts; thus, in addition to the work of policymakers, other stakeholders have a role to play. Companies affected by users' lack of digital literacy can invest in user education initiatives, and philanthropies can support nonprofits providing community-based digital skills training.

What is needed now is a policy shift to move from seeing the digital divide and cybersecurity as separate siloes to recognizing the overlooked nexus.

Embed Participatory Frameworks in Design and Governance

Ethical, human-centered design must be a core component of cybersecurity policy. Frameworks such as "Secure by Design" or "Privacy by Design" emphasize that technologies should reflect users' values and protect their rights by default.[41] Yet few cybersecurity policies are designed with the digital divide in mind—even though the values embedded in digital divide policy efforts, such as equitable access, digital literacy, and user empowerment, are precisely what ethical design should account for.

To operationalize these principles, participatory approaches such as collaborative policy audits (evaluations of implemented policies with robust community involvement) or participatory threat modeling (which allows users to participate in research and define their own threats) can play a critical role in identifying and articulating human vulnerabilities that often go unrecognized in cybersecurity policymaking.[42] These methods move beyond abstract design ideals by grounding policy in actual experience, allowing communities to articulate what access, risk, and protection mean in their context.

Only through collaborative and equitable engagement can the layered nature of human vulnerabilities be meaningfully explored. While RAND did create its framework through interviews of industry experts, this kind of top-down model often misses the lived experiences of those most impacted by poor

cybersecurity infrastructure or policy. Institutions like NIST or RAND should deepen their commitment to incorporating these participatory mechanisms—with an emphasis on gathering information from the everyday user—to ensure that cybersecurity policies reflect the realities of human vulnerabilities. For both design and implementation, participatory approaches can inform not only how technologies are built, but also how risks are identified, prioritized, and managed.

Policymakers should fund and institutionalize these participatory processes so that they are not perfunctory, one-off engagements but, rather, ongoing structures for gathering insight. These methods must also be resourced equitably, with accessible formats, multilingual support, and partnerships with trusted local organizations to ensure meaningful participation. In doing so, nuanced understandings of human vulnerabilities—and how they intersect and contribute to cybersecurity vulnerabilities—can be embedded into the foundation of cybersecurity governance.

Keep Internet Access Equitable

Cybersecurity policy must not be used as a justification to restrict or cut off access to the internet, especially for civil society actors or marginalized groups.[43] As organizations such as **Access Now** have documented, international internet shutdowns and surveillance regimes disproportionately target human rights defenders, journalists, and grassroots organizers, many of whom already lack the digital defenses they need to protect themselves. While these individuals lack consistent internet access, they may also lack digital literacy and skills—all of which are factors that can increase their exposure to cybersecurity vulnerabilities, which in turn can undermine their ability to safely carry out critical civic work.

Although internet shutdowns are typically associated with authoritarian contexts, U.S. cybersecurity policymakers must remain vigilant against these and other forms of digital exclusion. Restrictive content moderation due to cyber risks or poorly scoped threat response mechanisms can have similar exclusionary effects, particularly for marginalized communities.

Within the United States, access to the internet should continue to expand, not diminish. If cybersecurity justifications do emerge—such as emergencies prompting limited access—they should not curtail connectivity. Given the unpredictable level of federal investment in broadband programs like BEAD, it is crucial to ensure that cybersecurity concerns do not become a barrier to equitable access. This includes calls to restrict access based on identity, geography, or resource level under the guise of national security.

Security should not come at the cost of connectivity. Instead, policies should aim to fortify access (through programs like BEAD, but expanded) and support at-risk communities with the tools and training they need to stay safe online (through statutes like the DEA, but expanded).

Conclusion

Cybersecurity policy has long focused on strengthening infrastructure and mitigating technical risks. These efforts remain essential, but they are no longer sufficient: As the digital landscape evolves, so too must our understanding of where vulnerability resides. This report has argued that human vulnerabilities—stemming from a lack of digital access, skills, and literacy—must be recognized as core cybersecurity concerns, not peripheral issues.

The report has illustrated that the policy efforts related to the digital divide and cybersecurity are not separate challenges but are overlapping layers of the same goal: protecting, and even empowering, users. In this context, it becomes clear that digital divide policy cannot remain isolated from cybersecurity frameworks—and that cybersecurity policy cannot overlook the lived experiences of users.

Bridging these two domains will require expanding the scope of or redesigning existing initiatives like the Broadband Equity Access and Deployment Program and the Digital Equity Act to include cybersecurity awareness and funding for cyber-aware digital literacy and skills programming. Participatory approaches must be embedded into governance, where users help define what security means in their context. Further, there must be a consistent commitment to equitable internet access, even amid changing political conditions, as access remains a baseline for digital participation and protection.

Moving from risk to resilience requires reframing who cybersecurity is for and what it should protect. By recognizing that human vulnerabilities are more than simple user errors, policymakers can build a more inclusive and responsive cybersecurity ecosystem—one that secures not just systems, but people.

Notes

1 See Mark Evans et al., "Human Behaviour as an Aspect of Cybersecurity Assurance," *Security and Communication Networks* 9, no. 17 (October 20, 2016): 4667–79, https://doi.org/10.1002/sec.1657; Maher Alsharif, Shailendra Mishra, and Mohammed AlShehri, "Impact of Human Vulnerabilities on Cybersecurity," *Computer Systems Science and Engineering* 40, no. 3 (September 24, 2022): 1153–66, https://doi.org/10.32604/csse.2022.019938. Similar to the human factor is the concept of an insider threat, defined as "the potential for an insider to use their authorized access or understanding of an organization to harm that organization. This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities." "Defining Insider Threats," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats. An insider threat, if the insider makes a mistake, could be considered the "human factor."

2 Verizon Data Breach Investigations team, *2025 Data Breach Investigations Report* (Verizon Business, 2025), https://www.verizon.com/business/resources/Tdc/reports/2025-dbir-data-breach-investigations-report.pdf.

3 See Daniella DiPaola and Ryan Calo, "Socio-Digital Vulnerability," SSRN, January 17, 2024, http://dx.doi.org/10.2139/ssrn.4686874; Margret Hoehe and Florence Thibaut, "Going Digital: How Technology Use May Influence Human Brains and Behavior," *Dialogues in Clinical Neuroscience* 22, no. 2 (2022): 93–97, https://doi.org/10.31887/DCNS.2020.22.2/mhoehe; "Behavioral Indicators in Cybersecurity: A Comprehensive Guide," SearchInform, https://searchinform.com/articles/cybersecurity/analytics/ueba/behavioral-indicators/. The susceptibility one has to certain risks is described in many disciplines, but this report references the discussion on vulnerability in the 2016 RAND cybersecurity framework. Igor Mikolic-Torreira, et al., *A Framework for Exploring Cybersecurity Policy Options* (RAND Corporation, 2016), https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1700/RAND_RR1700.pdf.

4 Martha Fineman, "The Vulnerable Subject: Anchoring Equality in the Human Condition," *Yale Journal of Law & Feminism* 20, no. 1 (November 12, 2008): 1–23, https://doi.org/10.4324/9780203848531-26.

5 Benjamin Remillard, "Access Alone Isn't Enough," in *Designing for Care*, ed. Jerod Quinn, Martha Burtis, and Surita Jhangiani (Pressbooks, 2022).

6 National Telecommunications and Information Administration (NTIA), *Falling Through the Net: Defining the Digital Divide* (NTIA, July 1999), https://www.ntia.gov/sites/default/files/data/fttn99/FTTN.pdf.

7 See "What Is the Digital Divide?," Institute of Electrical and Electronics Engineers, https://ctu.ieee.org/blog/2022/12/14/what-is-the-digital-divide/; "Closing the Digital Divide for the Millions of Americans Without Broadband Posted," *WatchBlog*, General Accountability Office, February 1, 2023, https://www.gao.gov/blog/closing-digital-divide-millions-americans-without-broadband; Nicky Lauricella Coolberth, "The 'Digital Divide' Is About Access to Devices and the Internet—But It's Also About Access to Skills," National Skills Coalition, September 15, 2021, https://nationalskillscoalition.org/blog/future-of-work/the-digital-divide-is-about-access-to-devices-and-the-internet-but-its-also-about-access-to-skills/.

8 "Digital Literacy," American Library Association, https://literacy.ala.org/digital-literacy/.

9 See Musaddag Elrayah and Saima Jamil, "Impact of Digital Literacy and Online Privacy Concerns on Cybersecurity Behaviour: The Moderating Role of Cybersecurity Awareness," *Cyber Criminology* 17, no. 2 (November 8, 2023): 166–87, https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/205/76.

10 Steve Cisler, "Subtract the Digital Divide," *San Jose Mercury News*, January 15, 2000, archived at https://web.archive.org/web/20000510004646/http://www.mercurycenter.com:80/svtech/news/indepth/docs/soap011600.htm.

11 Florencia Luna, "Elucidating the Concept of Vulnerability: Layers Not Labels," *Feminist Approaches to Bioethics* 2, no. 1 (Spring 2009): 121–39, http://www.jstor.org/stable/40339200.

12 Charlotte Cowles, "The Day I Put $50,000 in a Shoe Box and Handed It to a Stranger," *The Cut* (blog), *New York Magazine*, February 15, 2024, https://www.thecut.com/article/amazon-scam-call-ftc-arrest-warrants.html.

13 "New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024," Federal Trade Commission, March 10, 2025, https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024.

14 Lana Swartz, Alice E. Marwick, and Kate Larson, "Scam GPT: GenAI and the Automation of Fraud," Data & Society, May 21 2025, https://datasociety.net/library/scam-gpt/; Emma Fletcher, "Social Media: A Golden Goose for Scammers," Federal Trade Commision, October 6, 2023, https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers.

15 Igor Mikolic-Torreira et al., *A Framework for Exploring Cybersecurity Policy Options* (RAND, 2016), https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1700/RAND_RR1700.pdf.

16 "Our Words Matter When It Comes to Fraud," AARP, https://www.aarp.org/lp/words-matter/.

17 See Tobi Opeyemi Amure, "The Surprising Truth About the Age Group Most Likely to Fall for Financial Fraud," Investopedia, April 17, 2025, https://www.investopedia.com/age-and-financial-fraud-11714608.

18 "Who Experiences Scams? A Story for All Ages," Federal Trade Commission, December 8, 2022, https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/12/who-experiences-scams-story-all-ages.

19 See Joshua Kendall, Anthony Colavito, and Zach Moller, "America's Digital Skills Divide," Third Way, January 12, 2023, https://www.thirdway.org/report/americas-digital-skills-divide.

20 Olivia Sidoti and Emily A. Vogels, "What Americans Know About AI, Cybersecurity, and Big Tech," Pew Research Center, August 17, 2023, https://www.pewresearch.org/internet/2023/08/17/what-americans-know-about-ai-cybersecurity-and-big-tech/.

21 Danna Lorch, "America's Digital Divide: Where Workers Are Falling Behind," Harvard Business School, February 10, 2025, https://www.library.hbs.edu/working-knowledge/americas-digital-divide-where-workers-are-falling-behind.

22 "Cybersecurity Framework," National Institute of Standards and Technology, https://www.nist.gov/cyberframework.

23 Mikolic-Torreira, et al., *A Framework for Exploring Cybersecurity Policy Options*, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1700/RAND_RR1700.pdf.

24 "Broadband Equity Access and Deployment Program," BroadbandUSA, National Telecommunications and Information Administration, https://broadbandusa.ntia.gov/funding-programs/

broadband-equity-access-and-deployment-bead-program; "Digital Equity Act," National Digital Inclusion Alliance, https://www.digitalinclusion.org/digital-equity-act/.

25 Justin Hendrix, "Digital Equity Advocates Rally to Restore Funds, Sustain Their Work," *Tech Policy Press*, July 24, 2025, https://www.techpolicy.press/digital-equity-advocates-rally-to-restore-funds-sustain-their-work/; Barbara Ortutay and Claire Rush, "The Digital Equity Act Tried to Close the Digital Divide. Trump Targets It in His War on 'Woke'," PBS News, May 25, 2025, https://www.pbs.org/newshour/politics/the-digital-equity-act-tried-to-close-the-digital-divide-trump-targets-it-in-his-war-on-woke.

26 Clara Easterday, "Bipartisan Bill Aims to Help Rural Communities Access Federal Broadband Funds," *Broadband Breakfast*, May 5, 2025, https://broadbandbreakfast.com/bipartisan-bill-aims-to-help-rural-communities-access-federal-broadband-funds/.

27 Imposter scams are conducted by a "trusted entity," but this report argues that the scammers became trusted entities only after talking to victims and developing a relationship, sometimes over the course of months.

28 Swartz, Marwick, and Larson, "Scam GPT," https://datasociety.net/library/scam-gpt/.

29 See Elrayah and Jamil, "Impact of Digital Literacy and Online Privacy Concerns on Cybersecurity Behaviour," https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/205/76.

30 Public Library Association (PLA), *2023 Public Library Technology Survey: Summary Report* (PLA, 2024), https://www.ala.org/sites/default/files/2024-07/PLA_Tech_Survey_Report_2024.pdf.

31 James K. Elmborg, "Libraries as the Spaces Between Us: Recognizing and Valuing the Third Space," *Reference & User Services Quarterly* 50, no. 4 (Summer 2011): 338–50, https://www.jstor.org/stable/20865425.

32 Digital Empowerment and Inclusion Working Group, *The Role of Public Libraries and Community Partnerships in Promoting Digital Adoption* (Federal Communications Commission, June 24, 2021), https://www.fcc.gov/sites/default/files/acdde-digital-empowerment-wg-digital-inclusion-report-06242021.pdf. See also "American Libraries and Museums Awarded $13.8 Million in IMLS CARES Act Grants," Institute of Museum and Library Services, September 24, 2020, https://www.imls.gov/news/american-libraries-and-museums-awarded-138-million-imls-cares-act-grants.

33 "Show Us the Money: Federal Broadband Support During the COVID-19 Pandemic," Benton Institute for Broadband & Society, April 23, 2021, https://www.benton.org/blog/show-us-money-federal-broadband-support-during-covid-19-pandemic.

34 National Digital Inclusion Alliance (NDIA), *The Digital Inclusion Program Manual* (NDIA, 2024), https://www.digitalinclusion.org/resource/digital-inclusion-program-manual/; "Digital Navigator Model," National Digital Inclusion Alliance, https://www.digitalinclusion.org/digitalnavigatormodel/.

35 For example, the Toledo Lucas County Public Library in Ohio provides local digital divide support and programming. "Digital Equity and Inclusion," Toledo Lucas County Public Library, https://www.toledolibrary.org/digital-equity/.

36 Caroline Stratton, "Three Questions About BEAD Non-Deployment Funding," Benton Institute for Broadband & Society, June 24, 2025, https://www.benton.org/blog/three-questions-about-bead-non-deployment-funding.

37 Caroline Stratton, "Three Questions About BEAD Non-Deployment Funding," Benton Institute for Broadband & Society, https://www.benton.org/blog/three-questions-about-bead-non-deployment-funding.

38 Christopher Ali, "For Millions of Americans, High-Speed Internet Is Unavailable or Unaffordable—A Telecommunications Expert Explains How to Bring Broadband to the Places That Need It the Most," *The Conversation*, April 24, 2024, https://theconversation.com/for-millions-of-americans-high-speed-internet-is-unavailable-or-unaffordable-a-telecommunications-expert-explains-how-to-bring-broadband-to-the-places-that-need-it-the-most-227666.

39 47 U.S.C. § 1723(c)(1)(B(iv) (2021).

40 For example, #BlackTechFutures aimed to use Digital Equity Act funding to establish "digital hubs offering internet access, shared workspaces, and tech training programs." This is important work, but it is not exactly the work that this report calls for. Habiba Katsha, "Trump Cuts Digital Equity Act Funding: Black Tech Nonprofit Loses $12M," People of Color in Tech, August 5, 2025, https://peopleofcolorintech.com/articles/trump-cuts-digital-equity-act-funding-black-tech-nonprofit-loses-12m/.

41 "Secure by Design," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/securebydesign; "What Is Privacy-by-Design and Why It's Important?," Institute of Electrical and Electronics Engineers, https://digitalprivacy.ieee.org/publications/topics/what-is-privacy-by-design-and-why-it-s-important/.

42 Julia Slupska et al., "Participatory Threat Modelling: Exploring Paths to Reconfigure Cybersecurity," *CHI EA '21: Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* 329 (May 8, 2021): 1–6, https://doi.org/10.1145/3411763.3451731.

43 Tina Nguyen, "Iran Is Going Offline to Prevent Purported Israeli Cyberattacks," *The Verge*, June 17, 2025, https://www.theverge.com/politics/688875/iran-cutting-off-internet-israel-war.

NEW AMERICA