Journal of Science Research International (JSRI)
ISSN: 2456-6365 (Online)

OPEN ACCESS

COMPLIANCE VS. FATIGUE: INVESTIGATING THE IMPACT OF SECURITY FATIGUE ON RISKY DIGITAL BEHAVIORS AMONG STUDENTS AND EMPLOYEES

Dhanya Vinish*, Tanvi Kocharekar, Pratham Kutty and Vaishnavi Sawant

Department of Information Technology,

Pillai College of Arts, Commerce & Science (Autonomous), New Panvel, Maharashtra, India 410206

**Corresponding author E-mail: dvinish@mes.ac.in*

Received: 11 December 2025	Revised: 11 January 2026	Accepted: 13 February 2026	Published: 28 February 2026

DOI: **https://doi.org/10.5281/zenodo.19030479**

Abstract:

Security fatigue—a state of cognitive exhaustion arising from relentless authentication demands and security alerts—represents an underexamined human vulnerability in modern cybersecurity. This paper investigates the relationship between cognitive depletion (commonly experienced as "brain fog") and non-compliant digital security behaviors among university students and employees. Drawing on Cognitive Load Theory and Decision Fatigue Theory, a cross-sectional, survey-based study was administered to 95 participants using an online structured questionnaire. The findings confirm that elevated brain fog strongly predicts heightened security fatigue, which in turn drives risky behaviors including habituation to warnings, password reuse, and deliberate deferral of critical system updates. A notable "confidence–competence gap" was also identified: respondents who reported high self-efficacy in recognizing phishing attempts simultaneously admitted to the highest rates of unsafe practices, indicating that awareness alone is insufficient when cognitive resources are depleted. The study further reveals a systemic gap in institutional support, with the majority of participants reporting inadequate access to digital-detox initiatives or mental health resources. These findings collectively argue that effective cybersecurity policy must address cognitive sustainability alongside technical enforcement.

Keywords: *Security Fatigue, Brain Fog, Cognitive Load, Decision Fatigue, Password Reuse, Cybersecurity Compliance, Digital Behavior.*

1. Introduction

Contemporary digital environments demand continuous security decisions: multi-factor authentication, pop-up warnings, mandatory password rotations, and software update prompts. Although each measure is individually justified, their cumulative burden generates a phenomenon termed security fatigue—a cognitive state in which users become desensitized or overwhelmed by security demands and subsequently bypass safeguards to reduce

mental strain [1]. This dynamic reveals a paradox: organizations that implement increasingly rigorous security architectures may inadvertently erode user compliance. When cognitive reserves are exhausted, even security-aware individuals are prone to heuristic shortcuts—mental efficiencies that trade accuracy for speed. The result is vulnerability not from ignorance, but from depletion.

The present study addresses this paradox by examining two target populations—university students and working professionals—whose distinct stress profiles (academic versus occupational) offer a comparative lens through which to evaluate how contextual cognitive load shapes cybersecurity behavior.

The paper's objectives are fourfold:

(i) To quantify the prevalence of brain fog and security fatigue
(ii) To analyze how cognitive overload shapes specific risky behaviors
(iii) To compare student and employee compliance tendencies
(iv) To evaluate perceived effectiveness of organizational mitigation strategies.

2. Literature review

Security fatigue has been defined as a saturation state characterized by mental exhaustion, diminished motivation, and a sense of loss of control over digital security requirements [1]. Elevated fatigue is particularly prevalent among populations with intensive digital system exposure: IT professionals and computer science students both reports disproportionately high fatigue rates [2], while healthcare workers experiencing time-pressured cognitive impairment exhibit compromised adherence to security protocols [3].

A primary mechanism linking fatigue to risk is "System 1" or fast, automatic decision-making, which users default to under cognitive strain [4]. Neurobiological research has documented that sustained exposure to security warnings triggers habituation, reducing attentional responses by more than 20 percentage points over a three-week period [5]. Survey-based studies have found that nearly 70% of employees acknowledge willingness to bypass cybersecurity policies when facing high workloads [6], and that fatigued students are significantly more likely to reuse passwords across multiple accounts [4].

Comparative research highlights group-specific vulnerabilities: students' security posture deteriorates markedly during high-stakes academic periods, while employees accumulate what Nobles terms "complexity debt"—where escalating technical controls strain rather than reinforce human performance [7]. University faculty and staff tend to show marginally stronger policy adherence than students, likely owing to greater organizational commitment [8].

Despite extensive scholarship, key limitations persist. Self-reported methodologies introduce social desirability bias [9], and laboratory paradigms suffer from ecological invalidity [5]. Existing tools seldom capture real-time fatigue fluctuations [2], and the field remains predominantly Western in geographic scope [4]. Critically, research emphasis has favored identifying fatigue's causes rather than evaluating practical countermeasures [10].

3. Research methodology

3.1 Theoretical framework

Two established theoretical constructs form the conceptual backbone of this investigation. The first, Cognitive Load Theory, holds that working memory operates within strict capacity boundaries; once those boundaries are breached by simultaneous demands, decision quality deteriorates measurably. Within a cybersecurity context, recurring authentication prompts, policy pop-ups, and alert notifications collectively represent unnecessary

mental overhead — draining the attentional reserves that users would otherwise direct toward vigilant security choices.

The second construct, Decision Fatigue Theory, introduces a temporal dimension: repeated choice-making across extended periods progressively weakens an individual's capacity for self-regulation. When both constructs are applied together, they yield a clear prediction — users whose cognitive reserves have been worn down by academic or occupational pressure will perceive routine security tasks as disproportionately burdensome, making non-compliant shortcuts increasingly likely.

3.2 Research design and sampling

The study adopted a quantitative, cross-sectional approach, capturing data at a single point in time through an online structured questionnaire. Ninety-five respondents participated, drawn from two distinct occupational groups: university students, who were mostly between 18 and 24 years old, and working professionals aged 25 and above. A small proportion reported belonging to both categories simultaneously, representing individuals navigating compounded academic and professional pressures. This composition allowed for a meaningful side-by-side examination of how differing stress environments shape security-related behavior.

3.3 Instrument design

The questionnaire was organized into four thematic blocks. The opening block gathered demographic details to classify each respondent into the appropriate occupational group. The second block measured cognitive fatigue through items addressing how frequently participants experienced difficulty concentrating, episodes of forgetfulness, and generally slower mental processing. The third block examined security-specific behaviors — particularly tendencies to dismiss warnings automatically, recycle passwords across platforms, postpone system updates, and reactions to perceived digital monitoring. The final block assessed whether participants believed their institution offered meaningful support for managing digital-related mental strain. Responses throughout were recorded on a five-point scale anchored at one (never / strongly disagree) and five (always / strongly agree).

Table 1: Summary of Key Survey Findings (n = 95)

Parameter	Key Observation
Brain fog prevalence (score 3–5)	~89% of respondents
Security overwhelm (score 3–5)	~69% of respondents
Warning habituation (score 3–5)	~66% of respondents
Password reuse (score 3–5)	~57% of respondents
Institutional support (score 1–2)	~62% felt unsupported
Phishing confidence (score 4–5)	~71% rated high confidence

4. Findings and Analysis

4.1 Cognitive depletion (Brain fog)

The data revealed high prevalence of self-reported brain fog, with approximately 47% of respondents selecting a frequency rating of 3 on the five-point scale, and a combined 27.7% selecting scores of 4 or 5. The remaining 25.2% selecting scores of 1 or 2 represent a comparatively low-depletion group, providing a useful contrast for evaluating fatigue-driven behavioral differences. Incidence was particularly concentrated within the student subgroup, consistent with the documented relationship between academic stress and cognitive depletion [4]. Notably, respondents identified as belonging to both student and employee categories displayed the highest brain fog

scores, suggesting that compound stressors — academic and occupational simultaneously — produce a compounding cognitive burden. This validates the presence of meaningful cognitive load variation within the sample and establishes the prerequisite for testing the study's central hypothesis.

4.2 Security fatigue / overwhelm

Responses regarding security task overwhelm showed a visible positive correspondence with brain fog scores. Approximately 41% of respondents rated security demands as moderately overwhelming (score 3), and over 40% selected the highest level of overwhelm (score 4 or 5), with only approximately 19% reporting low overwhelm (scores 1 or 2). This distribution suggests that cognitive depletion does not merely correlate with security fatigue — it actively amplifies the subjective burden of routine security tasks. When cognitive resources are depleted, even standard demands such as multi-factor authentication or password updates are perceived as disproportionately taxing. This supports the theoretical model wherein depleted cognitive resources inflate the perceived burden of security compliance, operationalizing the mediating role of security fatigue between cognitive state and behavioral outcomes.

4.3 Non-compliant behaviors

Habituation—clicking "Accept" or dismissing alerts without reading—was the most widely reported behavioral consequence, with roughly 73.6% of respondents selecting scores of 3 or higher when asked how often they do so when busy or tired. This pattern aligns with neurological evidence that warning attention deteriorates under sustained exposure [5].

Password reuse emerged as the single most consistent risky behavior across the entire dataset, with elevated scores distributed across both students and employees. While fatigue clearly exacerbates this practice, the data also indicate that a subset of respondents with low fatigue still reported frequent password reuse, suggesting convenience is an independent driver. This partial confirmation of the decision-fatigue pathway implies that password reuse is a default digital heuristic that fatigue intensifies but does not exclusively cause.

Workflow interference—delaying security updates due to productivity concerns—was slightly more prevalent among employees than students, reflecting the greater immediacy of occupational productivity pressures. When the cognitive cost of context-switching is high, security updates are perceived as interruptions rather than safeguards. These finding echoes workplace research documenting security as a perceived obstruction within deadline-driven environments [6, 7]. Notably, a separate indicator — perceived surveillance pressure from organizations or universities — returned predominantly low to moderate scores (1s, 2s, and 3s), suggesting that invasion of privacy is not a primary fatigue driver for this sample. Rather, fatigue stems from cognitive workload and task accumulation, not fear of monitoring — an important distinction for institutional policy design.

4.4 Fatalism and psychological resignation

Approximately 64% of respondents expressed at least moderate agreement with the belief that data breaches are inevitable regardless of personal effort, with students showing stronger fatalistic tendencies than employees. This distinction is meaningful: students, facing less institutional accountability than working professionals, are more susceptible to apathy when cognitive resources are strained. This psychological resignation represents the affective dimension of security fatigue — when cognitive resources are chronically depleted, users develop a sense of learned helplessness toward security outcomes. The resulting apathy lowers the motivational threshold for

compliance, creating a self-reinforcing cycle where fatigue breeds resignation and resignation deepens non-compliance [1].

4.5 The confidence–competence gap

A striking inconsistency emerged between self-assessed security knowledge and actual behavior. Over 70% of respondents rated their phishing-detection confidence at 4 or 5, yet the same individuals reported the highest frequencies of risky practices such as password reuse and warning dismissal. This gap between perceived competence and actual behavior indicates that awareness training, while valuable, is insufficient in isolation. Cognitive depletion functionally overrides existing knowledge under conditions of stress — users do not fail to recognize risk because they lack awareness, but because their depleted cognitive state prevents them from acting on it [11]. This finding has direct implications for cybersecurity training design: building knowledge without addressing cognitive sustainability will not translate into safer behavior.

4.6 Institutional support deficit

The vast majority of respondents — approximately 62% scoring 1 or 2 — reported that their institution provides inadequate support for managing digital stress. This finding underscores a systemic failure that directly sustains the fatigue cycle: without restorative interventions such as digital-detox policies, simplified security workflows, or mental health resources, brain fog persists unaddressed. Persistent brain fog amplifies security fatigue, which in turn drives non-compliant behaviors — creating a self-perpetuating loop that institutional neglect allows to continue unchecked. The data make clear that institutional security posture cannot be strengthened through technical enforcement alone; the human cognitive layer must be supported for compliance cultures to become genuinely resilient [11].

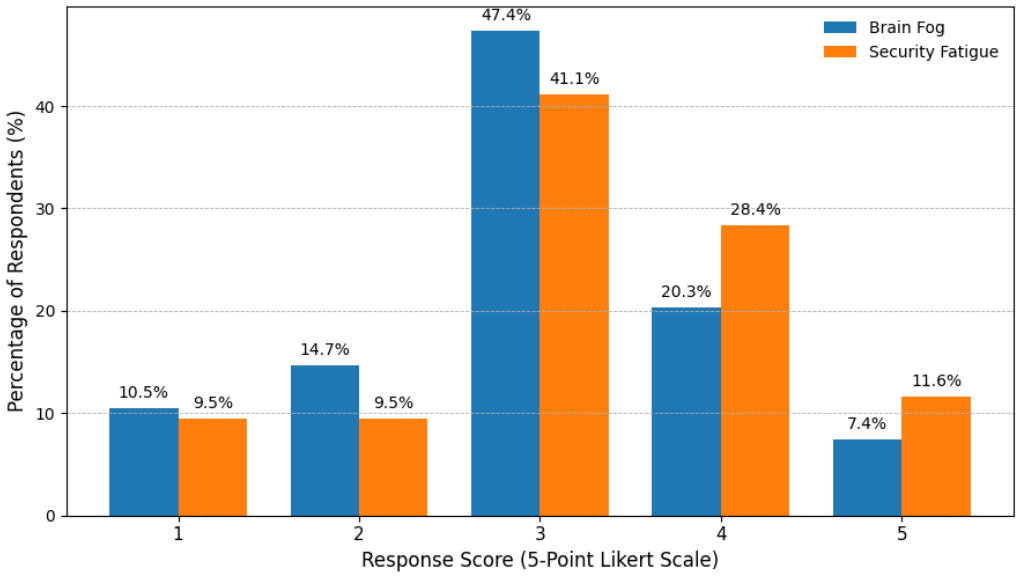

Figure 1: Distribution of brain fog and security fatigue ratings (n=95)

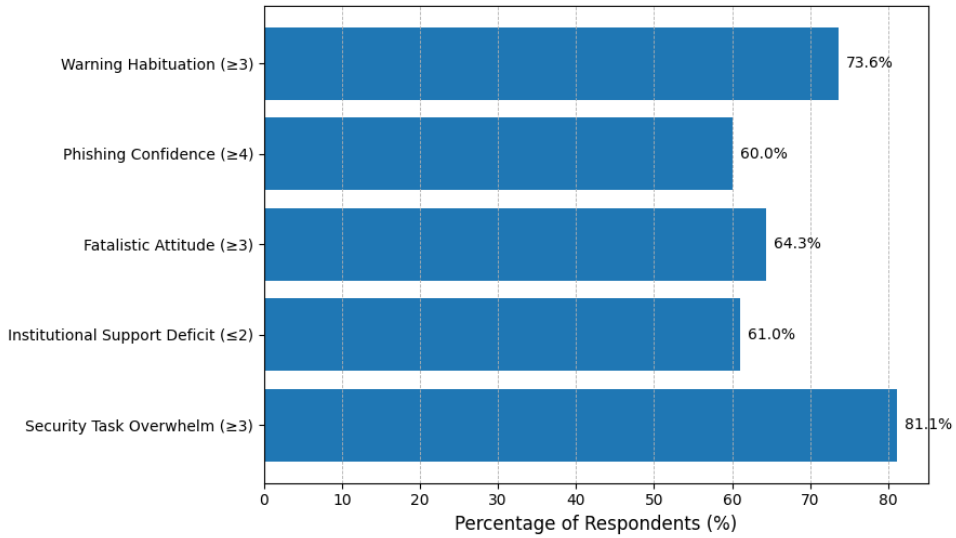

Figure 2: Prevalence of key risk indicators among respondents (n=95)

5. Hypothesis testing

Hypothesis 1: Relationship between brain fog and security fatigue

H_{01}: There is no significant relationship between brain fog and security fatigue among students and employees.

H_{11}: There is a significant relationship between brain fog and security fatigue among students and employees.

Result

The empirical findings indicate that higher levels of brain fog are consistently associated with higher levels of perceived security overwhelms across both students and employees. Respondents experiencing cognitive depletion reported greater difficulty managing security tasks and alerts. Therefore, H_{01} is rejected and H_{11} is accepted, confirming that cognitive depletion contributes significantly to security fatigue.

Hypothesis 2: Impact of security fatigue on cybersecurity behaviour

H_{02}: Security fatigue does not significantly influence non-compliant cybersecurity behaviors such as ignoring warnings or delaying updates.

H_{12}: Security fatigue significantly influences non-compliant cybersecurity behaviors such as ignoring warnings or delaying updates.

Result

Survey responses reveal that individuals who reported being busy or tired frequently clicked “Accept” or “Remind Me Later” on security prompts without carefully reviewing them. This pattern indicates that security overwhelm leads to habitual dismissal of warnings and reduced compliance with security protocols. Thus, H_{02} is rejected and H_{12} is accepted, demonstrating that security fatigue contributes to non-compliant cybersecurity behavior.

Hypothesis 3: Cognitive fatigue and password reuse

H_{03}: Cognitive fatigue does not significantly influence password reuse behavior.

H_{13}: Cognitive fatigue significantly increases password reuse behavior.

Result

The results indicate that security fatigue increases the likelihood of password reuse. However, password reuse

was also reported by some respondents with relatively low fatigue levels, suggesting that convenience and memorization challenges also play a role. Consequently, H_{03} is partially rejected, indicating partial support for H_{13}.

Hypothesis 4: Cognitive state and cybersecurity awareness

H_{04}: Cognitive state does not significantly influence cybersecurity behavior or override awareness of threats.

H_{14}: Cognitive state significantly influences cybersecurity behavior and can override awareness of threats.

Result

The analysis reveals a noticeable gap between respondents' confidence in identifying phishing attacks and their actual security practices. Many participants reported high confidence in detecting scams but still engaged in risky behaviors such as ignoring warnings or delaying updates. This confidence–competence gap suggests that cognitive overload can override security awareness. Therefore, H_{04} is rejected and H_{14} is accepted.

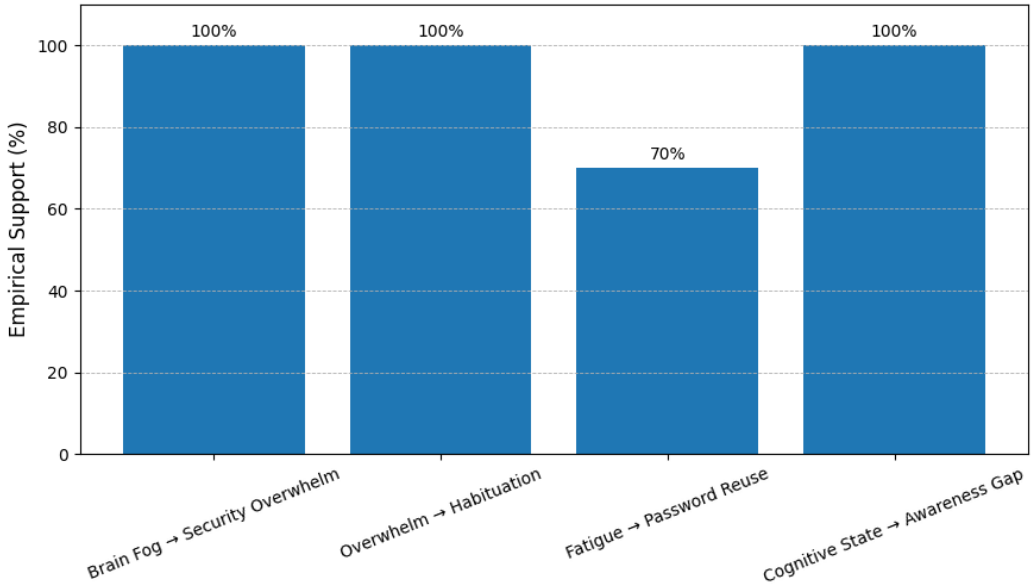

Figure 3: Hypothesis testing – Strength of pathway support

Conclusion

This investigation confirms that cybersecurity is as much a cognitive-psychological challenge as a technical one. The analysis of 95 participants establishes a robust empirical chain: academic and professional stressors generate brain fog, brain fog amplifies security fatigue, and security fatigue produces measurable non-compliant behaviors. The finding that high user confidence coexists with high behavioral risk is particularly significant—it challenges the prevailing emphasis on awareness training as the primary defense mechanism.

The study's implications are concrete. Organizations and universities must move beyond compliance mandates and address the cognitive sustainability of their security environments. Recommended interventions include streamlined authentication protocols that reduce extraneous cognitive load, dynamically varied security warnings to counteract habituation [5], scheduled digital-detox intervals embedded within work and study policies, and access to mental health resources that target stress-related cognitive impairment. Security architecture designed with human cognitive limits as a first-order constraint will produce more resilient compliance cultures than systems that simply demand more from already-depleted users.

Limitations

Several methodological constraints warrant acknowledgment. First, reliance on self-reported data introduces social desirability bias: respondents may under-report risky behaviors to appear more security-responsible [9]. Second, the cross-sectional design identifies correlational rather than causal relationships; longitudinal studies are required to establish temporal directionality [11]. Third, behavioral measures were based on hypothetical self-assessments rather than observed actions, limiting ecological validity [5]. Fourth, the convenience sample drawn from a single academic environment may not generalize to sector-specific populations such as healthcare or finance, where regulatory pressures generate distinct fatigue profiles [2, 3]. Finally, all fatigue metrics were subjective; future research would benefit from physiological corroboration through biometric or neuroimaging measures [5].

References

1. Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security fatigue. *IT Professional, 18*(5), 26–32.
2. Hatashima, T., Tanimoto, S., & Kanai, A. (2025). Security Fatigue Scale (SFS-18) and its reliability and validity. *Computers & Security*. Advance online publication.
3. Yılmaz, K., Alpar, Ş. E., & Yavuz, D. E. (2025). Brain fog and affecting factors in health care workers. *European Journal of Life Sciences, 4*(3), 184–192.
4. Malik, I., & Malik, A. (2025). Decision fatigue and cybersecurity behaviors: A qualitative study of university students. *Journal of Information Systems Engineering and Management, 10*(58s), 441–456.
5. Vance, A., Jenkins, J. L., Anderson, B. B., Bjornn, D. K., & Kirwan, C. B. (2018). Tuning out security warnings: A longitudinal examination of habituation through fMRI, eye tracking, and field experiments. *MIS Quarterly, 42*(2), 355–380.
6. Lee, S. C. (2024). Stress implications of compliance with information security policies. *Issues in Information Systems, 25*(1), 42–57.
7. Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *Holistica – Journal of Business and Public Administration, 13*(1), 49–72.
8. Li, L., Shen, Y., & Han, M. (2021). Perceptions of information systems security compliance: An empirical study in higher education setting. In *Proceedings of the 54th Hawaii International Conference on System Sciences* (pp. 6226–6231).
9. Sonali, S., & Shenoy, S. (2025). Voices from within: Analyzing employee perceptions of service quality in the Indian healthcare sector. *International Journal of Basic and Applied Sciences, 14*(6), 435–443.
10. Nobles, C. (2025). Exploring mitigative strategies to prevent burnout in cybersecurity (pp. 283–320).
11. Mizrak, F., Demirel, H. G., Yaşar, O., & Karakaya, T. (2025). Digital detox: Exploring the impact of cybersecurity fatigue on employee productivity and mental health. *Discover Mental Health, 5*, 25.