

# **Examining the Efficacy of Security Alerts: User Perception and Response**

**Early stage paper**

**Lakshika Vaishnav**  
University at Albany, SUNY  
lvaishnav@albany.edu

**Sanjay Goel**  
University at Albany, SUNY  
goel@albany.edu

## **ABSTRACT**

Users are significantly impacted by unconscious cognitive processes and automatic responses in security contexts. System-generated alerts are ubiquitous in personal computing, providing timely information but at the cost of increased stress and decreased productivity. This study investigates the interplay between multitasking, cognitive overload, attention deficits, and security errors, incorporating insights from psychology and human-computer interaction. As cognitive load and multitasking increase, users' ability to perform tasks accurately diminishes, leading to more errors and slips in security tasks. The research examines how cue utilization and cognitive load affect decision-making when responding to security alerts, using eye tracking and participant surveys to identify the cues relied upon. This research contributes to understanding the cognitive and psychological factors that influence security behaviors, offering insights for developing effective interventions to improve security task performance.

## ***Keywords***

Security Alert, Cognitive load, Security errors, Attention

## **INTRODUCTION**

Users have long been recognized as the weakest link in security. Accordingly, researchers have applied knowledge from the fields of psychology and human–computer interaction to understand the security behaviors of users. However, many cognitive processes and responses are unconscious or obligatory and yet still have a profound effect on users’ security behaviors. As their cognitive load increases and they multitask more, their ability to perform tasks accurately diminishes, resulting in increased errors and slips, for instance, in security tasks.

In a study by Hilburn (2004) discusses the concept of attention in the context of air traffic control (ATC) and cognitive complexity, particularly focusing on how attention resources are allocated and the implications for controller workload and performance. It highlights the importance of attention in managing the high cognitive demands faced by air traffic controllers, who must maintain situational awareness and make critical decisions in a complex, dynamic environment (Hilburn, 2004). Attentional costs, such as cognitive overload, can lead to attention and failures (Imbert et al., 2015). There are always some decisions that must be made eventually by users, and one type of unavoidable decision is the choice to take a risk that some users may take while others may reject (Bravo-Lillo et al., 2013).

In this study, we aim to examine how cue utilization and cognitive load affects decision making of users while they respond to security alerts. By using eye trackers and surveying the participants to understand what cues they relied on while making the decision we can start to understand the role of cognitive load on security behavior. We also examine whether training and expertise in security would reduce errors and slips while dealing with security alerts/tasks.

Research Objectives:

1. To understand the influence of cognitive load on slips and mistakes (security errors) in security tasks
2. The impact of mediating impact of attention between cognitive load and security behavior
3. To assess the impact of knowledge and experience on reduction in slips and mistakes

## **REVIEW OF LITERATURE**

### **Cognitive Load**

The human cognitive system, while remarkably adaptable and powerful, has inherent limitations that become particularly evident during multitasking. One such limitation is the brain's capacity to switch attention effectively between multiple tasks that are being attempted simultaneously (Nobles, 2022; Muke, 2022), this cognitive bottleneck occurs because the brain must rapidly redistribute its resources and focus, which can lead to a decrease in overall efficiency and performance (Pashler, 1994). The literature on cognitive psychology demonstrated evidence of an operative condition, as in the case of 'Air Traffic Controllers' that demands multitasking; this state can lead the user to the state of overload that could likely contribute to occurrences of errors (Arico et al., 2017).

When an individual tries to juggle several tasks at once, each task competes for the brain's limited attentional resources (Pashler, 1994; Zubak, 2008). Research by Jeffrey L. Jenkins et al. (2016) examines the impact of interruptive security messages on productivity and user behavior, revealing that such interruptions often lead to dual-task interference (DTI). This interference diminishes cognitive processing, increases stress, and reduces productivity, causing users to ignore crucial security alerts. Reduced brain activation in memory and control areas correlates with this disregard, heightening vulnerability to security threats (Jenkins et al., 2016). Cognitive skills affect an individual's judgment and decision-making (de Jong, 2010; Kolfschoten et al., 2014; Pfleeger

& Caputo, 2012). In a study by Bravo-Lillo et al. (2011) highlights ignorance of security warnings by users that have limited cognitive ability to switch between tasks (Bravo-Lillo C et al., 2011). Typically, people do not notice tasks interfering with each other unless both tasks are cognitively challenging, physically conflicting, or emotionally charged (Kolfschoten et al., 2014). However, the opposite of this perception is true; even when engaged in simple cognitive tasks, people struggle to effectively process information or carry out activities related to other tasks (Jenkins et al., 2016).

Employees aware of company policies are better at managing cybersecurity (Li et al., 2019) and security behavior (Anderson, C. L., & Agarwal, R. 2010). The study by Li et al., (2019) highlights awareness and knowledge of ‘cybersecurity affects cybersecurity behavior’ (Li et al., 2019). In terms of security behavior, when people are under time pressure or distracted, they are less able to engage in systematic processing and are more likely to rely on heuristic processing, making them more susceptible to phishing attacks (Luo et al., 2012; Pfleeger & Caputo 2012). High security-related stress can increase cognitive load, leading to negative emotions like frustration and fatigue (Nobles, 2022; D’Arcy et al., 2014). In a study by D’Arcy (2019), authors highlight that cognitive burden can impair an employee's ability to process information and make sound decisions, making them more likely to rationalize and engage in actions that compromise security policies (D’Arcy et al., 2019). They might take shortcuts or disregard security protocols to alleviate the perceived cognitive overload (Kim et al., 2024; D’Arcy et al., 2014). Studies have explored specific attention-related challenges, the difficulty of maintaining focus over long periods, and the need to rapidly shift attention between different tasks and information sources (Hilburn, 2004; Imbert et al., 2014; Murphy et al., 2016).

The NASA Task Load Index (NASA-TLX) is a widely recognized method for assessing subjective workload, utilizing six subscales: mental demand, physical demand, temporal demand, performance, effort, and frustration level, to calculate an overall workload score (Cao et al., 2009; NASA Task Load Index, 2005; Muke, 2022). Although this tool offers a quick estimation of an operator's mental workload, the process of weighting each subscale can be cumbersome and time-consuming (NASA Task Load Index, 2005). Moreover, the administration method of the NASA-TLX, such as via a computer screen, may influence the perceived cognitive workload, potentially resulting in higher reported levels of cognitive load (NASA-TLX - Wikipedia, 2010). Need for cognition scale developed by Cacioppo, 1984 measures individuals' motivation to think and engage in cognitive activities and it found that cognitive ability and performance on cognitive tasks are positively correlated (Cacioppo et al., 1984). Petty et al, 2009 concluded 'Need for cognition scale' as a stable and reliable trait that influences a variety of cognitive and social processes (Petty et al., 2009).

## **Security Behavior in Organization**

Human security behavior plays an important role in security, as 50% of cybersecurity incidents are tracked to be non-malicious actions of non-technical professionals (PwC, 2018). Non-secure behavior creates vulnerabilities in the existing systems and undermines cybersecurity overall. Wang et al., (2012) in her study emphasize the nature of a workplace where employees are under the strain of working to deadlines and multi-tasking to reach the aim of completing multiple projects and this additional strain is considered a negative factor on information processing that impacts judgments and decision making (Wang et al., 2012). In a study by Tally, (2023) discusses that trainings are insufficient to stop the massive increase in cyber-attacks on an organization, author used snow ball sampling approach by targeting employee's and corporations that allowed

to capture behavior and opinions of the employees at workplace and responses were recorded using questionnaire, unfortunately workers depended on twitter, colleagues and podcast as an information source for anti-phishing learning and less than 21% of participants really did had any formal anti phishing trainings (Tally, 2023).

Security behavior in organizations comes under a field known as ‘Behavioral InfoSec’ research (Crossler et al., 2013), this field of research focuses on behavior of individuals which relate to protecting information system and its assets including computer hardware, organizational information, and networking infrastructure (Stanton et al., 2006). Authors have used Theory of Diversity for Protection-Motivated Behaviors" by Posey et al. (2013), that explores the protective actions that organization insiders can take to safeguard organizational information assets. Anderson et al., (2010) explores a multimethod approach, integrating surveys and experiments to explore the factors influencing users’ intentions to engage in security behaviors, authors use ‘Protection Motivation Theory ‘considering social influences and psychological ownership (Anderson et al., 2010).

Information security messages tailored to specific employee groups, based on their organizational identification, are more effective. Johnston et al., 2018 used ‘Fear Appeal Theory’ and ‘Organizational Identification Theory’ to design fear appeals tailored to resonate with specific employee groups based on their organizational identification. This approach aimed to enhance message processing and ultimately improve employees' information security decision-making (Johnston et al., 2018). Anderson et al., (2010) examines how mix of cognitive, social and psychological factors can be influenced by specific messaging to enhance security behaviors intentions (Anderson et al., 2010).

## **Errors and Mistakes**

Safety and security research on human error remains crucial across various industries (Le Coze, 2022). Errors are unintentional deviations from goals or tasks (Hofmann & Frese, 2011; Frese & Keith, 2015). While software and hardware have become more reliable over time, system management relying on human operation contributes significantly to system unreliability—over 50% of system crashes result from mismanagement (Nobles, 2022).

Frese et al. (2015) differentiate risks from errors: Risks are inherent in the environment, whereas errors occur during an individual's interaction with that environment. Active failures, such as slips, lapses, and mistakes, play a role. Slips and lapses involve unintentionally incorrect plan execution, while mistakes stem from inadequately following a plan (Frese et al., 2015).

The error management theory explores how humans make decisions under uncertainty (Seixas et al., 2023). Additionally, humans exhibit a cognitive bias—preferring safety over risk—making them susceptible to errors (Seixas et al., 2023; Le et al., 2022; Hofmann & Frese, 2011; Frese & Keith, 2015; Nobles, 2022; Reason, 2000). The report "Flightpath 2050 Vision on Human Factors" states that human errors can be significantly reduced by implementing innovative designs, training programs, and technologies that aid decision-making (Arico et al., 2017), but at the same time, when the mental workload increases, it becomes harder to maintain user's task performance within an acceptable range, that results in the increase of error's occurrences.

## **Attention and Decision Making**

Information processing theory provides a foundational framework for human decision-making that also includes decision-making through interactions with the task environment (Chowdhury et al., 2020). Luo et al. (2012) highlight the use of a Heuristic-systematic model for information

processing to explain how individuals make decisions when confronted with phishing attempts (Luo et al. 2012). Frederick (2005) shows a relationship between cognitive ability and decision-making and explores its context in preferences to time and risk; he uses cognitive reflection test scores and shows a positive correlation between CRT and decision making with time and risks (Frederick, 2005). The design and timing of security warnings significantly affect user attention and adherence (Zaaba et al., 2024).

A study by Adrienne Porter Felt et al., (2012) revealed that only a small percentage of users (17%) pay attention to permissions during app installation, and even fewer (3%) fully understand the permissions they encounter (Adrienne Porter Felt et al., 2012). Dzubak (2008) explores the neurological aspects of multitasking, noting that different parts of the brain are activated for different types of tasks (e.g., declarative vs. procedural memory tasks). The implications of multitasking on learning and memory retention are significant, with divided attention shown to reduce the effectiveness of encoding information, thereby impairing learning outcomes (Dzubak, 2008; Klingberg 2009). Hilburn (2004) discusses the limits of human attention capacity and how exceeding these limits can lead to decreased performance and increased errors in Air traffic controllers operations.

## **Novice and Advanced Users**

In the study by Arianezhad et al. (2013), investigated how experts and novices use single sign-on (SSO) systems on websites. By employing eye-tracking technology, they observed where users focused while performing SSO tasks and analyzed differences in perceiving security indicators. Participants also completed a survey on their computer skills, understanding of SSO, and online habits (Arianezhad et al. 2013). In a study by Zaaba et al., (2024) they conduct an experiment comparing effectiveness of different presentation styles of security warnings to novice and



advanced users and the experiment assessed how each user group's attention and comprehension are impacted by variations in the visual and textual content of the warnings (Zaaba et al., 2024).

A study by Breve, B. et al. (2023) explores the mental models of cybersecurity experts and novices, mental models include beliefs, assumptions and expectations of an individual on how the things work, additionally they highlights to design 'Task Automation Systems' that are effective for both types of users to protect their smart environment from security and privacy threats (Breve, B. et al., 2023). A study by Bravo-Lillo et al., (2011) also introduced the concept of mental model on assessing security warnings by novice and advanced users (Bravo-Lillo et al., 2011). These authors also proposed design changes that will be able to help end users to make better decisions in security alerts related decisions (Breve, B. et al., 2023; Bravo-Lillo et al., 2011; Raja et al., 2011)

## **Security Warnings**

Security warnings and alerts are critical in preventing security attacks, intersecting human cognition, psychology, and cybersecurity. Notably, the Theory of Planned Behavior is instrumental in predicting both the intentions and actual behaviors of users regarding security, as it accounts for intentions influenced by the user's control over their actions (Sommestad, T et al., 2015). However, challenges like information overload can significantly impair decision-making (Andrade & Yoo, 2019), and this effect is similarly observed in high-stress environments such as the US Air Force or air traffic control, where high cognitive skills are crucial (Dykstra, 2021).

Research shows that understanding and responding to security warnings often pose difficulties for end-users, particularly when cognitive load is high. For instance, Zaaba et al. (2014) highlighted differences in how novices and advanced users perceive and respond to security alerts, noting the duration of gaze fixation as an indicator of attention. Additionally, a study incorporating

neurosecurity approaches used electroencephalography (EEG) to explore how biological factors like gender and color perception influence responses to security warnings, revealing that traditional methods may not always effectively capture user attention (Anderson et al., 2015).

Moreover, evidence from Vance et al. (2018) supports the use of polymorphic warnings—those that vary in appearance—to mitigate habituation effects, thereby maintaining the effectiveness of warnings in real-world applications. This body of research underscores the complexity of designing effective security warnings that must account for psychological, physiological, and behavioral factors in varying operational contexts.

## **Gap in Literature**

Despite extensive research on multitasking, task interruptions, and user behavior in organizational settings, there remains a specific gap in understanding how users' attention varies among different cognitive loads, measured by eye-tracking data, varies between users when responding to security alerts. Prior studies, such as Sobey et al. (2008), have demonstrated that expert users are more proficient at identifying security indicators within web browsers. Conversely, Jagatic et al. (2007) found that students from technical fields were significantly less likely to fall for phishing emails compared to their non-technical counterparts. These findings highlight differences in user behavior based on expertise; however, there is limited research integrating Cognitive Load Theory (CLT) and Treisman's Attention Model to explore how cognitive load influences attention to security alerts among different user groups. Specifically, there is a gap in our understanding of how cognitive load impacts the processing, filtering, and retention of information related to security alerts, particularly when comparing users with varying expertise and security awareness levels. Addressing this gap could enhance our understanding of security behavior across different user profiles and lead to more effective security interventions tailored to user expertise levels.

## **THEORY**

Cognitive Load Theory is a model of information processing that describes memory as having three main components, i.e., sensory, working, and long-term. Sensory memory filters out most of what is happening around us; working memory has limits to what it can simultaneously process (5-9 items) and categorizes information for storage in long term memory. Long-term memory stores information in structures called “schemas,” which organize information based on how we use it. The more we use these schemas, the more developed they become and the easier it is to recall them. Cognitive load refers to the amount of information our working memory can process at any given time and for workers, cognitive load theory helps us understand the limits of their multitasking. There are always many stimuli around us and the attention that the workers provide to any one task limited. When most people think of multitasking, they imagine themselves effectively juggling several tasks simultaneously. However, what they're often doing is not genuine simultaneous multitasking but rather "task-switching." This is a rapid shifting of attention from one task to another and back again. This can lead to increased cognitive load that can lead to lack of attention and lead to errors and mistakes while making a decision to respond to security alert.

Workers are continuously multitasking; one of the practical applications of studying attention is our understanding of how multitasking works. Treisman’s Attenuation Model (1964): Treisman’s Attenuation Model emphasizes that unattended information isn’t entirely filtered out but rather weakened. It provides a more nuanced view of allocating attention to relevant stimuli. Consequently, they are still processing information from multiple tasks simultaneously even if they are switching tasks.

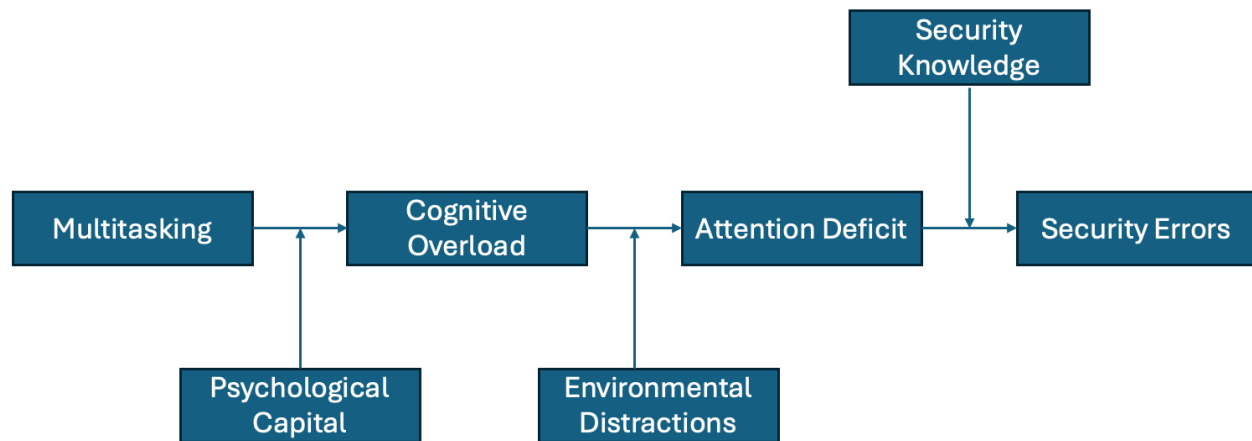
Cognitive overload occurs when the combination of intrinsic, extraneous, and germane loads becomes overwhelming for the worker, and they are not able to process so much information at

once. When overwhelmed, they may struggle to process new information or make appropriate security decisions. They may make mistakes at a task that should be manageable, given their knowledge and expertise.

Attention is based on two specific concepts: 1) as a filter of specific attention that allows channels of information from the environment to be processed and 2) as a resource to enable subsequent information processing while managing the collective demands of multiple tasks that need to be performed concurrently which limits the level of multitasking that an individual can engage in. As the level of multitasking increases and the cognitive load increases the users may no longer have to ability to engage in security tasks that can be suddenly imposed in the middle of multitasking leading to errors and slips.

Users that have more substantial knowledge and awareness of security behavior can influence how they process incoming sensory information. This knowledge allows them to effectively utilize cues and manage cognitive load, which helps in filtering and prioritizing information efficiently. Lack of security knowledge and awareness might hinder user's ability to effectively filter or prioritize sensory information and consequently they make more errors and slips.

Our nomological model leverages cognitive load theory and attention with moderating effects of psychological capital, environmental distractions, and security knowledge as shown in Figure 1.



**Figure 1: Nomological model of cognitive load and attention link for security errors**

The model illustrates how multitasking and environmental distractions contribute to cognitive overload, leading to attention deficits and ultimately resulting in security errors. Multitasking strains cognitive resources, causing overload, while environmental distractions exacerbate this condition by adding additional information to the process. Cognitive overload results in attention deficits, which increase the likelihood of security errors. Psychological capital refers to detrimental psychological states; psychological capital, characterized by self-efficacy, optimism, hope, and resilience, can mitigate the negative effects of multitasking on cognitive overload by providing better-coping mechanisms. At the same time, Negative psychological capital states such as low self-efficacy, pessimism, despair, and lack of resilience; individuals with low self-efficacy may feel less capable of managing multitasking and cognitive overload, leading to increased stress and a higher likelihood of attention deficits and security errors. Pessimism, characterized by a tendency to expect negative outcomes, can exacerbate cognitive overload, and reduce the ability to mitigate attention deficits effectively (Luthans & Morgan, 2017). Despair, a sense of hopelessness, impairs motivation and coping mechanisms, further increasing the risk of security errors.

Meanwhile, security knowledge moderates the impact of attention deficits on security errors, as individuals with higher security awareness are better equipped to handle lapses in attention and reduce errors. Thus, the model highlights the intricate interplay between cognitive demands, environmental factors, psychological resources, and knowledge in shaping security-related behaviors.

To explore how cognitive load and cue utilization impact user decision-making within Treisman's Attention Model framework. The study aims to understand the differences in attentional processes between novice and advanced users, with a specific focus on how multitasking influences these processes. Treisman's Attention Model describes how attention filters and processes information through several stages: the sensory store, attenuator, dictionary unit, and working memory.

### Hypothesis

H1: Users with knowledge of security behavior and higher cue utilization would make better decisions while responding to security alerts.

H2: While multitasking, if the user has less knowledge about responding to security alerts, the user will pay less attention to the alert and will not be able to make the right decision while responding to the alert.

H3: Interaction between cue utilization and cognitive load where higher cue utilization would be associated with higher attention and smaller reductions in performance as cognitive load increases.

H4: Environmental distractions will exacerbate cognitive overload, leading to a further decrease in attention to security alerts, regardless of the user's security knowledge level.

## **PROPOSED RESEARCH METHODOLOGY**

This experimental study employs a within-subject, controlled laboratory design to investigate how cognitive load influences user responses to security alerts, focusing on participants' varying levels of technical expertise and their handling of security errors. We will recruit 60-100 participants and collect demographic and technical expertise data through a pre-study questionnaire. The cognitive load will be manipulated at two levels (High and Low) through tasks such as arithmetic problems, graphical data interpretation, and logical reasoning. This creates four experimental conditions: High Cognitive Load, High Volume of Alerts; Low Cognitive Load, High Volume; High Cognitive Load, Low Volume; and Low Cognitive Load, Low Volume. During task engagement, participants will receive simulated security alerts, with their responses measured in terms of response time, accuracy, attention, and error-handling behavior (such as correctly identifying or ignoring security alerts). The dependent variables in this study will include responses to the number of security alerts, response times, and responses ignored which will help us to measure security errors. The independent variables under consideration are the cognitive load and attention of the user (Biondi et al., 2021; Galy et al., 2012).

Eye-tracking technology will capture gaze patterns, pupil dilation, and fixation duration to assess cognitive engagement, while key press data and micro-expressions will serve as indirect indicators of cognitive load. After task completion, a post-task survey will gather information on participants' experiences, understanding of security alerts, and security errors. Data from eye-tracking and behavioral responses will be analyzed to determine how cognitive load, task complexity, and task volume influence security behavior and how technical expertise moderates these effects.

Data analysis will be performed using SPSS or R, employing ANOVA and correlation analysis to examine the impact of cognitive load on security alert responses. The outcomes are expected to

reveal significant differences in response strategies between novice and advanced users, providing insights that could inform the design of more effective security systems that account for user cognitive load and expertise. Ethical considerations will be addressed with IRB approval, and participants will be informed about their rights, including the option to withdraw from the study at any time.

## **EXPECTED FINDINGS AND FUTURE RESEARCH**

The role of reducing cognitive load becomes important where digital interfaces vying for users' attention; therefore, Designing interfaces that prioritize clarity, simplicity, and efficiency are viable to enhance usability. The study endeavors to examine how cue utilization and cognitive load affect the decision-making of novice and advanced users while they respond to security alerts. By comprehending how these cognitive loads influence their susceptibility to falling into such traps, the aim is to identify strategies that reduce cognitive load for employees. We anticipate finding significant differences in how novice and advanced users respond to security alerts under varying levels of cognitive load. Insights from this research may inform the design of more effective security systems that consider user cognitive load and expertise, potentially improving compliance with security protocols.

Our study will also demonstrate a correlation between cognitive load, attention, and task performance (Neupane et al., 2015). Beyond raising people's awareness to malicious emails and warnings, introduction to interventional training programs will improve people's attention that can help reduce the impact of attacks (Chambers, R., 2008). Understanding of deception and social engineering techniques that trick individuals to click on malicious links or open an infected attachment can help employees to combat such security threats (Khaled, 2023). Additionally, the study seeks to enhance the effectiveness of training sessions to better equip employees in handling



the security challenges. Also, Organizations can improve the understanding of human behavior that can help build strategies to mitigate potential risks by analyzing the role of trust and decision-making in cybersecurity (Khaled, 2023). Future research will focus on developing a mental model that balances workloads by incorporating the various stages of the thinking process. Additionally, researchers will investigate how to design security warnings and alerts that effectively distinguish themselves from malicious emails and notifications. Furthermore, extended research on incorporating psychological and behavioral aspects based on trust and decision-making should be added to the security systems. More work on the concept of ‘cognitive overload’ using neuroscientific techniques can lead to a better understanding of brain patterns and how it can affect behavioral aspects in cybersecurity (Paas, 1992). There are different types of warnings such as information disclosure, disk encryption, execution of malicious code and many more that does not even state what is the risk, what are the ways it can be avoided that leaves the user with no safety and does not protect people from phishing attacks (Bravo-Lillo et al., 2011)

## **References**

- Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: user attention, comprehension, and behavior. In Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12). Association for Computing Machinery, New York, NY, USA, Article 3, 1–14. <https://doi.org/10.1145/2335356.2335360>
- Anderson, B. B., Kirwan, C. B., Eargle, D., Jensen, S. R., & Vance, A. (2015). Neural correlates of gender differences and color in distinguishing security warnings and legitimate websites: A neurosecurity study. *Journal of Cybersecurity*, 1(1), 109-120. <https://doi.org/10.1093/cybsec/tyv005>

- Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3), 613-643. <https://www.misq.org>
- Andrade, R. O., & Yoo, S. G. 2019. Cognitive security: A comprehensive study of cognitive science in cybersecurity. *Journal of Information Security and Applications*, 48, 102352.
- Biondi, F. N., Balasingam, B., & Ayare, P. 2021. "On the Cost of Detection Response Task Performance on Cognitive Load." *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 63(5), 804–812.
- Bravo-Lillo C, Cranor LF, Downs J, Komanduri S, Sleeper M (2011) Improving computer security dialogs. Campos P, Graham N, Jorge J, Nunes N, Palanque P, Winckler M, eds. *Human Computer Interaction—INTERACT 2011, Lecture Notes Comput. Sci.*, Vol. 6949 (Springer-Verlag, Berlin Heidelberg), 18–35.
- Bravo-Lillo, C., Cranor, L. F., Downs, J. S., & Komanduri, S. (2011). Bridging the Gap in Computer Security Warnings: A Mental Model Approach. *Security & Privacy, IEEE*, 9(2), 18-26.
- Breve, B., Desolda, G., Greco, F., Deufemia, V. (2023). Democratizing Cybersecurity in Smart Environments: Investigating the Mental Models of Novices and Experts. In: Spano, L.D., Schmidt, A., Santoro, C., Stumpf, S. (eds) *End-User Development. IS-EUD 2023. Lecture Notes in Computer Science*, vol 13917. Springer, Cham. [https://doi.org/10.1007/978-3-031-34433-6\\_9](https://doi.org/10.1007/978-3-031-34433-6_9)
- Cacioppo, J., Petty, R., & Kao, C. (1984). The efficient assessment of NFC. *Journal of Personality Assessment*, 48, 306–307. [https://doi.org/10.1207/s15327752jpa4803\\_13](https://doi.org/10.1207/s15327752jpa4803_13)

Cao, A., Chintamani, K. K., Pandya, A. K., & Ellis, R. D. (2009). NASA TLX: Software for assessing subjective mental workload. *Behavior Research Methods*, 41(1), 113-117. <https://doi.org/10.3758/BRM.41.1.113>

Chowdhury, N. H., Adam, M. T. P., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. *Computers & Security*.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, 31(2), 285–318. <https://doi.org/10.2753/MIS0742-1222310210>

D'Arcy, J., & Teh, P.-L. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management*, 56(7), 103151. <https://doi.org/10.1016/j.im.2019.02.006>

De Jong, T. (2010). Cognitive load theory, educational research, and instructional design: Some food for thought. *Instructional Science*, 38(2), 105–134. <https://doi.org/10.1007/s11251-009-9110-0>

Dykstra, J., & Paul, C. L. (2018, August). Cyber Operations Stress Survey (COSS): Studying fatigue, frustration, and cognitive workload in cybersecurity operations. 11th USENIX Workshop on Cyber Security Experimentation and Test (CSET 18). <https://www.usenix.org/conference/cset18/presentation/dykstra>

Dzubak, C. M. (2008). Multitasking: The good, the bad, and the unknown. *The Journal of the Association for the Tutoring Profession*, 1(2), 1-12.

Frederick, S. (2005). Cognitive Reflection and Decision Making. *Journal of Economic Perspectives*, 19(4), 25–42. <https://doi.org/10.1257/089533005775196732>

Galy, E., Cariou, M., & Mélan, C. 2012. "What is the relationship between mental workload factors and cognitive load types?" *International Journal of Psychophysiology*, 83(3), 269–275

J. Sobey, R. Biddle, P. van Oorschot, and A. S. Patrick. Exploring user reactions to new browser cues for extended validation certificates. In S. Jajodia and J. Lopez, editors, *Proc. 13th European Symposium on Research in Computer Security (ESORICS) 2008*, volume 5283 of LNCS, pages 411–427. Springer, 2008.

Jenkins et al.: How Messages That Interrupt Can Make Us Vulnerable 881 *Information Systems Research* 27(4), pp. 880–896, ©2016 The Author(s)

Kim, B.J., Kim, M.J. & Lee, J. Examining the impact of work overload on cybersecurity behavior: highlighting self-efficacy in the realm of artificial intelligence. *Curr Psychol* 43, 17146–17162 (2024). <https://doi.org/10.1007/s12144-024-05692-4>

Klingberg, T. (2009). *The overflowing brain: Information overload and the limits of working memory*. Oxford University Press.

Kolfschoten, G., French, S., & Brazier, F. (2014). A discussion of the cognitive load in collaborative problem-solving: The decision-making phase. *EURO Journal on Decision Processes*, 2(3), 257–280. <https://doi.org/10.1007/s40070-014-0034-9>

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*. <https://www.elsevier.com/locate/ijinfomgt>

Luthans, F., & Youssef-Morgan, C. M. (2017). Psychological capital: An evidence-based positive approach. *Annual Review of Organizational Psychology and Organizational Behavior*, 4, 339–366. <https://doi.org/10.1146/annurev-orgpsych-032516-113324>

Luo, X. R., Zhang, W., Burd, S., & Seazzu, A. (2012). Investigating phishing victimization with the Heuristic-Systematic Model: A theoretical framework and an exploration. *Decision Support Systems*, 55, 220–232. <https://doi.org/10.1016/j.dss.2012.12.002>

Murphy, G., Groeger, J.A. & Greene, C.M. Twenty years of load theory—Where are we now, and where should we go next?. *Psychon Bull Rev* 23, 1316–1340 (2016). <https://doi.org/10.3758/s13423-015-0982-5>

NASA (1986). Task Load Index (TLX): Computerized version (Version 1.0). Moffett Field, CA: Human Research Performance Group, NASA Ames Research Center.

Neupane, A., Rahman, Md. L., Saxena, N., & Hirshfield, L. (2015). A Multi-Modal Neuro-Physiological Study of Phishing Detection and Malware Warnings. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 479–491. <https://doi.org/10.1145/2810103.2813660>

Nobles, C. (2022) Stress, burnout and security fatigue in cybersecurity: A human factors problem, *Holistica Journal of Business and Public Administration*, Vol. 13, Iss. 1, pp. 49-72.

Paas, F. 1992. "Training strategies for attaining transfer of problem-solving skill in statistics: A cognitive load approach." *Journal of Educational Psychology*, 84, 429–434.

Pashler H (1994) Dual-task interference in simple tasks: Data and theory. *Psych. Bull.* 116(2):220–244.

Petty, R. E., Brinol, P., Loersch, C., & McCaslin, M. J. (2009). The need for cognition. In *Handbook of individual differences in social behavior*. (pp. 318–329). The Guilford Press.

PwC, (2018). The Global State of Information Security Survey 2018. Retrieved April 20, 2018.

Source: <https://www.pwc.com/us/en.html>

Raja, F., Hawkey, K., Hsu, S., Wang, K. L. C., & Beznosov, K. (2011). A Brick Wall, a Locked Door, and a Bandit: A Physical Security Metaphor For Firewall Warnings. *Proceedings of the Seventh Symposium on Usable Privacy and Security*. ACM, Pittsburgh, USA, pp. 1-20.

Shari Lawrence Pfleeger, Deanna D. Caputo (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, 31(4), 597-611. DOI: 10.1016/j.cose.2011.12.010

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). "The sufficiency of the theory of planned behavior for explaining information security policy compliance." *Information and Computer Security*, 23(2), 200-217.

Tally, A. C. (2023). *Negotiating privacy through deception and trust: A study of phishing in the workplace, usernames in gaming, and boundaries in online dating* (Doctoral dissertation, Luddy School of Informatics, Computing & Engineering, Indiana University).

T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer. Social phishing. *Communications of the ACM*, 50(10):94100, October 2007.

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. <https://doi.org/10.25300/MISQ/2018/14124>

Wang, J., Herath, T., Rui, C., Vishwanath, A., & Rao, H. R. (2012). Phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *Transactions on Professional Communication*, 55, 345–362. doi: 10.1109/TPC.2012.2208392

Zihisire Muke, P., Telec, Z., & Trawiński, B. (2022). Cognitive Load Measurement Using Arithmetic and Graphical Tasks and Galvanic Skin Response. In N. T. Nguyen, Y. Manolopoulos, R. Chbeir, A. Kozierkiewicz, & B. Trawiński (Eds.), *Computational Collective Intelligence* (Vol.

13501, pp. 836–850). Springer International Publishing. [https://doi.org/10.1007/978-3-031-16014-1\\_66](https://doi.org/10.1007/978-3-031-16014-1_66)

Z. F. Zaaba, S. M. Furnell and P. S. Dowland, "A study on improving security warnings," The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M), Kuching, Malaysia, 2014, pp. 1-5, doi: 10.1109/ICT4M.2014.7020633.