



UNIVERSITY
OF SKÖVDE

Exploring the Intersection of Cognitive Science and Information Security: The Impact of Short-term Cognitive Interventions on Security Behavior

Master Degree Project in Informatics with a
specialization in Privacy, Information and
Cyber Security

Second Cycle 30 ECTS

Spring term 2025

Student: Athira Sathi Krishnan

Supervisor: Nikolaos Kourentzes

Examiner: Marcus Nohlberg

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to University of Skövde for providing the necessary resources and support for conducting this research.

I would like to express my sincere gratitude to my supervisor, Nikolaos Kourntzes, and examiner, Marcus Nohlberg, for their invaluable guidance, constructive feedback, and support throughout this research. Their expertise and insights have been instrumental in refining the methodology and shaping the findings presented in this report.

Additionally, I would like to acknowledge the efforts of my colleagues, friends, and family, who offered unwavering support and motivation during the research, conducting survey and writing process. Special thanks to the participants who contributed to the experimental study, as their time and cooperation were crucial in gathering meaningful data.

Finally, I am grateful to the authors and researchers whose work provided foundational insights for this study. Their contributions to the field have greatly enriched the understanding of cognitive science and cybersecurity, forming the basis of this research.

ABSTRACT

As cybersecurity threats become increasingly sophisticated, human behaviour plays a critical role in protecting digital assets. Traditional cybersecurity strategies focus on technological defences, but cognitive science offers new insights into improving security behaviours. This study investigates the impact of short-term cognitive interventions, specifically focused breathing exercises, on password creation and risk evaluation. Using an experimental design with 100 participants, the research examines whether brief cognitive exercises enhance attention control and security decision making. Findings suggest that cognitive interventions lead to stronger password practices and improved detection of phishing risks, demonstrating the potential for integrating psychological strategies into cybersecurity training. By bridging cognitive science with cybersecurity awareness, this study contributes to human-centered security approaches that support better decision making in digital environments.

Keywords: Cybersecurity behaviour, cognitive interventions, password security, risk evaluation, mindfulness, attention control, human-centered security, phishing detection.

Table Of Contents

1 Introduction.....	1
1.1 Problem Description.....	3
1.2 Research Aim and Research Question.....	4
1.2.1 Research Aim.....	4
1.2.2 Research Question.....	5
2 Background.....	6
2.1 Overview of Fundamental Concepts.....	7
2.1.1 Cognitive Science and Human Behaviour in Cybersecurity.....	8
2.1.2 Mindfulness and Cognitive Interventions.....	9
2.2 Existing Research.....	10
2.2.1 Cognitive Science in Cybersecurity Behavior.....	11
2.2.2 Password Security and Cognitive Barriers.....	11
2.2.3 User Awareness and Cybersecurity Training.....	11
2.2.4 Risk Perception and Cognitive Overload.....	11
2.2.5 Mindfulness and Emotional Regulation in Cybersecurity.....	12
2.2.6 Human-Centered Cybersecurity Approaches.....	12
2.3 Expected Result.....	12
2.4 Addressing Gaps and Future Directions.....	12
3 Research Method.....	14
3.1 Systematic Literature Review.....	14
3.1.1 Databases.....	15
3.1.2 Search Terms.....	15
3.1.3 Article Selection Criteria.....	16
3.2 Survey.....	17
3.2.1 Design.....	17
3.2.2 Participant Recruitment and Sampling.....	18
3.2.3 Data Collection.....	19
3.2.4 Validity Threats.....	21
3.2.5 Ethical considerations.....	22
4 Results.....	24
4.1 Effectiveness of Short-Term Cognitive Interventions.....	24
4.2 Impact on Password Creation.....	25
4.2.1 Evaluation of Password Strength.....	25
4.3 Influence on Risk Evaluation.....	27

5 Discussion.....	29
5.1 Interpretation of Results	29
5.2 Practical Implications.....	29
5.3 Limitations.....	30
6 Conclusion.....	31
6.1 Ethical, Societal, and Scientific Impacts.....	32
6.2 Future work.....	32
References.....	33
Appendix – Survey.....	1

List of Tables

Table 1 Nominated Databases.....	15
Table 2 Inclusion and Exclusion Criteria.....	16
Table 3 Evaluation Criteria for Password Strength.....	26

1 Introduction

As digital systems and online platforms become increasingly central to daily life, the role of human behaviour in maintaining cybersecurity has become more apparent. While traditional cybersecurity strategies have focused heavily on technological defences such as firewalls, encryption, and access controls, it is now widely recognized that the actions, decisions, and awareness of individual users play a significant role in determining how secure a system truly is. That means security is all about people. Individuals often exhibit cognitive biases, decision fatigue, and inattentiveness, leading to poor security practices (Khadka & Ullah, 2025). Cybercriminals exploit these psychological weaknesses through deceptive techniques such as social engineering, misleading users into divulging sensitive information or clicking on malicious links (Maalem et al., 2020).

As per Liginlal, Sim, and Khansa (2009), many security breaches such as phishing attacks, data leaks, and account compromises can often be traced back to human error. Even when users are aware of certain security risks, they may still disregard best practices if the security measures are seen as obstructive to productivity or too difficult to understand. As noted by the authors, addressing the human factor in security requires not just technical solutions, but also behavioural strategies that align with users' cognitive and motivational limits.

Although the rise of newer methods like biometrics and security tokens, passwords are still the most common type of authentication (Nielsen et al., 2014; Woods and Siponen, 2018).

Every day, millions of users make small decisions that have big consequences: choosing a password, clicking a link, or opening an email. Unfortunately, many of these decisions are not made with security in mind. Despite years of awareness campaigns and training programs, users still fall for phishing scams, reuse weak passwords, and ignore security warnings.

Many users do not actively prioritize security in their daily routines, often relying on mental shortcuts, overlooking details, or making instinctive decisions especially under pressure. These behaviours, while entirely human, create vulnerabilities that cyber attacker's exploit.

This research addresses the discrepancy between recommended cybersecurity practices and actual user behavior. Rather than attributing security failures solely to user negligence or relying on extensive training programs, this study explores the potential of cognitive science based interventions to enhance security decision-making. By applying structured cognitive techniques, such as attention control and behavioral nudges, individuals may be guided toward more secure choices at critical moments, thereby improving overall cybersecurity resilience (Veksler et al., 2018).

Seigfried-Spellar, Rogers, and Thorpe (2017) argue that improving security behaviour requires a deeper understanding of the psychological and cognitive factors that influence human decision-making. According to the authors, designing security systems that account for the cognitive constraints can help reduce errors and improve compliance.

Mindfulness is a widely studied cognitive technique, defined as the practice of deliberate attention and awareness in the present moment without judgment. Charoensukmongkol (2014) highlights the significant role of mindfulness in enhancing emotional intelligence, particularly by improving self-awareness, emotional regulation, and cognitive clarity. These attributes are especially relevant in high-pressure security environments, where users are often put in situations that demand quick decisions. Mindfulness has been shown to improve cognitive control, reduce stress induced decision-making errors, and enhance rational responses to security threats (Roghanizad et al., 2021).

According to (Jarjoui, 2023), traditional cybersecurity awareness programs often fail to yield sustainable results because they focus on compliance rather than behavioral transformation. As argued by the author, mindfulness serves as the foundation for cybersecurity resilience, shifting the responsibility of security from IT teams to individual users. By cultivating mindfulness, individuals develop a human firewall, a proactive defense mechanism that enables them to make conscious security decisions in digital environments.

Studies, such as those by Tolga et al. (2023), have emphasized that emotional intelligence and mindfulness are closely linked, and that this connection can play a pivotal role in improving security behaviour. Emotional intelligence helps individuals recognize and manage their emotions, which, when combined with mindfulness, enhances a person's ability to stay calm, focused, and clear headed, even in stressful or potentially risky situations.

According to Anderson et al. (2015), most people tend to ignore security warnings online, not because they don't understand them, but because they have become so used to seeing them that they simply tune them out. Repeated exposure to security warnings leads to habituation, a psychological process in which individuals gradually become less responsive to a stimulus over time. Habituation occurs when a stimulus is presented repeatedly, causing a decline in attention and response, as the brain perceives it as non-threatening or irrelevant (Schmid et al., 2014). In cybersecurity, this phenomenon results in users ignoring security alerts, not due to a lack of understanding, but because they have encountered them so frequently that they no longer perceive them as urgent threats (Su, 2024).

Integrating cognitive science into cybersecurity frameworks such as real-time decision-support systems and emotional intelligence training has been shown to enhance security compliance and threat detection (Familoni, 2024). By bridging theoretical insights with practical applications, researchers aim to develop more effective security awareness programs that align with human psychological tendencies and decision-making processes.

By investigating the intersection of cognitive science and cybersecurity, this research aims to contribute practical insights for designing more effective security awareness programs ones that go beyond traditional knowledge delivery and actively equip users with cognitive tools to enhance their focus, decision-making, and threat detection abilities. Ultimately, the findings could help organizations cultivate a more mindful, attentive, and security conscious workforce, strengthening the human element in information security and reducing vulnerabilities to cyber threats. The idea is not to replace training or technical solutions but to complement them by supporting users when they need it most. While such interventions have been studied in fields like health behaviour and consumer decision-making, they are still relatively underexplored in the cybersecurity domain.

1.1 Problem Description

As the digital world continues to change at a fast pace, cybersecurity has become a major concern for everyone from individuals to large organizations and even governments. The rise of cyberattacks, data breaches, and privacy violations has made it clear that no one is immune to the risks of the online environment. These threats are no longer limited to large financial institutions or multinational corporations but are increasingly impacting ordinary users as well. Personal data, once considered private, is now vulnerable to unauthorized access and exploitation. Cybercriminals continuously evolve their tactics, making it difficult for traditional security measures to keep up. This widespread vulnerability underscores the importance of adopting proactive security measures, not just on an organizational level, but for individuals as well, to protect against the growing array of cyber threats that permeate every aspect of our digital lives (Wang, Li, & Zhang, 2023).

The tendency of users to engage in insecure behaviours even when they are aware of basic security principles, underscores a significant gap in current security awareness approaches, which often prioritize knowledge transfer over addressing the cognitive and psychological factors that influence behavior.

Taylor and Furnell (2020) emphasize the crucial role psychology plays in understanding user behaviour, decision-making, and risk perception within the context of cybersecurity. By examining how cognitive biases, social engineering tactics, and human factors influence security decisions, they argue that it is possible to design more effective security measures. For example, individuals often make security related decisions based on convenience or habit, which may lead them to disregard warnings or adopt weak passwords. Social engineering tactics, such as phishing, exploit psychological vulnerabilities by manipulating emotions like fear or urgency, making individuals more likely to fall for these attacks. Taylor and Furnell suggest that by applying insights from psychology, cybersecurity solutions can be tailored to account for these common human behaviours. This approach not only improves the effectiveness of security systems but also enhances user engagement by making security measures more intuitive and less intrusive. In essence, understanding the behavioural aspects of cybersecurity allows for the development of strategies that are both technically sound and aligned with human nature.

However, there is a lack of research directly exploring the relationship between cognitive interventions and security behaviour especially in practical scenarios like password creation and evaluating suspicious emails. Most existing studies focus either on technical training or general security awareness campaigns, leaving a knowledge gap in understanding how targeted cognitive exercises could directly improve realtime security decisions (Anderson & Dill, 2000). This research aims to fill that gap by examining whether short-term cognitive interventions can enhance individual's ability to create stronger passwords and make more accurate risk assessments. By addressing this intersection of cognitive science and information security, the study has the potential to inform the design of more effective, human-centered security training programs.

1.2 Research Aim and Research Question

Research Aim refers to the primary goal of the study, outlining what the research seeks to achieve. In the context of this study, the aim is to investigate how short-term cognitive interventions, such as focused breathing exercises, influence cybersecurity behavior. Specifically, the study examines whether these interventions improve users' ability to create secure passwords, accurately identify cybersecurity threats, and enhance overall risk evaluation in digital environments. The broader aim is to explore practical ways to integrate cognitive science into cybersecurity awareness programs for more effective security practices.

Research Questions define the specific focus areas of the study, helping to structure the methodology and guide data collection.

1.2.1 Research Aim

The goal of this research is to examine how short-term cognitive practices, like mindfulness meditation and focused breathing exercises, can impact and potentially improve user behaviour in cybersecurity tasks. More specifically, the study aims to explore whether these simple, brief techniques can help users create stronger passwords, assess security risks more accurately, and make more informed decisions when faced with potential online threats.

Cognitive processes are fundamental to how we engage with cybersecurity at every stage, from detecting potential threats to making decisions that impact our digital safety. According to Kannelønning and Katsikas (2023), understanding these cognitive processes is vital for designing security systems that not only protect against risks but also align with how users think and behave. For example, detecting a security threat like a phishing email often requires recognizing subtle cues, such as unfamiliar email addresses or suspicious links. However, this process is influenced by cognitive biases like the tendency to trust information that seems familiar or urgent which can lead users to overlook potential risks. Similarly, when it comes to making security related decisions, such as creating strong passwords or responding to system alerts, cognitive factors like mental fatigue, decision fatigue, and time pressure can result in poor choices that compromise security.

Kannelønning and Katsikas emphasize that developing effective security awareness programs, user training, and system designs requires a deeper understanding of these cognitive mechanisms. For example, training programs that incor-

porate strategies to mitigate cognitive biases, such as reminding users to carefully evaluate unfamiliar messages or offering simple, clear guidelines for secure behaviour, can greatly enhance security practices. Additionally, security systems can be designed with these cognitive factors in mind, creating interfaces that are intuitive and reduce the mental load on users. By bridging the gap between cognitive science and cybersecurity, we can develop more user-friendly and effective solutions that not only help prevent cyberattacks but also empower users to make safer decisions online.

1.2.2 Research Question

To focus this study, the following research questions have been developed:

- How effective are short-term cognitive interventions in improving user security behaviour, particularly in password creation and risk evaluation?

To break down this research aim, the study will also address key sub-questions, including:

1. How does undergoing brief cognitive interventions such as focused breathing exercises impact individuals' ability to create stronger passwords compared to those who do not?
2. How do brief cognitive interventions such as focused breathing exercises influence user's behaviour and awareness when assessing potentially risky situations, like phishing emails or suspicious prompts?

These research questions aim to examine the immediate impact of cognitive interventions and determine whether simple, low-cost techniques could play a meaningful role in enhancing user's real-time security awareness and decision-making capabilities.

This thesis will first explore the background and theories that connect cognitive science with cybersecurity. Then, it will describe an experiment designed to test short-term interventions in two common user tasks: password creation and phishing detection. Results will be analysed to understand what works, what does not, and why.

By the end of this work, the goal is to provide insights into how we can make cybersecurity more human-centered.

Instead of merely providing users with technical knowledge and instructions, these programs could incorporate cognitive strategies to improve attention, stress management, and decision-making skills which is the key elements in preventing security lapses.

2 Background

In today's digital age, where so much of our personal and professional lives are conducted online, cybersecurity has become an urgent and unavoidable concern. Every day, individuals and organizations alike face the ever present risk of cyberattacks, data breaches, and identity theft. Among the most basic yet critical ways to safe guard sensitive information are practices like creating strong passwords and evaluating risks effectively when interacting with digital platforms. Strong passwords, which combine complexity and unpredictability, serve as the first line of defence against unauthorized access to personal accounts and sensitive data. Similarly, the ability to assess security risks whether it is recognizing a phishing attempt, understanding the importance of software updates, or avoiding suspicious links is essential in mitigating the threats posed by cyber-criminals.

According to Forbes Advisor (2024), cybersecurity threats continue to escalate, making strong security practices essential for individuals and organizations. In 2023 alone, there were 2,365 cyberattacks, affecting over 343 million victims worldwide. Data breaches have surged by 72% since 2021, surpassing previous records. Additionally, identity theft remains a significant concern, with compromised business emails accounting for over \$2.9 billion in losses in 2023.

Strong passwords play a crucial role in mitigating these risks. Studies show that stolen credentials were responsible for four of the five largest data breaches in 2024. Similarly, phishing attacks remain one of the most common cyber threats, with email being the primary vector for malware 35% of malware was delivered via email in 2023 (Forbes Advisor, 2024).

These statistics underscore the urgent need for proactive cybersecurity practices in today's digital landscape.

However, despite the widespread awareness of these cybersecurity best practices, many individuals still struggle to implement them consistently. One of the key reasons for this disconnect is the challenge of balancing security with convenience. Strong, unique passwords can be difficult to remember, and the constant flow of security-related alerts can lead to security fatigue, where users ignore or dismiss important warnings. Security fatigue refers to the mental exhaustion or apathy that individuals experience due to the constant demands and complexities of managing cybersecurity Stanton et al. (2016).

Moreover, cognitive biases, such as the tendency to trust familiar sources or the desire for immediate convenience, often influence decision-making in ways that compromise security. The gap between knowledge and action is why there is a growing need for innovative approaches that not only raise awareness but also help individuals integrate secure behaviours into their everyday digital lives.

Confirmation bias leads individuals to trust familiar sources, even when those sources may not be secure. For example, users may ignore security warnings from unfamiliar websites while readily accepting information from frequently visited platforms, assuming they are safe. Similarly, availability heuristic causes individuals to rely on easily accessible information rather than critically evaluating security risks. If a user has never personally experienced a cyberattack, they may underestimate the likelihood of a security breach, leading to complacency in adopting protective measures (Greavu-Şerban et al., 2025).

The desire for immediate convenience is closely linked to optimism bias, where individuals believe they are less likely to be targeted by cyber threats compared to others. This bias often results in poor security practices, such as reusing passwords or bypassing multi-factor authentication for ease of access. Additionally, over-confidence bias leads users to assume they can recognize phishing attempts or security risks without formal training, making them more susceptible to social engineering attacks (Greavu-Şerban et al., 2025).

These biases contribute to the gap between cybersecurity awareness and actual implementation of secure behaviors. Research suggests that policy driven approaches and behavioral interventions can help mitigate the effects of cognitive biases by encouraging systematic security decision-making rather than relying on instinctive responses (Cuny, 2024). By integrating cognitive science into cybersecurity frameworks, organizations can develop more effective security awareness programs that address the psychological factors influencing user behavior.

Previous studies, such as the work by McCrohan et al. (2010), have explored the impact of training and awareness programs in improving cybersecurity practices. These programs typically focus on educating users about the risks of cyber threats and encouraging the adoption of safer online behaviours, such as creating strong passwords and recognizing phishing attempts. While these programs have shown some success, they often fall short in addressing the underlying psychological factors that influence user behaviour. This highlights the need for approaches that go beyond traditional awareness campaigns and delve into the cognitive and emotional processes that shape security related decision-making.

Despite the effectiveness of training programs, there has been limited research on how short-term cognitive interventions such as mindfulness exercises can further enhance security behaviours. Mindfulness, which involves being present and fully engaged in the moment without judgment, has been shown to improve attention, reduce stress, and increase self-awareness. This area of research is still in its early stages, but the potential to bridge cognitive science with cybersecurity practices is an exciting avenue for improving user security behaviours in a more holistic and effective manner.

2.1 Overview of Fundamental Concepts

To fully understand the scope and relevance of this research, it is important to first explore some of the key concepts that underpin the study. At the heart of the research lies cybersecurity, which refers to the practices and measures used to protect sensitive information and systems from digital threats. Cybersecurity is a complex field that encompasses a variety of strategies, from securing networks

and software to protecting individual user actions. One of the most basic yet critical aspects of cybersecurity is digital literacy the ability to navigate the digital world safely and responsibly. A digitally literate person is not only aware of the risks but knows how to mitigate them, such as by recognizing phishing attempts or understanding the importance of keeping software updated.

Central to this study is password creation, a key behaviour that directly impacts an individual's security. Despite common advice, many users still opt for weak, easily guessable passwords, like using the same password across multiple sites or choosing simple, memorable combinations. The process of creating strong passwords involves understanding the balance between security and usability, which often challenges users. Alongside passwords, risk evaluation is another critical concept. In the digital realm, users regularly encounter potential threats whether it is a suspicious email, a popup advertisement, or a request for personal information. Being able to effectively evaluate these situations and assess the associated risks is key to making informed decisions that can protect sensitive data.

Cognitive interventions such as mindfulness exercises and other short-term techniques, in influencing decision-making processes related to cybersecurity aim to improve the mental frameworks that guide decision-making by enhancing attention, focus, and emotional regulation. In the context of cybersecurity, these interventions could help users make more deliberate and secure choices when faced with security related tasks. By exploring these fundamental concepts, this section lays the groundwork for the research questions at the core of the study. It establishes how user behaviour, driven by both cognitive processes and environmental factors, plays a significant role in cybersecurity. Understanding these concepts is vital to grasping the significance of the study and its potential contribution to improving security behaviors in a world where digital threats are increasingly prevalent.

2.1.1 Cognitive Science and Human Behaviour in Cybersecurity

As Mylrea and Gourisetti (2017) emphasize, the effectiveness of any security infrastructure is heavily dependent on how individuals perceive and respond to potential threats. Cyberattacks such as phishing scams, social engineering ploys, and credential theft do not typically bypass technical barriers; instead, they exploit human psychology our habits, assumptions, cognitive shortcuts, and emotional responses. These attacks are designed to prey on trust, urgency, curiosity, or fear, leading people to fall into security risks. As the paper points out, the interplay between humans and technology creates a vulnerable interface one that attackers are increasingly targeting. Therefore, moving forward, cybersecurity must not only address software vulnerabilities but also consider cognitive and behavioural vulnerabilities as fundamental components of risk.

As Moustafa (2022) points out, many of the most common security lapses are not necessarily due to a lack of technical knowledge, but rather how the brain naturally processes information. In fast paced digital environments, users are frequently overwhelmed with decisions and cognitive stimuli, leading them to rely on mental shortcuts or heuristics that can compromise their judgment. By understanding how cognitive biases, fatigue, and decision-making frameworks influence security behaviour, we can begin to design systems and interventions

that align with natural human tendencies rather than working against them. Moustafa's work reinforces the idea that to truly strengthen cybersecurity, we must complement technical defences with psychologically informed strategies that support users in making better, safer choices.

Cognitive processes like attention, working memory, and decision making are at the very heart of how people perceive and respond to cybersecurity threats. Every time a user encounters a security warning, evaluates a suspicious message, or decides whether to trust a link or email, their mental faculties are actively at work. As Andrade and Yoo (2019) described, these processes are not static; they can be sharpened and supported through targeted cognitive interventions. For instance, by improving attention control, users may become more alert to subtle red flags in phishing emails. Enhancing working memory could help individuals hold onto important security guidelines while performing tasks online. Likewise, training decision-making through short-term exercises like mindfulness or scenario based reflection may help users pause, reflect, and choose safer options even under pressure. In our current digital environment, where threats evolve rapidly and often bypass traditional defences by manipulating human behaviour, these cognitive capacities form a critical line of defence. Andrade and Yoo's work suggest that bolstering users' cognitive strengths through simple, low cost interventions may not only improve how they process risk but also help build a more resilient and security conscious digital population.

2.1.2 Mindfulness and Cognitive Interventions

Mindfulness exercises such as meditation, focused breathing, and short reflective practices are increasingly recognized not just for their wellness benefits, but also for their potential to positively influence how individuals think and respond under pressure. These simple, accessible techniques can help quiet mental distractions, reduce stress, and improve one's ability to concentrate on the task at hand. As Seki et al. (2023) emphasize, in professional and high stakes environments, the impact of mindfulness goes even further: it enhances risk perception, strengthens impulse control, and supports better emotional regulation.

Modern users typically manage multiple accounts, each requiring a password, and best practices recommend using unique passwords for each one of the accounts (Ur et al., 2015). While this advice is intended to limit the impact of potential password breaches, many users struggle to follow it. As a result, they often resort to creating weak variations of the same password or reuse passwords entirely (Stobert & Biddle, 2014; Ur et al., 2015). Although alternative authentication methods like biometrics and password managers are available, they have yet to achieve widespread adoption, making passwords the default choice for most users (Ruoti et al., 2016).

As Lahza and Alsamani (2024) also point out that the usage of simple, easily guessed passwords or recycling the same password across multiple platforms is not necessarily due to ignorance, but rather due to the mental load and inconvenience involved in generating and remembering complex credentials. For many, the cognitive burden of memorizing a string of random characters outweighs the perceived benefits, especially when no immediate consequences are visible. Moreover, in a fast-paced digital environment filled with logins, pop-ups, and distractions, password creation becomes a task to get through rather than a

conscious act of securing one's identity. Some users write passwords down, save them in plain text, or use predictable patterns behaviours that expose them to significant risk. What makes this issue even more critical is that passwords often serve as the first line of defence against unauthorized access, meaning weak password habits can unravel even the most secure systems. Lahza and Alsamani (2024) emphasize that without addressing the psychological and cognitive dimensions of password behaviour such as memory limitations, attention span, and decision fatigue technical solutions alone will fall short. Therefore, improving user behaviour through thoughtful cognitive interventions, education, or design changes is key to strengthening this foundational layer of cybersecurity.

In a world where users are constantly juggling multiple accounts and the pressure to create numerous passwords, the cognitive load can be overwhelming. By fostering a mindset of awareness and deliberate thought, users may be more inclined to create stronger, more complex passwords and resist the ease of opting for something simple or repeated across accounts. These brief exercises help individuals pause and reflect before making potentially risky cybersecurity decisions, ultimately reducing the likelihood of security breaches caused by poor password habits.

Similarly, risk evaluation in online environments, such as identifying phishing emails, relies heavily on user's attention and ability to spot attacks. Research has suggested that stress reduction techniques improve rational processing and situational awareness, both critical for accurate risk evaluation (Sánchez-García et al., 2022).

2.2 Existing Research

This section provides a comprehensive review of existing literature relevant to the study. Cybersecurity threats continue to evolve, requiring innovative approaches that integrate cognitive science to enhance security behaviors. Traditional security awareness programs often focus on compliance rather than behavioral transformation, leading to gaps in user engagement and decisionmaking (Andrade et al., 2022). This review examines recent research on cognitive science applications in cybersecurity, highlighting key findings, methodologies, and future directions.

Previous studies have explored various cognitive and psychological factors influencing cybersecurity behavior, such as cognitive overload, stress, and memory limitations. While some research highlights the negative impact of these factors, few have tested practical interventions. A smaller subset, including work by Seki et al. (2023), suggests mindfulness may enhance decision-making, though largely through correlative analysis. Overall, while the literature provides strong theoretical grounding, there is a clear gap in empirical studies evaluating cognitive interventions precisely the focus of this thesis.

The following section presents a classified overview of the existing literature, organized according to key thematic categories relevant to this study.

2.2.1 Cognitive Science in Cybersecurity Behavior

Several papers emphasize the role of cognitive science in shaping cybersecurity-related decision-making. Andrade and Yoo (2022) offer a broad perspective on cognitive security, integrating principles from cognitive science into cybersecurity frameworks. While their study lays an important theoretical foundation, it does not directly test cognitive interventions in practical security contexts. Similarly, Moustafa (2023) expands this discussion by providing a comprehensive review of cognitive science applications in cybersecurity, reinforcing the idea that user cognition plays a key role in security effectiveness.

Cognitive science explores how individuals process information, make decisions, and regulate emotions critical factors in cybersecurity behavior. Studies suggest that cognitive interventions, such as mindfulness training and attention control techniques, can improve users' ability to recognize security threats and respond effectively (Kävrestad & Naqvi, 2024). Research also indicates that cognitive biases, such as optimism bias and overconfidence, contribute to poor security practices, making users more susceptible to cyberattacks (Greavu-Șerban et al., 2025).

2.2.2 Password Security and Cognitive Barriers

A subset of studies focuses on password security, exploring behavioural influences and cognitive challenges in adopting secure practices. Lahza and Alsamani (2024) analyse persuasive strategies that enhance password security, noting that cognitive biases often prevent users from adopting stronger passwords. However, their research does not address mindfulness based interventions that might mitigate these cognitive barriers which is an area that remains underexplored. Rooney (2023) builds on this by assessing password workarounds and the resulting cybersecurity risks, highlighting user tendencies to bypass security protocols due to cognitive overload and convenience driven decision-making.

2.2.3 User Awareness and Cybersecurity Training

User awareness and training play a crucial role in cybersecurity behavior modification. McCrohan et al. (2018) examine the influence of cybersecurity training and awareness initiatives, finding that users with prior exposure to security education demonstrate improved risk evaluation and threat detection. However, training strategies in existing literature often focus on procedural knowledge rather than cognitive interventions like attention training or stress reduction techniques. Rawat et al. (2021) extend this discussion by evaluating how big data can be leveraged to personalize security awareness programs, potentially creating more effective, user-adaptive training solutions.

2.2.4 Risk Perception and Cognitive Overload

The issue of cognitive overload affecting risk perception is also explored in several papers. Sánchez-García et al. (2022) demonstrate that cognitive fatigue impairs phishing threat detection, emphasizing the need for strategies to mitigate overload. However, their study does not implement an experimental approach to test such interventions. Liginlal et al. (2009) assess human error in cybersecurity, particularly privacy breaches, arguing that cognitive frameworks should be better integrated into security policies. Their findings are directly relevant to this

study, as they highlight the need for tailored cognitive strategies to improve security decision-making.

2.2.5 Mindfulness and Emotional Regulation in Cybersecurity

The influence of mindfulness and emotional intelligence on cybersecurity behaviours is a promising avenue explored by a few studies. Seki et al. (2023) investigate mindfulness as a tool to improve cybersecurity decision-making, showing positive effects on impulse control and risk perception. While their findings suggest that mindfulness can enhance security awareness, they do not directly explore its influence on password security. Sánchez-García et al. (2022) also touch upon cognitive influences on risk assessment, though without applying experimental methods to validate mindfulness based approaches.

2.2.6 Human-Centered Cybersecurity Approaches

Recent literature emphasizes the importance of human-centered cybersecurity, which integrates cognitive science principles to enhance user engagement. A systematic review by Andrade et al. (2022) demonstrated the role of cognitive load management in reducing security fatigue and improving compliance with security protocols. Similarly, Naqvi et al. (2023) examine how cognitive disabilities impact cybersecurity behavior, advocating for adaptive security frameworks that accommodate diverse cognitive abilities.

Several studies propose cognitive interventions to enhance cybersecurity awareness and decision-making. Research suggests that focused breathing exercises and real-time behavioral nudges can improve users' ability to detect phishing attempts and assess security risks (Kävrestad & Naqvi, 2024). Additionally, gamification techniques have been shown to increase engagement in security training programs, reinforcing cognitive resilience against cyber threats (Andrade et al., 2022).

2.3 Expected Result

This study expects that short-term cognitive interventions such as mindfulness or attention exercises will lead to improved security behaviour among users. Specifically, it is anticipated that participants who engage in these brief mental tasks will be more likely to create stronger, more secure passwords and make more careful decisions when faced with security risks, such as phishing attempts. By reducing mental fatigue and enhancing focus, these interventions may help users become more aware of their actions and less likely to fall into risky habits like password reuse or ignoring warnings. These findings could offer a practical and time-efficient addition to existing security awareness training, making it not only more engaging but also more effective.

2.4 Addressing Gaps and Future Directions

While existing research highlights the intersection of cognitive science and cybersecurity, there remains a gap in integrating cognitive interventions particularly attention training, mindfulness, and emotional regulation into cybersecurity strategies. Several studies provide foundational knowledge but stop short of applying cognitive techniques in a structured, experimental setting. By building on their findings, this study aims to bridge this gap by empirically investigating

how mindfulness and attention training techniques can enhance cybersecurity behaviours such as password creation and risk assessment.

While cognitive science offers promising solutions for cybersecurity, challenges remain in implementation and scalability. Future research should explore AI-driven cognitive security models that personalize security training based on individual cognitive profiles (Greavu-Şerban et al., 2025). Additionally, interdisciplinary collaborations between cognitive scientists and cybersecurity experts can enhance the effectiveness of security awareness programs.

3 Research Method

Qualitative research can draw on a variety of data collection methods, including document analysis, surveys, interviews, and observations (Creswell & Poth, 2018). In this study, two methods are used together: a systematic literature review and a survey. The goal of combining these approaches is to gather insights from different sources, allowing the findings to be cross verified for greater reliability (Arksey & Knight, 1999). Both methods are explained below.

As described by Kitchenham (2004), "a systematic literature review is a means of identifying, evaluating and interpreting all available research relevant to a particular research question, or topic area, or phenomenon of interest". Therefore, a well conducted systematic literature review is considered to meet the key criteria necessary for producing valid and reliable research outcomes. According to Kitchenham (2004), systematic literature reviews are often carried out to assess whether existing evidence can support current hypotheses or contribute to the development of new ones. Additionally, these reviews are commonly used to establish a solid foundation for future research projects.

Kitchenham (2004) emphasizes that systematic literature reviews demand significantly more effort than traditional reviews, yet they offer considerable advantages due to their structured and transparent methodology. Unlike conventional reviews, which may lack consistency and scientific rigor, systematic reviews enable readers to assess the completeness and neutrality of the search process, thereby enhancing the objectivity of the findings. Furthermore, the systematic reviews can offer insights into the effects of specific phenomena across diverse contexts and research methods. This feature is particularly valuable for the present study, which draws on a variety of individual studies conducted in different settings making the systematic approach especially relevant.

3.1 Systematic Literature Review

As demonstrated by Kitchenham (2004), a structured literature review typically involves three key phases such as

1. Planning the review
2. Conducting the review and
3. Reporting the review.

Jesson, Matheson and Lacey (2011) also described about the systematic literature review as "a review with clear stated purpose, a question, a defined search approach, stating inclusion and exclusion criteria, producing a qualitative appraisal of articles". This process includes the definition of a proper research question, designing an execution plan, searching for relevant literature, applying inclusion and exclusion criteria, assessing the quality of the chosen articles, and finally synthesizing the results.

3.1.1 Databases

Brereton, Kitchenham, Budgen, Turner, and Khalil (2007) emphasize the importance of searching multiple electronic databases when conducting research. This is because no single database contains all the relevant articles, so looking in several places increases the chances of finding all the important studies. By using different sources, researchers can gather a more complete and accurate set of information for their review.

Brereton et al. (2007) highlight IEEE Xplore and ScienceDirect as valuable electronic databases for software engineering research. Similarly, Kitchenham and Charters (2007) suggest using Scopus, as it offers a wide collection of abstracts and citations across various fields. Fink (2019) also points out that Web of Science is a useful multidisciplinary database, as it includes a broad range of journals from different subject areas.

To identify relevant studies for this thesis, a systematic search was conducted using academic databases such as Google Scholar, IEEE Xplore, Scopus, and SpringerLink which is demonstrated in Table 1. The search terms were carefully selected to align with the research focus on short-term cognitive interventions and cybersecurity behavior.

Table 1 Nominated Databases

Source	URL
Google Scholar	https://scholar.google.com
IEEE Xplore	https://ieeexplore.ieee.org
Scopus	https://www.scopus.com
SpringerLink	https://link.springer.com
Web of Science	https://www.webofscience.com

3.1.2 Search Terms

Jesson et al. (2011) emphasize that the careful selection of appropriate search terms is essential for conducting a successful and thorough systematic literature review. Since the results of a database search largely depend on the keywords used, the overall quality and completeness of the review are also influenced by them. The use of irrelevant or poorly chosen terms can lead to the exclusion of important studies.

Jesson et al. (2011) also argued that one way to enhance the search process is by using Boolean operators like AND and OR. These operators help combine or narrow down search terms to make the search more effective. Similarly, Kitchenham (2004) notes that including Boolean operators allows for the creation of more

precise and structured search strings, which can lead to more relevant and focused search results.

Therefore, having a solid understanding of topic related keywords is crucial for compiling a comprehensive and reliable bibliography.

The selected keywords cover core concepts such as cognitive interventions, cybersecurity behaviour, password creation, and risk evaluation. Related terms and synonyms were included to broaden the search scope, ensuring that studies using different terminology were also considered. For example, searches like "mindfulness AND cybersecurity AND password security" and "risk evaluation AND cybersecurity AND phishing" helped locate studies focusing on cognitive training's impact on cybersecurity decision-making.

3.1.3 Article Selection Criteria

Wohlin et al. (2012) state that the selection of primary studies should be guided by clearly defined inclusion and exclusion criteria. These criteria need to be established in advance to ensure objectivity and reduce the risk of bias during the selection process.

Table 2 Inclusion and Exclusion Criteria

Inclusion Criteria	Peer-reviewed journal articles and conference papers to ensure quality and credibility.
	Recent studies to reflect current developments.
	Research directly examining cognitive factors, mindfulness techniques, and cybersecurity behaviours.
	Studies focused on human factors such as password creation, phishing detection, and risk evaluation.
Exclusion Criteria	Studies focused solely on technical defences.
	Opinion pieces, editorials, and non-peer-reviewed sources
	Articles unrelated to human cognitive processes, psychological factors, or behaviour in cybersecurity contexts.

The inclusion and exclusion criteria is demonstrated in Table 2. A total of 48 articles were initially retrieved through the systematic literature review search process. After applying the predefined selection criteria, 29 articles remained for further evaluation. Following a thorough assessment and refinement process, 15 articles were ultimately included in the final review. These articles were selected based on their relevance to the research questions and alignment with the study's focus on cognitive interventions, cybersecurity behaviours, password creation, and risk evaluation. The articles were selected based on specific search criteria, including cognitive science applications in cybersecurity, user behavior, and decision-making processes.

The articles are diverse in their approach, incorporating different aspects of cognitive science (e.g., mindfulness, decision-making, emotional intelligence) into cybersecurity contexts. Several articles explore human behaviour in cybersecurity, emphasizing areas like password security, risk perception, and the influence of awareness and training. Mindfulness and cognitive training are explored in multiple articles as interventions to improve security behaviour. The focus is not only on theoretical aspects but also on empirical studies, as seen in doctoral dissertations and systematic literature reviews that assess existing research on cybersecurity related behaviour.

3.2 Survey

This study employed an offline, paper-based experimental design to investigate the effects of short-term cognitive interventions specifically focused breathing exercises on cybersecurity behaviour, namely password creation and risk evaluation. A total of 100 participants were recruited through convenience sampling and included a diverse group of individuals such as students, professionals, and homemakers, none of whom had specialized training in cybersecurity. Participants were randomly assigned to either an intervention group or a control group. The intervention group engaged in a brief guided breathing exercise intended to enhance cognitive control and focus, while the control group proceeded directly to the tasks. All tasks, including password generation and scenario based risk assessments, were completed using printed materials to simulate an everyday setting without the influence of digital tools. This approach was chosen to assess real world decision-making in a simple, accessible environment, reflecting how individuals from varied backgrounds might naturally approach cybersecurity behaviours.

3.2.1 Design

This study adopts a comparative research design to investigate how a specific short-term cognitive intervention such as focused breathing exercises which influences user behaviour in cybersecurity tasks. Focused breathing was selected as the intervention technique due to its well documented benefits in enhancing attention control, emotional regulation, and impulse management. All of which are essential cognitive factors when making security related decisions. By narrowing the intervention to a single, clearly defined practice, the study ensures consistency in application and avoids the confounding effects that might arise from combining multiple interventions with potentially different cognitive outcomes.

In the comparative component of the design, participants are divided into two groups: one group performs a brief focused breathing exercise prior to engaging in cybersecurity tasks, while the control group completes the same tasks without any prior intervention. This setup allows for direct comparison of behavioural outcomes between the two groups, helping to assess whether even a short cognitive reset through focused breathing can lead to more secure decision-making.

Hence, the study aims to offer a holistic understanding of how focused breathing as a simple and scalable cognitive intervention which might be integrated into broader cybersecurity training or awareness programs to support better user decision-making and security behaviour. This design is particularly well suited to studying non expert populations, such as students, professionals, and homemakers, who reflect the broader public most susceptible to cyber threats. By using a paper based format, the study simulates practical, low-tech environments and emphasizes cognitive processes over digital interaction. This structure allows for observing the potential of basic cognitive strategies to enhance security behaviour, independent of technical tools or expert knowledge.

3.2.2 Participant Recruitment and Sampling

To ensure a diverse and representative sample, this study recruited 100 participants from various backgrounds, including university students, working professionals, homemakers, and other members of the public. The recruitment process was conducted through a mixed approach of online and offline methods such as word-of-mouth, local community outreach and social media platforms. All participants were briefed about the study's purpose simply and informed consent was obtained. No prior cybersecurity expertise was required, as the study aimed to explore real world behaviours and decision-making among everyday users who typically face online security challenges. Participants were randomly assigned to either the intervention or control group, allowing for a fair comparison of outcomes. This inclusive approach not only adds ecological validity to the findings but also reflects the reality that cybersecurity is a universal concern affecting individuals regardless of their technical knowledge or occupation.

Inclusion Criteria - Adults from diverse backgrounds, including students, working professionals, homemakers, and general public. Individuals with no prior expertise in cybersecurity. Willingness to participate in the survey. Availability to take part in the experiment as scheduled. Basic ability to understand instructions and complete the study tasks.

Exclusion Criteria - Individuals with formal education or professional experience in cybersecurity. Participants unwilling to take part in the study.

Then the selected participants were divided into two primary groups to facilitate a comparative analysis:

- **Intervention Group (n = 50):** This group consisted of participants who engaged in a short cognitive exercise such as a focused breathing session prior to completing the cybersecurity tasks. The aim was to enhance their cognitive readiness, focus, and emotional regulation before evaluating their performance on security-related decisions.

- **Control Group (n = 50):** Participants in this group performed the same cybersecurity tasks without any preceding cognitive intervention. This allowed for a baseline comparison to assess whether the cognitive exercises had any measurable effect on their behaviour and decision-making during the tasks.

To ensure the reliability and integrity, this study was conducted through supervised, offline sessions. While an online format could have enabled broader reach and flexibility, it raised concerns regarding participant compliance and the authenticity of engagement particularly for the cognitive interventions. Without supervision, there would be no guarantee that participants completed the mindfulness or breathing exercises as instructed, or that they followed the task sequence without distractions. By conducting the experiment offline, in a controlled and supervised environment, the researcher was able to closely monitor participant behaviour, ensure consistent delivery of interventions, and maintain a standardised setting for all tasks. This approach enhances the credibility of the findings by minimizing external variables and ensuring that observed effects can be attributed more confidently to the intervention itself.

3.2.3 Data Collection

Participants gathered in a large hall, where the experiment was conducted over the course of five consecutive days. Each day, 20 participants completed the study in a structured session, ensuring an organized and controlled environment. The setup included individual workstations, allowing participants to focus on their assigned tasks without external digital distractions.

The experiment was conducted in a part of the researcher's apartment, specifically in a spacious hall designed to accommodate approximately 25–30 people at a time. The hall is equipped with individual tables and chairs arranged to provide each participant with a dedicated workstation, promoting focus and minimizing distractions. The environment is calm and quiet, which helped maintain participants' concentration throughout the study sessions. This setting allowed for a controlled and organized atmosphere, essential for the integrity of the experimental procedure.

A basic demographic analysis was conducted to examine the potential influence of age, gender, and background on the study outcomes. The participants ranged in age from 18 to 60. They were grouped into categories such as 18–25, 26–35, 36+ to investigate any variations in password strength and cybersecurity behaviours across different age groups. The sample comprised 40 males and 60 females, allowing for the assessment of gender differences in security related behaviours. Additionally, participants' educational and professional backgrounds, particularly their experience with technology and cybersecurity, were considered.

Before the actual task, participants were given a brief trial session to familiarize themselves with the format and task requirements.

The inclusion of a practice session ensured that all participants clearly understood the expectations before the formal evaluation, reducing confusion and improving the validity of the results. The five day structure allowed for efficient data collection while maintaining a standardized environment for all participants.

By conducting the study in a structured physical setting with an opportunity for trial practice, the research ensured consistent conditions for all participants, enabling valid comparisons between groups. For details regarding the content of the survey questionnaire, refer to Appendix – Survey.

No electronic devices were used for task completion to keep the study accessible and reduce technical complexity. Instead, task sheets were designed to be intuitive, with instructions clearly printed on the page.

Cognitive Intervention: Focused Breathing (Experimental Group Only)

Before beginning the main tasks, participants in the experimental group were guided through a 5-minute focused breathing exercise. This was delivered in-person by the researcher, reading from a standardised script. The exercise involved:

“Please close your eyes and sit comfortably. Take a slow, deep breath in for 4 seconds... hold for 2 seconds... and slowly exhale for 6 seconds. Focus only on your breathing. If your mind wanders, that is okay. Just gently return your attention to the breath.”

This technique was chosen to reduce mental clutter and improve attentional control before engaging in security relevant decision-making.

For the experimental group, a brief cybersecurity awareness session was conducted prior to the main tasks, equipping participants with essential knowledge on threats such as phishing attacks and malicious links. This included an overview of current digital threats, such as phishing emails, deceptive pop-ups, and misleading login pages, accompanied by visual examples to help participants better recognize suspicious content. The session aimed to build a foundational understanding of real-world security risks and enhance threat perception. Immediately following this, participants were guided through a 5-minute focused breathing exercise designed to improve cognitive control, reduce stress, and increase attentional focus. Once prepared, they proceeded to complete two cybersecurity related tasks: a password creation task and a risk evaluation task involving identification of potentially fraudulent or suspicious online elements.

In contrast, the control group completed the same tasks independently in their everyday environments, without supervision, cybersecurity briefings, or cognitive exercises. This design allows for a comparative analysis of how structured awareness and cognitive preparation impact secure behaviour and threat detection.

Cybersecurity Tasks (Paper-Based)

All participants completed two primary tasks designed to measure cybersecurity relevant behaviour. The paper format was intentionally low tech to make the experiment accessible and reflective of common cognitive processes.

Password Creation Task

Participants were asked to write down passwords for three different hypothetical accounts such as a banking account, a school portal and a social networking site.

They were not told how their responses would be evaluated. The sheet simply asked them to “create a password you would realistically use for each account.” Passwords were later evaluated for strength based on length, use of symbols/numbers/capital letters, and uniqueness across the three entries.

Risk Evaluation Task

Participants were given five short, printed scenarios, each describing a common cybersecurity situation. Examples included: Receiving a suspicious email from a bank, Seeing a pop-up asking to update browser security, being asked to enter a password on an unfamiliar page

For each scenario, they answered two questions:

- Do you believe this is a security risk? (Yes/No)
- What would you do? (Open-ended response)

Post-Task Feedback Survey

After completing the tasks, participants filled out a short paper-based feedback form, including:

- A 1–10 scale rating of how focused they felt during the task
- Self-reported stress or distraction levels
- For the experimental group: whether they felt the breathing exercise helped their focus
- Open-ended reflection on how they made password and risk decisions

This provided additional context to the quantitative task data.

3.2.4 Validity Threats

It’s important to think about the accuracy and trustworthiness of a study right from the start and throughout every stage of the research process. Wohlin et al. (2012) describe different types of validity and explain that validity is about how reliable the results are and whether they truly reflect what’s being studied without bias. This study carefully considered several kinds of validity and took specific steps to address each one.

1. Construct validity refers to how accurately a study captures what it aims to investigate. In this case, whether the selected literature truly helps answer the research questions. One of the main risks to construct validity in this study is the possibility of including irrelevant or low quality primary studies. To reduce this risk, the most reputable and widely used bibliographic databases were chosen as the main sources of literature.

2. According to internal validity, there is a causal relationship between the experiment's treatment and its outcome. In this survey, a possible issue is that participants were chosen through convenience sampling, which might not perfectly represent the wider population. However, by including people from different backgrounds and randomly assigning them to groups, the study aims to reduce bias and make the findings more reliable.

3. External validity refers to how well the results of a study can be applied or generalized to other situations or groups. In a systematic literature review, factors like the review process, types of publications included, and the dates of those studies affect external validity. To reduce these risks, this study carefully set inclusion and exclusion criteria. For the survey part, external validity is about whether the findings can apply beyond the group studied. Since the survey was conducted only in Sweden, its ability to be generalized to other countries or populations is limited.

4. Conclusion validity is all about the reproducibility of the review process based on a documented search process, extraction, coding, and analysis (Paré & Kitsiou, 2017). For the systematic literature review, this was ensured by carefully documenting every step and in case of survey, reliability depends on having a sample that represents the group well, so the results are trustworthy.

3.2.5 Ethical considerations

Ethical integrity was a central focus in the design and execution of this study, ensuring that all research procedures complied with recognized ethical standards and protected the rights and welfare of participants (Israel & Hay, 2006).

Prior to participation, all individuals were provided with a clear and detailed Informed Consent Form outlining the purpose of the study, the nature of the tasks involved, their right to withdraw at any point without penalty, and assurance that no personally identifiable information would be collected. Only those who voluntarily agreed and signed the form were included in the study.

Participation in the study was entirely voluntary. Participants were explicitly informed that they were free to decline or discontinue their participation at any stage of the study, without needing to provide a reason and without facing any negative consequences.

To ensure the anonymity of all participants, each individual was assigned a unique Participant ID, and no names or personal identifiers were recorded. All responses were handled confidentially and stored securely. The paper-based data was kept in a locked location accessible only to the researcher, and no identifying data was digitized.

The tasks included in the study password creation and risk evaluation posed no physical or psychological risk to participants. The experimental intervention, a focused breathing exercise, is a non-invasive, commonly used cognitive technique with minimal risk. Participants were not exposed to distressing content, and the materials were designed to be simple, relatable, and suitable for a general audience.

Following the completion of the tasks, participants were given a brief explanation of the study's aims and were thanked for their time. Any questions or concerns raised by participants were addressed immediately. Participants were also provided with contact details should they wish to discuss any aspect of the study further.

4 Results

This study combined insights from a systematic literature review (SLR) with primary data collected through a survey-based cognitive intervention to explore the impact of short-term cognitive exercises on cybersecurity behavior.

4.1 Effectiveness of Short-Term Cognitive Interventions

The SLR highlighted that while many studies (e.g., Sánchez-García et al., 2022; Lahza & Alsamani, 2024; Rooney, 2023) identified cognitive factors like cognitive load, stress, and attention as major influences on cybersecurity behaviours, few empirically tested practical interventions. Mindfulness and cognitive exercises were suggested as promising but lacked experimental validation, especially in tasks like password creation and phishing detection.

The survey experiment in this study provides that missing experimental evidence. Participants who completed brief cognitive interventions (focused breathing exercises) performed significantly better in both password creation and risk evaluation tasks than those who did not. This shows that short-term cognitive interventions can concretely enhance cybersecurity behaviours by improving cognitive control, attention, and emotional regulation.

Therefore the results of the study confirmed the hypothesis that participants who underwent a short cognitive intervention such as focused breathing exercises and a cybersecurity awareness session showed significantly improved cybersecurity behaviour compared to the control group. In the password creation task, participants in the experimental group demonstrated a higher level of adherence to recommended cybersecurity practices. Specifically, they created more complex passwords, with greater variability in character types, length, and complexity. This group avoided common patterns and personal information in their passwords more effectively than those in the control group, who tended to generate simpler, more predictable passwords.

In the risk evaluation task, the experimental group outperformed the control group in identifying suspicious links, fraudulent emails, and other deceptive elements within simulated digital content. Participants in the experimental group exhibited heightened awareness of phishing attempts and were more likely to flag suspicious emails and URLs correctly. Their improved decision-making was likely attributed to the cognitive intervention, which primed them for better attention and emotional regulation. In contrast, the control group struggled more frequently with identifying these threats, often missing key indicators of fraud or clicking on potentially harmful links.

The results were statistically significant, with the experimental group consistently outperforming the control group across both tasks. This suggests that short cognitive interventions can be a powerful tool in enhancing users cybersecurity behaviours, especially in areas like password security and risk evaluation.

The findings highlight the potential for integrating brief cognitive exercises, such as mindfulness or focused breathing, into cybersecurity training programs to improve user security behaviours in a practical and scalable way.

4.2 Impact on Password Creation

The SLR revealed cognitive barriers like forgetfulness, cognitive inertia, and defaulting to weak passwords (Lahza & Alsamani, 2024; Rooney, 2023), but did not evaluate interventions addressing these directly.

The survey results show that participants who received cognitive interventions created longer, more complex, and more unique passwords than those who did not. For example, 84% of passwords from the intervention group included a mix of symbols, numbers, and uppercase letters, compared to 57% in the control group.

This confirms that cognitive exercises improve executive functioning in password creation, overcoming cognitive biases and barriers noted in the SLR literature.

4.2.1 Evaluation of Password Strength

Passwords created by participants were evaluated using a structured scoring system based on the following four key criteria:

Length - Short passwords (<8 characters) were rated as weak. Medium-length passwords (8–12 characters) were rated as moderate. Long passwords (>12 characters) were rated as strong.

Complexity - (Use of Special Characters, Numbers, and Capital Letters).

Passwords containing only lowercase letters received a low complexity score.

Passwords with numbers or capital letters received a moderate complexity score.

Passwords incorporating symbols (e.g., @, #, !, \$) along with letters and numbers were rated as high complexity.

Uniqueness Across the Three Entries - If a participant reused the same password across multiple accounts, their password set was rated as low security.

If passwords shared similarities (e.g., variations of the same word), they were rated as moderate security.

If all three passwords were distinct and unpredictable, they were rated as high security.

Realism and Predictability - passwords using common words, personal names, or dictionary phrases were marked as predictable and weak.

Passwords using random character sequences or generated pass-phrases were rated as strong and difficult to guess. Below Table 3 illustrates the evaluation process.

Table 3 Evaluation Criteria for Password Strength

Criterion	Description	Example
Length	Short (<8 chars): weak	Weak: pass7
	Medium (8–12 chars): moderate	Moderate: Pass1234
	Long (>12 chars): strong.	Strong: MyPassword123!
Complexity (Based on use of special characters, numbers, capital letters.)	Lowercase only: low complexity	Low: password
	Numbers/caps: moderate.	Moderate: Password1
	Symbols + letters + numbers: high complexity	High: P@ssword!
Uniqueness Across Entries	Reused passwords across accounts: low security.	Low: password123 used multiple times
	Similar passwords (variations): moderate security.	Moderate:password123, password124
	Distinct, unpredictable passwords: high security.	High:p@ssWord1!, Myp@ss2#, Secr3t!
Realism and Predictability	Common words, names, dictionary phrases: predictable and weak.	Weak:John1234
	Random sequences or generated passphrases:	Strong: !v9X@8qRtZ

	strong and difficult to guess.	
--	--------------------------------	--

The average strength score for the intervention group was compared against the control group to determine if cognitive interventions (breathing exercises) had an impact on password security behavior.

Summary Statistics

The password creation task revealed significant differences in security behaviors between the experimental and control groups. Participants in the experimental group, who underwent cognitive interventions, demonstrated a higher level of password security compared to the control group. On average, passwords created by the experimental group were 13.2 characters long, whereas the control group's passwords averaged 8.9 characters, indicating a preference for longer and stronger passwords among those who received the intervention. Additionally, 84% of passwords generated by the experimental group contained a combination of symbols, numbers, and capital letters, compared to only 57% in the control group, suggesting improved adherence to cybersecurity best practices. Moreover, 92% of participants in the experimental group created unique passwords for all three accounts, whereas only 68% of control group participants did so, highlighting the positive effect of cognitive interventions on password uniqueness and security awareness. These findings support the hypothesis that short-term cognitive exercises enhance users' ability to implement stronger cybersecurity measures in everyday digital interactions.

4.3 Influence on Risk Evaluation

The SLR (Sánchez-García et al., 2022; Seki et al., 2023) established that high cognitive load and emotional dysregulation reduce users' ability to detect phishing attacks. Mindfulness was identified as potentially beneficial, but prior studies mostly showed correlational results without intervention testing.

The survey experiment demonstrated that participants in the intervention group detected phishing emails and suspicious links with significantly higher accuracy (89% and 85% respectively) than the control group (64% and 61%).

These findings provide experimental support for mindfulness based or focused-attention interventions improving risk perception and decision-making in cybersecurity contexts.

The risk evaluation task demonstrated a clear difference in cybersecurity awareness between the experimental and control groups, further supporting the impact of cognitive interventions on user behavior. Participants who underwent cognitive exercises successfully flagged phishing emails with an accuracy rate of 89%, compared to only 64% in the control group, indicating a heightened ability to recognize deceptive email content. Similarly, the experimental group correctly identified suspicious URLs in 85% of cases, while the control group achieved a lower accuracy of 61%, suggesting that cognitive interventions helped partici-

pants detect fraudulent web links more effectively. Overall, the average response accuracy across all risk scenarios was notably higher in the experimental group (87%) than in the control group (63%), reinforcing the hypothesis that brief cognitive exercises improve users' focus, decision-making, and ability to recognize security threats in digital environments. These findings highlight the potential of integrating cognitive interventions into cybersecurity training to enhance user vigilance and protection against cyber threats.

By combining the theoretical insights and identified gaps from the SLR with the empirical evidence from the survey, this study confirms:

- Cognitive interventions can effectively reduce cognitive overload and enhance attention, leading to stronger password practices.
- These interventions also improve users' situational awareness and threat detection capabilities during risk evaluation.
- The synergy between existing knowledge and new experimental results strengthens the case for incorporating cognitive exercises in cybersecurity training programs.

Thus, the study answers the main research question by demonstrating that short-term cognitive interventions are a practical and effective tool to improve user security behaviour across multiple critical domains.

5 Discussion

The results of this study provide compelling evidence supporting the role of short-term cognitive interventions, particularly focused breathing exercises and a brief cybersecurity awareness session, in improving user behaviour related to password creation and risk evaluation tasks. These findings contribute to the growing body of research exploring how cognitive science can inform cybersecurity practices, especially in addressing the human element of security.

5.1 Interpretation of Results

The significant improvement observed in the experimental group is consistent with previous research that links cognitive interventions to enhanced decision-making and emotional regulation (Seki et al., 2023; Andrade & Yoo, 2019). By focusing on simple, quick mindfulness exercises such as focused breathing, participants were able to reduce cognitive overload, enhance their focus, and make more informed decisions when it came to identifying suspicious links or creating strong passwords.

One of the most noteworthy outcomes of the study was the password creation task, where the experimental group showed a marked improvement in creating more complex passwords compared to the control group. This result underscores the importance of cognitive control in cybersecurity practices. Cognitive barriers, such as forgetfulness and cognitive inertia, often lead to weak password creation (Lahza & Alsamani, 2024). The focused breathing exercise appears to help participants overcome these barriers by improving their ability to concentrate and engage in more thoughtful decision-making, even in mundane tasks like password generation.

The risk evaluation task also demonstrated clear benefits for the experimental group. Participants who underwent the cognitive intervention displayed heightened sensitivity to phishing attempts and were more accurate in flagging suspicious emails and URLs. This suggests that even brief cognitive interventions can improve users' ability to identify common cybersecurity threats, which are often exploitative of human vulnerabilities rather than technical gaps. This aligns with findings from Moustafa (2022) and McCrohan et al. (2010), who emphasized the importance of attention and cognitive processes in cybersecurity decision-making.

5.2 Practical Implications

The practical implications of this study are significant for the design of future cybersecurity training programs. The findings suggest that integrating short, easily implementable cognitive exercises, such as focused breathing, can be a cost effective and scalable way to improve user security behaviours. As most cybersecurity breaches are due to human error, enhancing individual decision-making could substantially reduce vulnerabilities in digital systems.

Organizations and educational institutions could incorporate these exercises into their cybersecurity awareness programs to better prepare individuals to handle cybersecurity threats. Given the simplicity and low resource requirement

of cognitive interventions, these could be easily adopted in both online and offline training environments.

5.3 Limitations

Despite these promising results, several limitations must be acknowledged. First, the study was conducted in a controlled offline setting, which may not fully replicate the distractions and pressures of the real world digital environment. Future research could explore the efficacy of these interventions in more naturalistic settings, such as online training modules or as part of everyday digital interactions.

Additionally, the study focused on cognitive intervention such as focused breathing only. While these interventions were chosen based on existing research that suggests they improve focus and emotional regulation, other techniques, such as cognitive-behavioural approaches or attention training, could also be explored in future studies. Comparing the effectiveness of different interventions would provide a more comprehensive understanding of how cognitive strategies can be integrated into cybersecurity practices.

The study also relied on self reported data for the risk evaluation task, which may have introduced some bias in the participants assessments of phishing emails or suspicious links. Future studies could consider incorporating objective measures, such as time-to-detection or eye-tracking, to more accurately assess participants decision-making processes.

6 Conclusion

This study aimed to explore the effectiveness of short-term cognitive interventions specifically focused breathing exercises and brief cybersecurity awareness training in improving participants cybersecurity behaviours, particularly in the areas of password creation and risk evaluation. The results of the study provide valuable insights into how cognitive science can inform cybersecurity practices and contribute to reducing human errors, which are the leading cause of security breaches in today's digital world.

The study successfully addressed all the research questions posed. It demonstrated that short-term cognitive interventions, such as focused breathing exercises, significantly improve users' ability to create stronger passwords and enhance their awareness and behaviour when assessing cybersecurity risks like phishing attacks. These results highlight the effectiveness of cognitive techniques in promoting safer security practices and confirm their potential as practical tools for improving user cybersecurity behaviour.

Participants who engaged in the brief focused breathing exercise showed a marked increase in the strength and complexity of their passwords. This result aligns with prior research by Lahza and Alsamani (2024), which highlighted how cognitive inertia, forgetfulness, and mental fatigue often lead users to create weak or reused passwords. By enhancing participants' ability to concentrate and engage in more thoughtful decision-making, the focused breathing intervention effectively mitigated these cognitive barriers, leading to more secure password creation.

The risk evaluation task, which involved identifying suspicious emails and phishing attempts, also revealed significant improvements in the experimental group. This is consistent with findings from Seki et al. (2023), who established that mindfulness could enhance emotional regulation and decision-making. The results suggest that even brief cognitive interventions can improve users ability to detect common cybersecurity threats, which are often based on psychological manipulation rather than technical vulnerabilities.

These findings have important practical implications for cybersecurity training programs. Since human error remains a critical factor in most cyberattacks, integrating cognitive interventions such as focused breathing exercises into training programs could significantly enhance user behaviour. The simplicity and brevity of such exercises make them highly adaptable to a wide range of settings, from corporate training to educational programs. Given that cybersecurity threats, such as phishing and password vulnerabilities, rely heavily on human factors, improving cognitive control and decision-making processes in users can help mitigate these risks.

Moreover, this study adds to the growing body of literature on the intersection of cognitive science and cybersecurity. This research, therefore, fills a critical gap by providing experimental evidence that short cognitive interventions can have a tangible impact on improving user security behaviours.

In conclusion, the results highlight the potential of cognitive interventions to reduce the cognitive barriers that often lead to poor cybersecurity practices. By incorporating such interventions into cybersecurity training programs, organizations and individuals can enhance their ability to make more secure decisions, ultimately reducing the risk of cyberattacks. These findings represent an important step forward in integrating cognitive science into cybersecurity practices and underscore the need for future research to explore and refine these interventions further.

6.1 Ethical, Societal, and Scientific Impacts

This study carries several important implications across ethical, societal, and scientific domains. Ethically, the research promotes user empowerment by focusing on cognitive interventions that help individuals make better informed security decisions, rather than relying solely on restrictive or punitive security policies. It respects user autonomy and mental well being by offering supportive techniques like mindfulness and focused breathing, which are non-invasive and accessible. Societally, enhancing cybersecurity behaviour through simple cognitive exercises has the potential to reduce the frequency of data breaches caused by human error, thereby protecting individuals' privacy and reducing financial and emotional harm associated with cybercrime. This is especially relevant in an increasingly digital world where users of all ages interact with online systems daily. Scientifically, the study bridges the gap between cognitive science and cybersecurity by empirically testing how mental interventions influence digital behaviour. It contributes to the growing field of human-centered cybersecurity by offering evidence-based strategies that can be further explored and refined. The integration of survey data and systematic literature insights ensures both practical relevance and a strong theoretical foundation, supporting the advancement of interdisciplinary research.

6.2 Future work

Future research should explore the long term effects of cognitive interventions on cybersecurity behaviour, as this study focused only on short term improvements. Building on findings from both the survey and the systematic literature review, future work can examine how different types of cognitive techniques such as mindfulness, attention control, and emotional regulation compare in effectiveness across varied cybersecurity tasks. Additionally, expanding the research to diverse populations and digital contexts will help test the generalizability of these findings. Personalization of interventions based on user traits, as suggested in the literature, presents another promising direction. Integrating these cognitive strategies into real world security training programs, possibly in combination with gamification or behavioural nudges, could enhance user engagement and long term retention of secure practices.

References

- Anderson, B. B., Kirwan, C. B., Jenkins, J. L., and Eargle, D. (2015). "How polymorphic warnings reduce habituation in the brain—insights from an fmri study," in Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems CHI, Crossings, Seoul.
- Anderson, C. A., & Dill, K. E. (2000). Video games and aggressive thoughts, feelings, and behavior in the laboratory and in life. *Journal of Personality and Social Psychology*, 78(4), 772-790.
- Andrade, R. O., Fuertes, W., Cazares, M., Ortiz-Garcés, I., & Navas, G. (2022). An exploratory study of cognitive sciences applied to cybersecurity. *Electronics*, 11(11), 1692
- 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.
- Arksey, H. & Knight, P. (1999). *Interviewing for social scientists, an introductory resource with examples*. Sage Publications. ISBN 0 76 1 9 5869.
- Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. *Journal of Systems and Software*, 80(4), pp. 571-583. <https://doi.org/10.1016/j.jss.2006.07.009>.
- Charoensukmongkol, P. (2014). Benefits of Mindfulness Meditation on Emotional Intelligence, General Self-Efficacy, and Perceived Stress: Evidence from Thailand. *Journal of Spirituality in Mental Health*, 16(3), 171-192. <https://doi.org/10.1080/19349637.2014.925364>.
- Cuny, A. (2024). *Cognitive biases in cybersecurity*. Lappeenranta-Lahti University of Technology LUT.
- Creswell, J., & Poth, C. (2018). *Qualitative inquiry and research design: choosing among five approaches* (4th ed.). Sage Publications. ISBN 978-1-5063-3020-4.
- Familoni, B. T. (2024). Cybersecurity challenges in the age of AI: Theoretical approaches and practical solutions. *Cybersecurity and Information Technology Research Journal*, 12(3), 45-67.
- Forbes Advisor. (2024, August 28). *Cybersecurity stats: Facts and figures you should know*. Forbes.

Fink, A., (2019). *Conducting research literature reviews, from the Internet to paper* (5th ed.). Sage Publications. ISBN 978-1-4833-0103-7.

Frontiers. (2021). The role of user behavior in improving cyber security. *Frontiers in Psychology*, 12, 561011.

Greavu-Șerban, V., Constantin, F., & Necula, S.-C. (2025). Exploring heuristics and biases in cybersecurity: A factor analysis of social engineering vulnerabilities. *Systems*, 13(4), 280.

Israel, M., & Hay, I. (2006). *Research ethics for social scientists: Between ethical conduct and regulatory compliance*. Sage Publications. ISBN 13 978 1 4129 0389 9.

Jarjoui, S. (2023). Mindfulness: The first line of defense in cyberspace. In R. Raja & A. K. Dewangan (Eds.), *Online Identity - An Essential Guide*. IntechOpen.

Jesson, J., Matheson, L., & Lacey, F. M. (2011). *Doing your literature review: Traditional and systematic techniques*. Los Angeles, CA: Sage Publications.

Kannelønning, K., & Katsikas, S. K. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. *Information and Computer Security*, 31(4), 499-526.

Kävrestad, J., Eriksson, F., & Nohlberg, M. (2018). THE DEVELOPMENT OF A PASSWORD CLASSIFICATION MODEL. *Journal of Information System Security*, 14(1).

Kävrestad, J., & Naqvi, B. (2024). Cognitively available cybersecurity: A systematic literature review. *Human-Centered Software Engineering Conference*.

Khadka, R., & Ullah, M. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security*, 24(119).

Kitchenham, B. (2004). *Procedures for performing systematic reviews*. Keele, UK, Keele University, 33(2004), 1-26.

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering*. EBSE Technical Report EBSE-2007-01. http://cdn.elsevier.com/promis_misc/525444systematicreviewsguide.pdf.

Lahza, H., & Alsamani, B. (2024, September). Behavioral Cybersecurity: Dynamic Persuasive Strategies to Enhance Password Security. In *2024 7th International Conference of Computer and Informatics Engineering (IC2IE)* (pp. 1-9). IEEE.

Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *computers & security*, 28(3-4), 215-228.

Maalem, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, 3(10).

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of internet Commerce*, 9(1), 23-41.

Moustafa, A. (Ed.). (2022). *Cybersecurity and Cognitive Science*. Academic Press.

Mylrea, M., & Gourisetti, S. N. G. (2017). An introduction to buildings cybersecurity framework. In 2017 IEEE Symposium.

Naqvi, B., Kävrestad, J., & Islam, A. (2023). Ensuring usable cybersecurity for all: Examining cognitive disabilities from research to industry. *SSRN Electronic Journal*.

Nielsen, G., Vedel, M. and Jensen, C.D. (2014), "Improving usability of passphrase authentication", Paper presented at the Twelfth Annual International Conference on Privacy, Security and Trust.

Paré, G., & Kitsiou, S. (2017, Feb 27). Chapter 9 Methods for Literature Reviews. In *Handbook of eHealth Evaluation: An Evidence-based Approach*. [Online]. University of Victoria. Retrieved January 30, 2021 from <https://www.ncbi.nlm.nih.gov/books/NBK481583/>.

Petrides, K. V., Mikolajczak, M., Mavroveli, S., Sanchez-Ruiz, M. J., Furnham, A., & Pérez-González, J. C. (2016). Developments in trait emotional intelligence research. *Emotion review*, 8(4), 335-341.

Rankin, C. H., Abrams, T., Barry, R. J., Bhatnagar, S., Clayton, D. F., Colombo, J., et al. (2009). Habituation revisited: an updated and revised description of the behavioral characteristics of habituation. *Neurobiol. Learn. Mem.* 92, 135–138. doi: 10.1016/j.nlm.2008.09.012.

Rawat, D. B., Doku, R., & Garuba, M. (2021). Cybersecurity in big data era: From securing big data to data-driven security. *IEEE Transactions on Services Computing*, 14(6), 2055-2072.

Roghanizad, M., Choi, E., Mashatan, A., & Turetken, O. (2021). Mindfulness and cybersecurity behavior: A comparative analysis of rational and intuitive cybersecurity decisions. *Americas Conference on Information Systems (AMCIS 2021)*.

Rooney, M. J. (2023). *An Empirical Assessment of the Use of Password Workarounds and the Cybersecurity Risk of Data Breaches* (Doctoral dissertation, Nova Southeastern University).

Rue, R., Pfleger, S. L., & Ortiz, D. (2007). A framework for classifying and comparing models of cyber security investment to support policy and decision-making. *Workshop on the Economics of Information Security (WEIS)*, 1-16.

Ruoti, S., Andersen, J. and Seamons, K. (2016), "Strengthening password-based authentication", Paper presented at the Twelfth Symposium on Usable Privacy and Security (SOUPS).

Sánchez-García, I. D., Mejía, J., & San Feliu Gilabert, T. (2022). Cybersecurity risk assessment: a systematic mapping review, proposal, and validation. *Applied Sciences*, 13(1), 395.

Schmid, S., Wilson, D. A., & Rankin, C. H. (2014). Habituation mechanisms and their importance for cognitive function. *Frontiers in Integrative Neuroscience*, 8, 97.

Seigfried-Spellar, K. C., Rogers, M. K., & Thorpe, J. (2017). Exploring cyber-criminal activities, behaviors, and profiles. In *Cybercrime through an interdisciplinary lens* (pp. 123-144). Springer.

Seki, T., Çimen, F., & Dilmaç, B. (2023). The Effect of Emotional Intelligence on Cyber Security: The Mediator Role of Mindfulness. *Bartın University Journal of Faculty of Education*, 12(1), 190-199.

Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security fatigue. *It Professional*, 18(5), 26-32.

Stobert, E. and Biddle, R. (2014), "The password life cycle: user behaviour in managing passwords", Paper presented at the Proc. SOUPS.

Taylor, S., & Furnell, S. (2020). Review and insight on the behavioral aspects of cybersecurity. *Journal of Cybersecurity and Privacy*, 1(1), 1-15.

Ur, B., Noma, F., Bees, J. and Shay, R. (2015), "'I added!' at the end to make it secure": observing password creation in the lab", Paper presented at the SOUPS

Veksler, V. D., Buchler, N. E., & McLemore, L. (2018). The role of cognitive science in cybersecurity: Human factors and behavioral modeling. *Frontiers in Psychology*, 9, 691.

Wang, X., Li, J., & Zhang, X. (Eds.). (2023). *Cognitive sciences and their application in cybersecurity*. SpringerLink Collection.

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A., (2012). *Experimentation in software engineering*. Springer. ISBN 978-3-642-29044-2.

Woods, N. and Siponen, M. (2018), "Too many passwords? How understanding our memory can increase password memorability", *International Journal of Human-Computer Studies*, Vol. 111, pp. 36-48.

Appendix – Survey

Cybersecurity Behavior Study – Participant Form

SECTION A: Informed Consent Form

Title of Study: The Impact of Short-Term Cognitive Interventions on Cybersecurity Behavior

Researcher: _____

Institution: _____

Purpose:

This study explores whether a short breathing exercise can improve decision-making in cybersecurity tasks (like password creation or spotting phishing risks).

What You'll Do:

- Create sample passwords.
- Evaluate 5 cybersecurity scenarios.
- Optionally perform a short breathing exercise.
- Fill out a brief feedback form.

Rights:

- Participation is voluntary.
- You may withdraw at any time.
- No personal data will be collected.
- All responses are anonymous.

Consent:

- I have read and understood the study information.
- I voluntarily agree to participate.
- I understand I may stop at any time.
- I understand my data will remain anonymous.

Participant ID: _____

Participant Signature: _____

SECTION B: Main Task Sheet

Participant ID: _____

Group: Control Experimental

Part 1: Password Creation Task

Please write a password you'd realistically use for the following accounts:

1. Online Banking Account

Password: _____

2. University/School Portal

Password: _____

3. Social Networking Site

Password: _____

Part 2: Risk Evaluation Scenarios

Instructions: Read each scenario. Then answer:

- Q1: Is this a security risk? (Yes/No)

- Q2: What would you do?

- Scenario 1 – Email from your bank saying: 'Urgent: Verify your account immediately!'

Yes No

What would you do?

- Scenario 2 – Pop-up says: 'Your browser is out of date. Click here to update.'

Yes No

What would you do?

- Scenario 3 – Login screen appears similar to your university site but with a slightly different URL.

Yes No

What would you do?

- Scenario 4 – Social media message: 'Check out this video I made of you!' (with a link)

Yes No

What would you do?

- Scenario 5 – Online store offers 70% off if you provide full personal details immediately.

Yes No

What would you do?

SECTION C: Post-Task Feedback Survey

1. How focused did you feel during the task? (1 = Not at all, 10 = Extremely)

1 2 3 4 5 6 7 8 9 10

2. How stressed/distracted were you during the task?

1 2 3 4 5 6 7 8 9 10

3. (Experimental group only): Did the breathing exercise help your focus?

Yes No Not sure

4. If yes, how did it help?

5. How did you decide on your passwords?

6. What helped you assess the risk scenarios?

End of Form - Please return this to the researcher. Thank you!