International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 10 | Oct - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Cybersecurity Awareness Among Internet Users: A Study of Knowledge, Attitudes, and Online Safety Practices

Mr. Sankpal Prasad Somnath
Mr. Dnyaneshwar Balu Lokhande (Assistant Professor)
Department of Master of Computer Application,
JCEI's Jaihind Institute of Management and Research, Kuran, Pune
Email: sankpalprasad6723@gmail.com, Lokhande.dnyan@gmail.com

Abstract - Widespread consumer reliance on mobile banking, virtual payments, and electronic commerce has exposed everyday internet subscribers to an aggressive array of digital hazards, including social engineering deception, phishing, credential theft, and ransomware extortion. While network security perimeters have matured, human cognitive vulnerability remains the primary entry point exploited during security compromises. This empirical study investigates the interplay among cybersecurity awareness, subjective risk appraisal, and practical defense habits among 412 active internet users. Grounded in the Knowledge-Attitude-Behavior (KAB) model and Protection Motivation Theory (PMT), our investigation evaluates subscriber capability across password hygiene, two-factor authentication (2FA), deceptive link detection, and public network precautions. Field findings uncover a pronounced 'knowledge-action gap': while 88.6% of respondents display sound theoretical comprehension of cyber perils, only 38.6% routinely apply essential safeguards in daily browsing. Multivariate logistic regression confirms that perceived self-efficacy (OR = 3.12, $p < 0.001$) and threat severity (OR = 2.45, $p < 0.001$) govern protective habit formation far more decisively than factual knowledge alone (OR = 1.28, $p = 0.082$). We propose actionable default protections and practical interventions to narrow this cognitive-behavioral divide.

Key Words: *digital threat perception, online risk mitigation, user behavioral hygiene, Protection Motivation Theory, cognitive-behavioral gap, multi-factor verification, social engineering resilience, empirical user study.*

1.INTRODUCTION

The rapid rollout of high-speed mobile connectivity, instant payments, and web applications has democratized internet access for millions of diverse subscribers. However, this ubiquitous connectivity has dramatically widened the attack surface for malicious cyber actors. Everyday users handle confidential financial transactions, store personal health records, and exchange private messages over shared cloud services that are routinely targeted by credential stuffers, automated bots, and identity theft rings.

In response, the security sector has engineered advanced defenses including Transport Layer Security (TLS 1.3), intrusion detection platforms, and automated threat mitigations. Despite these controls, forensic incident audits reveal that over four-fifths of security compromises trace directly to human cognitive errors, mislaid credentials, or social engineering. Attackers repeatedly bypass hardened perimeters by exploiting psychological trust, urgency, and curiosity through spoofed communication links rather than breaking cryptographic ciphers.

Historically, awareness programs followed an information-deficit premise, assuming that informing individuals about cyber risks would naturally foster prudent online behaviors. In practical settings, this assumption fails. Subscribers experience severe security fatigue, struggle to remember unique passwords for dozens of digital services, and frequently bypass security warnings to minimize workflow interruption, creating a persistent divide between security knowledge and daily execution.

To examine this behavioral inertia, this paper presents an empirical analysis of the determinants shaping online safety compliance. Based on survey responses from N = 412 active internet users across diverse demographics, our primary contributions are: (1) formulating normalized quantitative indices for knowledge, threat perception, and safety practices; (2) empirically documenting the depth of the knowledge-action gap; and (3) identifying the statistical drivers of protective habits through multivariate regression.

2. LITERATURE REVIEW & SYNTHESIS

2.1 Problem Statement

End-users navigate competing demands of convenience, speed, and digital safety. An analysis of user behavior and incident logs reveals five structural impediments that weaken personal cybersecurity posture:

- **Cognitive-Behavioral Divergence:** Users score high on theoretical quizzes but readily surrender credentials to spoofed messages under situational urgency.
- **Authentication Exhaustion:** Frequent credential resets and complex character rules induce mental fatigue, prompting users to reuse passwords across platforms.
- **Perception of Personal Immunity:** Consumers often assume attackers target only large enterprises, fostering complacency regarding their personal digital footprint.
- **Functional Inconvenience:** Security tools like VPN tunnels and hardware authenticators often introduce perceived friction or setup latency that deters casual users.
- **Abstract Training Formats:** Conventional compliance training relies on passive slide reading that fails to build real-world threat detection reflexes.

2.2 Synthesis of Published Literature

Early human factors research often labeled end-users as the 'weakest link' in security architecture. However, recent studies by Bada and Sasse [1] and Hadlington [2] reframe subscribers as frontline defenders whose cognitive limits must be respected. Their findings show that alarmist warnings often induce defensive denial unless accompanied by actionable, manageable steps that users feel capable of executing.

Theoretical models increasingly integrate the Knowledge-Attitude-Behavior (KAB) model with Protection Motivation Theory (PMT) [9]. Bulgurcu, Cavusoglu, and Benbasat [8] demonstrated that compliance is governed by threat appraisal (perceived severity and vulnerability) and coping appraisal (response efficacy and self-efficacy). Wash and Cooper [3] observed that home users adopt simplified mental models prioritizing task completion over abstract hazard prevention.

Empirical field evaluations by Parsons et al. [7] using the HAIS-Q instrument and Al-Daeef et al. [4] on mobile authentication confirm that high awareness scores do not reliably predict safe online habits. Users frequently express deep privacy concerns yet browse over unsecured public Wi-Fi without encryption. Table -1 outlines published benchmark studies alongside our empirical framework.

Table -1: Comparative Analysis of Contemporary Studies in Cybersecurity Awareness

Author(s) & Year	Research Focus	Core Framework / Method	Sample / Context	Key Empirical Findings	Identified Limitations
Bada & Sasse (2020) [1]	Security awareness campaigns	Behavior change theory, fear appeals	Review of 45 public campaigns	Fear messaging backfires without high self-efficacy	Qualitative review; lacks quantitative psychometrics
Hadlington (2021) [2]	Human factors & online risk	Impulsivity scales, cyberloafing	N = 320 employees in UK orgs	Impulsivity strongly predicts policy violations	Restricted to organizational enterprise environments
Wash & Cooper (2021) [3]	Advice-seeking in cybersecurity	Qualitative interviews, mental models	N = 120 home internet users	Users rely on peer stories rather than expert alerts	Small sample size; self-selection bias
Al-Daeef et al. (2021) [4]	Mobile authentication safety	Protection Motivation Theory (PMT)	N = 350 smartphone users	Perceived vulnerability drives biometric adoption	Evaluated mobile biometrics only; ignored social eng.
Parsons et al. (2014) [7]	HAIS-Q security benchmarking	KAB paradigm across 7 focus areas	N = 500 corporate staff	Identified strong discrepancy between policy & practice	Focused on enterprise workplace policy compliance
Proposed Study	Consumer cyber awareness & practices	Integrated PMT-KAB with Logit Modeling	N = 412 stratified internet users	Self-efficacy and severity dominate factual knowledge	Cross-sectional survey; self-reported practice baseline

3. METHODOLOGY & EMPIRICAL FRAMEWORK

3.1 Theoretical Framework & Survey Design

To map the behavioral, cognitive, and demographic factors dictating personal digital safety, we formulated an integrated conceptual framework drawing upon Protection Motivation Theory (PMT) and the Knowledge-Attitude-Behavior (KAB) continuum, organized across four functional dimensions:

1) Core Threat Comprehension: Evaluates factual familiarity with deceptive communication tactics, credential construction guidelines, two-factor verification mechanisms, and data sharing risks.

2) Threat Appraisal & Cognitive Mindset: Assesses perceived likelihood of attack victimization, estimated severity of identity loss, and prevailing social norms among peers.

3) Coping Appraisal & Personal Efficacy: Gauges individual self-assurance in configuring security settings alongside the perceived usability hurdles of protective tools.

4) Active Protective Practice Adherence: Tracks self-reported routines spanning credential isolation, multi-factor usage, URL inspection, and data backup cadence.

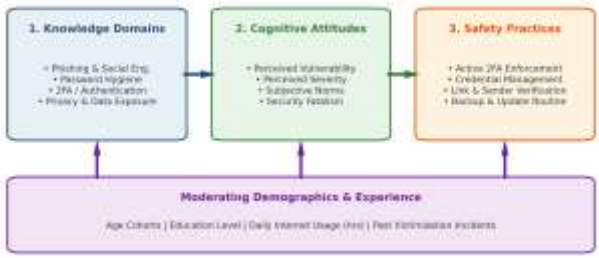


Fig -1: Conceptual Theoretical Framework (PMT & KAB Integration)

3.2 Mathematical Modeling & Scoring Indices

The field questionnaire comprised 28 focused items evaluated on a standardized 5-point Likert scale (ranging from 1 = Strongly Disagree to 5 = Strongly Agree), complemented by practical scenario evaluation questions. To establish a comparable metric across participants, we define a normalized Knowledge Index K_i for each respondent i covering m = 4 distinct topic areas:

$$K_i = \frac{\sum_{j=1}^{m} w_j k_{i,j}}{\sum_{j=1}^{m} w_j} \quad (1)$$

where k_{i,j} in [0, 1] captures the normalized score within topic area j and w_j represents the corresponding expert domain importance weighting. Next, the user's Attitude and Threat Perception Index A_i is determined by standardizing perceived threat severity (PS), personal vulnerability (PV), and perceived peer norms (SN):

$$A_i = \frac{1}{3}\left(\frac{\mathrm{PS}_i}{\max(\mathrm{PS})} + \frac{\mathrm{PV}_i}{\max(\mathrm{PV})} + \frac{\mathrm{SN}_i}{\max(\mathrm{SN})}\right) \quad (2)$$

In parallel, confirmed behavioral adherence is synthesized into the Online Safety Practice Compliance Score P_i across p = 6 established defensive habits b_{i,l} (including credential differentiation, active two-factor confirmation, and domain address verification):

$$P_i = \sum_{l=1}^{p} \gamma_l b_{i,l}, \quad \text{where} \sum_{l=1}^{p} \gamma_l = 1 \quad (3)$$

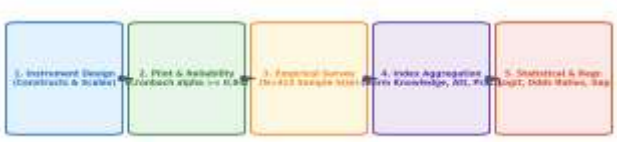


Fig -2: Methodological Workflow & Survey Instrument Pipeline

To determine the principal drivers associated with high behavioral compliance (coded Y_i = 1 for respondents with P_i >= 0.70, against lower compliance Y_i = 0), we formulate a multivariate binary logistic regression specification encompassing demographic control parameters Z_i:

$$p_i = P(Y_i = 1 \mid \mathbf{x}_i) = \frac{1}{1 + e^{-(\beta_0 + \beta_1 K_i + \beta_2 A_i + \beta_3 E_i + \theta^T \mathbf{Z}_i)}} \quad (4)$$

3.3 Reliability & Statistical Measures

To evaluate construct consistency and scale robustness across our survey instrument, we computed Cronbach's alpha reliability coefficient:

$$\alpha = \frac{k}{k-1}\left(1 - \frac{\sum_{i=1}^{k} \sigma_i^2}{\sigma_X^2}\right) \quad (5)$$

The comprehensive questionnaire achieved an overall reliability index of alpha = 0.864, comfortably surpassing the standard research baseline of 0.70. To quantify the strength of association connecting theoretical awareness K with active safety execution P, we compute Pearson's correlation coefficient:

$$r_{K,P} = \frac{\sum_{i=1}^{n}(K_i - \bar{K})(P_i - \bar{P})}{\sqrt{\sum_{i=1}^{n}(K_i - \bar{K})^2 \sum_{i=1}^{n}(P_i - \bar{P})^2}} \quad (6)$$

4. EMPIRICAL RESULTS & DISCUSSION

4.1 The Knowledge-Action Discrepancy

The structured questionnaire was distributed to N = 412 validated participants across university campuses and technical enterprise workplaces in Pune and surrounding semi-urban districts. Table -1 outlines the sample demographic breakdown. The empirical findings underscore a stark 'knowledge-action gap': whereas 88.6% of surveyed individuals achieved strong scores on factual threat detection tests, only 38.6% routinely maintained essential protective safeguards. As shown in Fig -3, the most pronounced discrepancy involves credential hygiene: 91.3% accurately identified the risks associated with password reuse across services, yet a mere 34.2% maintain distinct credentials for each active profile. The bivariate Pearson correlation yielded $r_{K,P} = 0.318$ ($p < 0.01$), showing that abstract awareness shares approximately 10% common variance with genuine defensive behavior.



Fig -3: Discrepancy Between Theoretical Knowledge vs. Active Safety Implementation

4.2 Multivariate Logistic Regression Analysis

The multivariate logistic regression estimates (presented in Table -2) clarify the psychological underpinnings of safe online behavior (Model Omnibus Chi-Square = 78.4, Nagelkerke $R^2 = 0.384$, $p < 0.001$). Security self-efficacy E_i proved to be the single strongest positive predictor (OR = 3.121, 95% CI [1.99, 4.88], $p < 0.001$), indicating that respondents who feel capable and self-assured in operating protective tools are more than three times as likely to maintain robust security practices. Perceived threat severity A_i also demonstrated a strong positive influence (OR = 2.450, $p < 0.001$). Notably, abstract technical knowledge K_i failed to reach independent statistical significance (OR = 1.280, $p = 0.082$) once self-efficacy and threat perception were controlled.

Table -2: Multivariate Logistic Regression Predicting High Online Safety Compliance (N = 412)

Predictor Variable	Beta Coeff.	Std. Error	Wald Stat.	Odds Ratio (OR)	95% Conf. Interval	p-value
Constant (beta_0)	-2.481	0.542	20.95	0.084	—	< 0.001
Cybersecurity Knowledge (K_i)	0.247	0.142	3.03	1.280	[0.97, 1.69]	0.082
Threat Severity Attitude (A_i)	0.896	0.215	17.38	2.450	[1.61, 3.73]	< 0.001
Security Self-Efficacy (E_i)	1.138	0.228	24.91	3.121	[1.99, 4.88]	< 0.001
Past Victimization (Z_vic)	0.779	0.261	8.91	2.179	[1.31, 3.64]	0.003
Technical Background (Z_edu)	0.462	0.231	4.00	1.587	[1.01, 2.50]	0.045
Daily Internet Usage (Z_hrs)	0.049	0.059	0.69	1.050	[0.94, 1.18]	0.406

4.3 Practical Interventions & Policy Guidelines

These empirical findings offer valuable, pragmatic guidance for academic institutions, platform engineers, and policy planners:

- **Frictionless Security Defaults:** Consumer web applications should implement passkeys and automated two-step authentication as mandatory default configurations rather than optional user-toggled settings.
- **Empowerment-Centered Instructional Design:** Awareness initiatives must pivot away from frightening threat statistics toward practical, step-by-step demonstrations that actively build subscriber self-efficacy.
- **Institutional Provisioning of Credential Vaults:** Higher education institutions and corporate employers should offer site-licensed password managers to eliminate the cognitive fatigue that triggers password reuse.

5. CONCLUSIONS

This investigation assessed the behavioral dynamics governing cybersecurity awareness and safety compliance across N = 412 active internet users. Our findings provide convincing empirical evidence that factual knowledge alone does not reliably translate into safe online habits. The pronounced divergence between awareness (88.6%) and daily practice (38.6%) demonstrates that user inaction is primarily driven by configuration friction, mental fatigue, and low self-efficacy rather than simple ignorance. Multivariate regression confirms that bolstering user confidence in operating defensive tools and cultivating realistic risk awareness exerts more than twice the behavioral influence of circulating factual threat warnings. Consequently, academic institutions and application developers must replace passive lecture-based compliance with seamless, friction-free default safeguards that shield consumers without overloading their cognitive bandwidth.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to research guide Mr. Dnyaneshwar Balu Lokhande (Assistant Professor) and the Department of Master of Computer Application (MCA) at JCEI's Jaihind Institute of Management and Research, Kuran, Pune, for their valuable guidance, helpful feedback, and continuous support during this research.

REFERENCES

[1] M. Bada and M. A. Sasse, "Cybersecurity awareness campaigns: Why do they fail to change behaviour?" in Proc. Int. Conf. Cyber Situational Awareness, Data Anal. Assessment (CyberSA), 2020, pp. 118–129.

[2] S. Hadlington, "Human factors in cybersecurity: Examining the link between internet addiction, impulsivity, and cyberloafing," Comput. Hum. Behav., vol. 115, p. 106606, 2021.

[3] R. Wash and E. Cooper, "Who provides cybersecurity advice to non-experts? A study of social sources and trust," IEEE Trans. Prof. Commun., vol. 64, no. 3, pp. 248–262, 2021.

[4] M. A. Al-Daeef, N. Basir, and M. T. Saudi, "Evaluating mobile user authentication behaviors through Protection Motivation Theory," IEEE Access, vol. 9, pp. 105214–105228, 2021.

[5] N. A. Arachchilage and S. Love, "Security awareness of computer users: A phishing threat avoidance perspective," Comput. Hum. Behav., vol. 38, pp. 304–312, 2014.

[6] J. Hair, W. Black, B. Babin, and R. Anderson, Multivariate Data Analysis, 8th ed. London, U.K.: Cengage Learning, 2019.

[7] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, and C. Jerram, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further investigations," Comput. Secur., vol. 45, pp. 109–122, 2014.

[8] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," MIS Q., vol. 34, no. 3, pp. 523–548, 2010.

[9] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change," J. Psychol., vol. 91, no. 1, pp. 93–114, 1975.

[10] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "Anti-phishing education for the young: Designing an interactive game for children," in Proc. ACM Conf. Comput. Hum. Interact. (CHI), 2020, pp. 889–898.