Social Engineering and Digital Literacy: Phishing as a form of attack

Adedoyin Folarin

Advisor: Harini Suresh
Second Reader: Indira Gil

A Thesis submitted in partial fulfillment of the requirements for Honors
in the Department of Computer Science at Brown University

Department of Computer Science
Brown University
Providence, RI

April 2026

Abstract

This research examines the relationship between three indicators of socio-economic inequality — income, broadband access, and education- and phishing reports in the United States from 2019 to 2024. It focuses on how digital literacy can serve as an effective strategy for raising awareness of social engineering techniques, specifically phishing, through education. This research finds an observed association between phishing victim counts, as compiled by the FBI's Internet Crime Complaint Center, and education levels, as measured by the American Community Survey data. Individuals with a Bachelor's degree or higher have an inverse association, while individuals with a high school education or higher have a positive association with phishing victim counts across states. It also discovers that more vulnerable states did not record higher phishing reports. In line with the findings, I propose an education curriculum focused on social engineering and cybersecurity practices for high school students to increase awareness of the risks of phishing attacks across the United States.

Contents

1 INTRODUCTION

Geography shapes digital infrastructure, and in turn, infrastructure influences security outcomes. Consider residents in regions such as Silicon Valley, California, a hub for technology companies and startups, or Northern Virginia, home to a vast concentration of data centers. These residents may face heightened exposure to cybersecurity threats and data breaches, due to their geographical proximity to dense technological ecosystems. However, this same exposure can drive development of advanced cybersecurity infrastructure, including improved reporting systems, protective technologies, and more robust institutional responses.

In this sense, geography not only determines risk and exposure but also shapes the capacity for protection, ultimately influencing their technical and digital security. As the world becomes increasingly globalized and technology becomes embedded in everyday life, the range of technical risks, from payment scams to artificial intelligence deepfakes, among others,[1] continues to increase. These evolving threats consequently motivate the development of new defensive measures such as multi-factor authentication, security software, or backup systems,[2] despite the pervasive methods devised to circumvent them by malicious actors.

The digital divide, when accounting for income, geography, and access, remains significant in the United States.[3] A survey conducted by the Pew Research Center found that "24% of adults with household incomes below $30,000 a year say they don't own a smartphone."[4] In parallel, an increasingly interconnected world is emerging with digital wallets, multiple devices, and the rise of revolutionary technologies like generative artificial intelligence, which collectively introduce new and evolving risks for individuals with socio-economic disadvantages.

In this research, I refer to these socio-economic disadvantages as disparities in income, gender, and race. Nicola F. Johnson argues that mainstream discourses regarding technology often support "a view of white, middle-class, educated, well-paid males as the typical user."[5] As a result, individuals who fall outside this demographic, or communities where this group is not the most prominent or dominant, may have limited access and reduced exposure to tech-

1. California Department of Financial Protection and Innovation, "The New Era of Tech-Enabled Scams," accessed April 1, 2026, https://dfpi.ca.gov/news/insights/the-new-era-of-tech-enabled-scams/.

2. Federal Trade Commission, "How to Recognize and Avoid Phishing Scams," accessed April 1, 2026, https://consumer.ftc.gov/articles/how-recognize-avoid-phishing-scams.

3. Thomas Kennedy, "The Digital Divide: Inequality in the Digital Age," Old Dominion University, accessed April 6, 2026, https://www.cs.odu.edu/~tkennedy/cs300/development/Public/M03-SocietalDigitalDivideII/index.html.

4. Pew Research Center, "Digital Divide Persists Even as Americans with Lower Incomes Make Gains in Tech Adoption," June 22, 2021, https://www.pewresearch.org/short-reads/2021/06/22/digital-divide-persists-even-as-americans-with-lower-incomes-make-gains-in-tech-adoption/.

5. Nicola Johnson, *Technological Disadvantage of the Digital Age*, 2004, https://ro.uow.edu.au/edupapers/16.

nical developments while simultaneously experiencing heightened vulnerability to some of the cybersecurity risks and exploitation described above.

Over 98% of cyberattacks involve some form of social engineering.[6] Social engineering is a broad topic, encompassing a range of attacks that target human vulnerabilities. I adopt a definition of social engineering that encompasses both physical components (requiring direct human involvement) and technical components (requiring digital or internet-based interaction). It is defined as "a type of attack wherein the attacker(s) exploit human vulnerabilities by means of social interaction to breach cybersecurity, with or without the use of technical means and technical vulnerabilities."[7] Social engineering can take on different forms, from social to technical, and physical-based attacks,[8] all of which require human involvement and interaction. These attacks are difficult to prevent due to their reliance on human behavior, as research has shown, "there is not a computer system that doesn't rely on humans on earth, no matter how well the security measures are designed and implemented."[9] Humans have often been referred to as "the weakest link in the security chain."[10]

A common type of social engineering is phishing. It is defined as "a type of computer attack that communicates socially engineered messages to humans via electronic communication channels to persuade them to perform certain actions for the attacker's benefit."[11] Phishing targets individuals as well as organizations. It has been used to bring down large organizations with extensive resources and security mechanisms, as well as individuals with a wealth of technical knowledge, by manipulating users to extract sensitive information. It poses a risk that may be exacerbated for individuals with limited technical/digital access and knowledge, the subject of this research.

Digital literacy is the second key component of this research and is examined as a means of increasing awareness of phishing attacks, whose origins and importance as a social engineering concept are explored through existing literature in Chapter 2. Digital literacy refers to the "individuals ability and skills to communicate on online networks, understand hypertext and multimedia texts as well as making judgments on online sources,"[12] and has been widely discussed in recent scholarship as a promising avenue to combat the effects of social engineering (see recent works by Zorica, Golubić and Katarinček 2025,[13] Phan, Do,

6. Proofpoint, Inc., "What Is Social Engineering?," accessed April 1, 2026, https://www.proofpoint.com/us/threat-reference/social-engineering.

7. Z. Wang, L. Sun, and H. Zhu, "Defining Social Engineering in Cybersecurity," *IEEE Access* 8 (2020): 85094–85115, https://doi.org/10.1109/ACCESS.2020.2992807.

8. Fatima Salahdine and Naima Kaabouch, "Social Engineering Attacks: A Survey," *Future Internet* 11, no. 4 (2019): 89, https://doi.org/10.3390/fi11040089.

9. Wang, Sun, and Zhu, "Defining Social Engineering in Cybersecurity."

10. Salahdine and Kaabouch, "Social Engineering Attacks: A Survey."

11. Mahmoud Khonji, Youssef Iraqi, and Andrew Jones, "Phishing Detection: A Literature Survey," *IEEE Communications Surveys & Tutorials* 15, no. 4 (2013): 2091–2121, https://ieeexplore.ieee.org/abstract/document/6497928.

12. Eva Bach, *The Impact of Digital Literacy on the Cyber Security of Digital Citizens*, University North, Croatia.

13. M. B. Zorica, G. Golubić, and T. Š. Katarinček, "Cybersecurity in Education: The Challenge of Social Engineering and Information Literacy," in *2025 MIPRO 48th ICT and Elec-*

and Le 2024,[14] Holt and Nicholson 2025.[15])

Digital literacy plays an increasingly important role in emerging cybersecurity discussions; therefore, I aim to examine how it is relevant in increasing awareness of phishing, particularly as states have varying levels of digital regulation and approaches to digitization.

I initially intended to focus on the effects of phishing attacks on marginalized communities and explore ways that they may or may not have borne a disproportionate burden of phishing attacks due to limited access to and knowledge of technology. However, throughout this research, I realized that marginalization can be better explored at a granular level. This could be done by examining communities based on similarities within a region, for example, examining each municipality, city, or census block group across states where there is relatively little variation in key characteristics such as income, race, and other socio-economic factors. Data on phishing attempts and success rates at the city or town level is not widely available and difficult to gather based on demographic classification across rural and urban environments within U.S. states. Hence, I focus on examining patterns and differences in phishing reports across states.

To conduct this analysis, I review state-based reports from individuals, examining their relative socio-economic disadvantage compared to other states, and exploring the differences in their use of technology and access to resources for mitigating social engineering risks. My research aims to understand which states exhibit higher vulnerability to social engineering, particularly phishing.

I examine the dynamics at the intersection of cybersecurity and state-wide vulnerabilities by breaking down the research topic into the sub-questions below. I follow existing research and adopt the view that systemic and socio-economic factors contribute to digital inequality and affect the overall composition of state development and progress.[16],[17] I explore the following questions, hypothesizing that the most significant disadvantages that contribute to vulnerability and social engineering within states are income, broadband access, and education.

- How do the hypothesized factors – income, broadband access, and education correlate with phishing attack counts across U.S. states?
- How can digital literacy strategies be designed as a solution that reflects

tronics Convention (Opatija, Croatia, 2025), 662–667, https://doi.org/10.1109/MIPRO65660.2025.11132065.

14. Bao Trung Phan, Phuong Huyen Do, and Da Quynh Le, "The Impact of Digital Literacy on Personal Information Security: Evidence from Vietnam," in *Proceedings of Atlantis Press* (2025), https://doi.org/10.2991/978-94-6463-694-9_32.

15. Jack Holt and James Nicholson, "Scaffolding Online Safety in Older Communities: Exploring the Relationship Between Digital Literacy and Cybersecurity," Forthcoming, *ACM Transactions on Computer-Human Interaction*, February 2026, https://doi.org/10.1145/3796705.

16. Tiina Pajuste, "The Digital Divide: Reinforcing Vulnerabilities," in *Human Rights in the Digital Domain: Core Questions*, ed. Tiina Pajuste (Cambridge: Cambridge University Press, 2025), 361–380.

17. Syracuse University School of Information Studies, "What Is the Digital Divide? Meaning, Causes & Impact," accessed April 1, 2026, https://ischool.syracuse.edu/what-is-the-digital-divide/.

the needs and experiences of more vulnerable states?

I begin by exploring existing literature on social engineering and digital inequality, aiming to understand the concepts and the contributing factors across communities. I proceed to an analysis of the phishing reports and the hypothesized factors described above, across the United States, using correlation and regression analysis to investigate whether there are associations between these factors. Subsequently, I use the results to develop an approach to digital literacy that is reflective of the factors that drive the gaps in knowledge across states, to prioritize state-level differences in educating residents about phishing and, more broadly, social engineering.

2 LITERATURE REVIEW

2.1 Background on Social Engineering Attacks and Phishing

Salahdine and Kaabouch outlined social engineering attacks as a four-phase process. These are to "collect information about the target; develop [a] relationship with the target; exploit the available information and execute the attack; and exit with no traces."[18] They augmented this by explaining the types of these attacks that exist, namely, human-based or computer-based attacks. Phishing is a key form of human-based social engineering, and scholars have considered it to be the most common form of cyberattacks.[19]

The exploration of "what" social engineering is has been conducted extensively by a range of authors, as seen in reviews by Hadnagy 2010,[20] Peltier 2006,[21] Mouton, Leenen, and Venter 2016,[22] Abraham and Chengalur-Smith 2010.[23] However, these works rarely focus on phishing and how it is exacerbated by systemic factors that lead to human vulnerabilities, an argument that I build upon. Existing research on phishing primarily focuses on detection systems and case-based reasoning, which can be understood as using historical data (such as past cases or experiences) to predict solutions to current problems.[24] Yet, there is a general lack of understanding of the systemic factors that are interwoven to increase vulnerability to phishing attacks or the extent to which it could affect individuals with limited access to technology, allowing for research to be conducted in a way that overlooks the populations most at risk.

Existing studies show that certain individuals, especially those from "low-income and rural areas", are "highly vulnerable to cyberattacks."[25] Technically vulnerable communities whose access to technology intersects with socioeconomic constraints are then left susceptible to phishing attacks due to limited access to both technological resources and relevant research, which exacerbates the lack of knowledge on their exposures to social engineering.

18. Salahdine and Kaabouch, "Social Engineering Attacks: A Survey."
19. Salahdine and Kaabouch.
20. Christopher Hadnagy, *Social Engineering: The Art of Human Hacking* (Indianapolis: Wiley Publishing, 2011).
21. Thomas R. Peltier, "Social Engineering: Concepts and Solutions," *Information Systems Security* 15, no. 5 (2006): 13–21.
22. François Mouton, Louise Leenen, and H. S. Venter, "Social Engineering Attack Examples, Templates and Scenarios," *Computers & Security* 59 (2016): 186–209, https://doi.org/10.1016/j.cose.2016.03.004.
23. Sherly Abraham and InduShobha Chengalur-Smith, "An Overview of Social Engineering Malware: Trends, Tactics, and Implications," *Technology in Society* 32, no. 3 (2010): 183–196, https://doi.org/10.1016/j.techsoc.2010.07.001.
24. Hassan Y. A. Abutair and Abdelfettah Belghith, "Using Case-Based Reasoning for Phishing Detection," *Procedia Computer Science* 109 (2017): 281–288, https://doi.org/10.1016/j.procs.2017.05.352.
25. Anirban Ghosh, S. Diyasi, and Debashis Dey, "Cybersecurity Literacy Programs for Marginalized Communities: Bridging the Gap in Digital Security," 2025, https://www.researchgate.net/publication/389441252.

2.2 Digital Inequality and Vulnerable Communities

Digital inequality can be seen as a reinforcing cycle, an insecurity that emboldens and magnifies the results of other inequalities. Consider a resident living in the District of Columbia, a state that exists as one of the most economically unequal areas in the U.S., as shown by the Gini Index, a metric measuring socioeconomic inequality,[26] and has the highest counts of phishing complaints, losses, and perpetrators per capita.[27] Such a resident may be unaware of the extent of the digital risks and vulnerabilities that they are exposed to compared to a resident in Maine, a state that demonstrates lower levels of digital and cyber vulnerability,[28] and is considered more equitable in its socio-economic conditions.[29]

As such, inequality becomes self-perpetuating and amplified due to other factors such as existing disparities in income, education, and access to resources, all of which deepen digital vulnerability. In the context of technological access, this inequality can be referred to as the digital divide. This divide is increasingly important as it contributes to "reinforc[ing] inequality in opportunities for economic mobility and social participation."[30] As one level of inequality is reinforced by existing systemic factors, it contributes to limited knowledge of and access to technological developments, which may further alienate and expose vulnerable groups to phishing and other forms of social engineering.

Digital inequality is significantly complex as it intersects with almost every aspect of everyday life. This perspective is supported by other researchers, with Imran Ahmed stating, "The impact of digital inequality is inseparable from growing societal inequality, with the vast majority of the population, daily laborers and wayfarers, mostly powerless against a widespread surge in digital transformation."[31] This is further explored by Zheng and Walsham, who describe this phenomenon of inequality as a problem that should be reviewed and analyzed while prioritizing "intersectionality."[32] In line with this research, they identify existing limitations to digital equality, referring to the "systematic social injustices" and the relationship between "digital infrastructure and technology", factors that often limit awareness of social engineering techniques and increase

26. World Population Review, "Income Inequality by State," accessed April 1, 2026, https://worldpopulationreview.com/state-rankings/income-inequality-by-state.

27. HighSpeedInternet.com, "The Safest and Most Dangerous States for Cybercrime in 2024," accessed April 1, 2026, https://www.highspeedinternet.com/resources/the-safest-and-most-dangerous-states-for-cybercrime-in-2024.

28. HighSpeedInternet.com.

29. World Population Review, "Income Inequality by State."

30. Paul DiMaggio et al., "From Unequal Access to Differentiated Use: A Literature Review and Agenda for Research on Digital Inequality," in *Social Inequality*, ed. Kathryn M. Neckerman (New York: Russell Sage Foundation, 2004), 355–400.

31. Ahmed Imran, "Why Addressing Digital Inequality Should Be a Priority," *Electronic Journal of Information Systems in Developing Countries* 89, no. 3 (2023): e12255, https://doi.org/10.1002/isd2.12255.

32. Yinjiao Zheng and Geoff Walsham, "Inequality of What? An Intersectional Approach to Digital Inequality under Covid-19," *Information and Organization* 31 (2021): 1–6, https://doi.org/10.1016/j.infoandorg.2021.100341.

the vulnerability of marginalized groups.[33]

2.3 Digital Literacy as a Solution to Social Engineering

Ghosh, Diyasi, and Dey's research on the vulnerability to cyberattacks suggests that digital literacy may serve as a solution to reducing the effects of social engineering across vulnerable individuals. This has been widely supported in existing research as seen in works by Phan, Do, and Le 2024,[34] Holt and Nicholson 2025.[35] While digital literacy approaches are effective in increasing awareness of these issues and making users more responsive, it focuses on generic solutions, rather than customizing digital literacy strategies to consider the state-dependent factors, such as broadband access and demographic composition, that make phishing attacks more successful. What might work in Mississippi may not work in Texas. By ignoring how communities within and across states access and use technology, how can effective solutions be derived that truly encompass the problem? I aim to close such a gap in the literature and develop a comprehensive understanding of why these attacks succeed by examining state vulnerabilities and their relationship to phishing as a form of social engineering.

33. Louis Everuss, *Digital Mobilities and Smart Borders: How Digital Technologies Transform Migration and Sovereign Borders* (Berlin: De Gruyter, 2024).

34. Phan, Do, and Le, "The Impact of Digital Literacy on Personal Information Security: Evidence from Vietnam."

35. Holt and Nicholson, "Scaffolding Online Safety in Older Communities: Exploring the Relationship Between Digital Literacy and Cybersecurity."

3 DATA AND METHODOLOGY

I primarily use a quantitative approach to answer the first research question. which states: How do the hypothesized factors – income, broadband access, and education correlate with phishing attack counts across U.S. states? I combine state-based phishing reports with census data to investigate the intersection of phishing and state-level vulnerabilities.

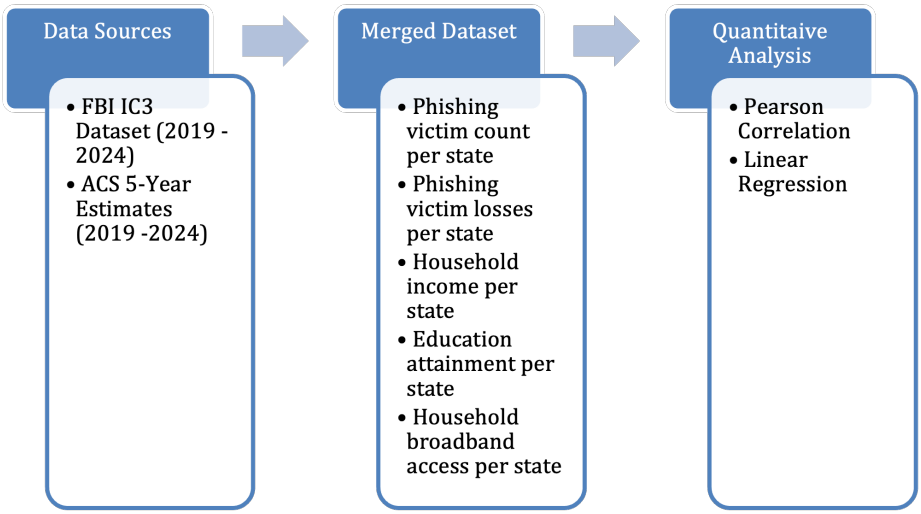


Figure 1: Quantitative Components

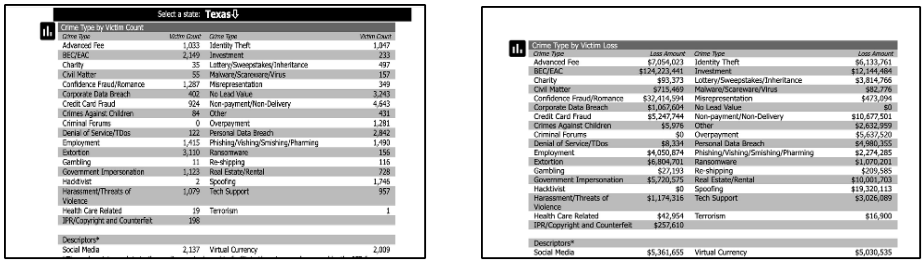
3.1 Variables and Sources

For the above question, I utilize annual reports created by the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) on state-reported phishing attacks from 2019 to 2024. These reports are built by compiling individually reported data through an FBI IC3 form on the different attacks experienced by an individual and specific details of loss and attack mechanism. The focus on FBI IC3 reports was primarily driven by the availability of data on confirmed cyberattacks.[36] Analysis of phishing targets can only be conducted from a victim's perspective, as there is no robust way to infer the scope or reach of phishing campaigns.

Attempts to analyze reported URLs from large databases such as URLHaus proved unreliable in determining the intended targets, especially when parsing through known URLs for location information. Therefore, I focus on data that has been reviewed by the FBI Internet Crime Complaint Center and reported

36. Federal Bureau of Investigation. Internet Crime Complaint Center (IC3), "Internet Crime Complaint Center," accessed April 1, 2026, https://www.ic3.gov/.

by individuals who have experienced phishing attacks. All IC3 complaints are reviewed by analysts before being included in state-level data, as noted by the FBI's IC3 Team. I analyzed this data across multiple years and selected variables from the following fields: "Crime Type by Victim Count" and "Crime Type by Victim Loss." A sample of the data is shown in Figure 3 below.



Select a state: Texas

Crime Type by Victim Count

Crime Type	Victim Count	Crime Type	Victim Count
Advanced Fee	1,033	Identity Theft	1,947
BEC/EAC	2,149	Investment	233
Charity	35	Lottery/Sweepstakes/Inheritance	497
Civil Matter	55	Malware/Scareware/Virus	157
Confidence Fraud/Romance	1,287	Misrepresentation	349
Corporate Data Breach	402	No Lead Value	3,243
Credit Card Fraud	924	Non-payment/Non-Delivery	4,643
Crimes Against Children	84	Other	431
Criminal Forums	0	Overpayment	1,281
Denial of Service/TDos	122	Personal Data Breach	2,842
Employment	1,415	Phishing/Vishing/Smishing/Pharming	1,490
Extortion	3,110	Ransomware	156
Gambling	11	Re-shipping	115
Government Impersonation	1,123	Real Estate/Rental	728
Hacktivist	2	Spoofing	1,746
Harassment/Threats of Violence	1,079	Tech Support	957
Health Care Related	19	Terrorism	1
IPR/Copyright and Counterfeit	198		
Descriptors*			
Social Media	2,137	Virtual Currency	2,009

Crime Type by Victim Loss

Crime Type	Loss Amount	Crime Type	Loss Amount
Advanced Fee	$7,054,023	Identity Theft	$6,133,761
BEC/EAC	$124,223,441	Investment	$12,144,484
Charity	$93,373	Lottery/Sweepstakes/Inheritance	$3,814,766
Civil Matter	$715,469	Malware/Scareware/Virus	$82,776
Confidence Fraud/Romance	$32,414,594	Misrepresentation	$473,094
Corporate Data Breach	$1,067,604	No Lead Value	$0
Credit Card Fraud	$5,247,744	Non-payment/Non-Delivery	$10,677,501
Crimes Against Children	$5,976	Other	$2,632,959
Criminal Forums	$0	Overpayment	$5,637,520
Denial of Service/TDos	$8,334	Personal Data Breach	$4,980,355
Employment	$4,050,874	Phishing/Vishing/Smishing/Pharming	$2,274,285
Extortion	$6,804,701	Ransomware	$1,070,201
Gambling	$27,193	Re-shipping	$209,585
Government Impersonation	$5,720,575	Real Estate/Rental	$10,001,703
Hacktivist	$0	Spoofing	$19,320,113
Harassment/Threats of Violence	$1,174,316	Tech Support	$3,026,089
Health Care Related	$42,954	Terrorism	$16,900
IPR/Copyright and Counterfeit	$257,610		
Descriptors*			
Social Media	$5,361,655	Virtual Currency	$5,030,535

Figure 2: IC3 Published State Report for Texas

The above figure shows the number of victims experiencing specific forms of cybercrime within each state. The "Crime Type by Victim Count" focuses on the type of cybercrime and the number of reported cases for that crime in a given year for each state while "Crime Type by Victim Loss" focuses on the total financial loss (in USD) recorded for the specific crime type for the year by aggregating the total losses reported by victims in each state.

To ensure consistency in defining phishing across years, I use the following categories. From 2019 to 2021, I use the crime category – "Phishing/Vishing/Smishing/Pharming," which is defined as "Unsolifootcited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials." In 2022, the IC3 report uses a similar definition and label – "Phishing," defined as the use of unsolifootcited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials[37] and state reports from 2023 and 2024 use the crime category "Phishing/Spoofing," which is defined as "the use of unsolifootcited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials."[38] All definitions and labels are similar.

To relate phishing information to community-specific information, I focus on the United States and investigate phishing attacks at the state level. Using the ACS (American Community Survey) Database, which collects "detailed social, economic, housing, and demographic information from a sample of households across the 50 states, the District of Columbia, and Puerto Rico,"[39] I compile

37. Federal Bureau of Investigation. Internet Crime Complaint Center (IC3), *2022 Internet Crime Report* (Washington, DC: Federal Bureau of Investigation, 2023), https://www.ic3.gov/AnnualReport/Reports/2022_IC3Report.pdf.

38. Federal Bureau of Investigation. Internet Crime Complaint Center (IC3), *2024 Internet Crime Report* (Washington, DC: Federal Bureau of Investigation, 2025), https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

39. U.S. Census Bureau, "American Community Survey (ACS)," accessed April 1, 2026,

information on the hypothesized factors – income, broadband access, and education to understand how phishing attacks differ across states based on these differences. The ACS 5-year estimates from Subject Tables is used.

Variable Code	Variable Name / Hypothesized Factor
S1901_C01_012E	Income and Benefits - Median Household Income
S1501_C02_014E	High School Graduates
S1501_C02_015E	Bachelor's Degree Holders
S1501_C02_013E	Graduate Degree Holders
S2801_C02_014E	Broadband Access

Figure 3: ACS Variables and Meaning
[40]

I join state-level IC3 data with the ACS dataset, which is also aggregated at the state level, by combining both datasets matched by state and year from 2019 to 2024. I investigate the victim counts per state and conduct a Pearson correlation and an OLS linear regression model across states. For each correlation and linear regression model, I utilize the ACS variable value associated with the state across 2019 to 2024. However, I also develop a joint education index, which is derived from the average of z-scores for ACS variables representing high school, bachelor's, and graduate degree attainment. I aim to develop a more explicit understanding of whether income, education, and broadband access correlate with phishing victim counts and what conclusions, if any, can be drawn.

3.2 Control Variables

Despite the aggregation of this data, the relationship between each factor and phishing rates across states alone cannot offer any direct or specific explanations for causation. There could be other factors that may offer explanations for associations between the dependent and independent variables beyond the control variables. The factors listed below are treated as control variables; however, these factors do not capture all relevant variables that may influence state reports. I select these based on existing research on population demographics relevant to the research questions.

[40] https://www.census.gov/programs-surveys/acs.html.

Variable Code	Variable Name / Hypothesized Factor
DP05_0001E	Total Population within a State
DP05_0021PE	% of Individuals under 18 pct_under_18
DP05_0024PE	% of Individuals over 65
DP05_0071PE	% of Individuals identifying as Hispanic
DP05_0077PE	% of Individuals identifying as White
DP05_0078PE	% of Individuals identifying as Black
DP05_0080PE	% of Individuals identifying as Asian
DP03_0062E	Median Household Income in USD
DP03_0128PE	Poverty Rate
DP03_0009PE	Unemployment Rate
DP02_0152PE	% of Households with a Computer
DP02_0151PE	% of Households with a Smartphone

Figure 4: ACS Variables and Meaning Continued
41

As mentioned earlier, the IC3 dataset is dependent on who reports. Therefore, the control variables above were selected considering the various demographic and economic factors that may influence the ability of individuals to report incidents or be aware of reporting channels. For example, age differences across states. A state with a significantly aging population may have fewer reports of phishing attacks due to a lack of awareness of reporting mechanisms or generally lower rates of internet and smartphone usage. Other factors may affect reporting culture, such as states with urban populations that may have more developed technical infrastructure, highly digitized economies, and awareness of the FBI IC3 and other protection programs. All of these may contribute to the varying levels of exposure of residents to phishing attacks and vary in their willingness and ability to report.

I account for these factors when examining the association between phishing victim reports and the hypothesized factors to develop possible explanations for these relationships. The figure below illustrates how these factors are used for the regression framework.

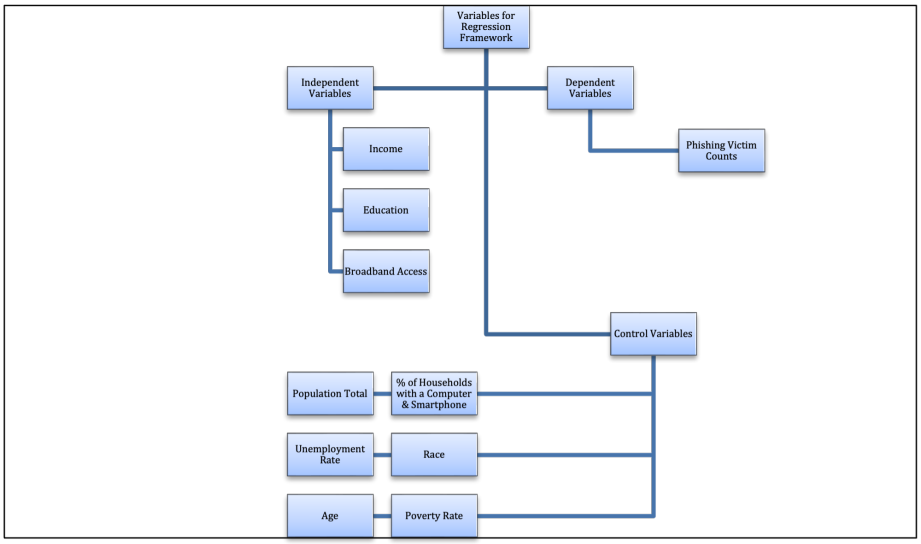


Figure 5: Correlation/Regression Variables

3.3 State-Based Vulnerability

There is no unilateral way to determine vulnerabilities across states, especially from a structural and socio-economic perspective. Therefore, I compute a vulnerability score based on the hypothesized variables – income, education, and broadband access. By negating the percentage computed, I derive a vulnerability score based on my hypothesized factors and standardize that value using a z-score. The vulnerability index is therefore the average of the negated z-score of all hypothesized factors.

Variables	Calculation	Z-score
% of Households without Broadband	pct_no_broadband = 100 - pct_households_broadband	z_no_broadband = zscore(pct_no_broadband)
% of Individuals without a High School Degree	pct_no_high_school = 100 - pct_high_school_or_higher	z_no_high_school = zscore(pct_no_high_school)
Median Household Income	neg_income = - median_household_income_usd	z_low_income = zscore(neg_income)

Figure 6: Vulnerability Index Breakdown

Vulnerability Index is calculated as:

$$\text{mean}\left(z_{\text{no\_broadband}},\ z_{\text{no\_high\_school}},\ z_{\text{low\_income}}\right)$$

By computing the vulnerability scores, the relative change in each factor is measured, and all variables are equally considered in reviewing how these states differ in their characteristics.

3.4 Data Utilization

In answering the research questions, I combine the ACS dataset and the FBI IC3 data and use these values for each state from 2019 to 2024 to compute a vulnerability score using the methods defined above. For the Pearson correlation, I utilize the three hypothesized variables - income, broadband access, and education as the independent variables, and state-level IC3 phishing victim counts as the dependent variable to assess their association. For the regression model, I use these variables alongside the control variables defined above and include state and year fixed effects to capture changes within states over time. The vulnerability score is used as a composite measure to summarize state-level disadvantage and is analyzed separately. The results are presented in the following chapter.

4 RESULTS

By aggregating the population information, Figure 7 presents the distribution of phishing victim rates from 2019 to 2024.

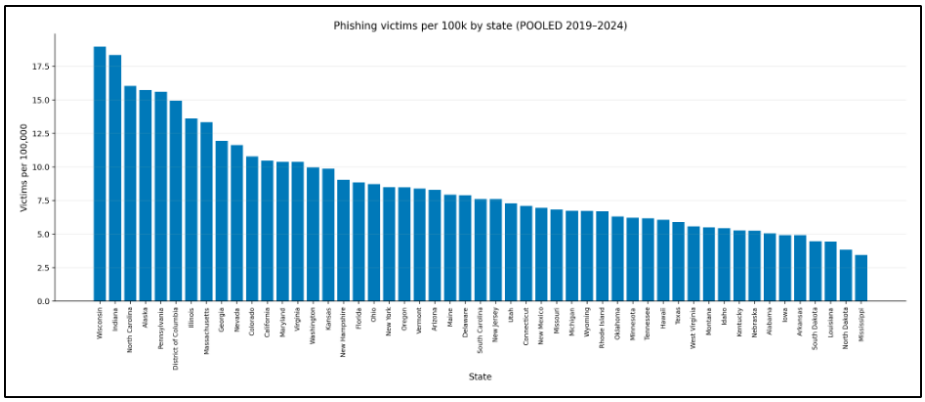


Figure 7: Phishing Victims Distribution by State

The figure above shows the states with the highest levels of phishing rates per hundred thousand people, highlighting the concentration of phishing victims across states.

To answer the question, how do the hypothesized factors – income, broadband access, and education correlate with phishing attack counts across U.S. states? I aim to understand the relationship between the hypothesized factors and phishing victim counts. I use the Pearson Correlation Coefficient to analyze this association. The p-value used across the research is $0.05 \leq p \leq 0.1$.

4.1 Vulnerability across States

I use the Z-score method explained in Chapter 3 and the independent variables to determine a measure of socio-economic disparity. Using income, broadband access, and education, in understanding state vulnerabilities, the most vulnerable states, understood by their disadvantages, are presented below:

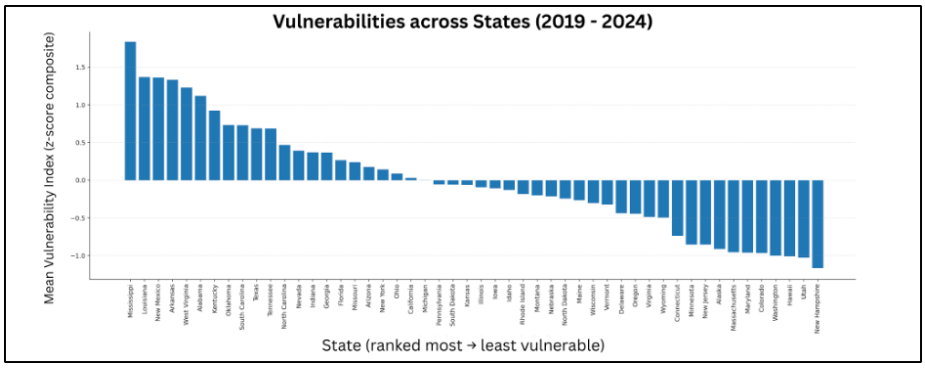


Figure 8: Vulnerability Distribution by State

States with higher vulnerability scores are considered the most vulnerable and often have lower household incomes, lower broadband access, and lower education attainment rates. Negative values suggest less vulnerability. States in the leftmost area of Figure 8 (with positive values) are considered more vulnerable. These are Mississippi, Louisiana, New Mexico, Arkansas, and West Virginia. States with at the rightmost area of the graph (less vulnerable) often have higher household incomes, higher broadband access, and higher education attainment rates. These include Massachusetts, New Hampshire, and Washington. Overall, states in the Southern United States generally demonstrate higher rates of vulnerability compared to others. This exemplifies and supports the definitions of other research regarding socio-economic inequalities across the United States, which claims that southern states exhibit higher vulnerability and socio-economic inequality.[42]

42. Chien D. Ng et al., "Validating the Social Vulnerability Index for Alternative Geographic Units in the United States," —, 2025, accessed April 1, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC11915720/.

4.2 Correlation Analysis

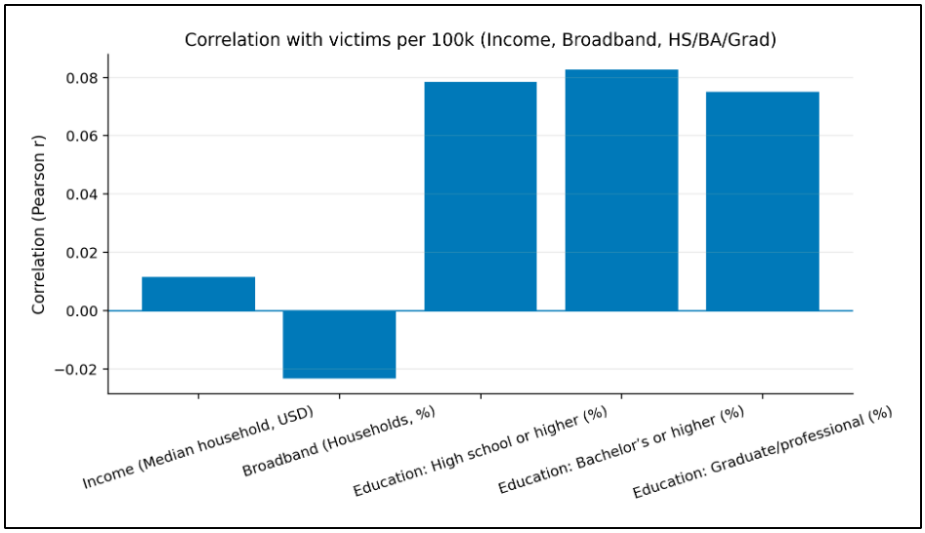


Figure 9: Pearson Correlation (Factors vs Phishing Rate)

Across the three independent variables, the correlations displayed above are not statistically significant as the p-values are greater than 0.1. While education seems to have the highest coefficient values and household broadband access has the least, it can't be used for statistical analysis as these relationships are extremely weak, with the coefficients, i.e., r values, ranging from -0.02 to 0.08, and show no evidence of a relationship with phishing victim counts across states. As these non-statistically significant correlations are not utilized as results, they show that the hypothesized factors, income, broadband access, and education, do not meaningfully correlate to any patterns or variation in phishing reports across states.

4.3 Regression Analysis

To further understand the differences across states in relationships with the hypothesized factors and phishing victim counts, I conduct a multiple OLS regression analysis using phishing victim counts per 100k as the dependent variable and the hypothesized factors as independent variables. Between 2019 and 2024, there were 250 observations analyzed, and the R^2 value is 0.408, which represents 41% of the variation in outcomes. This result reflects the variance rather than the predictive power of the variable on the outcome. The results are presented below:

Independent Variables and Phishing per 100k	Coefficient Value	*P*-Value
Income	0.000052	0.163
Broadband**	0.400**	0.001**
High School Education or higher**	0.155**	0.076**
Bachelor's Degree or higher **	-0.383**	0.002**
Graduate Degree or higher**	0.403**	0.032**

Figure 10: OLS Regression Analysis Breakdown

Note: ** denotes statistical significance.

Compared to the Pearson correlations, this regression provides a different insight. Broadband access levels have the highest coefficient value at 0.4, with a p-value $p < 0.001$, indicating that an increase in broadband access of 1% increases phishing victim counts by 0.400 per 100,000 people. Given the methods of phishing delivery — email, calls, videos, and others- this likely reflects the role of internet-based delivery mechanisms in phishing attacks.

Education levels show mixed results. For individuals with a high school education, the regression model has a coefficient of 0.155, and $p < 0.076$, indicating marginal significance as defined by the threshold in the earlier paragraphs. This suggests a positive relationship between the two variables (high school education and phishing reports), although it is not as strong or significant as the broadband level coefficient. The bachelor's degree or higher variable shows a negative relationship with a coefficient value of - 0.383, with $p < 0.002$; individuals with this degree are associated with lower phishing victim counts across states. Individuals with graduate degrees have a coefficient of 0.4023 with $p < 0.032$. This suggests that advanced (graduate) education is associated with higher levels of phishing victim counts. These education results collectively suggest that the relationship between education and phishing victimization is not all similar, with different levels of education exhibiting varying and sometimes opposing associations.

The graduate degree components are already encompassed by the previous term – "High School Education or Higher" or "Bachelor's Degree or Higher", as counted by the ACS. Therefore, the graduate degree component runs the risk of introducing multicollinearity due to overlapping explanatory power across education variables and is, therefore, excluded from interpretation and relative analysis in this research.

Compared to the other hypothesized variables, income has the lowest coef-

ficient value at 0.000052 with a p-value of 0.163. While this R value coefficient is positive, this relationship is not statistically significant. Income doesn't show a meaningful association with phishing victim counts when considered independently. Broadband access rates and education are two factors that show some level of association across states. Individuals with a high school education are more associated with higher phishing victim counts, while those with bachelor's degrees show a negative association.

These correlation and regression results offer both support and challenges to the hypothesis. The Pearson correlation above highlighted that education showed the strongest observed association with phishing victim counts, although this result was not statistically significant. The regression analysis showed that individuals with a bachelor's degree were associated with lower phishing victim counts across states, a result that is consistent with current literature that suggests digital literacy, specifically through education, as a promising avenue to reducing risks and increasing awareness of phishing. This suggests that higher levels of education may contribute to improved phishing awareness and therefore a reduction in risk compared to high school degree holders, who have the largest association with these reports.

4.4 Controlling for other factors

In addition, I run an OLS regression controlling for time and state-level factors. I review the hypothesized variables while controlling for other factors, such as state demographics (race and age), urbanization, alongside other proxies shown in Figure 4, to examine changes within a state over time. To avoid collinearity, I also use a singular education variable rather than all levels of education (High School, Bachelor's, and Graduate School). The model examines the relationship between income, education, and broadband access and phishing victim counts, while controlling for state-specific factors that remain constant over time, year-specific effects, and measurement error. The formula utilized is therefore:

$$\log\big(1+Y_{s,y}\big) = \beta_1 \,\text{Income}_{s,y} + \beta_2 \,\text{Education}_{s,y} + \beta_3 \,\text{Broadband}_{s,y} + l\theta \,\mathbf{X}_{s,y} + \gamma_s + \delta_y + \varepsilon_{s,y}$$

Where

- s denotes state
- y denotes year
- $Y_{s,y}$ denotes phishing victims per 100,000 people in state s and year y
- $\log(1 + Y_{s,y})$ is the log-transformed dependent variable for skewness
- $\text{Income}_{s,y}$ denotes median household income
- $\text{Education}_{s,y}$ denotes the education index (constructed from high school, bachelor's attainment)

- $\text{Broadband}_{s,y}$ denotes broadband access
- $\mathbf{X}_{s,y}$ denotes a vector of the control variable
- θ denotes the coefficients associated with the control variables
- γ_s denotes state fixed effects (time-invariant characteristics of each state)
- δ_y denotes year fixed effects (common shocks affecting all states in a given year)
- $\varepsilon_{s,y}$ denotes the error term

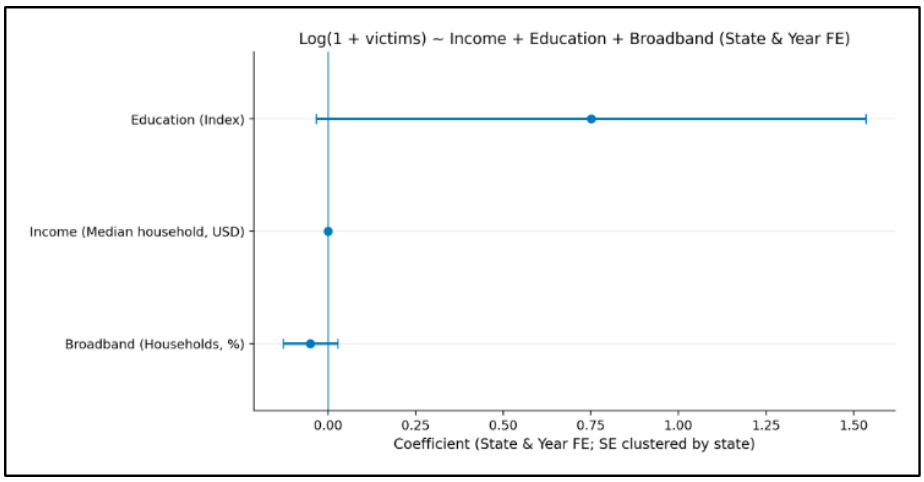


Figure 11: Fixed Effects OLS Regression Model

The figure above presents the coefficients from the two-way fixed effects and control variables regression model. The results show that the coefficient of income is 0; however, there is no statistically significant association or correlation detected, and changes in income within a state over time are not strongly associated with phishing victim counts. For broadband levels, the negative coefficient is not statistically significant, so no meaningful association can be inferred. The education variable has a coefficient of 0.75, suggesting a positive association between changes in education and phishing victim counts. However, despite controlling for state and year fixed effects, this estimate has a wide confidence interval, suggesting that there are other unobserved factors that may explain this relationship.

4.5 Further Regression based on Vulnerabilities

I conduct a separate regression model using phishing victim counts as the dependent variable and the vulnerability index and hypothesized factors as in-

dependent variables. In the results, the coefficient of the vulnerability index is 1.3482 with $p < 0.250$. This result is not statistically significant, showing that as vulnerability changes over time across states, there is no evidence of an association with changes in the counts of phishing victims.

4.6 Income, Education, Broadband Access, Phishing and Vulnerabilities

Figure 12 illustrates phishing victim counts relative to state population. Figure 12, alongside Figure 8 below, shows that relative to their state population, more vulnerable states record fewer phishing victim counts. The left-most parts of Figure 8 with positive values are more vulnerable states (lower income, broadband access, and education levels), while less vulnerable states show negative values, indicating higher income, education and broadband access levels. Wisconsin has higher broadband, income, and education levels, and recorded higher counts of phishing victims per population, compared to Texas, one of the largest states in the U.S, but is considered more vulnerable due to its larger population and therefore records fewer counts of phishing victims in relation to that.

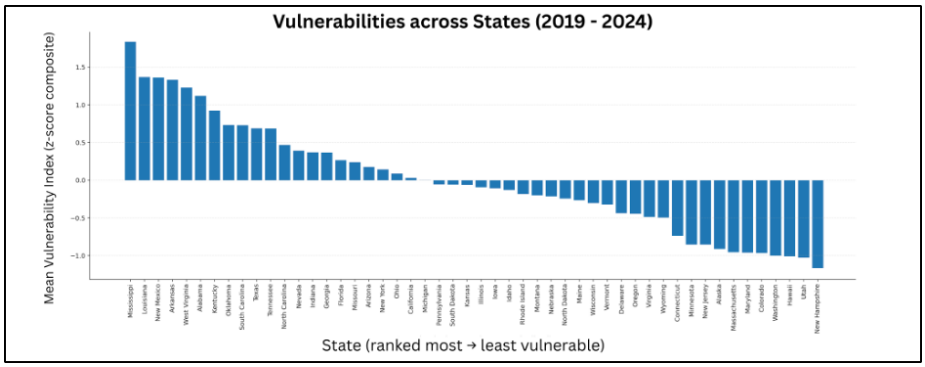


Figure 8: Vulnerability Distribution by State

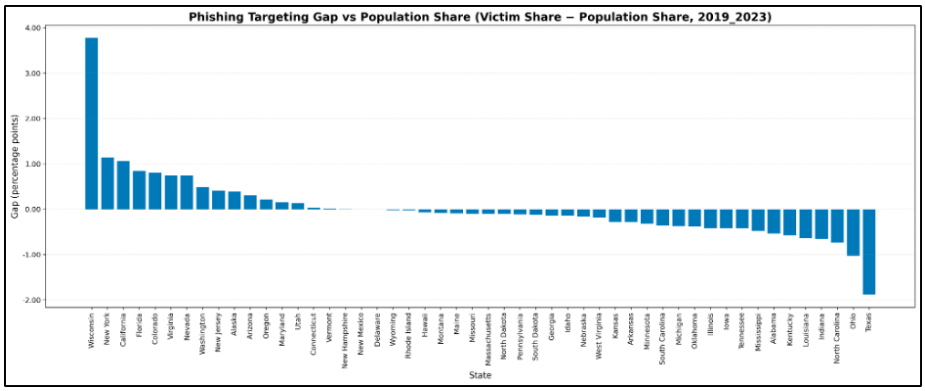


Figure 12: Phishing Victims relative to population

Vulnerability alone does not explain variation in phishing victim counts across states, as it didn't have a statistically significant relationship in the regression framework. Figure 12 could be understood as a reflection of differences in digital exposure and reporting mechanisms.

In interpreting vulnerability and how it is reflected through the phishing victim count analyses above, several arguments can be made. A possible explanation is that more educated states, while being the least vulnerable, are the most exposed, and this exposure is reflected in the figure above by an awareness of reporting mechanisms.

This pattern doesn't necessarily mean intentional targeting of less vulnerable states; it could mean that the more literate and less vulnerable a state is, the more likely its residents are to report these phishing attacks. My earlier hypothesis assumed that higher reports of phishing automatically equate to vulnerability; however, this is likely incorrect. More likely, less vulnerable populations have increased exposure and a higher likelihood to report these crimes, and as such, will record more counts per state. This reflects their capacity to identify these events and report using existing infrastructure, a key embodiment of digital literacy. However, there are many possible scenarios beyond the above, which may not depend on or relate to education or digital literacy but rather focus on other factors affecting these individuals, such as loss of amounts they consider small.

The results in this chapter suggest that education levels and broadband access are the most significant factors with an observed association with phishing victim counts per state, although this does not mean intentional targeting based on these factors.

5 EDUCATION AND DIGITAL LITERACY

This chapter answers the second question of this research, which states: how can digital literacy strategies be designed as a solution reflective of vulnerable states' needs and experiences?

Chapter 4 showed that education showed the strongest observed association (apart from broadband access) compared to the other variables in the regression analysis. The association in Chapter 4 offered insights into higher phishing reports among high school-educated individuals. It also offered an alternative understanding to my earlier hypothesis.

I initially assumed that higher education (Bachelor's or higher) would generally be associated with lower levels of phishing reports because they may experience fewer phishing attacks; the results support the assumed relationship, as across states, individuals with a Bachelor's education are associated with lower phishing victim counts. However, the other regression and distribution results showed the inverse, suggesting that less vulnerable states (often having higher education, income, and broadband access) are associated with higher counts of phishing reports, possibly due to increased knowledge of reporting mechanisms and relevant enforcement agencies.

Although some of the results in the previous chapter are not statistically significant, they provide insight into underlying trends and variations across the hypothesized variables. The statistically significant results, however, suggest that there are possible differences in how technical knowledge and digital usage may interact and affect exposure to phishing and subsequently reporting. Therefore, these results and findings contribute to providing a framework to address risks arising from limited exposure and lack of awareness. This finding – that education can be associated with reports of phishing by victims is supported by previous research that suggests that education is a promising avenue in increasing awareness of phishing capabilities, risks, and protection mechanisms (see Benjamin et al,[43] Uhomoibhi et al.[44])

This research is useful as it breaks down the education component by qualifications, i.e., high school, bachelor's, and graduate degrees, as shown in Chapter 4.

43. Benjamin Reinheimer et al., "An Investigation of Phishing Awareness and Education Over Time," in *Proceedings of the Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)* (USENIX Association, 2020), 259–284.

44. Juliet Uhomoibhi et al., "The Need for Education on Phishing," *Campus-Wide Information Systems* 28, no. 5 (2011): 308–319, https://doi.org/10.1108/10650741111181580.

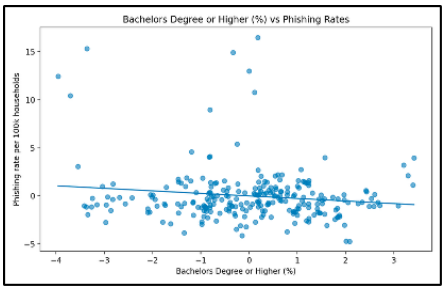


Figure 13: Bachelor's Degree vs Phishing Rate

$$p < 0.002$$

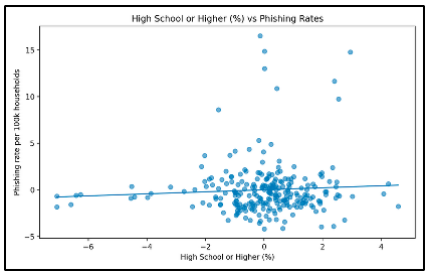


Figure 14: Education factors vs Phishing Rate

$$p < 0.076$$

Both figures above are statistically significant using the threshold defined earlier. The negative correlation in Figure 13 suggests that individuals with a Bachelor's degree or higher are associated with lower reported phishing victim counts compared to those with a high school degree in Figure 14. As a result, I argue that digital literacy strategies would be more suited to individuals with a high school education, who show an observed positive association with reported phishing victim counts. I propose that the most effective way to implement these strategies is to integrate phishing training into high school education, as it will encompass individuals who may later pursue higher education. This research provides a foundation for understanding the advantage of phishing education campaigns in high school, which may offer broader benefits as the first structured point of exposure to digital literacy for many individuals.

Phishing training often occurs within companies that aim to improve digital security, even among learned and experienced individuals, but barely across households or for specific individuals who may not go on to professions that have this requirement; therefore, incorporating such training in high school is important and required for individuals to be more aware and digitally literate. As mandatory high school education is determined by states, the adoption of

school-mandated phishing training as policy could be instrumental in mitigating future phishing risks across the United States. The following section presents a preliminary curriculum draft that incorporates digital literacy training into high school education.

5.1 Reframing Digital Literacy

To derive a solution that enhances the ability to identify, respond to phishing attacks, and encourage digital literacy, I develop a curriculum targeting high school students, as it has a high attainment rate nationwide.[45]

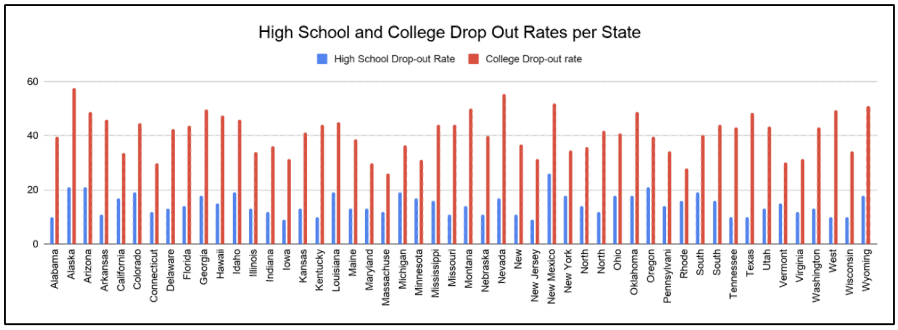


Figure 15: Dropout rates for high schools and colleges per U.S states

Figure 15 displays the average dropout rates, calculated by the National Center for Education Statistics (NCES) using the U.S. average adjusted cohort graduation rate (ACGR) for public high school students[46] and the average dropout rates, derived from the "graduation rate within 150% of normal time at 4-year postsecondary institutions."[47]

The figures above show that high school graduation rates are much higher than college graduation rates across the United States. For example, the highest high school dropout rate was 26% in New Mexico,[48] compared to the highest college dropout rate of about 57% in 2017 in Alaska. This suggests that students are generally more likely to complete high school than college; therefore, designing a curriculum for high school students increases the likelihood of reaching a broader population with phishing education. This raises the question: why not middle school? Research has shown that early access to CS education is crucial

45. U.S. Census Bureau, "Census Bureau Releases New Educational Attainment Data," February 24, 2022, https://www.census.gov/newsroom/press-releases/2022/educational-attainment.html.

46. National Center for Education Statistics, "Public High School Graduation Rates," Condition of Education, accessed April 1, 2026, https://nces.ed.gov/programs/coe/indicator/coi/high-school-graduation-rates.

47. National Center for Education Statistics, "IPEDS Trend Generator," accessed April 1, 2026, https://nces.ed.gov/ipeds/trendgenerator/app/build-table/7/19.

48. National Center for Education Statistics, "Public High School Graduation Rates."

in eliminating gaps in knowledge and future engagement.[49] Research often advocates for an effective middle-high school transition for CS education, as the data suggests that the beginning of high school in the United States (9th grade), "may be an effective point to invite a wide, diverse student population to CS."[50]

The contrast and variation between the dropout rates of college and high school, as well as research supporting high school as a strong foundation for the introduction of CS concepts, is used to design a curriculum that is more reflective of the state of the education system within the United States. It also provides additional justification for the introduction of this curriculum to high schools rather than college students, who may have different interests and specialty/concentration/major requirements.

5.2 Existing Computer Education Curriculum

Across the U.S., certain states have laws that require computer education in high schools. Some states, i.e., South Carolina, Nevada, Arkansas, Tennessee, and Nebraska, require computer science as a graduation requirement,[51] while other states require schools to offer these classes within the high school curriculum. The following image presents states within the U.S. that require computer science as a requirement for high school graduation. The table serves as a way to visualize how many states across the country have adopted this course. As of 2017, 24 states across the country allow for computer science credit to substitute Mathematics graduation credits, 9 states allow for it to substitute Science graduation credits, and 4 states allow for it to replace any other credit for graduation.

49. David J. Amiel and Cynthia L. Blitz, "The Middle-to-High School Transition: Key Factors Shaping 9th-Grade Computer Science Enrollment," *International Journal of Computer Science Education in Schools* 7, no. 2 (2025), https://doi.org/10.21585/ijcses.v7i2.234.

50. Amiel and Blitz.

51. Vicki Davis, "Why More States Are Requiring Computer Science Classes," Tech & Learning, accessed April 1, 2026, https://www.techlearning.com/news/why-more-states-are-requiring-computer-science-classes.

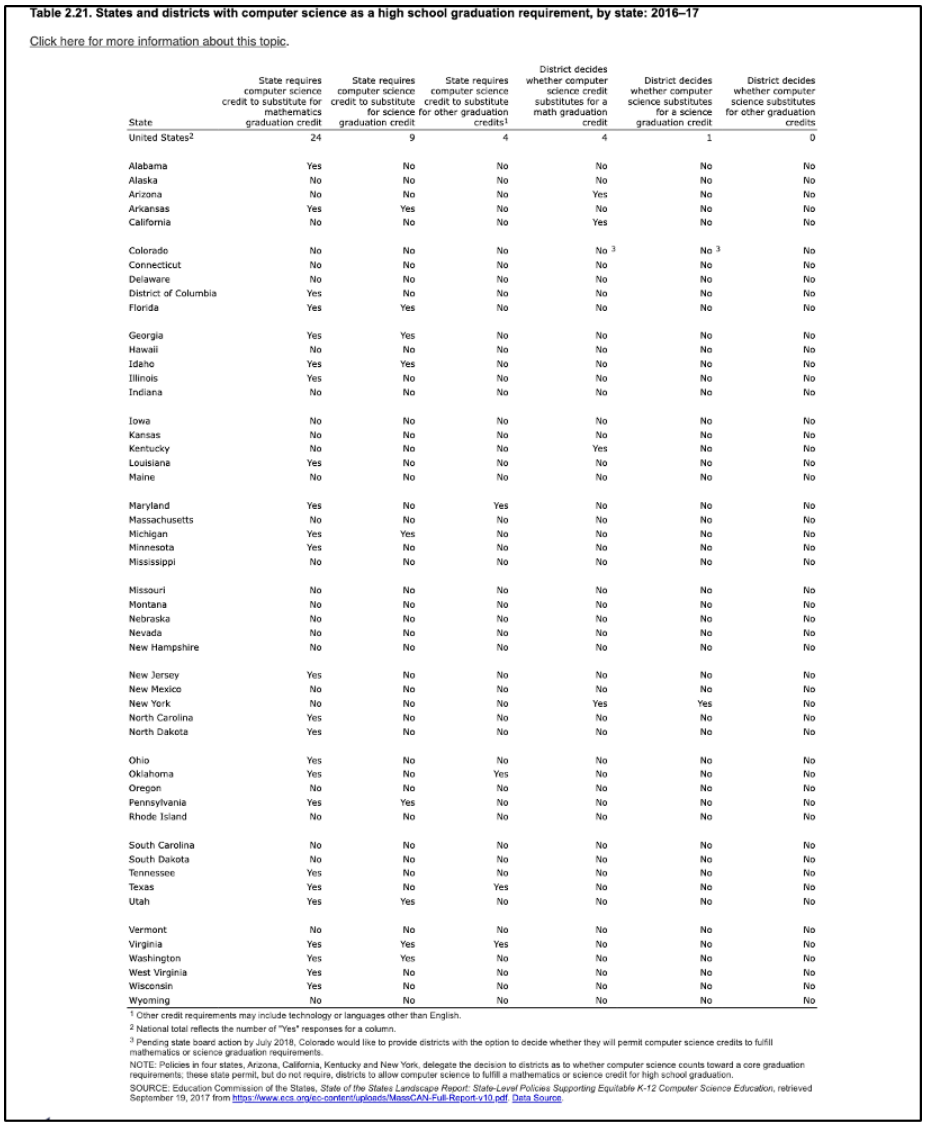


Table 2.21. States and districts with computer science as a high school graduation requirement, by state: 2016–17

Click here for more information about this topic.

State	State requires computer science credit to substitute for mathematics graduation credit	State requires computer science credit to substitute for science graduation credit	State requires computer science credit to substitute for other graduation credits[1]	District decides whether computer science credit substitutes for a math graduation credit	District decides whether computer science substitutes for a science graduation credit	District decides whether computer science substitutes for other graduation credits
United States[2]	24	9	4	4	1	0
Alabama	Yes	No	No	No	No	No
Alaska	No	No	No	No	No	No
Arizona	No	No	No	Yes	No	No
Arkansas	Yes	Yes	No	No	No	No
California	No	No	No	Yes	No	No
Colorado	No	No	No	No [3]	No [3]	No
Connecticut	No	No	No	No	No	No
Delaware	No	No	No	No	No	No
District of Columbia	Yes	No	No	No	No	No
Florida	Yes	Yes	No	No	No	No
Georgia	Yes	Yes	No	No	No	No
Hawaii	No	No	No	No	No	No
Idaho	Yes	Yes	No	No	No	No
Illinois	Yes	No	No	No	No	No
Indiana	No	No	No	No	No	No
Iowa	No	No	No	No	No	No
Kansas	No	No	No	No	No	No
Kentucky	No	No	No	Yes	No	No
Louisiana	Yes	No	No	No	No	No
Maine	No	No	No	No	No	No
Maryland	Yes	No	Yes	No	No	No
Massachusetts	No	No	No	No	No	No
Michigan	Yes	Yes	No	No	No	No
Minnesota	Yes	No	No	No	No	No
Mississippi	No	No	No	No	No	No
Missouri	No	No	No	No	No	No
Montana	No	No	No	No	No	No
Nebraska	No	No	No	No	No	No
Nevada	No	No	No	No	No	No
New Hampshire	No	No	No	No	No	No
New Jersey	Yes	No	No	No	No	No
New Mexico	No	No	No	No	No	No
New York	No	No	No	Yes	Yes	No
North Carolina	Yes	No	No	No	No	No
North Dakota	Yes	No	No	No	No	No
Ohio	Yes	No	No	No	No	No
Oklahoma	Yes	No	Yes	No	No	No
Oregon	No	No	No	No	No	No
Pennsylvania	Yes	Yes	No	No	No	No
Rhode Island	No	No	No	No	No	No
South Carolina	No	No	No	No	No	No
South Dakota	No	No	No	No	No	No
Tennessee	Yes	No	No	No	No	No
Texas	Yes	No	Yes	No	No	No
Utah	Yes	Yes	No	No	No	No
Vermont	No	No	No	No	No	No
Virginia	Yes	Yes	Yes	No	No	No
Washington	Yes	Yes	No	No	No	No
West Virginia	Yes	No	No	No	No	No
Wisconsin	Yes	No	No	No	No	No
Wyoming	No	No	No	No	No	No

[1] Other credit requirements may include technology or languages other than English.

[2] National total reflects the number of "Yes" responses for a column.

[3] Pending state board action by July 2018, Colorado would like to provide districts with the option to decide whether they will permit computer science credits to fulfill mathematics or science graduation requirements.

NOTE: Policies in four states, Arizona, California, Kentucky and New York, delegate the decision to districts as to whether computer science counts toward a core graduation requirements; these state permit, but do not require, districts to allow computer science to fulfill a mathematics or science credit for high school graduation.

SOURCE: Education Commission of the States, *State of the States Landscape Report: State-Level Policies Supporting Equitable K-12 Computer Science Education*, retrieved September 19, 2017 from https://www.ecs.org/ec-content/uploads/MassCAN-Full-Report-v10.pdf. Data Source.

Figure 16: Computer Science High School Education across U.S. States

52

5.3 States and Existing Curricula

Few states have mandatory high school requirements for computer science education. South Carolina's high school curriculum involves computer fundamentals such as "Computing Systems, Networks and the Internet, Data and Anal-

ysis, Algorithms and Programming, and Impact of Computing."[53] South Carolina also offers specialized courses in cybersecurity, among others.[54] Nevada's computer science curriculum begins before high school and spans from 1st to 12th grade, and similarly involves the topics above.[55] Arkansas's middle and high school curriculum seeks to empower students with programming skills and a good foundation of computer fundamentals. These curricula all feature a similar system of introducing students to concepts of programming, software development, and engineering, while practical concepts of cyber and computer security relevant to everyday use largely remain absent.

One of the most comprehensive computer science high school curricula comes from Rhode Island, which launched the CS4RI Initiative in 2016, intending to "establish computer science courses in schools throughout the state," making Rhode Island "the first state in the U.S. to teach the subject in every public school."[56] This initiative includes all forms of public high schools (traditional or charter) across districts.

I examine the CS4RI curriculum, which incorporates programming and computer system fundamentals as core topics in its State Standards Concept. These topics include "Programming, Networking/Systems, Cyber Security, Data, Digital Literacy, and Computing in Society"[57] under the banner of computer science. This curriculum is reflective of a more comprehensive education that considers non-technical concepts, e.g., human-computer interaction (HCI), graphics, and impact on society,[58] that govern daily lives and are related to digital and data literacy.

Within Rhode Island, the computer science curriculum is offered in two primary forms. Career & Technical Education (CTE) programs "consist of three or more courses which will help students earn an industry credential and prepare them to enter the workforce."[59] Certain schools in Rhode Island offer computer science as a CTE program, including specialized courses such as "Cybersecurity, Graphic Communications, Networking, Software Development."[60] Other schools offer computer science as an elective. In either form, I propose incorporating a

53. South Carolina Department of Education, "South Carolina Computer Science Standards for High School," Accessed April 1, 2026, n.d. https://www.ed.sc.gov/instruction/standards/computer-science/standards/draft-for-review-south-carolina-computer-science-standards-for-high-school/.

54. South Carolina Department of Education.

55. Nevada Department of Education, "Nevada Academic Content Standards," https://webapp-strapi-paas-prod-nde-001.azurewebsites.net/uploads/Nevada_Academic_Content_Standards_forrev_adf847c3ac.pdf.

56. Michelle Rafter, "Rhode Island's CompSci Education Project: How Is It Going?," Government Technology, accessed April 1, 2026, https://www.govtech.com/education/k-12/rhode-islands-compsci-education-project-how-is-it-going.html.

57. Computer Science for Rhode Island, "Programs," accessed April 1, 2026, https://www.cs4ri.org/programs.

58. Computer Science for Rhode Island, "Home," accessed April 1, 2026, https://www.cs4ri.org/.

59. Rhode Island Department of Education, "Career and Technical Education," accessed April 1, 2026, https://ride.ri.gov/students-families/career-technical-education.

60. Rhode Island Department of Education, "CTE Programs Map," accessed April 1, 2026, https://tableau.ride.ri.gov/t/Public/views/CTE_Programs_Map/CTEMAP.

social engineering module across all states, either within existing cybersecurity or computer science curricula, or as a standalone component in states where such courses aren't offered. This education will include a broader "cybersecurity" component and specifically social engineering, which relates to all people, regardless of computer expertise, and interest in engineering.

For states like Rhode Island with computer science curricula beyond programming and computer system fundamentals, the modification to the CS4RI curriculum includes an expansion of its cybersecurity core module to ensure that students have a foundational understanding of social engineering techniques and can identify and respond to real-life threats such as phishing.

My proposed social engineering component has been developed in line with the Next Generation Science Standards that emphasize "a three-dimensional approach to classroom instruction that is student-centered and progresses coherently from grades K-12."[61] Focusing on the Engineering, Technology and Application of Science Discipline, the three-dimensional approach enables students to develop an "understanding of multiple grade-appropriate elements of the science and engineering practices (SEPs), disciplinary core ideas (DCIs), and crosscutting concepts (CCCs) that are deliberately selected to aid student sense-making of phenomena and/or designing of solutions."[62] This approach enables students to examine why social engineering disproportionately affects certain groups and understand the underlying foundations of how different vulnerabilities interact to increase phishing susceptibility. These practice standards inform a curriculum where students are aware of the factors that influence digital risks and vulnerabilities, while developing practical solutions to safeguard sensitive information and contribute to improved digital security within their communities. In line with the SEPs, DCIs, and CCCs, the learning outcomes for the curriculum are to ensure that, at the end of this course, students would be able to:

- Understand the broad nature of social engineering
- Identify the different forms and techniques of social engineering attacks i.e., phishing, vishing, smishing, or other techniques in practice
- Distinguish between different forms of social engineering attacks
- Determine personally identifiable information and protection mechanisms
- Review ways to prevent and mitigate social engineering attacks
- Navigate tools to report to authorities and relevant organizations
- Understand the citizen's responsibility to report these crimes and educate others on reporting capabilities

61. National Science Teaching Association, "Next Generation Science Standards (NGSS)," accessed April 1, 2026, https://www.nsta.org/science-standards.

62. Achieve, Inc., "EQuIP Rubric for Science: Detailed Guidance," March 2021, https://www.nextgenscience.org/sites/default/files/EQuIPDetailedGuidanceMarch2021.pdf.

The modules for this curriculum are highlighted below and explained in more detail using a module plan, a form of backward design created and popularized by Grant Wiggins and Jay McTighe. An in-depth breakdown of this curriculum's core modules is presented below:

- An Introduction to Social Engineering
  This focuses on a general introduction to social engineering with an emphasis on the human aspects of using manipulation to derive personally identifiable information and utilize it for adverse purposes. It expands on the types of social engineering highlighted below.

  - Physical: Social engineering that involves "some form of physical action in order to gather information on a future victim."[63]
  - Social: Social engineering that utilizes "socio-psychological techniques such as Cialdini's principles of persuasion to manipulate their victims."[64] This is particularly common and effective in divulging personal information.
  - Technical: Social engineering that is "mainly carried out over the Internet."[65]

63. Maria Bada, Angela M. Sasse, and Jason R. C. Nurse, "Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?," *Computers & Security*, https://www.sciencedirect.com/science/article/pii/S2214212614001343.
64. Bada, Sasse, and Nurse.
65. Bada, Sasse, and Nurse.

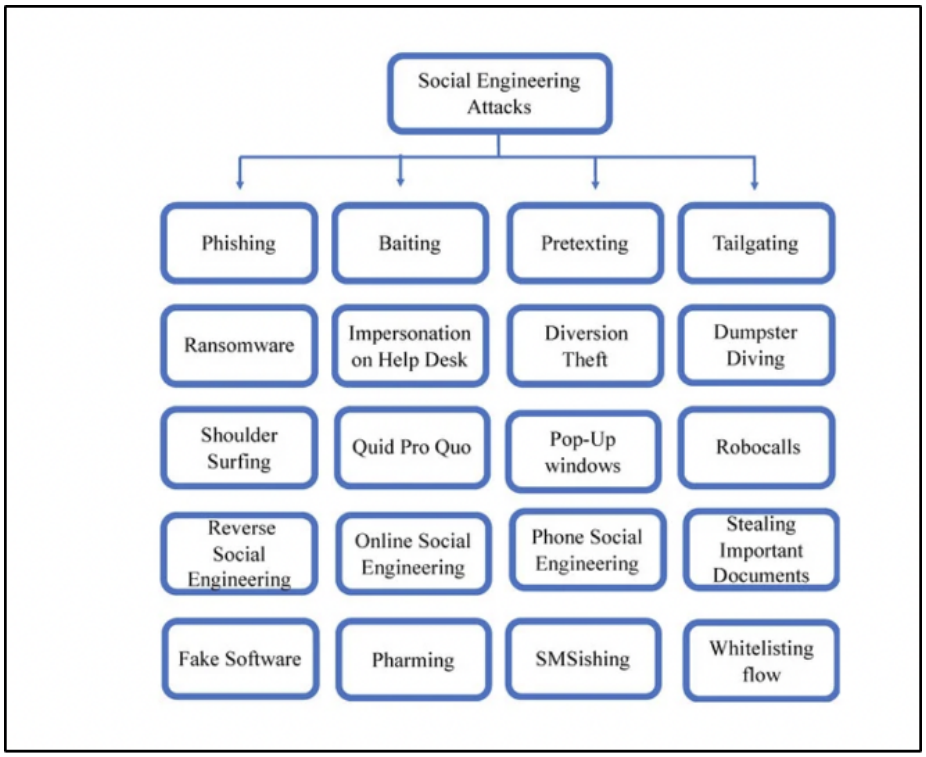


Figure 17: Social Engineering Attack Types by Adel Alshamrani.
[66]

- Social Engineering Attacks
  This module provides details on the breadth of social engineering attacks that exist and how they can be carried out. It will focus mainly on the first level shown in the image, i.e., phishing, baiting, pretexting, and tailgating, due to their common nature and their relevance to the target groups.

- Personally Identifiable Information and Incident Response
  This module ensures that the students are able to identify the attack types through different presentations, training, and simulations. A key component of this topic is that it teaches them how to determine and identify Personally Identifiable Information (PII) and why these details are important. It also includes how to safeguard PII and how to manage social engineering attacks, specifically through prevention and mitigation.

- Cybersecurity Awareness
  This module puts the work being learnt into practice and provides the students with the ability to utilize knowledge learnt to determine phishing strategies or unusual conversations that lead to the revelation of private information in ways that can be harmful.

- Threat Resolution
  This module encompasses the process of reporting an attack as well as final documentation processes. It provides a variety of individuals to notify, i.e., financial institutions or companies involved, government agencies, and external management to report immediate and long-winded attacks. Finally, it teaches about compiling documentation in case of enquiries as well as for other agencies to ensure it doesn't become a repeated occurrence.

  The plans for each module are as follows:

MODULE 1
STAGE 1 - DESIRED RESULTS

Practice Standards (SEPs):
- Asking questions and defining problems,
- Constructing explanations and designing solutions
- Planning and carrying out investigations

Content Standards:
- HS-ETS1-2: Developing technical solutions to engineering and real-world problems
- HS-ETS1-3: Evaluating technical solutions using specific criteria and trade-offs

Essential Question(s)
- Overarching Question(s):
  - What can be explained by the word social?
  - How do we understand engineering in our daily activities?
  - How does the internet show up in our daily lives?
- Topical Question(s):
  - What is social engineering?
  - Why does social engineering matter?
  - How does social engineering manifest daily?

Student Knowledge: Students will know...	*Student Skills: Students will be <u>able to</u>...*
● How to define social engineering ● The personal element, i.e., humans, that make it successful ● Types of social engineering	● Differentiate between physical, social, and technical social engineering ● State and recall examples of forms of social engineering that commonly occur in scenarios

STAGE 2 - ASSESSMENT EVIDENCE

What summative assessment tasks will students PRODUCE?
- Task: Individual project to identify social engineering
- Model: Given a hypothetical town, Wonderland, where there are mainly older people/younger people, explain how social engineering would exist or be presented?
- Rubric Checklist:
  - Does the project demonstrate an understanding of social engineering?
  - Does the project identify relevant techniques or forms of social engineering e.g. phishing?
  - Does the project include or define scenarios that exemplify these techniques in practice?

STAGE 3 - LEARNING PLAN

What instructional activities will you use to teach the identified learning objectives?
- Lecture-based Introduction to social engineering
  - Focus on guided lecture discussions on the meaning of “social” and “engineering.” This allows students to understand possible relations between these two terms
- Anecdotes as Experiences:
  - Providing a scenario of possible attacks and allowing students to identify or evaluate the impact of certain information, e.g., personal bank details, and possible consequences if compromised

- Scenario samples
    - An individual claiming to be a representative of Citizens Bank sends you an email asking you to review last “suspicious login attempts” using a specific link embedded in the email. The link is malicious and clicking on it allows third party access to your bank account.
    - You get a phone call from the Apple Store saying you won the Latest iPhone 17 Pro Max. In order to receive it, they need your name, social security number, address and card details to secure delivery and shipping.
- Reviewing those scenarios and deconstructing each element to identify the human element that made it possible

MODULE 2
STAGE 1 - DESIRED RESULTS

Practice Standards (SEPs):
- Constructing explanations and designing solutions
- Asking questions and defining problems
- Obtaining, evaluating, and communicating information

Content Standards:
- HS-ETS1-1: Defining and delimiting engineering problems
- HS-ETS1-3: Evaluating technical solutions using specific criteria and trade-offs

Essential Question(s)
- Overarching Question(s):
  - Given what we learnt about social engineering, who can be a victim of it?
  - How can people be targeted?
  - What is Phishing?
- Topical Question(s):
  - Privacy and Security: How do you know someone is who they claim to be?
  - Modes of communication across the internet
  - Forms of social engineering in practice

Student Knowledge: Students will know...	*Student Skills: Students will be able to...*
● Forms of social engineering attacks ● Phishing and its mutated forms	● Identify various forms of social engineering attacks ● Differentiate between phishing, smishing, and other variations ● Understand who can be attacked and why

STAGE 2 - ASSESSMENT EVIDENCE

Summative Assessments:
- Task: Can you identify a phishing/social engineering attack?
- Model: Given a set of scenarios, match each scenario to an attack form and explain the reasons behind your decisions. Finally, provide a suggestion on how to prevent it if possible.
- Rubric Checklist:
  - Does the presentation correctly match a scenario to an attack form?
  - Does the presentation identify at risk populations for each scenario?
  - Does the presentation provide an adequate solution for mitigation?
  - For future happenings, does it outline a prevention strategy?

STAGE 3 - LEARNING PLAN

Instructional Activities:
- Concept Mapping:
  - Explaining the forms of social engineering by mapping meanings to scenarios

MODULE 3
STAGE 1 - DESIRED RESULTS

Practice Standards (SEPs):
- Analyzing and interpreting data
- Constructing explanations and designing solutions
- Obtaining, evaluating, and communicating information

Content Standards:
- HS-ETS1-1: Defining and delimiting engineering problems
- HS-ETS1-3: Evaluating technical solutions using specific criteria and trade-offs

Essential Question(s)
- Overarching Question(s):
  - What is data, and what is information?
  - How does personal information lead to identification?
- Topical Question(s):
  - Foundations of Personally Identifiable Information and its importance
  - Responding to a phishing attack
  - Digital consent and ethics

Student Knowledge: Students will know...	*Student Skills: Students will be <u>able to</u>...*
● What part of their information is considered personally identifiable ● What to do if they/someone else experiences a phishing attack ● What digital consent entails	● Design plans to protect personal information ● Illustrate methods of appropriate conduct on social media ● Understand digital footprint and its impact ● Prepare and contact relevant bodies in case of a phishing attack

STAGE 2 - ASSESSMENT EVIDENCE

Summative Assessments:
- Task: What can I find out from an individual's social media?
- Model: Individual presentation on personal research.
  - Students should demonstrate understanding of what public information leads to the release of personally identifiable information.
- Rubric Checklist:
  - Does the presentation demonstrate well thought out research processes with appropriate citations/references?
  - Does the presentation identify sources of personally identifiable information and state reasoning for possible compromise?
  - Does the presentation deal with immediate attacks involving personally identifiable information?

Formative Assessments:
- Quiz:
  - Identifying which information is personally identifiable and poses security risks
- Essay:

- How to safeguard personal information

STAGE 3 - LEARNING PLAN

Instructional Activities:

- Demonstration: Exploring the public profile of a public figure

MODULE 4
STAGE 1 - DESIRED RESULTS

Practice Standards (SEPs):
- Asking questions and defining problems
- Developing and using models
- Engaging in argument from evidence

Content Standards:
- HS-ETS1-1: Defining and delimiting engineering problems
- HS-ETS1-2: Developing technical solutions to engineering and real-world problems
- HS-ETS1-3: Evaluating technical solutions using specific criteria and trade-offs

Essential Question(s)
- Overarching Questions(s):
  - What does security mean?
  - What is Cybersecurity?
- Topical Question(s):
  - Internet Usage
  - Online Rules of Engagements

Student Knowledge: Students will know...	*Student Skills: Students will be able to...*
● Why are security strategies, e.g. password are compounded ● What to say and what not to say when online ● The importance of multi-factor authentication	● Identify phishing emails/websites ● Create a secure password strategy ● Construct systems that protect multiple layers of information

STAGE 2 - ASSESSMENT EVIDENCE

Summative Assessments:
- Task: Quiz on security strategies
- Model: Multiple choice solutions on the identification of appropriate strategy and short form questions on the internet conduct

STAGE 3 - LEARNING PLAN

Instructional Activities
- Role-Playing: Requiring identification on the phone or the internet
- Group demonstration/lecture: Identifying minute details in known websites, e.g., ı vs I and various manipulations that are oblivious to the human eye

MODULE 5
STAGE 1 - DESIRED RESULTS

Practice Standards (SEPs):
- Asking questions and defining problems
- Obtaining, evaluating, and communicating information
- Analyzing and interpreting data

Content Standards:
- HS-ETS1-2: Developing technical solutions to engineering and real-world problems
- HS-ETS1-3: Evaluating technical solutions using specific criteria and trade-offs
- HS-ETS1-4: Using models and simulations to test engineering solutions

Essential Question(s)
- Overarching Question(s):
  - How do you report a crime, and who do you report to?
  - What are some common industries where phishing/social engineering attacks face?
- Topical Question(s):
  - Platform Awareness: Does your platform have alerts for phishing and other threats? Does your bank have a reporting mechanism?
  - Mechanisms of reporting and existing organizations e.g. FBI IC3
  - Compiling Documentation: Worst Case Scenarios

Student Knowledge: Students will know...	*Student Skills: Students will be <u>able to</u>...*
● What to do immediately after a possible social engineering attack ● What mechanisms are available for submitting cybercrime reports ● How to document incidents	● Explain incidents, document, and submit reports ● Demonstrate knowledge of threat resolution and contact relevant organizations ● Analyze the existing system's protection tools while using internet applications, and assess its effectiveness

STAGE 2 - ASSESSMENT EVIDENCE

Summative Assessments:
- Task: Final Project
- Model: Design an essay/project/presentation that describes the phenomenon of social engineering and a proposed solution and resolution in today's world
- Rubric Checklist:
  - Does the output demonstrate a comprehensive cycle of mitigating social engineering i.e. knowledge of attack form, target population and plausible solution?
  - Does the output include processes of documentation and awareness?
  - Does the output use external sources and research?
  - Is the solution supported by evidence?

STAGE 3 - LEARNING PLAN

Instructional Activities:

- Guest lectures from financial organizations i.e. Banks e.g. Bank of America, Chase Bank on reporting procedures of scams and possible models of communications with customers
- Scenario-based simulations of phishing and online attacks
- Scenario-based simulations of reporting an attack

5.4 Validation

As part of understanding the broader importance and impact of the CS4RI curriculum, I had semi-formal discussions with computer science teachers in Rhode Island to understand how computer science is taught in schools and to refine the proposed curriculum. While this discussion was largely unstructured to understand how the CS curriculum is taught, some of the questions when discussing core topics and student receptivity included: How do you introduce engineering concepts to your students? What years or grades do you find are receptive to what types of information, and why?

The responses indicated that in Rhode Island and many other schools across the United States, the teaching of the computer science curriculum is not confined to a specific class year. While schools and districts often implement these classes in different ways, a computer science elective class may include students across all four high school grades, 9 to 12. Hence, modifications and improvements to the curriculum must be comprehensive yet simple enough to be understood by all students in ways that offer a practical understanding of these techniques.

Compared to my earlier assumption that teachers develop specific materials based on the curriculum, I discovered that the CS4RI curriculum is integrated with online education platforms like Khan Academy and Code.org, which offer personalized education in Computer Science and programming concepts. This allowed me to consider a curriculum with terminology that is widely used and also easily translatable across different languages or learning tools. Teachers have mentioned that part of implementing the existing curriculum requires having students engage with these educational platforms. Therefore, the proposed curriculum must be flexible and adaptable to incorporate these learning components and external resources where necessary, to support the teaching process.

My proposed curriculum is designed to increase high school students' understanding in the U.S. of global and local threats that may affect their privacy and independence, especially through phishing schemes. While not solely focused on phishing tactics, it broadly focuses on bringing awareness to methods of social engineering, with phishing as a core component. It is presented as a course, designed and recommended for high school students, that not only informs their knowledge of social engineering but could serve as a bridge that connects their interests and encourages the pursuit of other computer science and HCI disciplines beyond high school.

6 LIMITATIONS

Earlier chapters provided explanations and analysis of state-based reports of phishing across vulnerable states. It reviewed the hypothesized factors individually and collectively, while using the ACS dataset for population-based information. However, this combined dataset has some limitations. Figure 18 below highlights which states have higher phishing victim counts.

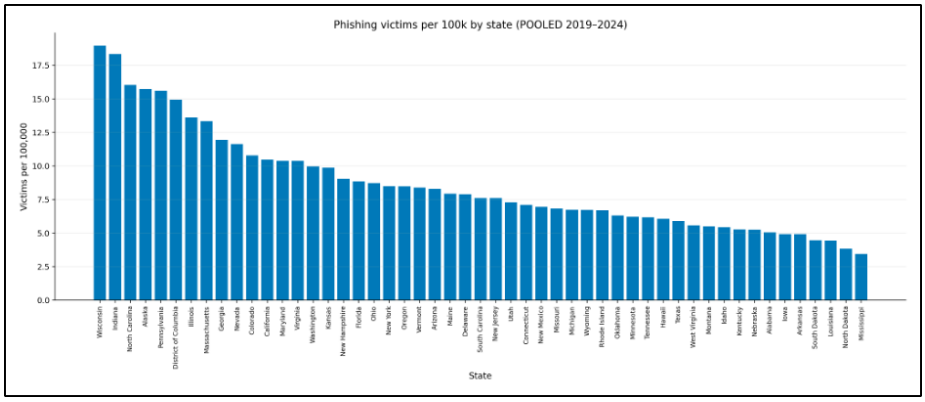


Figure 18: Phishing Victims Distribution by State

States like Wisconsin, Nevada, and Colorado, among others, show higher phishing victim rates compared to the 50 states, despite being some of the least vulnerable, a factor that may be influenced by their relatively small population and households compared to their high phishing victim rates. There is no single method of aggregating data uniformly, except that outliers will be present across the data. States with moderate populations that are more educated will often experience higher counts per 100k people due to population demographics compared to other states. In 2019, 1490 victims in Texas reported phishing, compared to Alaska with 152 victim reports, yet Alaska has a higher frequency in the figure above. Texas can also be compared to New York, which recorded 1487 victim reports of phishing despite New York being comparably less vulnerable and having a large population. Hence, the results from this research will often be skewed toward states with smaller populations compared to their larger counterparts, despite there being a higher raw frequency of reports in those other states.

My analysis primarily focuses on phishing victim counts by reports; however, the FBI IC3 reports also provide phishing loss estimates per state.

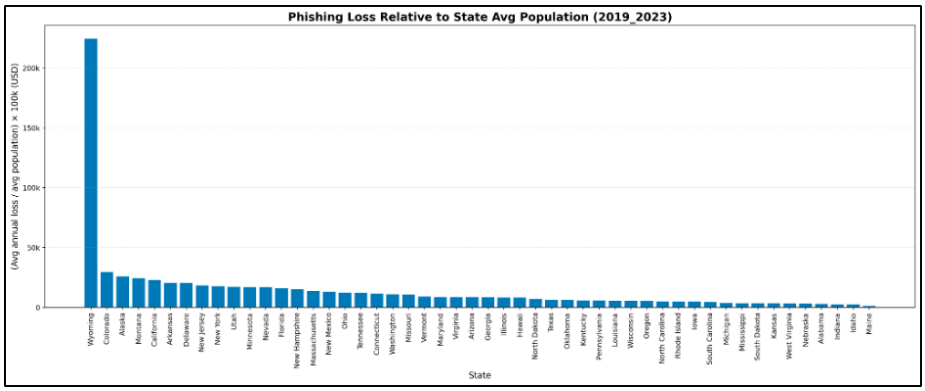


Figure 19: Phishing Loss in USD Distribution by State

While Wyoming records high loss values across years, in 2019, its estimated loss per victim on average is $6,140,368 compared to Texas's $2,274,285. These losses are significantly distant, heavily skewed relative to their populations, and are less representative of the relationship between these variables when compared to larger states with higher populations. From 2020 to 2024, Wyoming did not receive up to 100 victim reports on phishing, and 2019 was the only year such a high loss was recorded. Texas consistently received between 500 and 3900 reports of phishing by victims from 2019 until 2024, but the losses and counts are considered lower relative to its population. Montana recorded only 49 counts of phishing victims but $244,585 in losses per victim, while Idaho recorded 100 victims reported phishing, but $65,516 in losses per victim, yet the population demographics significantly make Montana's losses steeper due to its population size.

Apart from the population share limitations, I also considered age limitations. From 2019 until 2024, IC3 reports that individuals aged 60+ are the largest victims of internet crimes, constantly resulting in over 1 billion in losses. These numbers may reflect higher reporting rates of elderly victims or may be a result of intentional targeting by attackers. Conversely, the inverse is possible, as states with a higher elderly population may record fewer counts of victim reports compared to states with a younger population concentration due to more awareness of reporting tools.

The most significant limitation of this research is that the association between variables does not equal causality. I examine the relationship between income, broadband access, and education individually and phishing reports by state. The data is heavily dependent on who decides to report phishing crimes. My research serves to explore possibilities and plausible explanations. The coefficients of the correlation and linear regression can offer important insights for identifying patterns, but they do not imply that the factors — income, broadband access, and education levels alone cause the rates of phishing victim rates. It provides insights into how vulnerabilities may reflect differences in awareness and exposure. However, it does not assert that the reason why less vulnerable

states are recording high numbers of losses and victim counts is due to increased exposure and digital literacy.

Finally, the solution produced by this research builds upon existing programs across various U.S. states. It acknowledges that there may exist impracticabilities and potential challenges in implementation, from the teaching staff to other capabilities. Expert interviews revealed that the intent of the program does not always align with the impact, as certain roadblocks, including language barriers and the limitations in translation of several concepts, difficulties in modifying and customizing core concepts to suit various educational needs, and effectively communicating these concepts to students, all present significant impediments to the success and accessibility of this social engineering curriculum.

7 CONCLUSION

I set out to investigate whether systemic factors contribute to inequality, digital divide, and affect vulnerability across states. Understanding the relationship between these factors and phishing is important in understanding how they relate to the broader conversation on digital vulnerability, especially as the world continues to become increasingly digitized.

I hypothesized that income, broadband access, and education, factors shaped by geography or access, would be associated with vulnerability across states, and used quantitative and qualitative processes to answer these questions. While I aimed to investigate the frequency of phishing reports by state, depending on the factors defined above, I discovered that increased vulnerabilities were not associated with higher phishing reports; rather, the opposite pattern was observed. I examine the results through the lens of underexposure and lack of awareness of reporting mechanisms in states with lower levels of socio-economic capabilities. This led to my research's proposed solution of education and digital literacy, in support of existing literature, as a way to increase awareness of phishing and relevant solutions.

Additionally, I consider phishing as a form of internet crime that requires the existence of broadband access; hence, broadband access should be interpreted cautiously as a factor in how phishing victim counts are recorded, as there is no way to conduct phishing without this access. Therefore, I conclude that education showed the strongest observed association with victim reports, and individuals with a high school degree or higher showed an observed association with higher phishing victim counts across the U.S.

While the solution presented infers that high school phishing training incorporation is a useful tool in rethinking digital literacy strategies to increase awareness about the risks of phishing, more research is needed to understand why individuals are less likely to report phishing attacks compared to others, especially in states where the victim losses are smaller on average. To exemplify, there is a need to research whether someone is likely to report $5 losses over time in Utah through phishing scams compared to a $20 loss in Colorado. Social engineering requires understanding individual patterns and manipulating information for specific purposes; hence, more studies through focus groups, observations, and interviews may be useful in improving the digital literacy program for high school students and also adopting protection mechanisms for vulnerable populations.

Less vulnerable states not only recorded high counts of phishing reports but also high losses, suggesting greater exposure or reporting of phishing attacks, as well as greater economic capability. These states are associated with more victim reports, a realization that is possibly linked to these states being highly digitally aware, having more technologically advanced tools for interaction, and, therefore, more pathways for phishing attacks to take place. It is highly likely that, alongside increased avenues for internet-based crimes, they are also better equipped to repel and identify these attacks compared to their less-digitally

aware counterparts, an implication that future research may consider. Hence, education on safeguarding PII (personally identifiable information), as shown in the solution, can be applied to a range of individuals beyond high school students. This is particularly useful in states with elderly populations, who are also the most frequent victims of this form of social engineering.

Finally, I reiterate very strongly that the quantitative tools used, i.e., correlation and regression, are not to be mistaken for causality, and the focus of this research was dependent on identifying and interpreting the patterns shown across the combined datasets to derive understanding and proffer solutions, a lot of which are useful for phishing-related social engineering future research.

Beyond corporations and organizations, this research is particularly relevant to people who interact with technology daily, which encompasses nearly all individuals in the United States. Not all individuals operate in environments with strong cybersecurity infrastructure, and systems are constantly being modified to address security risks; therefore, understanding the factors that increase susceptibility and vulnerability is essential for developing safer digital practices and behaviors. The social engineering curriculum solution, as well as the examination of existing computer science curricula across high schools in the U.S., offers a starting point for strengthening existing learning systems and assessing the existing curricula within a broader societal context in an increasingly digital society.

Works Cited

Abraham, Sherly, and InduShobha Chengalur-Smith. "An Overview of Social Engineering Malware: Trends, Tactics, and Implications." *Technology in Society* 32, no. 3 (2010): 183–196. https://doi.org/10.1016/j.techsoc.2010.07.001.

Abutair, Hassan Y. A., and Abdelfettah Belghith. "Using Case-Based Reasoning for Phishing Detection." *Procedia Computer Science* 109 (2017): 281–288. https://doi.org/10.1016/j.procs.2017.05.352.

Achieve, Inc. "EQuIP Rubric for Science: Detailed Guidance," March 2021. https://www.nextgenscience.org/sites/default/files/EQuIPDetailedGuidanceMarch2021.pdf.

Alshamrani, Adel. "A Comparison of Cybersecurity Education in Saudi Arabia and the United States." *Future Internet* 11, no. 4 (2019). https://www.mdpi.com/1999-5903/11/4/89.

Amiel, David J., and Cynthia L. Blitz. "The Middle-to-High School Transition: Key Factors Shaping 9th-Grade Computer Science Enrollment." *International Journal of Computer Science Education in Schools* 7, no. 2 (2025). https://doi.org/10.21585/ijcses.v7i2.234.

Bach, Eva. *The Impact of Digital Literacy on the Cyber Security of Digital Citizens*. University North, Croatia.

Bada, Maria, Angela M. Sasse, and Jason R. C. Nurse. "Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?" *Computers & Security*. https://www.sciencedirect.com/science/article/pii/S2214212614001343.

California Department of Financial Protection and Innovation. "The New Era of Tech-Enabled Scams." Accessed April 1, 2026. https://dfpi.ca.gov/news/insights/the-new-era-of-tech-enabled-scams/.

Computer Science for Rhode Island. "Home." Accessed April 1, 2026. https://www.cs4ri.org/.

Computer Science for Rhode Island. "Programs." Accessed April 1, 2026. https://www.cs4ri.org/programs.

Davis, Vicki. "Why More States Are Requiring Computer Science Classes." Tech & Learning. Accessed April 1, 2026. https://www.techlearning.com/news/why-more-states-are-requiring-computer-science-classes.

DiMaggio, Paul, Eszter Hargittai, Coral Celeste, and Steven Shafer. "From Unequal Access to Differentiated Use: A Literature Review and Agenda for Research on Digital Inequality." In *Social Inequality*, edited by Kathryn M. Neckerman, 355–400. New York: Russell Sage Foundation, 2004.

Everuss, Louis. *Digital Mobilities and Smart Borders: How Digital Technologies Transform Migration and Sovereign Borders*. Berlin: De Gruyter, 2024.

Federal Bureau of Investigation. Internet Crime Complaint Center (IC3). *2022 Internet Crime Report*. Washington, DC: Federal Bureau of Investigation, 2023. https://www.ic3.gov/AnnualReport/Reports/2022_IC3Report.pdf.

Federal Bureau of Investigation. Internet Crime Complaint Center (IC3). *2024 Internet Crime Report*. Washington, DC: Federal Bureau of Investigation, 2025. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

Federal Bureau of Investigation. Internet Crime Complaint Center (IC3). "Internet Crime Complaint Center." Accessed April 1, 2026. https://www.ic3.gov/.

Federal Trade Commission. "How to Recognize and Avoid Phishing Scams." Accessed April 1, 2026. https://consumer.ftc.gov/articles/how-recognize-avoid-phishing-scams.

Ghosh, Anirban, S. Diyasi, and Debashis Dey. "Cybersecurity Literacy Programs for Marginalized Communities: Bridging the Gap in Digital Security," 2025. https://www.researchgate.net/publication/389441252.

Hadnagy, Christopher. *Social Engineering: The Art of Human Hacking*. Indianapolis: Wiley Publishing, 2011.

HighSpeedInternet.com. "The Safest and Most Dangerous States for Cybercrime in 2024." Accessed April 1, 2026. https://www.highspeedinternet.com/resources/the-safest-and-most-dangerous-states-for-cybercrime-in-2024.

Holt, Jack, and James Nicholson. "Scaffolding Online Safety in Older Communities: Exploring the Relationship Between Digital Literacy and Cybersecurity." Forthcoming, *ACM Transactions on Computer-Human Interaction*, February 2026. https://doi.org/10.1145/3796705.

Imran, Ahmed. "Why Addressing Digital Inequality Should Be a Priority." *Electronic Journal of Information Systems in Developing Countries* 89, no. 3 (2023): e12255. https://doi.org/10.1002/isd2.12255.

Johnson, Nicola. *Technological Disadvantage of the Digital Age*, 2004. https://ro.uow.edu.au/edupapers/16.

Kennedy, Thomas. "The Digital Divide: Inequality in the Digital Age." Old Dominion University. Accessed April 6, 2026. https://www.cs.odu.edu/~tkennedy/cs300/development/Public/M03-SocietalDigitalDivideII/index.html.

Khonji, Mahmoud, Youssef Iraqi, and Andrew Jones. "Phishing Detection: A Literature Survey." *IEEE Communications Surveys & Tutorials* 15, no. 4 (2013): 2091–2121. https://ieeexplore.ieee.org/abstract/document/6497928.

Mouton, François, Louise Leenen, and H. S. Venter. "Social Engineering Attack Examples, Templates and Scenarios." *Computers & Security* 59 (2016): 186–209. https://doi.org/10.1016/j.cose.2016.03.004.

National Center for Education Statistics. "IPEDS Trend Generator." Accessed April 1, 2026. https://nces.ed.gov/ipeds/trendgenerator/app/build-table/7/19.

National Center for Education Statistics. "Public High School Graduation Rates." Condition of Education. Accessed April 1, 2026. https://nces.ed.gov/programs/coe/indicator/coi/high-school-graduation-rates.

National Center for Education Statistics. "State Reform Efforts, Table 3.3." Accessed April 1, 2026. https://nces.ed.gov/programs/statereform/tab3_3-2020.asp.

National Science Teaching Association. "Next Generation Science Standards (NGSS)." Accessed April 1, 2026. https://www.nsta.org/science-standards.

Nevada Department of Education. "Nevada Academic Content Standards." https://webapp-strapi-paas-prod-nde-001.azurewebsites.net/uploads/Nevada_Academic_Content_Standards_forrev_adf847c3ac.pdf.

Ng, Chien D., et al. "Validating the Social Vulnerability Index for Alternative Geographic Units in the United States." —, 2025. Accessed April 1, 2026. https://pmc.ncbi.nlm.nih.gov/articles/PMC11915720/.

Pajuste, Tiina. "The Digital Divide: Reinforcing Vulnerabilities." In *Human Rights in the Digital Domain: Core Questions*, edited by Tiina Pajuste, 361–380. Cambridge: Cambridge University Press, 2025.

Peltier, Thomas R. "Social Engineering: Concepts and Solutions." *Information Systems Security* 15, no. 5 (2006): 13–21.

Pew Research Center. "Digital Divide Persists Even as Americans with Lower Incomes Make Gains in Tech Adoption," June 22, 2021. https://www.pewresearch.org/short-reads/2021/06/22/digital-divide-persists-even-as-americans-with-lower-incomes-make-gains-in-tech-adoption/.

Phan, Bao Trung, Phuong Huyen Do, and Da Quynh Le. "The Impact of Digital Literacy on Personal Information Security: Evidence from Vietnam." In *Proceedings of Atlantis Press*. 2025. https://doi.org/10.2991/978-94-6463-694-9_32.

Proofpoint, Inc. "What Is Social Engineering?" Accessed April 1, 2026. https://www.proofpoint.com/us/threat-reference/social-engineering.

Rafter, Michelle. "Rhode Island's CompSci Education Project: How Is It Going?" Government Technology. Accessed April 1, 2026. https://www.govtech.com/education/k-12/rhode-islands-compsci-education-project-how-is-it-going.html.

Reinheimer, Benjamin, et al. "An Investigation of Phishing Awareness and Education Over Time." In *Proceedings of the Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, 259–284. USENIX Association, 2020.

Rhode Island Department of Education. "Career and Technical Education." Accessed April 1, 2026. https://ride.ri.gov/students-families/career-technical-education.

Rhode Island Department of Education. "CTE Programs Map." Accessed April 1, 2026. https://tableau.ride.ri.gov/t/Public/views/CTE_Programs_Map/CTEMAP.

Salahdine, Fatima, and Naima Kaabouch. "Social Engineering Attacks: A Survey." *Future Internet* 11, no. 4 (2019): 89. https://doi.org/10.3390/fi11040089.

South Carolina Department of Education. "South Carolina Computer Science Standards for High School." Accessed April 1, 2026, n.d. https://www.ed.sc.gov/instruction/standards/computer-science/standards/draft-for-review-south-carolina-computer-science-standards-for-high-school/.

Syracuse University School of Information Studies. "What Is the Digital Divide? Meaning, Causes & Impact." Accessed April 1, 2026. https://ischool.syracuse.edu/what-is-the-digital-divide/.

U.S. Census Bureau. "American Community Survey (ACS)." Accessed April 1, 2026. https://www.census.gov/programs-surveys/acs.html.

U.S. Census Bureau. "Census Bureau Releases New Educational Attainment Data," February 24, 2022. https://www.census.gov/newsroom/press-releases/2022/educational-attainment.html.

U.S. Census Bureau. "Subject Tables: S1901—Income in the Past 12 Months." American Community Survey 1-Year Estimates, 2018. http://api.census.gov/data/2018/acs/acs1/subject/groups/S1901.html.

Uhomoibhi, Juliet, et al. "The Need for Education on Phishing." *Campus-Wide Information Systems* 28, no. 5 (2011): 308–319. https://doi.org/10.1108/10650741111181580.

Wang, Z., L. Sun, and H. Zhu. "Defining Social Engineering in Cybersecurity." *IEEE Access* 8 (2020): 85094–85115. https://doi.org/10.1109/ACCESS.2020.2992807.

World Population Review. "Income Inequality by State." Accessed April 1, 2026. https://worldpopulationreview.com/state-rankings/income-inequality-by-state.

Zheng, Yinjiao, and Geoff Walsham. "Inequality of What? An Intersectional Approach to Digital Inequality under Covid-19." *Information and Organization* 31 (2021): 1–6. https://doi.org/10.1016/j.infoandorg.2021.100341.

Zorica, M. B., G. Golubić, and T. Š. Katarinček. "Cybersecurity in Education: The Challenge of Social Engineering and Information Literacy." In *2025 MIPRO 48th ICT and Electronics Convention*, 662–667. Opatija, Croatia, 2025. https://doi.org/10.1109/MIPRO65660.2025.11132065.