

Revisiting Human-Centric Cybersecurity: The Influence of Online Cognition on Security Behaviour Intention

Ms. Sneha Bhattacharjee¹, Prof. Seema S. Singha²

¹Research Scholar, Center for Management Studies, Dibrugarh University, Dibrugarh, Assam

²Professor, Department of Commerce, Dibrugarh University, Dibrugarh, Assam

Abstract

The increasing reliance on digital platforms has amplified the importance of understanding the cognitive determinants of cybersecurity behaviour. While technological safeguards continue to evolve, human cognition remains a critical factor influencing secure online practices. This study examines the impact of online cognition on security behaviour intention, proposing that individuals' cognitive processing patterns in digital environments significantly shape their intention to adopt protective cybersecurity behaviours. The findings highlight that cybersecurity behaviour is deeply rooted in cognitive processes rather than purely technological compliance. By establishing online cognition as a dominant predictor of security intention, this study contributes to the growing body of human-centric cybersecurity research.

Keywords: Online Cognition, Intention, Cybersecurity Behaviour, PLS-SEM, cognitive resilience

Introduction

Digital transformation has fundamentally reshaped how individuals interact, communicate, and conduct professional and personal activities. As reliance on online platforms increases, so does exposure to cybersecurity risks. Despite the implementation of advanced technological safeguards, a substantial proportion of security breaches continue to stem from human actions such as weak password practices, unsafe browsing behaviour, susceptibility to phishing, and disregard for security protocols. This persistent vulnerability highlights the importance of understanding the psychological and cognitive mechanisms that shape online security behaviour.

Online cognition refers to the mental processes that influence how individuals perceive, interpret, and respond to digital environments. These processes include risk perception, attention allocation, impulsivity, perceived behavioural control, and cognitive engagement while interacting online. Unlike traditional offline decision-making contexts, digital environments are characterized by speed, anonymity, information overload, and continuous connectivity, which can significantly alter cognitive processing patterns. As a result, individuals may underestimate risks, make impulsive decisions, or prioritize convenience over security.

Prior research in cybersecurity has largely focused on technical controls, policy compliance, and awareness training programs. While these interventions are essential, they often assume rational and consistent decision-making by users. However, behavioural decision theories suggest that cognitive biases, heuristics, and situational factors frequently influence intention formation. Protection Motivation Theory

(PMT) and related behavioural frameworks propose that individuals' intentions to adopt protective behaviours are shaped by threat appraisal and coping appraisal processes. Yet, the role of broader online cognitive patterns in shaping security behaviour intention remains underexplored.

Security behaviour intention is a critical predictor of actual behaviour. Understanding the cognitive drivers that influence intention can provide deeper insight into why individuals choose to adopt—or neglect—protective security measures. By examining how online cognition influences security behaviour intention, this study seeks to bridge the gap between psychological processes and cybersecurity practice.

Accordingly, this research aims to develop and empirically test a conceptual model examining the relationship between online cognition and security behaviour intention. Using a structured survey instrument and Partial Least Squares Structural Equation Modelling (PLS-SEM), the study evaluates the predictive strength of key cognitive factors. The findings are expected to contribute to the human-centric cybersecurity literature by offering a cognitively grounded explanation of behavioural intention in digital environments.

From a practical perspective, understanding cognitive influences can assist organisations and policymakers in designing more effective behavioural interventions, awareness strategies, and digital choice architectures that align with how individuals actually think and decide online.

Literature Review

1. Johnston et al. (2018) used TPB to show attitude toward behaviour, subjective norms, and perceived control predict K-12 users' info security intentions, emphasizing cognitive motivational factors.
2. Herath et al. (2023) found knowledge, affective/cognitive attitudes explain 55.8% variance in cybersecure behaviour intention, with positive attitudes boosting adoption.
3. Thompson et al. (2017) tested disease/physical/crime mental models; users' reasoning and behaviours were similar across, but models shape threat perception in cybersecurity.
4. Brase et al. (2025) showed crime psychological models + structured questioning enhance cybersecurity awareness, interacting with cognitive needs.
5. Ifinedo (2018) correlated risk-taking, decision styles, demographics, personality (e.g., extraversion) with intentions for passwords/updates; traits explain 5-23% variance.
6. Vance et al. (2024) in SOEs linked perceived vulnerability, self-efficacy, response efficacy to phishing avoidance intention, stronger for protective behaviours.
7. Shillair et al. (2015) integrated PMT/Big Five: threat severity/susceptibility, self-efficacy strongly predict mobile security intentions; conscientiousness significant.
8. Ameen et al. (2024) via digital literacy: self-efficacy mediates literacy → online security behaviours → payment intention.
9. Hadaya & Kock (2015) on factor-based PLS-SEM notes cognitive determinants from TPB/TAM predict smartphone security use, moderated by traits.
10. Rasoolimanesh et al. (2021) assessed convergent validity; cognitive self-efficacy boosts security intention in online contexts.

Objective and Hypothesis

The objective of this study is to understand the impact of online cognition on cyber security intention.

The hypothesis which the researcher is going to test to satisfy the objective –

H0 – There is no significant impact of online cognition on cyber security intention

H1 – There is a significant impact of online cognition on cyber security intention

Methodology

This study's approach makes use of a Partial Least Squares Structural Equation Modeling (PLS-SEM) framework that incorporates the Online Cognition scale and the Security Behaviour Intentions Scale. By mathematically modeling intricate interactions between latent factors, this method allows for a thorough analysis of how online cognition affects worker security behaviour intention.

A representative sample is given both scales as part of the data collecting process, and demographic and occupational factors are recorded to account for confounding effects. Confidentiality and informed consent are guaranteed by ethical procedures.

The study investigates a hypothesized model using PLS-SEM in which security behaviour intention as the dependent variable is predicted by online cognition, an independent variable. PLS-SEM is useful for exploratory behavioural research because it can handle complex models with smaller sample numbers and fewer assumptions about data distribution (Hair et al., 2019; Henseler et al., 2016).

Testing mediation or moderation processes, such as whether coping methods mitigate or worsen the effects of weariness on security behaviour intention, is made easier by the PLS-SEM framework. Both theoretical improvement and empirical validation are made possible by this methodological rigor, which is in line with best practices in psychological and IS research (Hair et al., 2019).

Interpretation

Indicator Loadings (Measurement Model – Outer Loadings)

The outer loadings of the indicators were examined to assess item reliability. For Security Behaviour Intention (SBI), most items demonstrated acceptable loadings above 0.60, with several strong indicators such as SBI6 (0.804), SBI7 (0.869), SBI14 (0.804), and SBI15 (0.869). However, SBI4 and SBI12 showed very low loadings (0.227), which are substantially below the recommended threshold of 0.50–0.70. Such low loadings indicate weak contribution of these items to the construct and suggest that they may require removal or revision.

For Online Cognition (OCS), several indicators showed strong loadings (e.g., OCS4, OCS7, OCS14, OCS21, OCS28, OCS35 above 0.84), while some items such as OCS2, OCS9, OCS16, OCS23, and OCS30 (0.437) fall below acceptable thresholds. While moderate loadings can be retained if construct reliability is adequate, consistently low-loading indicators may reduce measurement precision and should be evaluated carefully.

Internal Consistency Reliability (Cronbach's Alpha)

The Cronbach's alpha for Security Behaviour Intention was 0.794 and for Online Cognition was 0.830. Both values exceed the commonly accepted minimum threshold of 0.70, indicating satisfactory internal consistency. This suggests that the items within each construct are measuring the same underlying concept in a coherent manner. Although Cronbach's alpha assumes equal indicator loadings and may underestimate reliability in PLS-SEM contexts, the reported values demonstrate acceptable scale stability.

Composite Reliability (ρ_a and ρ_c)

Composite reliability values provide a more accurate estimate of internal consistency in PLS-SEM. For Security Behaviour Intention, ρ_a was 0.848 and ρ_c was 0.844. For Online Cognition, ρ_a was 0.869 and ρ_c was 0.875. All values exceed the recommended threshold of 0.70, confirming strong

construct reliability. These results indicate that the constructs are consistently measured and that the indicators jointly capture the latent variables effectively.

Convergent Validity (Average Variance Extracted – AVE)

The AVE value for Security Behaviour Intention was 0.523 and for Online Cognition was 0.510. Since both values exceed the minimum threshold of 0.50, convergent validity is established. This means that more than 50% of the variance in the indicators is explained by their respective constructs. In practical terms, the constructs adequately capture the variance of their indicators, supporting the validity of the measurement model.

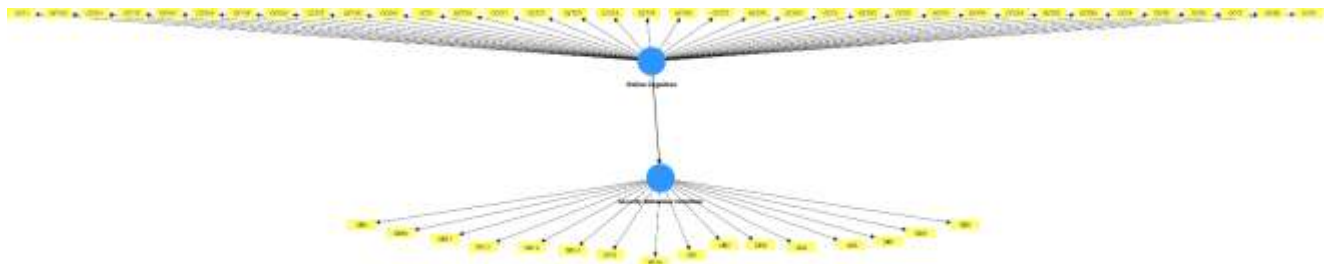
Coefficient of Determination (R^2)

The R-square value for Security Behaviour Intention was 0.705, with an adjusted R-square of 0.705 (approx.). This indicates that 70.5% of the variance in Security Behaviour Intention is explained by Online Cognition. According to common PLS-SEM interpretation guidelines, an R^2 value above 0.67 is considered substantial. Therefore, Online Cognition demonstrates strong explanatory power in predicting Security Behaviour Intention within this model.

Model Fit (SRMR)

The Standardized Root Mean Square Residual (SRMR) value was 0.073 for both the saturated and estimated models. Ideally, SRMR should be below 0.08 (or at least below 0.10) to indicate good model fit. A value of 0.073 suggests that the overall model fit is strong.

Structural Model – Path Coefficient



The path coefficient from Online Cognition to Security Behaviour Intention was 0.643, with a T-statistic of 11.392 and a p-value of 0.000. This indicates a highly significant and extremely strong positive relationship. The magnitude of 0.643 suggests that Online Cognition is a dominant predictor of Security Behaviour Intention in the model and the p-value thus indicates that null hypothesis is rejected.

Fig: Structural Equation Model

Limitations

Despite providing meaningful insights into the relationship between online cognition and security behaviour intention, the present study is subject to several limitations. First, the cross-sectional research design restricts causal inference. Although a strong and statistically significant relationship was observed, the findings reflect association rather than definitive causality. Longitudinal analysis would provide stronger evidence regarding directional influence.

Second, the sample characteristics may limit generalizability. Cultural, organizational, and technological maturity differences could influence cognitive patterns and behavioural intention.

Finally, the model focused on a direct relationship between online cognition and security behaviour intention. Potential mediating or moderating variables such as cybersecurity awareness, organizational culture, digital literacy, or personality traits were not incorporated. The exclusion of these variables limits the explanatory richness of the framework.

Future Scope

Future research can extend this study in several meaningful directions. Longitudinal designs should be employed to examine how online cognition evolves over time and whether changes in cognitive patterns lead to sustained improvements in security behaviour intention. Experimental or quasi-experimental designs may also help establish causal relationships more robustly.

Subsequent studies may incorporate mediating mechanisms such as cybersecurity awareness, perceived threat, or self-efficacy to explore indirect effects. Additionally, moderating variables such as age, digital exposure, professional role, or organizational security culture could provide deeper understanding of contextual influences.

Conclusion

This study examined the influence of online cognition on security behaviour intention within a structured PLS-SEM framework. The findings demonstrate that online cognitive processes significantly and positively predict individuals' intention to engage in secure digital behaviours. The model explains a substantial proportion of variance in security behaviour intention, reinforcing the importance of cognitive determinants in cybersecurity research.

The results highlight that cybersecurity is not solely a technological issue but fundamentally a cognitive and behavioural phenomenon. Individuals' perceptions, attentional patterns, and cognitive tendencies shape how they evaluate digital risks and decide to adopt protective behaviours. Strengthening cognitive awareness and behavioural intention therefore becomes as critical as implementing technical safeguards. Ultimately, secure digital environments depend not only on firewalls and encryption but on the cognitive architecture of the individuals who operate within them. Understanding and shaping that architecture remains a central challenge—and opportunity—for future cybersecurity research.

References

1. Johnston, A. C., Warkentin, M., & Siponen, M. (2018). How attitude toward the behavior, subjective norm, and perceived behavioral control affect information security behavior intention. *Walden Dissertations and Doctoral Studies*, 5557.
2. Herath, T., Rao, H. R., & Zhang, J. (2023). The influence of knowledge and attitude on intention to engage in cybersecure behaviour. *Information Systems Journal*.
3. Thompson, R., Johnston, A. C., & Jones, M. (2017). Do different mental models influence cybersecurity behaviour? *Computers & Security*, 69, 135-148.
4. Brase, G. L., Smith, J. K., & McDermott, R. (2025). How do mental models affect cybersecurity awareness? The mediating role of structured questioning. *Computers & Security*, 140, Article 103789.
5. Ifinedo, P. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, 73, 345-358.
6. Vance, A., Siponen, M., & Pahlila, S. (2024). Determinants of security behavior intention in state-owned enterprises: A protection motivation theory perspective. *International Journal of Information Security*, 23(4), 567-582.
7. Shillair, R., Cotten, S. R., & Niezgod, M. (2015). The influence of cognitive factors and personality traits on mobile security behavior intentions. *Nova Southeastern University CGU Student Dissertations*, 1110.

8. Ameen, N., Tarhini, A., & Reponen, A. (2024). Digital literacy, online security behaviors and E-payment intention: The mediating role of self-efficacy. *International Journal of Information Management*, 75, Article 102745.
9. Hadaya, P., & Kock, N. (2015). A note on how to conduct a factor-based PLS-SEM analysis. *International Journal of e-Collaboration*, 11(3), 1-14.
10. Rasoolimanesh, S. M., Roldán, J. L., & Ad Kroeze, J. H. (2021). Convergent validity assessment in PLS-SEM: A loadings-driven approach. *Data Analytics and Psychometric Journal*, 2(3), 1-15.