https://aurj.aror.edu.pk/index.php/AURJ/article/view/43

Cyber K2D: An Uncertainty-Aware Index for Measuring the Knowledge-to-Doing Gap in Cyber Hygiene

Iqra Qamar Solangi [a,*], Dr. Samina Rajper [a], Hira Junejo [a], Sadaf Bibi [b]

[a] *Institute of Computer Science, Shah Abdul Latif University, Khairpur Mirs, Sindh, Pakistan*
[b] *Department of Artificial Intelligence, Aror University of Art, Architecture, Design and Heritage, Sukkur, Sindh, Pakistan*
[*] *Corresponding Author: Iqra Qamar Solangi, Email: iqrasolangi550@gmail.com*

Received: 25-02-2026, **Revision:** 05-06-2026, **Accepted:** 23-10-2026

KEYWORDS

Cyber K2D, Cybersecurity Awareness, Cyber Hygiene, Human Factors, Self-Efficacy, Phishing

ABSTRACT

Cybersecurity awareness studies often show that students know basic safety rules but do not always apply them in daily digital routines. Existing work has measured awareness, intentions, or training outcomes, yet many studies provide limited item-level uncertainty reporting and do not directly quantify the distance between factual knowledge and recent protective behavior. This paper presents Cyber K2D, a lightweight Knowledge-to-Doing gap measure for cyber hygiene. An anonymous cross-sectional survey was completed by 302 university respondents; after consent-based screening, 272 responses were included. The instrument contained seven knowledge items, five self-efficacy items, and six recent-behavior items. Knowledge was normalized as a knowledge rate, behavior was normalized as a safe-practice rate, and the Cyber K2D Gap was defined as knowledge rate minus behavior rate. Item-level percentages were reported with Wilson 95% confidence intervals, and uncertainty responses were treated as a visible risk signal. The results show moderate knowledge (mean Knowledge Score = 4.01/7) and moderate behavior adoption (mean Behavior Rate = 0.51). The mean Cyber K2D Gap was 0.07, indicating that knowledge slightly exceeded reported safe behavior. Knowledge was positively associated with safe behavior (Spearman rho = 0.40, p = 1.91e-11), while self-efficacy showed a smaller positive association (rho = 0.24, p = 8.56e-05). The weakest areas were deception-cue recognition, password reuse, risky public-Wi-Fi login behavior, and uncertainty about whether protections were active. The main contribution is not another general awareness message, but a reproducible diagnostic method that ranks specific knowledge-behavior gaps with uncertainty estimates so that universities can design focused micro-interventions and evaluate behavior-focused progress over time.

1. Introduction

Cybersecurity incidents often begin with ordinary user actions: clicking a deceptive message, reusing a password, trusting a familiar-looking link preview, approving an unexpected login prompt, or entering credentials on an unsafe network. Large incident reports continue to identify credential misuse, phishing, and human decision-making as important parts of the threat landscape [1]-[3]. For this reason, cybersecurity awareness remains a necessary part of institutional protection, especially in universities where students use many personal and academic services across shared networks and devices.

However, awareness alone is not the same as protection. A person may know that strong passwords, multi-factor authentication, safe updates, and careful link checking are important, but still fail to apply these practices consistently. This difference is the knowledge-to-doing gap. The gap matters because many awareness programs are still judged mainly through quiz scores or general satisfaction measures, even though real risk depends on daily behavior. Training research also shows mixed outcomes, especially when awareness content is generic, delivered only once, or not connected to specific real-world actions [4], [6], [7].

The present study reframes cybersecurity awareness as a measurable movement from knowledge to action. The purpose is not to claim that practical

demonstrations, multi-factor authentication, or password guidance are new by themselves. These practices already exist in many institutions. The new outcome of this work is a compact diagnostic index that shows where knowledge is not becoming behavior, reports confidence intervals for each item, and treats "Not sure" responses as meaningful risk signals. This makes the survey useful for choosing targeted micro-interventions instead of repeating broad awareness messages.

The study is grounded in established behavior theory. Protection Motivation Theory explains that protective behavior depends on perceived threat, response effectiveness, and the belief that the action can be performed [14]. The Theory of Planned Behavior emphasizes attitudes, social norms, and perceived control [13]. Self-efficacy is also central because users may know the correct rule but still avoid action if the task feels confusing or inconvenient [12], [15]. Cyber K2D uses these ideas in a simple measurement structure: knowledge, self-efficacy, recent behavior, and the difference between knowledge and behavior.

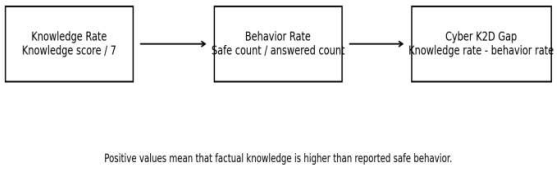

Fig.1 Cyber K2D measurement logic used in this study.

This paper makes three contributions:

- Operationalizes the Cyber K2D Gap as a reproducible Knowledge Rate minus Behavior Rate measure for cyber hygiene, allowing knowledge and recent practice to be compared on the same 0 to 1 scale.
- Quantifies item-level knowledge and safe-practice adoption with Wilson 95% confidence intervals, so weak areas can be ranked with statistical uncertainty rather than reported only as raw percentages.
- Prioritizes behavior-focused micro-interventions by identifying high-risk items where knowledge, behavior, and uncertainty patterns suggest that students may struggle during real security decisions.

2. Related Work and Research Gap

Cybersecurity awareness has been measured through many survey-based approaches. University-focused studies continue to show that students may report moderate to high awareness while still showing weaknesses in password behavior, phishing judgment, and safe technology use [8], [10], [22], [23]. Such studies are useful for describing awareness levels, but instruments and reporting practices often differ, which makes direct comparison difficult.

Table 1: Positioning of Cyber K2D against related approaches.

Approach	Main strength	Typical limitation for local decision-making	How Cyber K2D extends it
Awareness surveys among students [8], [10], [22], [23]	Describe awareness and education levels in student populations.	Often emphasize overall scores and may not quantify the gap between correct answers and recent practice.	Adds a normalized knowledge-to-doing gap and ranks specific weak items.
HAIS-Q and KAB-style measurement [17], [18]	Provide structured and validated measurement of human security dimensions.	Broader and longer instruments may be less convenient for repeated local diagnosis.	Uses a shorter three-block instrument for quick benchmarking and repeated evaluation.
SeBIS and intention scales [19]	Measure security behavior intentions across important domains.	Intentions do not always represent recent behavior.	Uses recent self-reported behavior and safe-practice coding.
Training and phishing intervention studies [6], [7]	Evaluate training methods and real-world training effectiveness.	Intervention results may not show which local behaviors need immediate attention.	Uses item-level gaps to choose micro-interventions before or after training.
Security culture models [9]	Frame security as knowledge, values, risk perception, responsibility, and habits.	Conceptual models may not offer a simple short index for classroom or institutional audits.	Operationalizes the culture-to-behavior idea in a short measurable instrument.

More structured measurement instruments have also been proposed. The Human Aspects of Information Security Questionnaire (HAIS-Q) measures knowledge, attitudes, and behavior across several security domains and has been validated in later studies [17], [18]. The Security Behavior Intentions Scale (SeBIS) measures intentions across passwords, securement, updates, and proactive awareness [19].

These instruments provide important psychometric foundations, but their main purpose is not short diagnostic ranking of item-level knowledge-to-behavior gaps in a local training setting.

Recent literature also emphasizes security behavior, self-efficacy, and information security culture. Studies on MFA adoption, password-manager usability, phishing reporting, and self-efficacy show that behavior is shaped by usability, confidence, perceived value, and social context, not only by factual knowledge [15], [16], [20], [21]. Conceptual work on personal information security culture also supports a wider view in which knowledge, values, risk perception, responsibility, and habits interact [9].

The research gap addressed here is therefore practical and methodological. Many surveys report awareness scores, and many training papers discuss interventions. Fewer short survey studies directly combine: (i) a normalized knowledge-to-behavior gap, (ii) Wilson confidence intervals for item-level priorities, (iii) visible "Not sure" patterns, and (iv) a clear instrument appendix for replication. Table 1 summarizes how the present paper is positioned against related approaches.

3. Methodology

3.1 Study design and participants

A cross-sectional online survey design was used. Respondents completed the survey voluntarily after reading an information sheet and giving consent. The survey was administered in a university context and was analyzed anonymously. After applying the consent-based inclusion rule, 272 responses were included in the final analytical dataset.

The study used available demographic fields only for aggregate description and subgroup planning. No individual respondent was identified in the analysis. The sample should be interpreted as a convenience sample rather than a probability sample of all university students.

3.2 Instrument

The questionnaire was organized into three blocks. The knowledge block included seven True/False/Not sure items about common cyber hygiene concepts. The self-efficacy block included five Likert-scale "I can..." items measuring confidence in performing protective actions. The behavior block included six Yes/No/Not sure items about protective actions during the previous three months. The complete analysis instrument and coding scheme are provided in Appendix A to support replication.

3.3 Scoring model

Knowledge Score. Each correct knowledge answer was coded as 1. Incorrect and "Not sure" answers were coded as 0 because both represent lack of usable knowledge in a real decision. The Knowledge Score ranged from 0 to 7.

Self-Efficacy Score. The five self-efficacy items were scored from 1 (strongly disagree) to 5 (strongly agree). The respondent-level Self-Efficacy Score was calculated as the mean of completed items. The scale reliability reported for SE1-SE5 was Cronbach alpha = 0.715, which is acceptable for a short exploratory scale.

Behavior Rate. Each behavior item was converted into a safe-practice indicator. For protective actions, "Yes" was coded as safe. For risky actions, such as password reuse and risky public-Wi-Fi login, coding was reversed so that higher values always indicated safer behavior. "Not sure" responses were excluded from the denominator in the primary analysis and reported separately. The Behavior Rate was calculated as:

$$\text{Behavior Rate} = \text{Safe Count} / \text{Answered Count}$$

Cyber K2D Gap. To remove the earlier ambiguity between a behavior rate and a gap score, this version uses one canonical definition:

$$\text{Cyber K2D Gap} = (\text{Knowledge Score} / 7) - \text{Behavior Rate}$$

The Cyber K2D Gap ranges approximately from -1 to +1. Positive values mean that knowledge is higher than reported safe behavior. Values near zero mean that knowledge and behavior are aligned. Negative values mean that reported safe behavior is higher than factual knowledge. Respondents with no Yes/No behavior answers were excluded from behavior-rate and gap calculations.

3.4 Statistical analysis

Descriptive statistics were calculated for composite scores. Item-level knowledge and behavior percentages were reported with Wilson 95% confidence intervals because Wilson intervals perform well for binomial proportions, including values near 0 or 1 [26], [27]. Spearman rank correlation was used to examine associations between Knowledge Score,

Self-Efficacy Score, and behavior because the scores are bounded and not assumed to be normally distributed. A Poisson rate model with robust standard errors was used for Safe Count, with log (Answered Count) as an offset, so the coefficients can be interpreted as changes in the rate of safe practice per answered behavior item.

4. Results

4.1 Sample and completeness

The survey received 302 submissions. No duplicate submissions were removed. After consent-based screening, 272 responses were included. Age was available for 257 respondents. The mean age was 22.24 years (SD = 4.30), with a median of 21 years (IQR = 20-23). Reported gender distribution was 151 male, 118 female, and 3 missing. Reported training exposure was 192 with no training, 55 with a short workshop, 23 with a course, and 2 missing.

Table 2: Sample flow and score completeness.

Measure	Value
Raw submissions	302
After de-duplication	302
Duplicates removed	0
Included after consent screening	272
Missing Knowledge Score	0.00%
Missing Self-Efficacy Score	1.84%
Missing Behavior Rate	4.41%

4.2 Composite scores and Cyber K2D Gap

Table 3 presents the cleaned composite results. The mean Knowledge Score was 4.01 out of 7. The mean Self-Efficacy Score was 3.26 out of 5. The mean Behavior Rate was 0.51, which means that respondents reported safe practice for about half of the answered behavior items. The mean Cyber K2D Gap was 0.07, indicating that knowledge was slightly higher than safe behavior in the sample.

Table 3: Composite score summaries after applying the unified K2D definition.

Measure	n	Mean	SD	Median	IQR	Range
Knowledge Score (0-7)	272	4.01	2.11	4.00	2.00-6.00	0-7
Self-Efficacy Score (1-5)	267	3.26	0.80	3.25	2.75-3.75	1-5
Behavior Rate (0-1)	260	0.51	0.28	0.50	0.25-0.75	0-1
Cyber K2D Gap (-1 to +1)	260	0.07	0.36	0.06	-0.17-0.32	-1 to 1
Answered behavior items	272	4.10	1.34	5.00	4.00-5.00	0-5

4.3 Knowledge Accuracy

Knowledge accuracy varied by item (Table 4 and Figure 2). The strongest knowledge item was A7, related to the malware risk of unofficial app stores (71.69%, 95% CI 66.06-76.71). The weakest item was A1, related to spoofed display names or link previews (37.50%, 95% CI 31.96-43.39). The highest "Not sure" rates occurred for A1 (37.13%), A6 (27.57%), and A3 (23.53%), suggesting uncertainty around deception cues, public-network risk, and shortened-link destination risk.

Table 4: Knowledge items: percent correct with Wilson 95% confidence intervals.

Item	Operational topic	Correct (%)	95% CI
A7	Unofficial app stores raise malware risk	71.69	66.06-76.71
A2	MFA helps if a password leaks	63.24	57.36-68.74
A5	Limit app permissions	62.87	56.98-68.39
A4	Strong passwords/passphrases	58.46	52.52-64.15
A3	Shortened links can hide destination	55.88	49.94-61.66
A6	Public Wi-Fi and non-HTTPS risk	51.10	45.19-56.99
A1	Spoofed display name/link preview	37.50	31.96-43.39

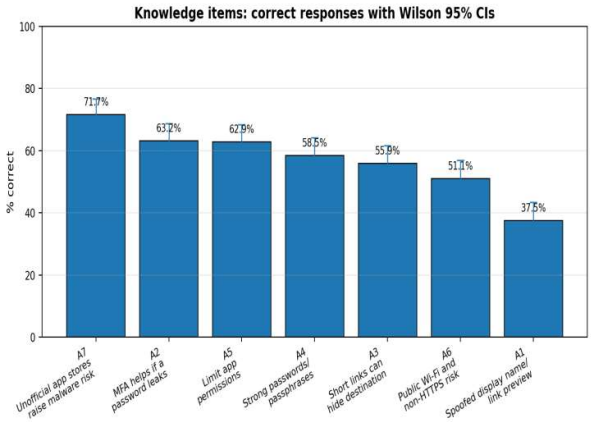

Fig.2 Knowledge item accuracy with Wilson 95% confidence intervals.

4.4 Behavior adoption

Safe behavior adoption also varied across items (Table 5 and Figure 3). The strongest behavior item was reviewing app permissions (B4: 67.14%, 95% CI 60.57-73.09). The weakest behavior item was avoiding password reuse (B3: 39.66%, 95% CI 33.65-46.01), followed by avoiding risky public-Wi-Fi logins (B6: 46.53%, 95% CI 40.39-52.78). These results show that students may understand several

safety concepts but still struggle with practices that require ongoing habits or setup effort.

Uncertainty in behavior items was also meaningful. The highest "Not sure" shares were found for enabled MFA (B1: 24.63%), installed updates within a week (B5: 22.06%), and reviewed app permissions (B4: 21.69%). These responses may indicate that some respondents did not know whether a security setting was active or could not recall recent protective actions.

Table 5: Behavior items: percent safe with Wilson 95% confidence intervals.

Item	Safe behavior topic	Safe (%)	95% CI	Not sure (%)	n (Yes/No)
B4	Reviewed app permissions	67.14	60.57-73.09	21.69	213
B5	Installed updates within a week	64.62	57.98-70.75	22.06	212
B2	Used a password manager	56.94	50.28-63.37	20.59	216
B1	Enabled MFA	52.68	45.86-59.41	24.63	205
B6	Avoided risky public-Wi-Fi logins	46.53	40.39-52.78	9.93	245
B3	Did not reuse passwords	39.66	33.65-46.01	12.87	237

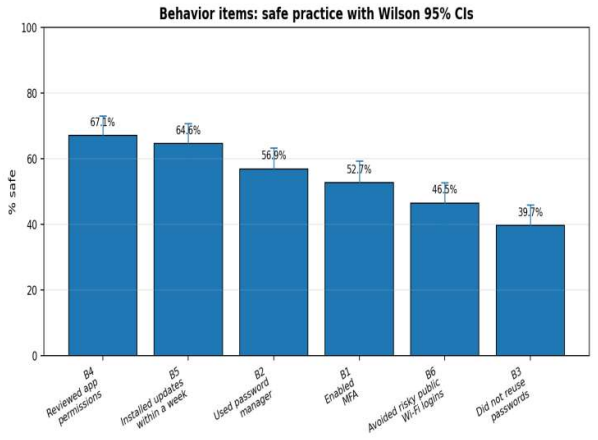

Fig.3 Safe behavior adoption with Wilson 95% confidence intervals.

4.5 Associations and predictors of safe behavior

Knowledge and behavior were positively associated. Spearman rank correlation between Knowledge Score and Behavior Score was rho = 0.40 (p = 1.91e-11, n = 258). Self-efficacy also had a positive but smaller association with behavior (rho = 0.24, p = 8.56e-05, n = 258). These results show that knowledge and confidence matter, but neither fully explains safe behavior.

In the Poisson rate model, Knowledge Score remained a significant predictor of safe behavior. The incidence rate ratio for Knowledge Score was 1.06 (95% CI 1.02-1.10, p = 0.005), meaning that each additional correct knowledge item was associated with approximately 6% higher expected safe-practice rate, holding self-efficacy constant. Self-efficacy had a positive but less precise association (IRR = 1.07, 95% CI 0.98-1.16, p = 0.118).

Table 6: Predictors of safe behavior in the Poisson rate model.

Predictor	IRR	95% CI	p-value	Interpretation
Knowledge Score (per +1 correct item)	1.06	1.02-1.10	0.005	About 6% higher safe-practice rate
Self-Efficacy Score (per +1 point)	1.07	0.98-1.16	0.118	Positive but not statistically precise

5. Discussion

The main finding is straightforward: the sample showed moderate cybersecurity knowledge, but recent safe behavior was only moderate. The positive association between knowledge and behavior confirms that knowledge is useful. The Cyber K2D Gap shows that knowledge is not enough. Safe action also depends on confidence, convenience, habit, and the ability to check whether a protection is actually enabled.

This result helps clarify the novelty of the paper. The recommended actions, such as MFA guidance, password-manager support, update reminders, and link-verification demonstrations, are not new as individual practices. The contribution is the measurement approach that identifies which of these actions should be prioritized for a particular population. For example, the data suggest that password reuse and public-Wi-Fi login behavior require more attention than app-permission review in this sample. A general awareness lecture would not reveal this ordering.

The weakest knowledge item involved spoofed display names and link previews. This is important because phishing attacks often rely on surface trust cues. A student may know the phrase "avoid suspicious links" but still trust a message that looks official. The gap therefore lies in mental models, not only in recall. Training should show how deception works through short live examples, not only through written rules.

The weakest behavior item was password reuse. This is consistent with prior work showing that password-manager adoption and strong password routines involve usability barriers, first-use friction, and habit formation [21]. The practical implication is that "do not reuse passwords" is not enough. The safer behavior becomes more realistic when users are guided through a password-manager setup, recovery-code storage, and account-by-account replacement of reused passwords.

The "Not sure" results are also important. Uncertainty is not simply missing knowledge. In real security decisions, uncertainty can lead to quick unsafe choices. If a respondent does not know whether MFA is enabled, whether updates were installed, or whether a link preview can be trusted, the institution has not created a dependable safety habit. For this reason, training evaluation should measure uncertainty reduction along with knowledge and behavior.

Compared with previous awareness surveys, the present paper gives a more actionable output: a ranked list of weak concepts and weak behaviors with confidence intervals. Compared with broad security culture models, Cyber K2D is narrower but easier to repeat in a classroom, department, or university-wide audit. Its value is strongest as a local diagnostic benchmark rather than as a full psychometric replacement for larger validated instruments.

5.1 Practical Implications

The results support behavior-focused micro-interventions. A suitable program could include: (i) a two-minute demonstration showing how display names, previews, and shortened URLs can mislead users; (ii) a short password-manager onboarding session; (iii) a public-Wi-Fi checklist for avoiding sensitive logins on unsafe networks; and (iv) a guided MFA verification activity where students check whether MFA is enabled and save recovery codes. These actions are practical because friction is reduced and advice becomes a visible task.

For institutions, Cyber K2D can be used before and after such interventions. A useful evaluation would not ask only whether students learned the content. It would ask whether the lowest-ranked behavior items improved, whether the Cyber K2D Gap decreased, and whether "Not sure" responses declined on high-risk items. This connects training design with measurable behavior-oriented outcomes.

5.2 Limitations and Threats to Validity

Self-report bias. The behavior items relied on self-report. Respondents may forget past actions or provide answers that seem socially desirable. This can overestimate safe behavior. Future work should add objective checks where ethical and practical, such as voluntary device-setting verification or controlled security tasks.

Convenience sample. The sample came from a university context and should not be treated as representative of all students or all users. Cyber K2D should be repeated in other institutions, age groups, and professional settings before wider generalization.

Cross-sectional design. The data were collected at one time point. Associations between knowledge, self-efficacy, and behavior should not be interpreted as causal effects. Longitudinal or intervention-based designs are needed to test whether improving a specific knowledge item changes the related behavior.

Short instrument. The instrument was intentionally brief. This reduces respondent burden but limits depth. It does not replace larger validated tools such as HAIS-Q or SeBIS. Its main purpose is practical diagnosis and repeated local benchmarking.

Behavior frequency. Behavior items used Yes/No/Not sure responses. This makes scoring simple but does not capture how often a risky behavior occurs. A future version should test frequency-based behavior items while keeping survey length manageable.

Measurement reliability. The self-efficacy block showed acceptable internal consistency for a short scale. However, additional psychometric work is needed, including exploratory factor analysis, confirmatory factor analysis in a larger sample, and measurement invariance testing across gender, program, and training-exposure groups.

9. Conclusion

This paper presented Cyber K2D as a simple uncertainty-aware method for measuring the knowledge-to-doing gap in cyber hygiene. In a university sample of 272 consented respondents, knowledge was moderate, self-efficacy was moderate, and recent safe behavior was only moderate. The unified Cyber K2D Gap showed that knowledge slightly exceeded behavior, while item-level results identified the clearest priority areas: deception-cue

recognition, password reuse, risky public-Wi-Fi login behavior, and uncertainty about active protections. The findings support a shift from broad awareness delivery to targeted behavior support. Cyber K2D can help universities and organizations decide which safe practices need immediate attention, evaluate whether micro-interventions reduce the gap, and report results with clearer uncertainty estimates.

8. Future Recommendations

First, Cyber K2D should be tested as a pre-post intervention measure. A short intervention can target the weakest items, and the same instrument can be repeated after two to four weeks to assess whether knowledge, behavior, and uncertainty changed.

Second, training-exposure subgroups should be analyzed more deeply. The current dataset includes respondents with no training, a short workshop, and a course. A Kruskal-Wallis test or ordinal/rate model could compare these groups and show whether different training exposure is associated with lower K2D gaps.

Third, future studies should combine Cyber K2D with objective or semi-objective behavior indicators, such as MFA setting checks, password-manager setup confirmation, or simulated link-verification tasks. This would reduce dependence on self-report.

Fourth, the instrument should be refined through cognitive interviews and factor analysis. This would improve item clarity, confirm the structure of self-efficacy items, and support stronger claims about measurement validity.

Finally, the framework can be adapted to other behavior-change domains where knowledge does not reliably become action. Cross-domain comparison may help cybersecurity training borrow stronger behavior-change methods from health and safety research.

References

[1] *Verizon, 2025 Data Breach Investigations Report. Verizon Business, 2025.*

[2] *Anti-Phishing Working Group (APWG), Phishing Activity Trends Report, 2nd Quarter 2025, Aug. 2025.*

[3] *European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2024. ENISA, Sept. 2024.*

[4] *M. Merritt et al., Building a Cybersecurity and Privacy Learning Program, NIST Special Publication 800-50r1. National Institute of Standards and Technology, 2024. doi: 10.6028/NIST.SP.800-50r1.*

[5] *D. Temoshok et al., Digital Identity Guidelines: Authentication and Authenticator Management, NIST Special Publication 800-63B-4. National Institute of Standards and Technology, 2025. doi: 10.6028/NIST.SP.800-63B-4.*

[6] *J. Prümmer, T. van Steen, and B. van den Berg, "A systematic review of current cybersecurity training methods," Computers & Security, vol. 136, Article 103585, 2024. doi: 10.1016/j.cose.2023.103585.*

[7] *G. Ho et al., "Understanding the efficacy of phishing training in practice," in Proceedings of the 2025 IEEE Symposium on Security and Privacy (SP), 2025. doi: 10.1109/SP61157.2025.00076.*

[8] *B. Palao, N. A. Cruz, G. L. Lualhati, E. Pascual, and J. M. Santos, "The Human Firewall: Evaluation of Cybersecurity Awareness Among Students of Bulacan State University," Journal of Critical Social Sciences and Review, vol. 1, no. 1, pp. 1-10, 2026. doi: 10.5281/zenodo.19413443.*

[9] *R. Mahmudova, "Development of a conceptual model for assessing personal information security culture," Problems of Information Society, vol. 17, no. 1, pp. 70-80, 2026. doi: 10.25045/jpis.v17.i1.08.*

[10] *A. K. Gwenhure, "University students' security behavior against email phishing attacks: insights from the health belief model," Journal of Cybersecurity, vol. 11, no. 1, Article tyaf034, 2025. doi: 10.1093/cybsec/tyaf034.*

[11] *B.-Y. Ng, A. Kankanhalli, and Y. C. Xu, "Studying users' computer security behavior: A health belief perspective," Decision Support Systems, vol. 46, no. 4, pp. 815-825, 2009. doi: 10.1016/j.dss.2008.11.010.*

[12] *A. Bandura, "Self-efficacy: Toward a unifying theory of behavioral change," Psychological Review, vol. 84, no. 2, pp. 191-215, 1977. doi: 10.1037/0033-295X.84.2.191.*

[13] *I. Ajzen, "The theory of planned behavior," Organizational Behavior and Human Decision Processes, vol. 50, no. 2, pp. 179-211, 1991. doi: 10.1016/0749-5978(91)90020-T.*

[14] *R. W. Rogers, "A Protection Motivation Theory of fear appeals and attitude change," The Journal of Psychology, vol. 91, no. 1, pp. 93-114, 1975. doi: 10.1080/00223980.1975.9915803.*

[15] N. Borgert, L. Jansen, I. Böse, J. Friedauer, M. A. Sasse, and M. Elson, "Self-Efficacy and Security Behavior: Results from a Systematic Review of Research Methods," in Proceedings of the CHI Conference on Human Factors in Computing Systems, 2024. doi: 10.1145/3613904.3642432.

[16] O. M. Ogbanufe and C. Baham, "Using Multi-Factor Authentication for Online Account Security: Examining the Influence of Anticipated Regret," Information Systems Frontiers, vol. 25, no. 2, pp. 897-916, 2023. doi: 10.1007/s10796-022-10278-1.

[17] K. Parsons et al., "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," Computers & Security, vol. 66, pp. 40-51, 2017. doi: 10.1016/j.cose.2017.01.004.

[18] K. Parsons et al., "The development of the Human Aspects of Information Security Questionnaire (HAIS-Q)," in Proceedings of the 24th Australasian Conference on Information Systems, 2013.

[19] S. Egelman and E. Peer, "Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS)," in Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 2015, pp. 2873-2882. doi: 10.1145/2702123.2702249.

[20] I. A. Marin, P. Burda, N. Zannone, and L. Allodi, "The Influence of Human Factors on the Intention to Report Phishing Emails," in Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, 2023. doi: 10.1145/3544548.3580985.

[21] P. A. Cabarcos and P. Mayer, "'The more accounts I use, the less I have to think': A Longitudinal Study on the Usability of Password Managers for Novice Users," in Proceedings of the Twenty-First Symposium on Usable Privacy and Security (SOUPS 2025), Seattle, WA, USA, 2025, pp. 351-369.

[22] N. Bromall, P. Draus, S. Mishra, K. Slonka, and J. Trunkos, "Cybersecurity Awareness Among Post-Secondary Students," Issues in Information Systems, vol. 26, no. 3, pp. 149-157, 2025. doi: 10.48009/3_iis_2025_2025_111.

[23] I. Dunđer, S. Seljan, and M. Odak, "Information Security Awareness in the University Environment: A Focus on Undergraduates," TEM Journal, vol. 14, no. 2, pp. 1621-1628, 2025. doi: 10.18421/TEM142-59.

[24] S. Michie, M. M. van Stralen, and R. West, "The behaviour change wheel: A new method for characterising and designing behaviour change interventions," Implementation Science, vol. 6, Article 42, 2011. doi: 10.1186/1748-5908-6-42.

[25] R. N. Rimal, "Closing the knowledge-behavior gap in health promotion: The mediating role of self-efficacy," Health Communication, vol. 12, no. 3, pp. 219-237, 2000. doi: 10.1207/S15327027HC1203_01.

[26] R. G. Newcombe, "Two-sided confidence intervals for the single proportion: Comparison of seven methods," Statistics in Medicine, vol. 17, no. 8, pp. 857-872, 1998. doi: 10.1002/(SICI)1097-0258(19980430)17:8<857::AID-SIM777>3.0.CO;2-E.

[27] L. D. Brown, T. T. Cai, and A. DasGupta, "Interval estimation for a binomial proportion," Statistical Science, vol. 16, no. 2, pp. 101-133, 2001. doi: 10.1214/ss/1009213286.

© Aror University of Art, Architecture, Design & Heritage, Sukkur, 2026