Journal of Business Administration Online

ARKANSAS TECH UNIVERSITY
College of Business
HTTPS://JBAO.ATU.EDU

Spring 2026, Vol. 20 No. 1

Assessing Cybersecurity Awareness: Examining Demographics, Knowledge, and Actionable Practices

Wyatt Held, University of Central Arkansas

Joseph Y. Thomas, University of Central Arkansas

ABSTRACT

This study examines cybersecurity awareness by separating what people know from what they actually do with that knowledge. The survey was administered through Luth Research Institute to a diverse United States sample. The broader project produced 814 responses, while the cleaned working file used for this manuscript contained 741 respondents, with item-level valid counts ranging from 739 to 741. The instrument included demographic questions and awareness items on phishing, passwords, multifactor authentication, public Wi-Fi, ransomware, identity theft, backup habits, social media exposure, and related security topics. The analysis is primarily descriptive and exploratory, with the demographic profile used to clarify how findings may inform audience-specific training. Results show a mixed pattern. Respondents showed relatively strong awareness of broad threats that receive regular public attention, including ransomware, public Wi-Fi risk, and the ease of discovering personal information through social media. At the same time, many participants struggled with procedural and behavior-based items that matter in everyday security decisions. Only 30.8% correctly rejected the claim that turning off smartphone GPS prevents location tracking, 47.5% knew email is not encrypted by default, and 48.3% recognized that private browsing does not prevent ISP monitoring. Reported protective behavior was also uneven: 71.9% reused passwords at least sometimes, only 42.6% reported using two-step verification always or often, and 31.0% had not backed up data in more than six months. Identity-theft response knowledge was also fragmented, as fewer than half of respondents said they knew where to place a fraud alert. These results point to clear training priorities: unique password habits, routine multifactor authentication, backup routines, limits of private browsing and default email settings, safe public Wi-Fi use, and concrete first steps after suspected identity theft.

INTRODUCTION

Cybersecurity is easy to treat as a technical problem until someone clicks the wrong link, reuses the wrong password, or finds out too late that a phone or laptop was sharing more information than expected. Phones, computers, and online accounts hold financial records, personal messages, location data, and other forms of personally identifiable information. Because of that, cybersecurity is not only an issue for specialists. It is part of everyday life.

Cybersecurity includes the policies, technologies, and human practices used to protect information assets in cyberspace (Schatz et al., 2017). The human side matters because many attacks succeed by getting users to make one bad decision at the wrong time. Phishing attacks commonly rely on pressure, urgency, and misleading cues to push people toward unsafe action (Loggen & Leukfeldt, 2022; Wright et al., 2023). Malware and ransomware create similar risk. Users do not need deep technical knowledge to avoid every attack, but they do need enough awareness to recognize warning signs and respond in practical ways (Greengard, 2022).

That practical side of awareness is what makes this topic important. A person may have heard of cybersecurity and still not know whether public Wi-Fi is safe, what multifactor authentication does, or who to contact after identity theft. In the same way, someone may know a few safe habits without understanding the technical terms behind them. This gap between recognition and action is where training programs often succeed or fail.

The present study examines cybersecurity awareness in a United States survey sample by looking at both knowledge and actionable practice. Rather than treating awareness as one broad idea, the study separates general familiarity with cyber risk from the specific behaviors and judgments that people can use right away. This approach keeps the project close to its main purpose: identify practical gaps in awareness and point toward training topics that can improve everyday security behavior.

BACKGROUND AND PRIOR RESEARCH

Prior research consistently shows that basic awareness does not always turn into safe behavior. Ahamed et al. (2024) found that cybersecurity knowledge, password security, and attitudes were important to student awareness outcomes. Concepcion and Palaoag (2024) similarly reported that employees may have general awareness while still showing weak device-security practices. In a student-focused scale-development study, Bognar and Bottyan (2024) found that awareness varied across demographic groups and argued for targeted education rather than one-size-fits-all training.

Other studies place even more emphasis on cyber hygiene and repeatable habits. Argyridou et al. (2023) argued that awareness programs are strongest when they are tied to human-centered risk reduction strategies rather than only technical information. Research on social media behavior also shows that people often understand digital risk in general terms while still disclosing information that makes them easier to target (Naurin et al., 2023). Taken together, these studies suggest that awareness should be measured not only by what respondents have heard of, but also by what they can do with that knowledge in routine situations.

This study contributes to that literature in three ways. First, it uses a broader United States sample rather than a single classroom, campus, or workplace. Second, it keeps a clear distinction between knowledge and action-oriented items. Third, it translates the descriptive results into training priorities that are concrete enough for educators, managers, and awareness programs to use. The project addresses the

following exploratory questions: What topics show relatively strong or weak awareness in the sample? Where do the results suggest a gap between risk awareness and protective behavior? What training priorities emerge from those patterns?

METHOD

Data Source and Sample

The survey used in this study was designed by the second author and administered through Luth Research Institute. Project materials indicate that the data collection drew on online panels and telephone interviews to reach respondents from multiple demographic groups across the United States. The broader project produced 814 responses. For the present manuscript, the cleaned working file contained 741 respondents, and valid item counts ranged from 739 to 741 depending on the question.

The sample was diverse, but it was not state-balanced or weighted to mirror the United States population. As a result, the findings are best read as a descriptive baseline rather than as a national estimate.

Instrument

The instrument contained 53 items. Eight items captured demographics, including gender, age, generation, marital status, state of residence, education, income, and ethnicity. The remaining 45 items focused on cybersecurity awareness.

For analysis and presentation, those 45 awareness items were grouped into two broad categories. The first category included action-oriented items that asked about behaviors or practical security judgments respondents could use right away, such as password reuse, multifactor authentication, backup habits, public Wi-Fi practices, and email or browser settings. The second category included broader knowledge and perception items, such as ransomware, social engineering, identity-theft trends, blockchain security, and related awareness questions. Appendix A summarizes the survey structure.

Analytic Approach

This manuscript uses a descriptive, exploratory approach. The primary purpose of the analysis is to identify where awareness appears strongest, where practical behavior appears weakest, and what training areas are most likely to produce useful improvement. In response to the demographic composition of the sample, the Results section reports the distribution of respondents across major strata and interprets those strata as training-planning context rather than as nationally weighted estimates. Because several demographic groups were uneven in size, especially the oldest age categories and smaller ethnic categories, subgroup patterns are treated cautiously.

The present article does not claim causal relationships. Where inferential or subgroup-oriented findings are discussed, they are framed as exploratory and are intended to guide future research rather than to establish definitive population-level differences.

RESULTS

Sample Profile

The sample was close to evenly split by gender, with 51.4% male and 48.6% female respondents. The largest age group was 35-54 years old (32.8%), followed by 26-34 (20.0%), 65-74 (16.2%), and 55-64 (15.1%). Education levels were relatively high: 81.9% of respondents reported at least some college, and 52.9% held either a bachelor's degree or graduate-level education. The largest single income category was $50,000 to $74,999 (20.0%). Most respondents identified as White or Caucasian (68.8%), followed by Hispanic or Latino (13.5%) and Black or African American (10.3%).

Table 1. Demographic Profile of the Working Sample

Variable	Category	n (%)
Gender	Male	381 (51.4%)
Gender	Female	360 (48.6%)
Age	18-25	81 (10.9%)
Age	26-34	148 (20.0%)
Age	35-54	243 (32.8%)
Age	55-64	112 (15.1%)
Age	65-74	120 (16.2%)
Age	75-84	34 (4.6%)
Age	85 or older	3 (0.4%)
Education	High school or less	134 (18.1%)
Education	Some college/associate/vocational	215 (29.0%)
Education	Bachelor's degree	255 (34.4%)
Education	Graduate work or degree	137 (18.5%)
Ethnicity	White or Caucasian	510 (68.8%)
Ethnicity	Black or African American	76 (10.3%)
Ethnicity	Hispanic or Latino	100 (13.5%)
Ethnicity	Asian or Asian American	39 (5.3%)
Ethnicity	Other / multiracial categories	16 (2.2%)

Note. Percentages are based on the valid response count for each demographic item (n = 741).

Demographic Context for Interpreting the Findings

The demographic profile provides useful context for interpreting the awareness results. The sample included meaningful representation across age, education, income, and ethnicity; however, the strata were not equally sized. For example, the 35-54 age group was the largest age category, while the oldest age categories were comparatively small. Similarly, White or Caucasian respondents made up the largest ethnic group, with smaller numbers in several other categories. These distributions make the sample useful for identifying broad training needs, but they also argue against overinterpreting small subgroup differences without additional stratified testing or a weighted design.

For training purposes, the demographic results suggest that cybersecurity education should not assume a single audience. Older adults may need especially clear guidance on identity-theft response steps, account recovery, fraud alerts, and authentication workflows, while younger and middle-aged adults may benefit from training that connects frequent online activity to routine practices such as unique passwords, two-step verification, browser privacy limits, and secure use of public Wi-Fi. Because the present study emphasizes a descriptive baseline, these recommendations are framed as practical training implications rather than as statistically confirmed subgroup differences.

Awareness of Common Threats

Several items suggest that respondents recognized widely discussed cyber risks. A large majority identified the basic definition of ransomware (86.8%). Most respondents also believed their personal information is at risk when using public Wi-Fi (83.4%) and agreed that personal or sensitive information can be discovered fairly easily through social media (87.3%). Most also rejected the idea that stealing information online is less serious than stealing other kinds of property (81.6% selected 'No'). These items suggest that many respondents understood cybersecurity as a real and personal risk rather than a distant technical issue.

Gaps in Actionable Practice

The more practical items told a different story. Only 30.8% correctly rejected the statement that turning off smartphone GPS prevents location tracking, while 27.8% said they were not sure. Fewer than half of respondents recognized that email is not encrypted by default (47.5%) or that private browsing does not prevent internet service providers from monitoring online activity (48.3%). Just over half knew that traffic on public wireless routers is not encrypted by default (53.4%), and 30.1% were unsure.

Behavioral items showed the same pattern. Only 37.0% reported using a cell phone as a multifactor authentication tool, and 25.6% said they did not know what multifactor authentication was. For two-step verification, 13.5% reported always using it and 29.1% reported often using it, but 42.0% used it only sometimes and 10.0% did not know what it was. Password behavior stood out as a clear weakness: 71.9% reported using the same password on different systems at least sometimes, and only 28.1% said they never reuse passwords. Backup behavior was also uneven. While 51.1% had backed up their data within the last month, 31.0% had not done so in more than six months.

Exploratory Sex-Based Score Differences

A supplemental score-based analysis was conducted on cases with complete total, knowledge, and behavior scoring data (n = 735) to examine whether overall awareness scores differed by sex. These tests are included as exploratory context because the primary study remains descriptive. One-way ANOVAs indicated statistically significant differences for total correct scores, knowledge correct scores, and behavior correct scores. Because the sample is relatively large, practical interpretation should

emphasize effect sizes rather than p values alone. The sex difference was small for knowledge scores and medium for total and behavior scores, suggesting that the largest difference was concentrated in the behavior-oriented portion of the measure.

Table 2. Selected Awareness Findings on Common Threats and Protective Practices

Domain	Survey item	Most relevant response	%
Threat recognition	Identified the definition of ransomware	Correct response	86.8%
Threat recognition	Believes personal information is at risk on public Wi-Fi	Yes	83.4%
Threat recognition	Believes personal information is easy to discover through social media	Yes	87.3%
Practical knowledge	Turning off smartphone GPS prevents location tracking	Correct rejection	30.8%
Practical knowledge	Email is encrypted by default	Correct rejection	47.5%
Practical knowledge	Private browsing prevents ISP monitoring	Correct rejection	48.3%
Protective behavior	Has used a cell phone as an MFA tool	Yes	37.0%
Protective behavior	Uses two-step verification	Always or often	42.6%
Protective behavior	Uses the same password on different systems	At least sometimes	71.9%
Protective behavior	Backed up data within the last month	Yes	51.1%

Note. Password reuse was based on 740 valid responses; all other rows were based on 741 valid responses.

Table 3. Exploratory Sex Differences in Cybersecurity Awareness Scores

Outcome	Male M	Female M	Mean Difference	F(1, 733)	p	Cohen's d
Total Correct	12.85	11.59	1.26	39.51	< .001	0.46
Knowledge Correct	9.66	9.17	0.49	9.82	.002	0.23
Behavior Correct	3.19	2.43	0.76	51.71	< .001	0.53

Note. Positive mean differences indicate higher male scores. Cohen's d was calculated using the pooled standard deviation. These analyses are exploratory and based on the complete scored subset rather than the full item-level descriptive sample.

Identity Theft Knowledge and Response

Identity-theft items showed a similar mix of awareness and uncertainty. More than one quarter of respondents (26.9%) reported having been a victim of identity theft. Yet only 44.7% said they knew who to place a fraud alert with. When asked who they would contact for help if they became a victim, responses were scattered across police,

credit bureaus, credit grantors, attorneys, state consumer agencies, the Federal Trade Commission, and even no one at all. Even if some of these choices may be part of a broader response process, the spread suggests that many respondents do not have a clear first step in mind.

Advanced or more technical topics were less familiar. Only 22.1% had heard of blockchain security, 7.6% reported knowing how to use blockchain encryption, and 15.4% said they were aware of the Year 2038 problem. These results do not mean that advanced topics are unimportant. They do suggest, however, that cybersecurity training for general audiences may have more immediate value when it focuses first on practical cyber hygiene.

Table 4. Identity-Theft Knowledge and Response Patterns

Item	Response	%
Reported prior identity-theft victimization	Yes	26.9%
Knows who to place a fraud alert with	Yes	44.7%
Primary help contact after identity theft	Police	36.0%
Primary help contact after identity theft	Credit bureau	27.1%
Primary help contact after identity theft	Credit grantor	12.4%
Primary help contact after identity theft	Lawyer	3.6%
Primary help contact after identity theft	State AG / consumer agency	8.0%
Primary help contact after identity theft	DMV	0.7%
Primary help contact after identity theft	Federal Trade Commission	4.7%
Primary help contact after identity theft	Do not contact anyone	7.4%

Note. All percentages in Table 4 are based on 741 valid responses.

DISCUSSION

This study set out to examine cybersecurity awareness in a way that keeps one basic question in view: what do people know, and what can they actually do with that knowledge? The answer from this sample is mixed. General threat awareness is present, especially for prominent issues such as ransomware, public Wi-Fi risk, and the exposure created by social media. But that awareness does not consistently translate into protective action. Password reuse remains common, multifactor authentication is not yet routine, backup practices are inconsistent, and many respondents are uncertain about practical response steps after identity theft.

That gap between knowing and doing matters for cybersecurity education. Training programs often miss the mark when they spend too much time on broad warnings and not enough time on concrete decisions. The present findings suggest that awareness campaigns should focus on a short list of repeatable behaviors: use unique passwords, enable multifactor authentication consistently, understand the limits of private browsing, recognize how public Wi-Fi and default email settings work, keep recent backups, and know where to turn after suspected identity theft. These are not

highly technical skills, but they can make a real difference in day-to-day security behavior.

The results are broadly consistent with prior awareness research. Ahamed et al. (2024), Bognar and Bottyan (2024), and Concepcion and Palaoag (2024) each found that broad awareness and safe practice do not always move together. The present study extends that point by showing it in a broader United States sample and by making the difference between general knowledge and actionable practice central to the analysis.

Training Priorities

The results point to a focused set of training priorities. First, training should emphasize password hygiene, particularly the use of unique passwords and password managers, because password reuse was common. Second, multifactor authentication should be presented as a routine default rather than an optional advanced feature, since fewer than half of respondents reported using two-step verification always or often. Third, training should address common misconceptions about privacy tools and device settings, including the limits of private browsing, default email encryption, smartphone location tracking, and public Wi-Fi protections. Fourth, programs should include a short identity-theft response protocol that identifies immediate steps, such as contacting credit bureaus, placing fraud alerts, and documenting suspected fraud.

These priorities are intentionally practical. The findings do not suggest that general audiences need advanced technical instruction before they can improve their security behavior. Instead, the data suggest that the highest-value training is likely to be short, repeated, behavior-focused, and organized around decisions respondents face in everyday life.

LIMITATIONS AND FUTURE RESEARCH

This study has several limitations. First, the article remains primarily descriptive. Although this study includes exploratory score-based sex comparisons, the available analysis does not provide a full set of statistically tested response patterns across all demographic strata. This decision is intentional. Some strata were small, the sample was not nationally weighted, and comparisons such as item-level two-step verification differences by older age groups, would require a fuller stratified study than is appropriate for this data set. Second, the survey was designed in 2019, and some identity-theft items were tied to 2017 and 2018 conditions. That makes the study most useful as a pre-COVID baseline rather than as a complete picture of today's threat landscape. Third, the sample was diverse but not nationally weighted, so the results should be interpreted as indicative rather than fully representative of the United States population.

These limits point directly to future work. A follow-up study should test whether age, education, income, and prior victimization predict stronger cyber hygiene. It should also revisit time-sensitive items and compare the pre-COVID baseline with a post-

COVID survey environment, where remote work, mobile authentication, and public discussion of cyber risk have become more common.

CONCLUSION

Cybersecurity awareness is not only about recognizing the word ransomware or knowing that the internet can be risky. It is also about knowing what to do next. In this study, respondents showed meaningful awareness of general cyber threats, but everyday protective behavior was much less consistent. That gap is where educators, managers, and awareness programs can do the most good.

The clearest opportunities are not the most technical ones. They are the habits people can start using right away: unique passwords, routine multifactor authentication, recent backups, careful handling of public Wi-Fi, understanding the limits of browser and device privacy settings, and a clear response plan for identity theft. If training stays focused on those practical steps and is adapted to the needs of different audience groups, it has a better chance of changing behavior instead of only increasing recognition.

REFERENCES

Ahamed, B., Polas, M. R. H., Kabir, A. I., Sohel-Uz-Zaman, A. S. M., Al Fahad, A., Chowdhury, S., & Dey, M. R. (2024). Empowering students for cybersecurity awareness management in the emerging digital era: The role of cybersecurity attitude in the 4.0 industrial revolution era. SAGE Open, 14(1), 21582440241228920. https://doi.org/10.1177/21582440241228920

Argyridou, E., Nifakos, S., Laoudias, C., Panda, S., Panaousis, E., Chandramouli, K., Navarro-Llobet, D., Mora Zamorano, J., Papachristou, P., & Bonacina, S. (2023). Cyber hygiene methodology for raising cybersecurity and data privacy awareness in health care organizations: Concept study. Journal of Medical Internet Research, 25, e41294.

Bognar, L., & Bottyan, L. (2024). Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. Education Sciences, 14(6), 588. https://doi.org/10.3390/educsci14060588

Concepcion, J. D., & Palaoag, T. D. (2024). An assessment of cybersecurity awareness among academic employees at Quirino State University: Promoting cyber hygiene. Journal of Electrical Systems, 20(7), 769-775.

Greengard, S. (2022). Hidden malware ratchets up cybersecurity risks. Communications of the ACM, 65(10), 16-18. https://doi.org/10.1145/3554925

Loggen, J., & Leukfeldt, R. (2022). Unraveling the crime scripts of phishing networks: An analysis of 45 court cases in the Netherlands. Trends in Organized Crime, 25(2), 205-225. https://doi.org/10.1007/s12117-022-09448-z

Naurin, F. K., Ikram, N., Murtaza, H., & Muhammad, A. A. (2023). Social media users and cybersecurity awareness: Predicting self-disclosure using a hybrid artificial

intelligence approach. Kybernetes, 52(1), 401-421. https://doi.org/10.1108/K-05-2021-0377

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. Journal of Digital Forensics, Security and Law, 12(2), Article 8. https://doi.org/10.15394/jdfsl.2017.1476

Wright, R., Johnson, S., & Kitchens, B. (2023). Phishing susceptibility in context: A multilevel information processing perspective on deception detection. MIS Quarterly, 47(2), 803-832. https://doi.org/10.25300/MISQ/2022/16625

APPENDIX A

Survey Structure Summary

Appendix A summarizes the structure of the survey instrument used in this study. The appendix is included to clarify how the manuscript distinguishes between demographic items, action-oriented practice items, and broader knowledge or perception items.

Survey domain	Number of items	Examples
Demographics	8	Gender, age, generation, marital status, state, education, income, ethnicity
Action-oriented practice items	20	Phishing cues, multifactor authentication, password reuse, backups, public Wi-Fi, email settings
Knowledge and perception items	25	Ransomware, blockchain security, identity-theft patterns, social engineering, public-risk perception