Master Degree Project

UNIVERSITY OF SKÖVDE

The Effect of Time Pressure on Human Behavior Regarding Phishing Susceptibility

Human Aspects in Information Security

Master Degree Project in Informatics
Second Cycle 30 credits
Spring term 2023
Student: Muhammad Abbas Khan Abbasi
Supervisor: Joakim Kävrestad
Examiner: Marcus Nohlberg

ABSTRACT

Human errors are common in the contemporary cyber ecosystem, and in an organization’s cybersecurity chain, humans are considered the weakest link. Cybercriminals exploit human vulnerabilities using sophisticated attacks such as phishing. Human susceptibility to phishing is a persistent threat, and has a devastating effect on organizational and personal security. Previous researchers found that human susceptibility to phishing increases in presence of some factors such as organizational, individual, and environmental. Various studies highlight time pressure as one of the influencing factors that can negatively or positively impact human behavior. This research study aimed to investigate the effect of time pressure on human cybersecurity behavior regarding the ability to detect phishing. The study used quantitative research and developed a questionnaire comprising interactive phishing emails distributed online to 03 random groups having different time limits to complete the questionnaire. The study received 356 complete responses. The study's result shows a slight change in user behavior under time pressure, and the impact of time pressure can be positive or negative. However, the results are not statistically significant for all demographic groups to accept this slight change in variance. Moreover, this study's results validate previous studies on human susceptibility to phishing and found more than 50 % of respondents vulnerable to phishing.

Thus, the results of this study indicate that the factor of time pressure itself does not significantly impact the human ability to detect phishing. However, it is essential to note that other work-related tasks or stress associated with time pressure can influence human behavior in detecting phishing attempts.

In conclusion, the author also proposes further testing and some methodology tweaking by modifying the time given to each tested group and adding more elements to the questionnaire. Finally, the study also suggested conducting the same analysis on physically controlled groups in an organizational or institutional setting.

Keywords: Cybersecurity Behavior, Phishing susceptibility, Cybersecurity Awareness, Time pressure, the human factor.

ACKNOWLEDGMENT

I am very grateful and acknowledge the continued support of my thesis supervisor Joakim Kävrestad. Joakim Kävrestad helped me a lot during the entire process. He identified various areas of improvement, which improved my conceptual knowledge and helped me meet my thesis goals.

I would also like to appreciate and acknowledge the help and inputs provided by my Examiner, Marcus Nohlberg, during the entire learning process by giving valuable inputs in periodic reviews and discussions during examiners' open doors.

Moreover, I would appreciate and acknowledge the input of experts who reviewed this study’s questionnaire and other methodological aspects. Maintaining quality and usability was fairly hard to achieve without their precious input.

In addition, I would love to give credit to all PICS staff who empowered me by providing knowledge and understanding about Privacy, Information security, and cybersecurity. Besides this, I also acknowledge the efforts of the Swedish government and the administration of the University of Skovde, who provided us conducive learning and development environment.

I am also profoundly thankful to the Swedish Institute (SI), which gave me financial support by granting the Swedish Institute Scholarship for Global Professionals (SISGP). With SISGP support, my dream of studying abroad has come true.

Finally, I am very thankful to my family and friends who supported me throughout my studies and thesis.

Table of Contents

1 Introduction

The emergence of new technologies and digitalization enables data resource accessibility at a glance, whereas it is also providing an access landscape to cybercriminals (Alqahtani, 2022; Hazari, Hargrave, & Clenney, 2008). Furthermore, cybercriminals are exploiting vulnerabilities of these newly developed and existing technologies for several offenses and crimes using a variety of ways, thus bringing many actors at risk of breaching their personal, organizational, or even state critical data (Abd Rahim, Hamid, Kiah, Shamshirband, & Furnell, 2015; Aslam et al., 2022). Therefore, this sophistication and substantial rise in cyber threats leave no space for information and cybersecurity personnel to merely rely on technical security controls (McCormac et al., 2018).

To mitigate such threats, organizations use various preventive measures and continuously update these implemented measures according to the sophistication of threats and technological evolutions (Abd Rahim et al., 2015). These measures have a positive impact on organizational security posture. However, such mechanisms' effectiveness depends on factors such as organizational security culture, people's awareness of the threat landscape, and administrative controls (Aslam et al., 2022). The issues mentioned above revolve around humans who are an essential part of this process, having a role as leaders, middle managers, or ordinary workers. This paradigm shift demands fostering a security culture within the organization and considering human factors as one of the major priorities. An expensive state-of-the-art security mechanism is of no means if humans interacting with it have an obstacle in adopting it. This is due to its design, users' lack of awareness about its use, and its importance from users' and organizations' perspectives. These obstacles result in a low positive impact from reduced data breach incidents and open an easy attack path for adversaries (Zwilling et al., 2022). In the contemporary cyber ecosystem, human errors are common, and in an organization's cybersecurity chain, humans are considered the weakest link (Chaudhary, Gkioulos, & Katsikas, 2022; Zwilling et al., 2022).

A study by Yang et al. (2022) reported that more than 40 million internet users fall into phishing attacks yearly, which is growing, making it a significant risk for people using online services. Similarly, various studies on phishing susceptibility among the employees of an organization also found more than 60 % of employees susceptible to phishing. However, the experiment found good cybersecurity awareness in general regarding password security and device use (Ikhsan & Ramli, 2019). According to Yang et al. (2022), studies reported that 40-80 % of internet users failed to identify the malicious links and perform transactions on malicious sites. Similarly, this situation worsens in complex and pressured working environments (Williams & Joinson, 2020).

The issues mentioned above raise the importance of awareness and training programs regarding the latest challenges in the cyber world and their redressal mechanisms. In literature, these awareness and training programs are defined as information security awareness (ISA) (Fertig & Schütz, 2020; Wiley, McCormac, & Calic, 2020) or cybersecurity awareness (CSA) programs (Chaudhary et al., 2022; Zwilling et al., 2022). These names are used interchangeably or in contrast by different authors in the literature. However, some authors used the terms according to the scope of the programs. For instance, CSA is used to primarily focus on cyber threats which arise from the use of the internet and its related implications (Abd Rahim et al., 2015).

These awareness and training programs enhance human understanding of a particular situation and help them transform learning into practice (Chaudhary et al., 2022). Hence, an organization that possesses a strong security posture and culture updates these programs, and provides awareness and training through state-of-the-art methods, taking into account the latest trends and technologies. Furthermore, these methods focus on human aspects such as usability, adaptability, and sustainability (Abd Rahim et al., 2015; Chaudhary et al., 2022).

A good CSA program aims to improve knowledge and bring positive changes in people's attitudes and behavior, which subsequently help people and organizations collectively contribute towards protected cyberspace (Chaudhary et al., 2022). Therefore, developed nations and organizations need pre-emptive approaches to inform people, such as their employees and common citizens, of information and cybersecurity threats, by creating information and cybersecurity awareness programs (Alqahtani, 2022). These awareness programs enable users to enhance their capabilities and readiness to adopt a particular behavior and are vital in mitigating information and cybersecurity risk (Parsons et al., 2017).

Both subjective and objective methods evaluate the success of the CSA program. For instance, diagnostic, formative, and summative assessments are used for knowledge assessment, whereas anonymous surveys assess human attitudes. On the other hand, measuring behavior is complex, and at present different approaches are used to evaluate user behavior, such as self-reporting, surveys, monitoring online user trends, checking audit logs, observation, simulated attacks, and passive data analysis (Abd Rahim et al., 2015; Chaudhary et al., 2022).

Studies show that the effectiveness of CSA programs is also subject to many aspects, such as usability, adaptability, and people's attitude and behavior (Abd Rahim et al., 2015; Chaudhary et al., 2022). Therefore, significant work has been done on the human aspect considering usability and adoptability by making user-friendly training programs, interfaces, and easily understandable technology (Chaudhary et al., 2022). However, user behavior is also vital in making all efforts successful. Research shows that improved user behavior significantly reduces security breach risk by up to 45-70 percent (McCormac et al., 2018). The study found that even after going through a comprehensive CSA program, the users do not exhibit safe behavior in real-time, therefore, assessing CSA using knowledge assessment and behavioral actions is essential (Chaudhary et al., 2022; Fertig, Schütz & Weber, 2020).

The unsecured user behavior has several reasons, such as personal attitude, skill, knowledge, fatigue, self-efficacy, stress, workload, time pressure, unconsciousness, culture, demographics, lack of interest, the habit of non-compliance, risk-taking, controllability, emotional stability, etc., and all these issues have an impact on awareness (Abd Rahim et al., 2015; Chowdhury, Adam, & Skinner, 2018; Hong et al., 2022; McCormac et al., 2017; Skinner & Parrey, 2019; Zwilling et al., 2022). Assessing behavior without considering the aforementioned barriers can result in incorrect assessment results, ultimately leading to ineffective feedback for CSA program improvement (Chaudhary et al., 2022). Studies also found that awareness and training programs without having components of resilience skills can never be helpful because if people are not trained to absorb pressure or stress, they behave unsafely and also ignore important security alerts (Chowdhury et al., 2018; McCormac et al., 2018).

Apart from the aforementioned aspects, research studies also demonstrate that training as a standalone approach is not a comprehensive solution to existing cyber threats like phishing. Because even after attaining extensive formal training, people still click phishing links and find it hard to detect any email or link as phishing (Kävrestad et al., 2022; Yang et al., 2022). A recent study on susceptibility to phishing found cognitive abilities, personal traits, and individual differences as influential factors that are mostly exploited by attackers while planting a phishing attack (Goel, Williams, & Dincelli, 2017). Therefore, context-based training considering user needs and style emerge as a viable solution (Kävrestad et al., 2022). However, studies also highlighted the sources of difficulty in detecting phishing and found stress induced by time constraint pressured environment as a significant contributing factor (Goel et al., 2017; Williams & Joinson, 2020; Yang et al., 2022). In such situations, most people instantly process email messages and information, overseeing clues showing deception (Goel et al., 2017). In contrast, another study on employee behavior found time pressure to induce positive and negative effects (Zhang, Yao, Qunchao, & Tsai, 2022).

Therefore, quantifying factors impacting this susceptibility is essential to mediate human exposure to phishing. Hence, making the significance of conducting behavioral assessments considering factors affecting user behavior, such as time pressure that lead to unsafe practices and open threat to organizational security by exploiting these human vulnerabilities.

Different methodical approaches measure user behavior, such as questionnaires, surveys, observances, simulated attacks, or passive data analysis. The result generated by using these methodical approaches leads to input for improvement in training programs. However, all methods have limitations and maturity issues, which demand further validation and improvements.

1.1 Problem Description

To improve awareness and training programs, organizations need to assess employees' levels of understanding before and after a training program. These assessments evaluate knowledge, attitude, and behavior or practice (KAB/P) using various methods. Studies prove that behavioral assessment is vital in assessing actual user actions that a user exhibit being online or interacting with digital devices (Abd Rahim et al., 2015; Ayyagari & Crowell, 2020; Chaudhary et al., 2022; Nunes, Antunes, & Silva, 2021).

The contemporary sophistication of phishing attacks is making them harder to detect for most people, despite having training and knowledge (Kävrestad et al., 2022). However, research shows that users' careful behavior and search capabilities for details about email sources, used language, and targeted directed URLs considerably reduce deception chances. According to Goel et al. (2017), in reality, most people ignore such information and cues that quickly get them into an attacker trap. For example, a study by Ikhsan & Ramli (2019) found that 69 % of employees working at an anonymous government sector organization clicked the phishing links during phishing assessment because of a lack of knowledge about phishing. However, the same study found a good CSA knowledge level among employees but found them mainly vulnerable to phishing. Therefore, author emphasizes periodic phishing assessments to improve people's knowledge about phishing attacks to reduce people's susceptibility to phishing (Ikhsan & Ramli, 2019).

During research on individual difference in human behavior, various studies found that different demographic group exhibits varied behavior when exposed to the cyber world, which makes them vulnerable to cyber threats such as scam and phishing (Goel et al., 2017; Zwilling et al., 2022). For example, studies show that women are more susceptible to phishing than men (Goel, Williams, & Dincelli, 2017). Similarly, young people are more exposed to threats while being online than older people. Hence young people are also more susceptible to phishing (Abd Rahim et al., 2015; Goel et al., 2017).

Similarly, the studies also found that people with a higher education level behave more securely because they possess more CSA (Chua, Wong, Low, & Chang, 2018; Wiley, McCormac, & Calic, 2020). Apart from that, studies also found interesting facts about the level of CSA among various citizens. For example, the authors found that different nations also possess varied cybersecurity behavior because of their culture (Rocha Flores, Holm, Nohlberg, & Ekstedt, 2015) and the availability of technological and economic resources (Zwilling et al., 2022). In addition, the study also shows that people having more IT knowledge are less vulnerable to phishing (Rocha Flores et al., 2015). Therefore, the design of the training program without considering these variations, their impacts, and aftermaths cannot yield specified goals (Abd Rahim et al., 2015).

In addition, the assessment of KAB without considering individual, organizational, and intervention factors cannot expose actual assessment results. Among these factors, various research studies evaluated individual factors, “The Big Five,” and found correlation and impact on user behavior (McCormac et al., 2017). However, according to this research findings, factors such as job stress and time pressure are merely addressed. Only a few studies have been found on these critical aspects. For example, a study by McCormac et al. (2018) assessed the effect of resilience and job stress on cybersecurity behavior. Still, no further validation was done to verify the results (McCormac et al., 2018). Similarly, the “time pressure” factor is only considered qualitatively (Chowdhury et al., 2018; Chowdhury, Adam, & Teubner, 2020; Skinner & Parrey, 2019). According to studies, the stress factor induced by time pressure increases significantly in the complexity of communication systems and technologies. Furthermore, when both factors are considered together, they weaken the human firewall. As a result, this affects security measures (Chowdhury, Adam, & Skinner, 2019; Chowdhury et al., 2020).

Studies also found that time pressure-induced stress during extensive workloads makes users more susceptible to unsafe practices, which lead to incorrect decision-making, such as detecting phishing attempts and finding cues to deception. The time-bound activities reduce cognition abilities to process information, and people ignore security requirements. In addition, too many security requirements also pose a threat because, under time pressure, such condition induces stress, and studies define this issue as security overload.

Therefore, to manage the task, the user starts disregarding and disclosing information and security requirements (Chowdhury, Adam, & Teubner, 2020; Parsons et al., 2017; Skinner & Parrey, 2019). However, to detect phishing attacks, one of the critical approaches is finding clues to see any emails as fraudulent. Therefore, in a time-pressured environment, human susceptibility to phishing increases because of the habit of disregarding and avoiding information to meet workload requirements (Chowdhury et al., 2020). However, a study on the impact of time pressure on employee performance gives a new dimension and found that time pressure has both positive and negative effect on people (Zhang et al., 2022).

The aforementioned aspects and their dynamic nature emphasize the significance of adopting a context-based training approach that considers individual needs. Inadequate training programs and a lack of awareness among individuals regarding specific situational factors that influence user behavior can expand the threat landscape and increase the frequency of successful breaches. Consequently, there is a need to quantify factors contributing to the exploitation of human vulnerabilities, such as assessing resilience to phishing susceptibility under time pressure and stress conditions.

Various tools have utilized to measure user behavior, such as questionnaires, surveys, observances, simulated attacks, or passive data analysis. These measures provide valuable insights for improving awareness and training programs. However, all these tools have some limitations, which can be quantified using suggestions proposed in various studies, such as by ensuring user responses privacy through anonymized questionnaires and surveys to avoid response bias or conducting a simulated assessment to check user real behavior through an online questionnaire, passive data analysis, etc. (Chaudhary et al., 2022; Egelman, Harbach, & Peer, 2016; Fertig et al., 2020; Parsons et al., 2017). However, passive data analysis is an extensive, time-consuming process and also has some ethical issues, if such data is inadequately used (Chaudhary, Gkioulos, & Katsikas, 2022).

The aforementioned methodological aspect and research gaps in the quantification of CSA programs and not understanding the impact of factors affecting user susceptibility to cyber-attacks such as phishing significantly increase cyber-attacks, ultimately resulting in catastrophic effects. Hence, this opens an avenue for the researcher to identify and test appropriate further opportunities and solutions that can effectively bridge the abovementioned gaps by limiting the impact of such cyber threats. Therefore, this research aims to identify the effect of time pressure on human behavior to phishing susceptibility and how time pressure impacts different demographics to phishing susceptibility.

1.2 Research Aim and Research Question

The aforementioned problems raise the necessity of testing and retesting factors affecting human cybersecurity behavior among the different demographic groups so awareness and training programs can be molded to specific individual needs and people can be trained to more context-based approaches.

Therefore, this research aims to identify the impact of time pressure on human behavior regarding phishing susceptibility and how time pressure-induced stress affects different people, which practically leads to unsafe cybersecurity practices while interacting with phishing emails. On the other hand, the study also supports Zhang et al. (2022) results by having results that show a positive impact on user performance regarding phishing detection.

This study is influenced by concepts described in recent studies for using metrics for assessing human behavior and theoretical motivation about time pressure impact on human cybersecurity behavior (Chaudhary et al., 2022; Chowdhury et al., 2018, 2019; Chowdhury et al., 2020). This study will adopt a metrics solution described in Chaudhary et al. (2022) consisting of an impact indicator, measuring factor, and measurement method. The adopted metrics will help decision-making and map Chaudhary et al. (2022) methodology in the following context. The impact indicator of this research study is time pressure. The measured factor is user behavior toward a phishing email, and the measurement method is a simulated questionnaire-based survey. This metric also defines the measurement scale, which in this study is accurate responses to detecting phishing emails. The user with a more precise detection rate demonstrates a higher awareness and resilience to time pressure by not being deceived by phishing attempts and vice versa.

This research work aimed at targeting the general public across the world. It measures the effect of time pressure on phishing susceptibility in different demographic groups such as gender, age groups, nationality, level of education, and IT competence.

The result of this study contributes in the following ways:

1. It will help quantify the impact of time pressure on human behavior to phishing susceptibility.
2. It helps identify the existing level of CSA to phishing vulnerability and resilience to time pressure among different demographic groups.
3. Assists in planning CSA programs for diverse government authorities and organizations, ensuring that such programs are tailored to meet the specific needs of different demographic groups. This is achieved by leveraging the findings of this study, particularly within the context of phishing, to make the programs more meaningful and effective.
4. This study will also help the future researchers by providing a method and approach to measure the effect of time pressure in different cybersecurity scenarios.

In order to answer the research problem, the following research question (RQ) was explored.

RQ. How does time pressure affect human behavior regarding phishing susceptibility?

Based on the background literature, this study assumed that increased time pressure would lead to a lowered or raised ability to detect phishing e-mails accurately. Consequently, the following hypothesis (H1) will be tested in this research,

H1: Time pressure affects human behavior regarding phishing susceptibility.

The answer to the hypothesis can be a positive or negative impact. However, if no such relationship is established, the NULL hypothesis will establish, showing that no relationship exists among studied variables. H1 was tested using five different demographic aspects. These demographic aspects were gender, age, IT competence, level of education, and nationality. These demographics were tested as subgroups, where subgroup 1 was developed according to Goel et al. (2017) findings, where the authors found that women are more susceptible to phishing. Therefore, subgroup 1 was set accordingly to check does females are more vulnerable to phishing under time pressure. Then subgroup 2 was developed according to the findings of Goel et al. (2017) and Abd Rahim et al. (2015), where the authors found that young people are more susceptible to phishing. So subgroup was tested to check if young people are more vulnerable to phishing under time pressure.

Likewise, subgroup 3 was developed on the finding of Rocha Flores et al. (2015), where authors found that people having more IT knowledge have better level of CSA, so they are less susceptible to phishing. Therefore, subgroup 3 was tested to check if people having less IT competence are more vulnerable to phishing under time pressure. Similarly, a study by Chua et al. (2018) and Wiley et al. (2020) found that people with a higher education level possess better levels of CSA; hence, they are less vulnerable to cyber threats. Therefore, subgroup 4 was constructed accordingly to test if people with a low education level are more susceptible to phishing under time pressure.

Finally, subgroup 5 was constructed according to the findings of Zwilling et al. (2022), where the authors found that citizens having more economic and technological resources have better level of CSA; hence they are less vulnerable to cyber threats. So, subgroup 5 was tested to check if different nationalities with less economic and technological resources are more susceptible to phishing under time pressure.

On the contrary, if any of the hypotheses are not established, then the null hypothesis will establish, meaning no relation exists among studied variables.

In order to answer the research question, this thesis composition is as follows. Section 2 describes the background of this research, where various research articles have been added to understand the problem and give an overview of existing solutions. Section 3 describes the methodology of how this research was carried out. Section 4 presents the results from the analysis of the questionnaire collected data. Finally, section 5 provides the discussion section, and section 6 concludes the study by summarizing the results and reflecting on future work.

2 Background

This chapter presents the background of the study and consists of research work from past research articles in a related area. Section 2.1 describes factors affecting human cybersecurity behavior and their quantification approaches, and section 2.2 describes phishing susceptibility and human cybersecurity behavior to time pressure.

2.1 Factors Affecting Human Cybersecurity Behavior and Their Quantification Approaches

The evolving cyber threat landscape makes CSA fluid which changes over time. Therefore, organization continues to offer new awareness and training programs that increase employee awareness of the latest threats. However, improvement in these programs is only possible by having an effective feedback system in the form of results from existing approaches (Chaudhary et al., 2022). These results can be extracted by measuring the level of awareness after the successful conduct of the CSA program.

In order to assess the CSA program, different studies have been conducted where some studies only focus on the evaluation of the program without considering demographic, personal factors, intervention factors, and organizational factors which affect or influence CSA (McCormac et al., 2017; Ngoqo & Flowerday, 2015; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014). These factors are shown in Figure 1 below and are described in “The Human Aspects of Information Security Model (HAIS)”(Parsons et al., 2014). In addition, some studies focused on one or two aspects, such as individual or intervention factors (Lebek, Uffen, Neumann, Hohler, & Breitner, 2014; Wiley et al., 2020; Zwilling et al., 2022). Such studies used questionnaires, surveys, formative and summative assessments, skill assessments, simulation, and passive data to assess CSA.

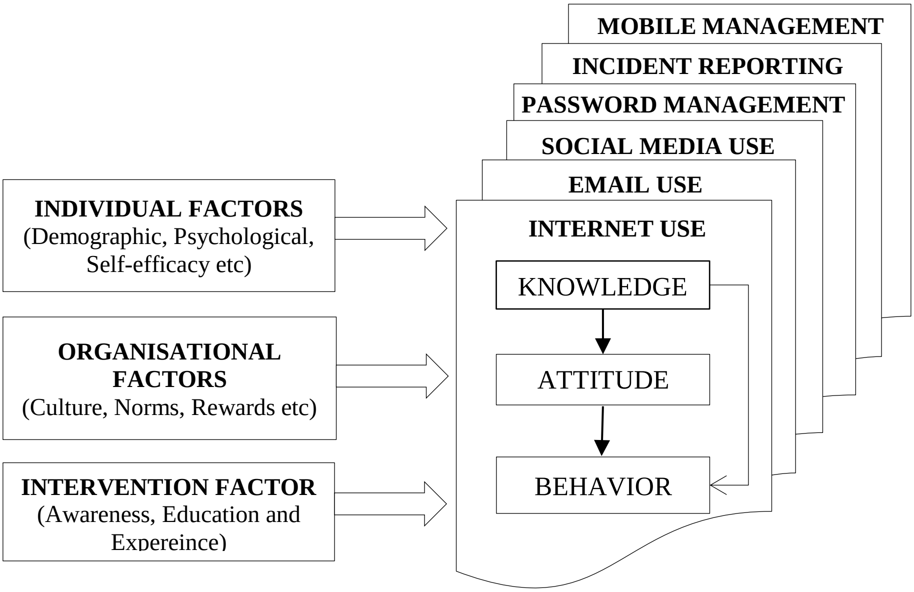


Figure 1 HAIS Model Showing Factors Influencing ISA (Parsons et al., 2014) (Redrawn)

Similarly, researchers also used social or behavioral science to assess CSA by relating various factors with behavioral intentions (Abd Rahim et al., 2015; Lebek et al., 2014). The methodologies used in these studies were mainly qualitative and quantitative (Abd Rahim et al., 2015). All these approaches have advantages and disadvantages, and some are not recommended as standard evaluation benchmarks due to various constraints such as time limitations, cost, and privacy issues (Chaudhary et al., 2022; Enisa, 2018). Common examples of the aforementioned approaches are passive data analysis in the context of time and privacy and real-time behavioral analysis in the context of cost and privacy. Whereas few studies shed light on the importance of metrics-based solutions to measure CSA (Chaudhary et al., 2022), and some researchers identified the behavior as an important measuring metric (Enisa, 2018; Fertig & Schütz, 2020; Scholl, Leiner, & Fuhrmann, 2017). The summary of research efforts in this regard is described below.

According to Chaudhary et al. (2022), knowledge, attitude, and behavior (KAB) are the key aspects of CSA programs. However, CSA's primary objective is to motivate a person to exhibit secure online behavior. Therefore, various studies used different behavioral modeling and social and psychological theories to analyze the knowledge and attitude impact on change in behavior. Chaudhary et al. (2022) conducted qualitative research and proposed a metrics-based approach to assess CSA. The study has two major contributions that it identified a) the criteria of good metrics development, b) the European Literacy Policy Network (ELINET) four indicators, measured factor, and their measurement methods which are effective for evaluating CSA. Figure 2 below shows the identified CSA evaluation metrics. The author claimed these identified metrics are a good benchmark for assessing the CSA program and discourages using metrics that constitute motivation, ability, and trigger. Furthermore, the authors of this paper recommended applying proposed metrics in parts to save cost and suggest assessment automation. However, the authors have not given any proof of concept for the proposed model. Whereas the authors of this study also praised the survey-based questionnaire method as a cost-effective and easily adoptable method despite some limited disadvantages (Chaudhary et al., 2022).

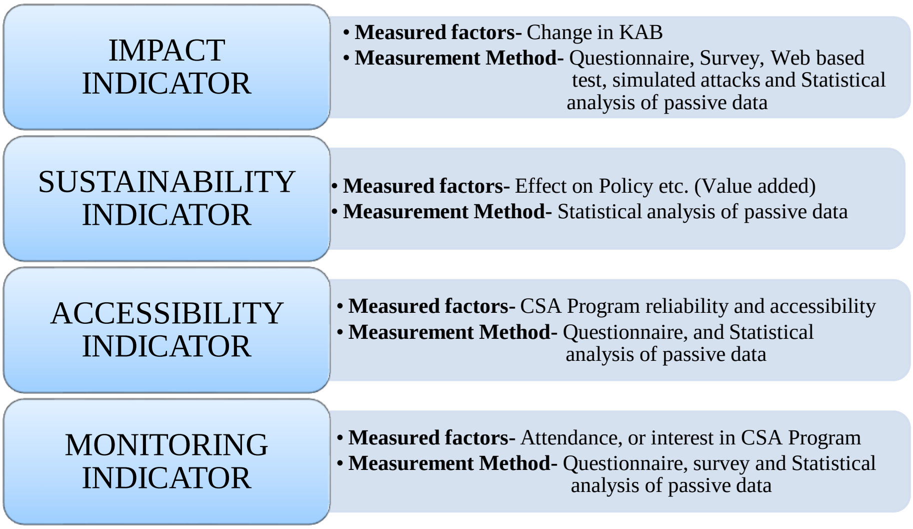

IMPACT INDICATOR
• Measured factors- Change in KAB
• Measurement Method- Questionnaire, Survey, Web based test, simulated attacks and Statistical analysis of passive data
SUSTAINABILITY INDICATOR
• Measured factors- Effect on Policy etc. (Value added)
• Measurement Method- Statistical analysis of passive data
ACCESSIBILITY INDICATOR
• Measured factors- CSA Program reliability and accessibility
• Measurement Method- Questionnaire, and Statistical analysis of passive data
MONITORING INDICATOR
• Measured factors- Attendance, or interest in CSA Program
• Measurement Method- Questionnaire, survey and Statistical analysis of passive data

Figure 2 CSA Evaluation Metrics (Chaudhary et al., 2022) (Redrawn)

Similarly, another popular and widely adopted approach by different studies is the Human Aspects of Information Security Questionnaire (HAIS-Q) (Parsons et al., 2017; Parsons et al., 2014). Parsons et al. designed HAIS-Q by adopting both qualitative and quantitative approaches. HAIS-Q is accepted as a validated tool to access CSA. HAIS-Q has been adopted by the subsequent researcher for analysis of demographic aspects where the author applied this approach to Australia (Parsons et al., 2017), South Africa (Kritzinger, Da Veiga, & van Staden, 2022), and the Netherlands (Witsenboer, Sijtsma, & Scheele, 2022) the result of the analysis found different CSA results among demographic groups segmented upon gender, age, education, experience, and region, etc. HAIS-Q has been used to access individual factors, "The Big Five": conscientiousness, openness, emotional stability, extraversion and agreeableness, and risk-taking. The results found different variances in ISA for each aspect (McCormac et al., 2017).

A similar questionnaire was also adopted by (McCormac et al., 2018) to measure the relationship between job stress, resilience, and ISA and found these aspects dependent on each other. For instance, higher resilience can help the employee to absorb stress and vice-versa. The study also highlighted that HAIS-Q, self-reported data, and other similar approaches could provide valuable results, but this approach can be biased and result in measurement errors. Similarly (Kritzinger et al., 2022) also identified and suggested a few question removal from HAIS-Q according to demographics. However, the application of HAIS-Q is still not applied to all organizational aspects and demographic studies for applicability and validity, such as compliance with policies, individual confidence, frequency of using the internet, organization culture, and mitigating privacy concerns and socially desirable manner (McCormac et al., 2017; Parsons et al., 2017).

Another study Security Behavior Intentions Scale (SeBIS), developed a questionnaire and scale to measure user behavior intention. The study identified 16 items mapped on four factors that assess attitude toward behavior: selecting passwords, securing devices, ensuring updates, and using a preemptive approach to awareness. The authors of this paper proposed validation of SeBIS for correlating intended behavior to actual behavior since it only measures behavior intention (Egelman & Peer, 2015). To validate the study for measuring behavior, Egelman et al. conducted a second study and constructed an argument that intention leads to behavior, and their high results of correlation in SeBIS four sub-scales and secure security behavior found this tool valid and reliable to measure security behavior. (Egelman, Harbach, & Peer, 2016).

Moreover, a study on "Risk and Demographics, Influence on Security Behavior Intentions" suggested improvement in SeBIS and proposed the addition of the Risk factor in SeBIS, which helps predict user behavior intention. The study results found a good correlation between risk factors and other factors, motivating the inclusion of 5 factors in SeBIS. In addition, the study also identified various questions of SeBIS to be updated according to the latest technology trend to ensure up-to-date user security awareness (Ayyagari & Crowell, 2020).

Abd Rahim et al. (2015) conducted a systematic literature review to find current methodologies, target audience, and scope of various studies assessing CSA. According to Abd Rahim et al. (2015), CSA programs are designed to achieve behavior change, mainly assessed by program evaluation models such as Kirkpatrick's four-level learning model derived from social science theory. This model used qualitative and quantitative methods to evaluate the program's impact on human factors based on reactions, learning, behaviors, and results. Subsequently, the results of this model can be used to improve the CSA program. In this study, the authors focused on categorizing users for assessing CSA and mainly evaluated youngsters in assessment. The author's review found that youngsters are highly exposed to internet usage, whereas their awareness of the online threat is limited. This lack of awareness makes youngsters more vulnerable to online fraud and identity theft. Therefore, CSA programs for youngsters must have distinct features corresponding to their age group (Abd Rahim et al., 2015). Hence establishing the concept that demographic such as age impacts users' online behavior. However, a study identified that women have a high score of ISA than men, which contradicts some studies (McCormac et al., 2018).

Zwilling et al. (2022) study also found that human cybersecurity behavior is influenced by many factors such as age, gender, workplace satisfaction, stress, conscientiousness, emotional stability, risktaking, amount of self-efficacy, and controllability. The study also highlighted the importance of the theory of planned behavior (TPB) in predicting planned behavior using intention and motivation. Similarly, the study also suggested TPB as a helpful approach in researching more effect of psychological factors such as self-efficacy and cultural values on user behavior. In this study, the authors used a quantitative approach and performed a paper-based survey to analyze the relation between CSA, knowledge, and behavior with protection tools. The authors also found the usable design option of security tools as an essential aspect of improved online protected behavior (Zwilling et al., 2022).

Similarly, Lebek et al. (2014) identified various theories from psychology, sociology, and criminology, which are used to explain behavioral intention (BI) and actual behaviors (AB). These theories provide different factors which can be used to evaluate CSA and behavior. For instance, the most frequently used theories are TPB or theory of reasoned action (TRA), general deterrence theory (GDT), protection motivation theory (PMT), and technology acceptance model (TAM). All these theories have a specific scope; however, they help in explaining people's BI and AB (Lebek et al., 2014).

A study by Bhagavatula et al. (2021) adopted a different approach, where the authors used behavioral data of home computer users and studied real-world browsing data to access online awareness of security incidents. The authors preferred to use an empirical measurement of actual behavior and avoided using self-reported data. In this study, the behavioral dataset was taken from the consented Security Behavioral Observatory (SBO) project after approval from the ethics review board. SBO is a study of Windows computer users' security behavior and consists of a dataset of people gathered over a couple of years. This data was based on private browsing history, password reuse habits, maintenance of computer security, and the ability to detect phishing attacks. This study only considered browsing data and performed analysis using various algorithms to look for people's habits in accessing the web and learn about incidents. The study found less awareness among sample data and shed light on the importance of security awareness (Bhagavatula, Bauer, & Kapadia, 2021). However, the approach of using browsing data to access user awareness looks passable in addition to measuring CSA.

Similarly, a study, "Information Security Behavior Profiling Framework (ISBPF)," on mobile users proposed a framework to access ISA. The framework assessed and tracked changes in mobile users' awareness levels and behavior intention after a training program. The study adopted three cycle action research approach to evaluate the framework using a questionnaire, survey, observance of simulated attack, and mapping the awareness level on a designed scorecard. Furthermore, since the study is also using a questionnaire, the author changed the dimension of behavior to perceive behavioral intention to mitigate the issue of bias somehow or acknowledge the results of what the user professed (Ngoqo & Flowerday, 2015).

In addition, a study to evaluate cybersecurity attitudes and behavior was conducted on healthcare institutions in Portuguese. This study also adopted a validated questionnaire to assess employee awareness levels using quantitative analysis. The questionnaire was only filled out by 3.8 % of employees, representing a low response rate. However, the analysis of the result found a significant correlation between risky behavior with cybersecurity attitudes and behavior. The article's authors suggested an increase in sample size for subsequent studies to better reflect CSA in Portuguese healthcare institutions (Nunes, Antunes, & Silva, 2021).

2.2 Time Pressure and Human Cybersecurity Behavior Regarding Phishing

In organizations, security breaches are mainly caused by human vulnerabilities; among them, the contributing factors are susceptibility to deception and trust (Goel et al., 2017). Hackers exploit this vulnerability by planting phishing attacks in various ways, such as sending malicious emails with web links directing to malicious sites or asking for critical information such as Personal Identity Identifiers (PIIs) (Goel et al., 2017).

Researchers found that training and awareness also cannot mediate this cyber threat; hence, human susceptibility to phishing is still an ongoing serious issue in the cyber world (Kävrestad et al., 2022). Research studies found this due to many contributing factors (Chowdhury et al., 2020; Goel et al., 2017; Kävrestad et al., 2022; Scholl et al., 2017).

A study on Human cybersecurity (HCS) behavior by Chowdhury et al. (2020) found that HCS behavior can be affected by many psychological factors, such as emotions, stress, risk preferences, cognitive abilities, and perceptions. According to Chowdhury et al. (2020), various sources of time pressure can primarily affect these psychological factors, leading to non-secure HCS practices.

In this context, a study by Chowdhury et al.(2018) proposed a theoretical framework to determine the time pressure impact on HCS behavior. In this study, authors developed a framework by validating it from different stakeholder groups by conducting semi-structured interviews and finally used thematic analysis to make different themes. The author of these studies theoretically described time pressure as a significant contributor to non-secure HCS behavior, resulting in phishing exploits. The summary of the list of a subcomponent of this framework is shown in Figure 3 below.

This framework defines various sources of time pressure, cybersecurity behavioral context, psychological constructs, non-secure HCS behavior, and moderating factors (Chowdhury, Adam, & Skinner, 2018, 2019; Chowdhury et al., 2020).

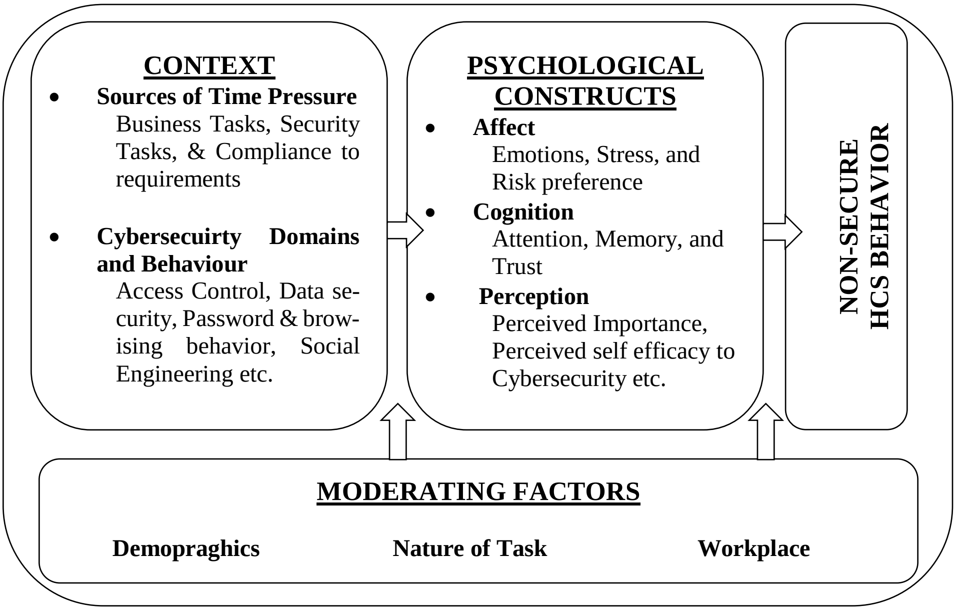

CONTEXT
Sources of Time Pressure
Business Tasks, Security Tasks, & Compliance to requirements
Cybersecuirty Domains and Behaviour
Access Control, Data security, Password & browising behavior, Social Engineering etc.
PSYCHOLOGICAL CONSTRUCTS
Affect
Emotions, Stress, and Risk preference
Cognition
Attention, Memory, and Trust
Perception
Perceived Importance, Perceived self efficacy to Cybersecurity etc.
NON-SECURE HCS BEHAVIOR
MODERATING FACTORS
Demopraghics
Nature of Task
Workplace

Figure 3 Sub-Components in the Theoretical Framework of Time Pressure Impact on HCS Behavior (Chowdhury et al., 2018) (*Redrawn*)

Similarly, various studies found that time pressure plays a vital role in non-secure HCS behavior, and attackers can exploit it for attacks such as phishing (Chowdhury et al., 2018, 2019; Chowdhury et al., 2020). More importantly, the studies also highlight that the factor of time pressure more often directly trunks information and communication services. In addition, a significant growth in the complexity of communication systems and technologies increases the stress factor induced by time pressure. When both of these factors are considered, it weakens the human firewall. This, as a result, affects security measures. However, in conclusion, increasing stress and time pressure affect decision-making power which makes the user vulnerable to phishing, setting a weak password, disclosing information, avoiding policies, and disregarding security controls (Chowdhury et al., 2019; Chowdhury et al., 2020).

However, in contrast to the previous studies, the research on the time pressure impact on employees' performance and knowledge hiding by Zhang et al. (2022) reviewed controversies in the debates and existing literature about the effects of time pressure. The authors found time pressure as a positive and negative influential factor in the workplace. The study presented two dimensions of time pressure a) challenge time pressure (CTP) and b) hindrance time pressure (HTP).

According to Zhang et al. (2022), the transformation between CTP and HTP depends on how the employees perceive time pressure. The study found that some employees take challenging time pressure as a motivating factor toward goals achievements and hindrance time pressure as a barrier to attaining goals. The study also found that in CTP, people's work concentration will increase, resulting in better performance and promotes good well-being (Zhang et al., 2022).

Another study on “measuring ISA level of government employee using phishing assessment” used a hybrid approach to measure ISA. For the knowledge approach, the author used a questionnaire-based HAIS-Q method, and for the behavioral approach simulated phishing attack was used. The study found that 69 % of the employees were vulnerable to phishing. The authors of this study found a significant correlation between knowledge assessment and behavioral assessment. The authors of this study also identified one potential challenge, which is privacy issues while assessing user behavior in real-time using log collection or activity observance. The author suggested taking consent from authorities while assessing behavior assessment in real-time (Ikhsan & Ramli, 2019).

The aforementioned literature gives an overview of efforts to bridge gaps in the assessment of CSA from distinct factors and finds behavior as an essential impact factor on CSA. In addition, studies proved that many data breaches only occurred because of behavioral issues which fail strong security control (Zwilling et al., 2022). However, evaluating CSA from a behavioral aspect is done mainly by adopting a questionnaire-based approach and then conducting quantitative analysis to find final results.

In conclusion, according to this study's findings from the studied literature, there exists a research gap to comprehensively address CSA evaluation from a behavioral aspect considering many factors such as behavioral assessment as proposed in the study “Developing metrics to assess the effectiveness of cybersecurity awareness program” by Chaudhary et al.(2022). The advantage of using behavioral assessment is motivated by various studies (Chaudhary et al., 2022; Enisa, 2018; Fertig & Schütz, 2020; Fertig, Schütz, & Weber, 2020) where all studies described measuring behavior as a helpful way of decision making to improve training programs. So when it comes to assessing CSA, the behavioral metrics-based solution can help decision-making by providing concrete results of predicting the KAB of users using some standardized approach such as scenario-based simulated questions.

Similarly, the studies on time pressure impact on human security behavior and the effect of resilience and job stress on ISA also highlight the importance of factors that affects people's awareness (Chowdhury et al., 2019; Chowdhury et al., 2020; McCormac et al., 2018). The theoretical framework proposed by Chowdhury et al. (2019), as shown in Figure 3, can be the expansion of metrics for CSA evaluation to measure the impact of time pressure on user behavior to phishing susceptibility. This can help the researchers quantify the effect of time pressure on phishing susceptibility and let them think about framing or researching resilience approaches accordingly.

The literature described above also emphasized further validation of results presented in various studies. The aforementioned background study found various areas of improvement, such as finding behavioral metrics, revising questionnaires, and adopting a comprehensive approach to systematically evaluating factors affecting human behavior. Gaps in these areas are potential barriers to actual recommendations for improvement in the CSA program and limiting the threat landscape.

The author found CSA as a socio-technical problem (where human factors and awareness or behavior make it a social issue (Abd Rahim et al., 2015), and protection tools as well as technology interaction make it technical (Mujinga, Eloff, & Kroeze, 2017)). In a nutshell, the initial research on the topic highlights the necessity of solving this problem as a social-technical challenge. Therefore, the intent of this study is aimed accordingly and motivated by the approach adopted in previous studies (Chaudhary et al., 2022), experts' opinions (Chowdhury et al., 2018), using a questionnaire (Ayyagari & Crowell, 2020; Egelman et al., 2016; Parsons et al., 2017), and finally adding measuring factor in metrics that enables actual behavioral assessment (Chaudhary et al., 2022; Fertig et al., 2020). The study also found human susceptibility to phishing as a major challenge that directly links to humans, which leads to catastrophic effects on organizational security (Goel et al., 2017; Ikhsan & Ramli, 2019; Kävrestad et al., 2022; Rocha Flores et al., 2015; Yang et al., 2022).

3 Methodology

This section describes the scientific methodology and process used in this research work, such as Questionnaire development, data collection, data analysis, and evaluating results. The generic study model is described in Figure 4 below.

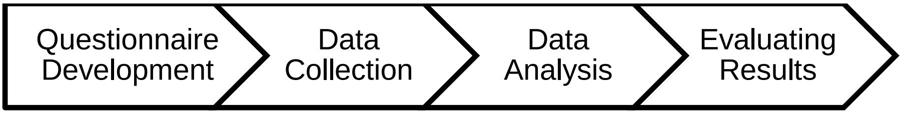


Figure 4 Generic Research Model (Author's Own)

3.1 Data Collection Methodology

According to the studies (Abd Rahim et al., 2015; Chaudhary et al., 2022), CSA evaluation can be made through hybrid approaches. However, quantification is widely done through well-established quantitative research methods such as surveys, questionnaires, and experiments. These surveys and questionnaires can be self-reported data or scenario-based questions (Chaudhary et al., 2022). Therefore, to identify the impact of time pressure on human cybersecurity behavior and its variation on different demographics, the primary methodological approach used in this study is also a quantitative research method. This quantitative research method uses an online anonymous survey questionnaire consisting of scenario-based questions. These scenario-based questions present actual attacks, and the idea is to analyze how many responders can detect these scenarios as malicious and report their findings as a correct response. The complete methodology used in this research work is described below and shown in Figure 5.

The choice of using an anonymous online questionnaire was motivated by keeping in view various ethical and privacy aspects, such as avoiding observance of behavior using real-time monitoring, which poses certain biases in the context of the pressure of monitoring, or control on responder (Abd Rahim et al., 2015; Chaudhary et al., 2022; McCormac et al., 2017). In addition, online questionnaires are economical and easy to disseminate to a large population using an online tool for the survey, and the responders can respond at their wish (Chaudhary et al., 2022).

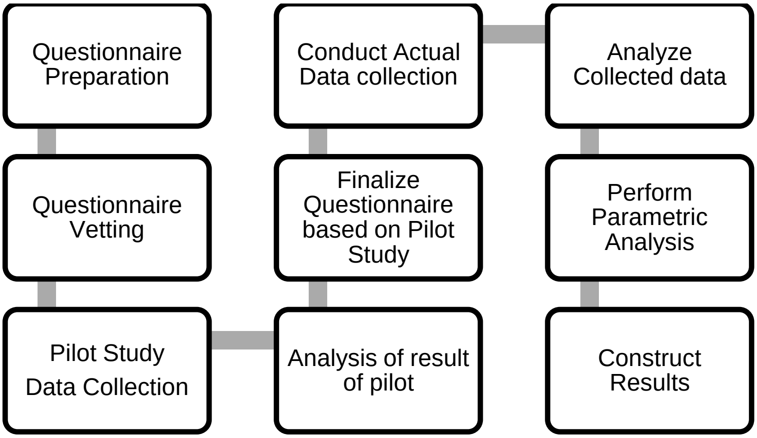

Questionnaire Preparation
Questionnaire Vetting
Pilot Study
Data Collection
Analysis of result of pilot
Finalize Questionnaire based on Pilot Study
Conduct Actual Data collection
Analyze Collected data
Perform Parametric Analysis
Construct Results

Figure 5 Methodological Approach (Author's Own)

3.1.2 Questionnaire Preparation Process

As shown in Figure 5 above, this study first started by developing a comprehensive and specific survey questionnaire focusing on phishing emails as the central theme of analysis. Five (5) interactive phishing-related email scenarios were designed in this questionnaire. In these scenarios, participants have the ability to hover over links and buttons, enabling them to view the actual links in the browser's status bar. By carefully analyzing the links and other indicators, such as suspicious attachment extensions or malicious email addresses, participants can draw upon their knowledge and experience to assess whether the scenario is indicative of a malicious or legitimate email. This determination is then reported by responding to the question, "Do you believe it is a malicious or phishing email?" with a "YES" or "NO" answer.

Here, the five phishing scenarios consisted of an email regarding a SWEDBANK transaction alert redirecting to a malicious link, a Netflix account-related email with a malicious link, an iCloud account storage issue email with a malicious link, the University finance office email regarding payment of a fee containing a malicious attachment, and a Firefox account login alert with a malicious link. All emails are randomized in a survey, so participants get a different order of questions whenever they click the survey link. The complete questionnaire is annexed in Appendix 1 at the end.

Secondly, to collect demographic data, questions regarding demographics were also added, such as nationality, age, gender, IT competence, and level of education. The reason behind adding these questions was to test the variance of the impact of time pressure on different segments, which was already presented by various studies as a major issue considering human aspects in information security (Abd Rahim et al., 2015; Ayyagari & Crowell, 2020; Chua et al., 2018; Goel et al., 2017; Wiley et al., 2020; Zwilling et al., 2022). So, the results of the study can be manipulated to identify various segments' resilience to time pressure in the context of protected cybersecurity behavior. In order to ensure the participant's anonymity and eliminate response bias, personal data such as email addresses, names, and dates of birth were not collected.

Along with demographic data, information regarding the survey and privacy policy was also added at the very beginning of the questionnaire. The participants were briefed adequately about the aims and objectives of this survey. After describing this, consent was collected to get the right to use collected data for research proposes considering compliance with General Data Protection Regulation (GDPR), as shown in Appendix 1.

The questionnaire used in this study also contained ten (10) more questions from another related research about the effect of human memory on password behavior. Where five (5) are regarding setting up passwords, and the second five (5) are regarding testing memory capacity. Both the studies were tested together as a project named as a factor affecting human cybersecurity behavior. The combination of the questionnaire has also added various advantages, such as it offers efficiency, cost, and time-saving benefits, resulting in improved response rates. Additionally, a single survey enables a comprehensive assessment, establishing connections between variables and capturing the broader context of the study. This approach also enhances participant engagement and reduces the burden. In this thesis report, the author only discusses and presents the impact of time pressure on human cybersecurity behavior, considering the first five phishing questions.

Afterward, the method for measuring time pressure was decided. In this regard, this study chose to proceed with having three separate random groups (A, B, and C), where each group responded to a similar randomized questionnaire but under different time limits. In this context, group A responded to a questionnaire having no time limit, group B responded to a questionnaire with perceived time pressure where there exists a time limit, but it is significant time to answer a question, and finally, group C responded to a questionnaire having actual time pressure where the time limit is comparatively less, and it is set according to the level of questions based on the conclusion of feedback from experts which is described afterwards and shown in table 1. Here, three questionnaires were randomized by a small programming code deployed on the survey's landing page. This code ensured that whenever a respondent clicked the survey link, the respondents received a random method.

After deciding the methodology for inducing time pressure, the next phase was to decide on the data collection tool. The author of this study chose to use an online survey conducting tool, "Limesurvey," for collecting data. Limesurvey is a professional surveying tool and provides all mechanisms that this study needs, such as question randomization, setting an individual timer on the question, data visualization, and mass sharing of questioning using email (LimeSurvey, n.d-a). On deciding on the data collection tool, a complete questionnaire was created on the survey collection tool and final vetting was done through the supervisor. After vetting the final questionnaire, the actual data collection process was initiated, where the questionnaire was shared with the general public using social media, email addresses, and contacts.

3.1.2 Questionnaire Validation

Since this study approach was a significantly new approach to existing standards such as HAIS-Q (Parsons et al., 2014) and SeBIS (Egelman & Peer, 2015) that specifically address user-intended behavior and consider self-reported data. Therefore, this study was intended to do the cyclic vetting and validation process on the approach adopted in this study using scenario-based questions instead of self-report data. The adopted scenario-based interactive questionnaire approach was influenced by Rocha et al. (2015) and Ikhsan & Ramli (2019). According to Chaudhary et al. (2022), a scenario-based questionnaire assessing human behavior is an effective behavior measurement mechanism because it presents both knowledge and behavior. Without knowledge, the user lacks behavior, and knowledge is somehow a reflection of behavior (Chaudhary et al., 2022).

In order to ensure the quality and validity of the adopted method and questionnaire, the partially developed questionnaire was first vetted through a supervisor's critical review. Then, based on the supervisor's input, the complete questionnaire was developed. Afterward, on the development of the questionnaire, the pilot study was conducted, where the aim was to get feedback from external experts on what they perceived and recommended about the questionnaire. Apart from getting their feedback, the author of this study was also observing the responses and behavior of responders on how well reviewers are identifying timers and following instructions given before each question group.

This pilot study was done by nine (9) experts and peers from social and professional circle through online and face-to-face meetings. In these meetings, a questionnaire was shared with them individually, and feedback and observation of responses on each section were accounted. These experts professionally belonged to the IT industry and academia and had higher education degrees with some academic publications and research experience. Among these experts, seven (7) had a university education of 3 plus years, and the remaining two (2) had a university education of 1-3 years. All of the experts had professional-level of IT competence. Eight (8) experts worked in the IT industry, and one (1) studied IT and cybersecurity. Besides all, these experts were selected based on their expert knowledge and cybersecurity awareness. The approach of using online and face-to-face meetings was influenced by Chowdhury et al. (2019).

The aforementioned pilot study came up with many recommendations, such as changes in the introduction screen, writing concise text, visibility issues in questions, changes in phrases of questions, and criteria for setting up a time limit on each questionnaire. Here, the primary discussion was carried out on time criteria. Initially, the time limit was set considering how much time an ordinary person could require to read the questions, plus choosing some options as a response. Initially, for actual time pressure, the time limit was set to 30 seconds, and for perceived, it was set to 3 times of actual, which was 90 seconds. However, during the pilot study, experts found the aforementioned time limits to be somewhat insufficient, as they encountered difficulties when attempting the phishing scenarios within the given time constraints. Therefore, the experts recommended increasing the time limits for perceived and actual time pressure to analyze participants' actual behavior. Ultimately, based on the supervisor's recommendation, observations, and expert input, this study finalized the specific time criteria for each random group, as outlined in Table 1 below.

Table 1 Time Pressure Criteria for Each Random Group

S.NO	Group A No Time Pressure	Group B Perceived Time Pressure	Group C Actual Time Pressure
01	Unlimited Time	180 Seconds	45 Seconds

3.1.3 Ethics and Privacy in Data Collection

One of the prime elements considered in this research was user privacy and ethics. While developing the questionnaire and collecting data, this study evaluated both aspects. According to the research, people avoid responding to a questionnaire where they feel insecure or worried about revealing their behavior from which they can be further assessed or evaluated (Chaudhary et al., 2022; Egelman et al., 2016; Parsons et al., 2017). Similarly, regulations such as GDPR bind data processors and collectors to inform data owners about the purpose and scope of data collection and the assurance of privacy (Voigt & Von dem Bussche, 2017).

Therefore, the following aspects were considered in this research work to ensure compliance with GDPR and assuring ethical practices.

- Individual privacy was ensured,
- The purpose of collecting data was defined,
- The scope of using collected data was clearly explained and consented to in the privacy policy, as evident in Appendix 1,
- Moreover, participants were given the right to ask about the use of collected data or any other information by contacting the authors of this study.

To ensure the aforementioned aspects in practice, first, no such data is collected that can reveal the individual identity. Therefore, no Personal Identity Identifiers (PII) were collected, such as name, email address, or date of birth. Second, the study participants were also given complete information and authority about leaving or discontinuing their response to the questionnaire at any time during responding questionnaire.

Finally, the data collection platform LimeSurvey was also chosen after considering and verifying that the platform complies with GDPR (LimeSurvey, n.d-b).

3.2 Data Analysis Methodology

After gathering data from the online survey, a dataset was analyzed for quality checks regarding response rate, completeness, and representation of different demographics such as age group, gender, level of education, IT competence, and nationality. During this phase, all incomplete responses were filtered out. Afterward, clean data was presented for statistical analysis, where the impact of time pressure on the human ability to detect phishing was tested across different demographic. To analyze the collected data SPSS tool was selected.

The validity and reliability test was first conducted in the data analysis phase to validate the questionnaire, where exploratory factor analysis (EFA) and Cronbach Alpha were calculated (Suter, 2011). This EFA and Cronbach Alpha was calculated for all the random groups' sample. Afterward, to analyze the difference between the three groups, A, B, and C, parametric analysis of ANOVA was tested to see does time pressure affect the ability to detect a phishing attack. ANOVA is a statistical analysis used to measure variance of two or more means or groups and uses F-test (Suter, 2011).

Finally, one-way ANOVA was used to check the statistically significant difference between the two demographic subgroups (Suter, 2011). For instance, women are more susceptible to phishing attacks under time pressure than men. Similarly, the same approach was adopted to test all other demographic subgroups.

4 Results

This section describes the results of responses received from the online questionnaire.

4.1 Questionnaire results

In response to the online questionnaire, this study was facilitated by 356 valid, complete responses. Table 2 below summarizes the total number of complete responses in each group. The table illustrates the specific count of complete responses received in each random group: Group 1 or A, Group 2 or B, and Group 3 or C, respectively.

Table 2 Total Responses in Each Random Group

Group	Method	Total Responses N=356
1 (A)	No Time Pressure	N_1= 107
2 (B)	Perceived Time Pressure	N_2=120
3 (C)	Actual Time Pressure	N_3=129

This study also received 119 partial or incomplete responses, which were excluded from the analysis. Among these 119 partial responses, a significant number of respondents discontinued their engagement right after finishing the demographic background section. Table 3 also indicates that most respondents possess higher education degrees. This observation raises the possibility that participants abandoned the questionnaire upon completing the demographic background section because, based on their higher education levels, participants may have suspected the questionnaire's legitimacy and perceived it as a potential threat. Furthermore, the inclusion of phishing-related questions containing suspicious links could have contributed to the high dropout rate among respondents.

In order to get further information about respondents in each group, descriptive analysis was conducted, giving the following results as shown in Table 3 below. Here each demographic item was changed to some scale value between 0-4 for analysis purposes, and results are presented for frequency and percentage of sample in each random group (1-3) and subgroup, which is demographics in this study such as gender, age, level of education, and IT Proficiency.

Table 3 Information About Respondents in Each Random Group

Information about respondents	**Frequency N=356**			**%**		
	1	**2**	**3**	**1**	**2**	**3**
Gender at Scale (0-2)						
Male=0	54	71	68	50.5	59.2	52.7
Female=1	53	49	58	49.5	40.8	45.0
Others=2	0	0	3	0	0	2.3
Age at Scale (0-5)						
18-24=0	37	41	44	34.6	34.2	34.1
25-34=1	34	36	43	31.8	30.0	33.3
35-44=2	24	27	27	22.4	22.5	20.9
45-54=3	8	8	11	7.5	6.7	8.5
55-64=4	2	6	2	1.9	5.0	1.6
65+=5	2	2	2	1.9	1.7	1.6
Level of Education at Scale (0-4)						
Primary=0	1	0	1	0.9	0	0.8
Secondary/Higher Secondary=1	6	4	9	5.6	7.0	7.0
Vocational Education=2	4	7	4	3.7	4.0	3.1
University Education 1-3 Years =3	44	69	37	41.1	40.0	28.7
University Education 3 Year +=4	52	40	78	48.6	69.0	60.5
IT Competence at Scale (0-3)						
Below Average =0	10	14	9	9.3	11.7	7.0
Average=1	31	44	48	29	36.7	37.2
Expert=2	35	28	31	32.7	23.3	24.0
Professional=3	31	34	41	29	28.3	31.8

Similarly, the results of this study also contain data from different nationalities which is presented separately in Table 4 below. This study received responses from 30 countries, where the significant number and existence of responses in each group were received from only Pakistan and Sweden. Whereas the USA, Australia, and India samples were received in all the groups but were insignificant in numbers. Keeping in view subgroup 5 testing to check if different nationalities with less economic and technological resources are more susceptible to phishing under time pressure, this study ranked nationality. The nationalities are ranked according to per capita income and presented in scale in this study. Where 0 represents the lowest rank in the groups sampled in each method ("Countries by GDP," 2023; "GDP by Country," 2023). The country with the highest GDP per capita rank is given a scale value of largest, and the country with the lowest GDP per capita is ranked as lowest on a scale, i.e., 0, and respectively for all countries according to their ranking shown on the website ("Countries by GDP," 2023; "GDP by Country," 2023). Due to the limited response rate from various countries, this study decided to focus on Pakistan and Sweden for subgroup 5 testing, which will be conducted in a later section. When ranking nationalities using the approach mentioned above, Pakistan was assigned a rank of "0" while Sweden was assigned a rank of "1," taking into consideration their respective GDP per capita.

Table 4 Information About Respondents' Nationality in Each Random Group

Information about Respondents	**Frequency N=356**			**%**		
	1	**2**	**3**	**1**	**2**	**3**
Nationality						
Afghanistan	-	-	1	-	-	0.8
Brunei	-	1	-	-	0.8	-
Jordan	1	-	-	0.9	-	-
Myanmar (formerly Burma)	-	-	1	-	-	0.8
Lithuania	-	1	-	-	0.8	-
Srilanka	-	1	-		0.8	-
Croatia	1	-	-	0.9	-	-
Bulgaria	-	-	1	-	-	0.8
Kenya	1	1	-	0.9	-	-
Ethiopia	2	-	1	1.9	-	0.8
Morocco	-	1	-	-	0.8	-
Hungary	1	-	-	0.9	-	-
Iraq	-	1	-	-	0.8	-
Finland	-	-	1	-	-	0.8
Pakistan	61	80	81	57.0	66.7	62.8
Vietnam	-	-	1	-	-	0.8
Egypt	-	1	1	-	0.8	0.8
Bangladesh	-	-	4	-	-	3.1
Nigeria	-	2	1	--	1.7	0.8
Ireland	1	-	-	0.9	-	-
Belgium	-	-	1	-	-	0.8
Sweden	26	16	18	24.3	13.3	14.0
Spain	-	2	-	-	1.7	-
Australia	2	7	4	1.9	5.8	3.1
Canada	-	1	-	-	0.8	-
United Kingdom	1	-	2	0.9	-	1.6
India	4	2	3	3.7	1.7	2.3
Germany	-	-	1	-	-	0.8
China	-	-	1	-	-	0.8
United States of America	6	4	6	5.6	3.3	4.7

4.2 Validity and Reliability of Questionnaire

Before analyzing the hypothesis, first, this study conducted the validity and reliability test of the questionnaire to test the construct correlation items across each other. A validity test is essential to see whether the instrument measures the same constructs (Ehizibue, 2022; Rocha Flores et al., 2015; Urbach & Ahlemann, 2010). Therefore, this study conducted an exploratory factor analysis (EFA). According to Ehizibue (2022), Rocha Flores et al. (2015), and Urbach & Ahlemann (2010), for the construct to be valid, the acceptable loading coefficient should be above 0.5 and below 0.8. The loading coefficient above 0.6 is considered high, and the coefficient below 0.4 is considered low.

However, before doing EFA, the sample appropriateness should be tested using the Bartletts and Kaiser-Meyer-Olkin (KMO) test.

According to Ehizibue (2022), a KMO value above 0.5 is acceptable for a sample to be appropriate, whereas Bartletts'test results should be statistically significant. According to this study's results, the loading of all the items of the construct was above 0.4, which is above low, and the KMO was also above 0.5, with a significant Bartlett test result. The results of the tests are shown in Table 5 below. This result shows that the construct is valid.

Table 5 KMO and Bartlett's Test Results

Group	Method	KMO	Bartlett Test	
1 (A)	No Time Pressure N_1= 107	.728	**Approx. Chi-Square**	59.300
			df	10
			Sig.	<.001
2 (B)	Perceived Time Pressure N_2=120	.595	**Approx. Chi-Square**	27.511
			df	10
			Sig.	.002
3 (C)	Actual Time Pressure N_3=129	.668	**Approx. Chi-Square**	47.20
			df	10
			Sig.	<.001

Similarly, the loading value for most items was above 0.5, which was acceptable. The loading summary is presented in Table 6 below for all the random Groups.

Table 6 EFA (Loading) Results

Item No.	Construct	Frequency N=356		
		1	**2**	**3**
01	email from Netflix	.661	.492	.469
02	email from SWEDBANK	.635	.505	.582
03	email from the Finance Office	.487	.578	.597
04	email from Firefox	.639	.655	.636
05	email from Apple iCloud	.762	.584	.717

Whereas to test the internal consistency of the item reliability test was conducted, and Cronbach's alpha was evaluated. According to the studies, the value of Cronbach's alpha above 0.6 is acceptable and represents that the items in the construct are related (Urbach & Ahlemann, 2010; Van Griethuijsen et al., 2015). Where a value above 0.5 and below 0.6 shows an average construct. The reason behind low Cronbach's alpha can be fewer items in the construct that have contributed to the factor (Eisinga, Grotenhuis, & Pelzer, 2013; Van Griethuijsen et al., 2015). Such issues can be handled by increasing the number of items. This can be done or verified using the Spearman-Brown prediction formula by testing the slight changes in items that increase Cronbach's alpha (Eisinga et al., 2013; Van Griethuijsen et al., 2015).

This study's internal consistency scores, i.e., Cronbach's Alphas, were low and can be seen in Table 7 below for all random groups. In addition, this study does not present data for Cronback's alpha if the item is deleted because none of the items, if deleted, positively impacts Cronbach's alpha.

Table 7 Cronbach's Alpha for All Random Groups

Method No.	Method	Cronbach's Alpha
01	Group A (No Time Pressure)	.638
02	Group B (Perceived Time Pressure)	.465
03	Group C (Actual Time Pressure)	.556
Total		.556

However, this study's internal consistency can be improved in future work by increasing the number of items in the construct as per the theory described by Eisinga et al. (2013) and Van Griethuijsen et al. (2015), which is already described above. On the contrary, since the aim was to measure whether the participants detect phishing emails or not by choosing Yes or No can only be met using two scale options, adding items in the scale such as "Do not know" or adding more phishing questions can give even more desirable results, as well as can reduce some bias.

4.3 Time Pressure and Phishing Susceptibility

The primary objective of this study was to measure the effect of time pressure on the human ability to detect phishing. In order to ensure this, all three random groups were grouped, and an ANOVA test was conducted to show that does their exists statistical significance among them. The result of the analysis shows that time pressure does not affect human susceptibility to phishing. The result of the study is above the significance level, i.e., Sig. <0.01 and 0.05 and is 0.553, which shows that this is due to chance (Suter, 2011). The results of the analysis are presented in Table 8 and Table 9 below.

Table 8 Descriptive Analysis of All Random Groups

Method	N	Mean	Std. Deviation	Std. Error	95 % Confidence Interval for Mean	
					Lower Bound	Upper bound
1	107	2.26	1.592	.154	1.96	2.57
2	120	2.44	1.407	.128	2.19	2.70
3	129	2.46	1.500	.132	2.20	2.72
Total	356	2.39	1.496	.079	2.24	2.55

Table 9 ANOVA Test Results

ANOVA					
Total Score					
	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Between Groups	2.664	2	1.332	.593	.553
Within Groups	792.280	353	2.244		
Total	794.944	355			

4.4 The Demographic Differences under Time Pressure Impact on Phishing Susceptibility

The next important part of this study is to investigate the individual differences in phishing susceptibility under time pressure. Here the following demographics will be tested, i.e., gender, age, level of education, IT competence, and nationality.

4.4.1 Gender

In order to test the Gender differences regarding phishing susceptibility under time pressure, this study applied the ANOVA test to each group and compared results. The analysis shows that among all random groups, there is no statistical significance between genders and time pressure effect on human susceptibility to phishing. The results of the study are above the significance level, i.e., Sig. <0.01 and 0.05. The analysis received a Sig. of 0.150 for No time pressure, 0.053 for perceived time pressure, and 0.420 for actual time pressure, which shows that this is due to chance (Suter, 2011). The analysis results are presented in Tables 10, 11, and 12 for all random groups below.

Table 10 Subgroup-Gender ANOVA Test for No Time Pressure

ANOVA FOR GENDER					
Total Score No Time Pressure					
	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Between Groups	5.267	1	5.267	2.100	.150
Within Groups	263.406	105	2.509		
Total	268.673	106			

Table 11 Subgroup-Gender ANOVA Test for Perceived Time Pressure

ANOVA FOR GENDER					
Total Score Perceived					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	7.394	1	7.394	3.824	.053
Within Groups	228.197	118	1.934		
Total	235.592	119			

Table 12 Subgroup-Gender ANOVA Test for Actual Time Pressure

ANOVA FOR GENDER					
Total Score Actual					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	3.939	2	1.970	.874	.420
Within Groups	284.076	126	2.255		
Total	288.016	128			

4.4.2 Age

This study applied the ANOVA test to each group to test age as a subgroup and compared results. The analysis shows that under all random groups, there is no statistical significance between age and time pressure effect on human susceptibility to phishing. The study results are above the significance level, i.e., Sig. <0.01 and 0.05. The analysis received a Sig. of 0.117 for No time pressure, 0.064 for perceived time pressure, and 0.887 for actual time pressure, which shows that this is due to chance (Suter, 2011). The analysis results are presented in Tables 13, 14, and 15 for all random groups below.

Table 13 Subgroup-Age ANOVA Test for No Time Pressure

ANOVA FOR AGE					
Total Score No Time Pressure					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	22.137	5	4.427	1.814	.117
Within Groups	246.536	101	2.441		
Total	268.673	106			

Table 14 Subgroup-Age ANOVA Test for Perceived Time Pressure

ANOVA FOR AGE					
Total Score Perceived					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	20.310	5	4.062	2.151	.064
Within Groups	215.282	114	1.888		
Total	235.592	119			

Table 15 Subgroup-Age ANOVA Test for Actual Time Pressure

ANOVA FOR AGE					
Total Score Actual					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	3.967	5	.793	.341	.887
Within Groups	283.751	122	2.326		
Total	287.719	127			

4.4.3 Level of Education

Similarly, to analyze the Level of Education as a subgroup, this study applied the ANOVA test to each group and compared the results. The analysis shows that under no time pressure and actual time pressure random groups, no statistical significance exists between the level of education and time pressure effect on human susceptibility to phishing. The study results are above the significance level, i.e., Sig. <0.01 and 0.05. The analysis received a Sig. of 0.251 for No time pressure, 0.064, and 0.403 for actual time pressure, which shows that this is due to chance (Suter, 2011). However, statistical significance exists for perceived time pressure, and the study received a Sig. of .020. The analysis results are presented in Tables 16, 17, and 18 for all random groups below.

Table 16 Subgroup-Level of Education ANOVA Test for No Time Pressure

ANOVA FOR LEVEL OF EDUCATION					
Total Score No Time Pressure					
	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Between Groups	13.670	4	3.417	1.367	.251
Within Groups	255.003	102	2.500		
Total	268.673	106			

Table 17 Subgroup-Level of Education ANOVA Test for Perceived Time Pressure

ANOVA FOR LEVEL OF EDUCATION					
Total Score Perceived					
	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Between Groups	19.032	3	6.344	3.398	.020
Within Groups	216.560	116	1.867		
Total	235.592	119			

Table 18 Subgroup-Level of Education ANOVA Test for Actual Time Pressure

ANOVA FOR LEVEL OF EDUCATION					
Total Score Actual					
	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Between Groups	6.690	3	2.230	.984	.403
Within Groups	281.029	124	2.266		
Total	287.719	127			

4.4.4 IT Competency

Similarly, this study applied the ANOVA test to each group for IT Competence as a subgroup and then compared the results. The analysis shows that under no time pressure and perceived random groups, statistical significance exists between the IT competency and time pressure effect on human susceptibility to phishing. Whereas under actual time pressure, there exists no statistical significance. The study results for actual time pressure are above the significance level, i.e., Sig. <0.01 and 0.05. The analysis received a Sig. of 0.057 for actual time pressure, which shows that this is due to chance (Suter, 2011). Where for no time pressure and perceived time pressure Sig. is <.001. The analysis results are presented in Tables 19, 20, and 21 for all random groups below.

Table 19 Subgroup-IT Competence ANOVA Test for No Time Pressure

ANOVA FOR IT COMPETENCE					
Total Score No Time Pressure					
	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Between Groups	55.589	3	18.530	8.957	<.001
Within Groups	213.084	103	2.069		
Total	268.673	106			

Table 20 Subgroup-IT Competence ANOVA Test for Perceived Time Pressure

ANOVA FOR IT COMPETENCE					
Total Score Perceived					
	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Between Groups	33.772	3	11.257	6.470	<.001
Within Groups	201.820	116	1.740		
Total	235.592	119			

Table 21 Subgroup-IT Competence ANOVA Test for Actual Time Pressure

ANOVA FOR IT COMPETENCE					
Total Score Actual					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	16.841	3	5.614	2.570	.057
Within Groups	270.877	124	2.184		
Total	287.719	127			

4.4.5 Nationality

Similarly, for Nationality as a subgroup, this study applied the ANOVA test to each group and compared the results. The analysis shows statistical significance between the Nationality and time pressure effect on human susceptibility to phishing under no time pressure, perceived time pressure, and actual time pressure random groups. The study results for all methods are within the significance level, i.e., Sig. <0.01 and 0.05. The analysis results are presented in Tables 22, 23, and 24 below for all the random groups.

Here, the results shown in Figures 6,7 and 8 clearly show that Swedish people are more aware of phishing since they have a higher mean score than Pakistani nationals in all random groups. However, the means difference shown in Tables 25 and 26 reveals that time pressure has a negative impact on Swedish Nationals compared to Pakistani Nationals, as their susceptibility to phishing increases with an increase in time pressure. Whereas the ANOVA test results presented in Table 27 shows that this influence has no statistical significance, and this is due to chance.

Table 22 ANOVA Results for Nationality for No Time Pressure

ANOVA FOR NATIONALITY					
Total Score No Time Pressure					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	68.840	1	68.840	37.129	<.001
Within Groups	157.596	85	1.854		
Total	226.437	86			

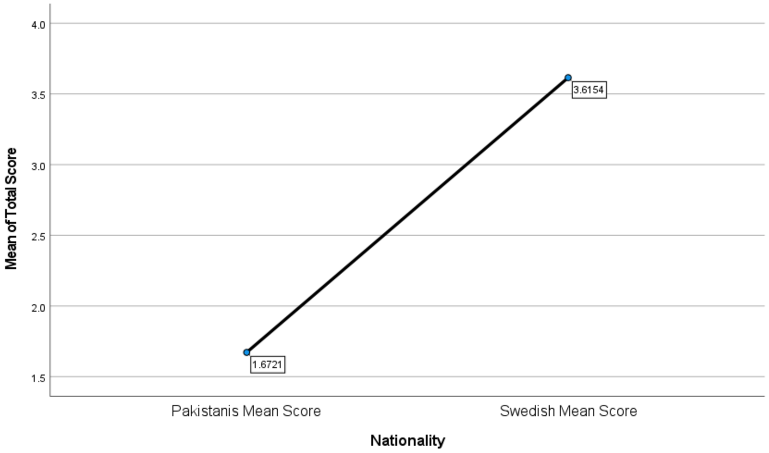


Figure 6 Comparison of Nationality For No Time Pressure

Table 23 ANOVA Results for Nationality for Perceived Time Pressure

ANOVA FOR NATIONALITY					
Total Score Perceived					
	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Between Groups	13.669	1	13.669	7.649	.007
Within Groups	167.987	94	1.787		
Total	181.656	95			

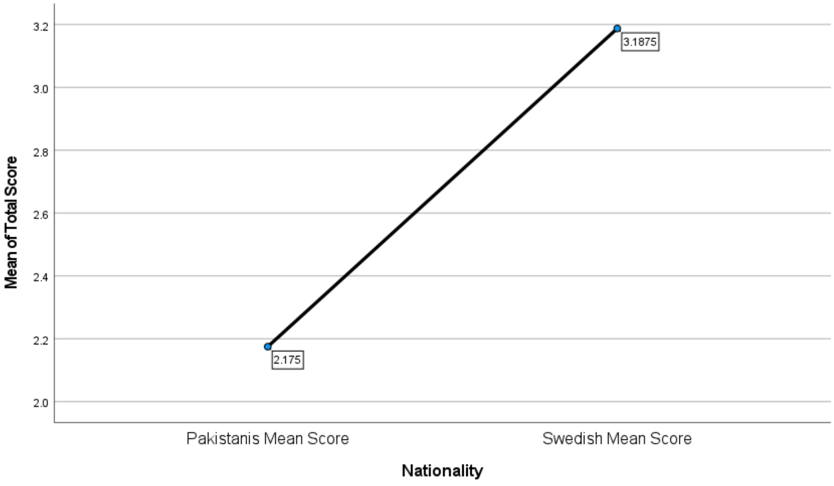


Figure 7 Comparison of Nationality for Perceived Time Pressure

Table 24 ANOVA Results for Nationality for Actual Time Pressure

ANOVA FOR NATIONALITY					
Total Score Actual					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	16.022	1	16.022	8.201	.007
Within Groups	72.286	37	1.954		
Total	88.308	38			

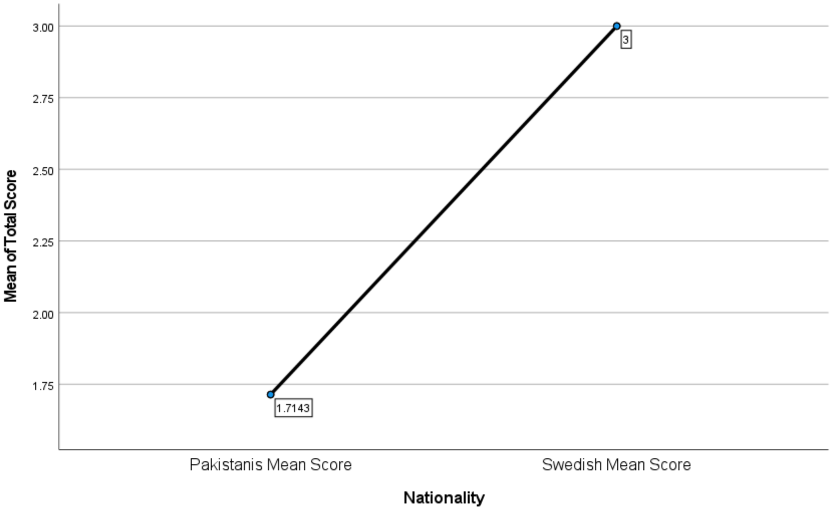


Figure 8 Comparison of Nationality for Actual Time Pressure

Table 25 Descriptive Analysis of Pakistani Nationals in Each Random Group

Method	N	Mean	Std. Deviation	Std. Error	95 % Confidence Interval for Mean	
					Lower Bound	Upper bound
1	61	1.67	1.326	.170	1.33	2.01
2	80	2.17	1.367	.153	1.87	2.48
3	21	1.71	1.384	.302	1.08	2.34
Total	162	1.93	1.368	.107	1.71	2.14

Table 26 Descriptive Analysis of Swedish Nationals in Each Random Group

Method	N	Mean	Std. Deviation	Std. Error	95 % Confidence Interval for Mean	
					Lower Bound	Upper bound
1	26	3.62	1.444	.283	3.03	4.20
2	16	3.19	1.167	.292	2.57	3.81
3	18	3.00	1.414	.333	2.30	3.70
Total	60	3.32	1.372	.177	2.96	3.67

Table 27 ANOVA Test Results for Swedish National for All Random Groups

ANOVA FOR NATIONALITY(SWEDISH NATIONALS)					
Total Score Actual					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	4.392	2	2.196	1.174	.316
Within Groups	106.591	57	1.870		
Total	110.983	59			

4.5 Dichotomized Demographic Differences in Time Pressure Impact on Phishing Susceptibility

This section is about analyzing results using dichotomized demographic subgroups. In order to do this, each subgroup was combined into two groups, i.e., group 1 and 2, to test which group has a stronger effect under time pressure. Here the following demographics will be tested, i.e., gender, age, level of education, and IT competence.

4.5.1 Gender

In order to test the gender differences under dichotomized demographic subgroups, this study applied the ANOVA test and used a filter for “male” and “female”. First, the analysis results show that under subgroup filters for gender=Males, there is no statistical significance between the method and phishing susceptibility for males. The study results are above the significance level, i.e., Sig. <0.01 and 0.05. The analysis received a Sig. of .828, which shows this is due to chance (Suter, 2011). The analysis results are presented below in Tables 28 and 29, respectively.

Table 28 Descriptive Analysis of Dichotomized Demographic Subgroup- Gender -Male

Method	N	Mean	Std. Deviation	Std. Error	95 % Confidence Interval for Mean	
					Lower Bound	Upper bound
1	54	2.48	1.713	.233	2.01	2.95
2	71	2.65	1.475	.175	2.30	3.00
3	68	2.62	1.536	.186	2.25	2.99
Total	193	2.59	1.559	.112	2.37	2.81

Table 29 ANOVA Results for Dichotomized Subgroup-Gender-Male

ANOVA FOR DICHOTOMIZED GENDER-MALE					
Total Score					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	.926	2	.463	.189	.828
Within Groups	465.737	190	2.451		
Total	466.663	192			

Second, the analysis results show that under subgroup filters for gender=females, there is no statistical significance between the method and phishing susceptibility for females. The results of the study are above the significance level, i.e., Sig. <0.01 and 0.05. The analysis received a Sig. of .616, which shows this is due to chance (Suter, 2011). The analysis results are presented below in Tables 30 and 31, respectively.

Table 30 Descriptive Analysis of Dichotomized Demographic Subgroup- Gender -Female

Method	N	Mean	Std. Deviation	Std. Error	95 % Confidence Interval for Mean	
					Lower Bound	Upper bound
1	53	2.04	1.441	.198	1.64	2.43
2	49	2.14	1.258	.180	1.78	2.50
3	58	2.29	1.402	.184	1.92	2.66
Total	160	2.16	1.369	.108	1.95	2.38

Table 31 ANOVA Results for Dichotomized Subgroup-Gender-Female

ANOVA FOR DICHOTOMIZED GENDER-FEMALE					
Total Score					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	1.833	2	.917	.486	.616
Within Groups	295.942	157	1.885		
Total	297.775	159			

4.5.2 Age

Next, to investigate age as dichotomized demographic, this study combined the age group and made two groups. The groups are combined based on a theory found in the article about digital generations, where the author said people aged 18-34 are more related to technology. The author of this article called them digital natives (Pilette, 2021). Therefore, this study combined ages group 18-24 and 25-34 as one group, and 35-44, 45-54,55-64, and 65+ as one group. Therefore, ANOVA was used to test the method and phishing susceptibility for young people aged 18-24 and 25-34. The results of the test are shown below in Tables 32 and 33. The results of the analysis show that there exists no statistical significance between the method and phishing susceptibility for young people.

Table 32 Descriptive Analysis of Dichotomized Subgroup-Age Group 1

Method	N	Mean	Std. Deviation	Std. Error	95 % Confidence Interval for Mean	
					Lower Bound	Upper bound
1	71	2.10	1.426	.169	1.76	2.44
2	77	2.19	1.288	.147	1.90	2.49
3	87	2.44	1.492	.160	2.12	2.75
Total	235	2.26	1.409	.092	2.07	2.44

Table 33 ANOVA Results for Dichotomized Subgroup-Age Group 1

ANOVA FOR DICHOTOMIZED AGE GROUP 1					
Total Score					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	4.891	2	2.445	1.234	.293
Within Groups	459.790	232	1.982		
Total	464.681	234			

Similarly, the ANOVA test was used to test the method and phishing susceptibility for mature or older people aged 35-44, 45-54, 55-64, and 65 +. Again, the analysis results show no statistical significance between the method and phishing susceptibility for mature people. The results of the test are shown below in Tables 34 and 35.

Table 34 Descriptive Analysis of Dichotomized Subgroup-Age Group 2

Method	N	Mean	Std. Deviation	Std. Error	95 % Confidence Interval for Mean	
					Lower Bound	Upper bound
1	36	2.58	1.857	.310	1.95	3.21
2	43	2.88	1.515	.231	2.42	3.35
3	42	2.50	1.534	.237	2.02	2.98
Total	121	2.66	1.626	.148	2.37	2.95

Table 35 ANOVA Results for Dichotomized Subgroup-Age Group 2

ANOVA FOR DICHOTOMIZED AGE GROUP 2					
Total Score					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	3.439	2	1.719	.647	.526
Within Groups	313.669	118	2.658		
Total	317.107	120			

4.5.3 Level of Education

In continuation to the approach adopted to previous demographics, the level of education was also combined into two groups by making one group of people having University education of 1-3 years and 3 years plus and the second group of people having Vocational, Secondary/Higher education and Primary. Here a University education of 1-3 years and 3 years plus was considered high education, and other groups as low education. Then to investigate the level of education as a dichotomized demographic ANOVA test was used. First, the test was conducted to analyze the method and phishing susceptibility for highly educated people. The results of the test are shown below in Tables 36 and 37. The results of the analysis show that there exists no statistical significance between the method and phishing susceptibility in the first context.

Table 36 Descriptive Analysis of Dichotomized Subgroup-Level of Education Group 1

Method	N	Mean	Std. Deviation	Std. Error	95 % Confidence Interval for Mean	
					Lower Bound	Upper bound
1	96	2.35	1.622	.166	2.03	2.68
2	109	2.54	1.418	.136	2.27	2.81
3	115	2.50	1.477	.138	2.23	2.78
Total	320	2.47	1.500	.084	2.31	2.64

Table 37 ANOVA Results for Dichotomized Subgroup-Level of Education Group 1

ANOVA FOR DICHOTOMIZED LEVEL OF EDUCATION GROUP 1					
Total Score					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	1.976	2	.988	.438	.646
Within Groups	715.770	317	2.258		
Total	717.747	319			

Similarly, the same approach was used to test the method and phishing susceptibility for low education. Again, the analysis results show no statistical significance between the method and phishing susceptibility against low education. The results of the test are shown below in Tables 38 and 39.

Table 38 Descriptive Analysis of Dichotomized Subgroup- Level of Education Group 2

Method	N	Mean	Std. Deviation	Std. Error	95 % Confidence Interval for Mean	
					Lower Bound	Upper bound
1	11	1.45	1.036	.312	.76	2.15
2	11	1.45	.820	.247	.90	2.01
3	14	2.07	1.685	.450	1.10	3.04
Total	36	1.69	1.283	.214	1.26	2.13

Table 39 ANOVA Results for Dichotomized Subgroup- Level of Education Group 2

ANOVA FOR DICHOTOMIZED LEVEL OF EDUCATION GROUP 2					
Total Score					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	3.256	2	1.628	.988	.383
Within Groups	54.383	33	1.648		
Total	57.639	35			

4.5.4 IT Competence

This demographic was dichotomized into low IT competence and high IT competency, where IT competence as a Professional was considered High IT competency, and Expert, Average user, and below average were considered low competency. Afterward, an ANOVA test was used to investigate the level of education as a dichotomized demographic. First, the test was conducted to analyze the method and phishing susceptibility for high IT competence. The results of the analysis show that there exists no statistical significance between the method and phishing susceptibility against high IT competence. The results of the test are shown below in Tables 40 and 41.

Table 40 Descriptive Analysis of Dichotomized Subgroup-IT Competence Group 1

Method	N	Mean	Std. Deviation	Std. Error	95 % Confidence Interval for Mean	
					Lower Bound	Upper bound
1	31	3.06	1.692	.304	2.44	3.69
2	34	3.09	1.288	.221	2.64	3.54
3	41	2.98	1.541	.241	2.49	3.46
Total	106	3.04	1.499	.146	2.75	3.33

Table 41 ANOVA Results for Dichotomized Subgroup-IT Competence Group 1

ANOVA FOR DICHOTOMIZED IT COMPETENCE GROUP 1					
Total Score					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	.267	2	.134	.058	.943
Within Groups	235.582	103	2.287		
Total	235.849	105			

Afterward, a similar approach was used to test the method and phishing susceptibility for low IT competence. The results of the analysis show that there exists no statistical significance between the method and phishing susceptibility against low IT competence. The results of the test are shown below in Tables 42 and 43.

Table 42 Descriptive Analysis of Dichotomized Subgroup-IT Competence Group 2

Method	N	Mean	Std. Deviation	Std. Error	95 % Confidence Interval for Mean	
					Lower Bound	Upper bound
1	76	1.93	1.436	.165	1.61	2.26
2	86	2.19	1.376	.148	1.89	2.48
3	88	2.22	1.426	.152	1.91	2.52
Total	250	2.12	1.412	.089	1.94	2.30

Table 43 ANOVA Results for Dichotomized Subgroup-IT Competence Group 2

ANOVA FOR DICHOTOMIZED IT COMPETENCE GROUP 2					
Total Score					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	3.808	2	1.904	.955	.386
Within Groups	492.592	247	1.994		
Total	496.400	249			

5 Discussion

This study analysis shows how a factor of Time Pressure can affect human behavior to detect phishing. A study by Chowdhury et al. (2019) described various sources of time pressure and found time pressure as an essential factor that leads to non-secure cybersecurity behavior, such as susceptibility to phishing. However, Zhang et al. (2022) study result linked time pressure impact to how an employee perceives it. Zhang et al. (2022) described time pressure as a positive and negative influence. Therefore, this study investigated how time pressure can influence human behavior regarding phishing detection. This section of the report describes this study's results and compares them with existing literature in light of this study's aims and hypothesis. The RQ and Hypothesis of this study was the following:

RQ. How does time pressure affect human behavior regarding phishing susceptibility?

Based on the background literature, this study assumed that increased time pressure would lead to a lowered or raised ability to detect phishing e-mails accurately. Consequently, the following hypothesis (H1) was tested in this research, using various demographic subgroups such as gender, age, level of education, IT competency, and nationality.

H1: Time pressure affects human behavior regarding phishing susceptibility

However, if no such relationship is established, the NULL hypothesis establishes showing that no relationship exists among studied variables.

5.1 Time Pressure and Phishing Susceptibility

According to a research study by Zhang et al. (2022), various authors found mixed opinions about time pressure's impact on human performance. The results of this study also found different results. This study results found that factor time pressure generally has no impact on phishing susceptibility. This study has received no statistical significance of time pressure on human behavior. However, all random groups (A, B, and C) were found susceptible to phishing by detecting below-average phishing scenarios. Whereas between different groups, the average variance is not significant. Table 8 also shows some means difference between all three groups, but it is not significant. Therefore, the Null hypothesis exists, and the study found that time pressure does not affect the human ability to detect phishing. Similarly, considering the Zhang et al. (2022) theory, on comparing the mean score shown in Table 8, this study found actual time pressure as CTP, which has a slightly positive impact on people's performance. However, this impact is not significant.

Apart from the aforementioned results, the results of this study, however, validate the results of studies that previously identified phishing as a major threat and reported that more than 50 % of the employees or participants were found vulnerable to phishing (Ikhsan & Ramli, 2019; Yang et al., 2022). This study also identified more than half of the sample as susceptible to phishing. According to Table 8, the average total means score for all tested groups is 2.39 on a scale of 5, which highlights the necessity of security awareness and training regarding phishing detection because most of the participant's ability to detect phishing was found below average, i.e., 50 % score.

Therefore, the results indicate that the factor of time pressure does not induce stress individually. However, more factors can help this factor impact user performance, such as stress, security requirements, work task complexity, and personal factors, (Chowdhury et al., 2020), which needs further investigation.

5.2 The Demographic Differences in Time Pressure Impact on Phishing Susceptibility

Various studies on individual differences in human behavior found that different demographic groups exhibit varied behavior when exposed to the cyber world, making them vulnerable to cyber threats such as scams and phishing (Goel et al., 2017; Zwilling et al., 2022). However, the results found in this study have no statistical significance in any of the demographic groups. All participants, on average, performed more or less similarly. However, only the results of IT Competence for no time pressure and perceived time pressure were statistically significant. The results show that under the group testing method, with no time pressure and perceived time pressure, an increased means score in IT Competence positively impacts the human ability to detect phishing emails. The result has no significance in the same demographics for actual time pressure, and the NULL hypothesis is not rejected. Similarly, for all the demographic groups testing, the NULL hypothesis on the tested sample is not rejected.

However, the results of the comparison between Pakistan and Sweden in Figure 6,7, and 8 clearly shows that Swedish people possess a better ability to detect phishing since they have a higher mean score than Pakistani nationals, and the ANOVA test also shows the statistical significance of the results. According to Zwilling et al. (2022), countries having better economic indicators and resources invest more in citizens, and their citizens possess better CSA levels. The results of this study on each random group validate the findings of Zwilling et al. (2022). Where Sweden natives detected phishing emails in a better way by scoring a means value of 3.0 and above in all random groups. The results also reveal that time pressure has impacted Swedish natives negatively, where their mean score for phishing detection decreases with improved time pressure, as shown in Table 26. However, the variance is not significant to reject the NULL hypothesis.

5.3 Dichotimized Demographic Differences in Time Pressure Impact to Phishing Susceptibility

The authors of various studies found different demographic subgroups more vulnerable to phishing. Such as according to the findings of Goel et al. (2017), the authors found that women are more susceptible to phishing. Similarly, Goel et al. (2017) and Abd Rahim et al. (2015) found that young people are more vulnerable to phishing. Moreover, Rocha Flores et al. (2015) found that people with more IT knowledge have better CSA, making them less susceptible to phishing. Furthermore, Chua et al. (2018) and Wiley et al. (2020) found that people with a higher education level possess better levels of CSA; hence they are less vulnerable to cyber threats. Finally, Zwilling et al. (2022) found that citizens having more economic and technological resources have better levels of CSA; hence they are less vulnerable to cyber threats.

However, in contrast to all previous studies, this study found no statistical significance of results showing any impact of time pressure on the human ability to detect phishing in subgroups. Therefore, the NULL hypothesis is not rejected.

Moreover, the study also found that the nationals of economically stable and technological advance countries such as Sweden are less prone to phishing than underdevelopment or less economically stable countries such as Pakistan. According to Zwilling et al. (2022), economically stable and technological advance countries invest more in people's awareness and training in organizations or even publically through government institutions (Zwilling et al., 2022).

5.4 Sample Bias and Errors

This study underwent a detailed review process where the questionnaire was validated online and through face-to-face interviews with experts during the pilot phase. The questionnaire and time limit was modified according to experts' inputs. So, after seeing the result, certain possibilities exist for method bias. For example, the expert suggestion on the time limit for each random group can be too high. Which, as a result, put no pressure on participants. Moreover, the received sample includes responses that do not adequately represent all groups, and few responses are dominant in various demographic groups, as shown in Tables 3 and 4. Therefore, the sample does not reflect the actual population size, which adds sampling bias (Ten Berge & Sočan, 2007).

Similarly, the second possibility exists keeping in view Zhang et al. (2022) study, where the authors found that if people perceive time pressure as CTP, they behave better. As in the results section, it can be examined that a slight increase under time pressure is persistent for most demographic cases. However, it is not significant to reject the NULL hypothesis. Moreover, this study does not ignore response bias issues. There is a chance that people who responded to the survey have not given due care in their responses and have chosen random answers from yes or no. Although to avoid such issues, this study ensured respondent anonymity by not collecting any PIIs and making this survey completely anonymous. Moreover, as the participation in this study was voluntary and random, incorrect responses could impact the results (Ten Berge & Sočan, 2007).

The author of this study perhaps has not rejected issues such as sample bias and errors in the method due to the factors mentioned above, which can be tweaked using suggestions made in the following sub-section.

5.5 Practical Implementation and Method Tweaking

Though the study has not found a significant impact of the tested factor on the tested sample, implementing a similar method requires further validation and testing on a large sample. The methodical approach used in this study is practical, and the study by Chaudhary et al. (2022) also found this approach a suitable behavioral assessment mechanism. However, the author of this study also assumes that testing this study primarily on a control group in a lab environment is essential before assessing it across a large sample in an uncontrolled online environment using a survey questionnaire.

This lab-based testing is necessary to tweak the time factor to see how limiting time influences responded behavior. Although the controlled environment will also bring certain biases (Chaudhary et al., 2022), however can help in method tweaking. Implementing this study on the organizational level is also practical and will bring positive change in the behavior of the employees by practicing phishing detection under time pressure environment. Moreover, a similar approach can be used as an exercise part of security awareness and training. Moreover, adding more questions and some open-ended questions can also help in method improvement to achieve study objectives.

In contrast, there is also a possibility to test the same survey during extreme workload hours and examine how people behave under time pressure. The author assumes that time pressure does not impact human behavior to detect phishing, but the extensive work task, security requirements, and time pressure to meet the deadline influence this ability. Since this study was conducted online as a questionnaire, the respondents who participated were not affected by a single "Time Limit" factor. However, a slight variance change in the mean score represents an impact on a few people who took this time pressure as CTP but not HTP.

Therefore, the implementation method should also identify, elaborate and optimize the type of time pressure under which such a system needs to be analyzed. Besides using this study to detect phishing susceptibility, the same method can be used to test various cyber threats.

The timeframe and limitation of access to large people in a controlled environment significantly impacted the research objectives. However, this issue can be improved in future research by attaining ethical approval from authorities and testing pilots in a lab environment on a hybrid group. This will help in method tweaking for each random group. However, if such tweaking also reached a similar conclusion, then we can assume that factor time pressure has no impact on the human ability to detect phishing, or it improves human detection and vice versa.

5.6 Ethical Consideration

Ethical consideration remained the core practice in this study. Therefore, the author of this study ensured anonymity, flexibility, and objectivity for participants. Anonymity was ensured by not getting any personal data from participants. Similarly, flexibility was facilitated by giving the right to leave the questionnaire response at any stage by clearly writing it in the study's introduction. Finally, objectivity was ensured by clearly defining the objective and further use of this research data at the very beginning of the questionnaire and taking consent from them regarding using their data (Buchanan & Hvizdak, 2009; Hammer, 2017; Voigt & Von dem Bussche, 2017). Though ensuring privacy and ethics has a significant impact on our results, and the study deviated from some goals of testing human behavior, which is usually tested in real-time by observing real-time data or analysis of passive data from user activity (Chaudhary et al., 2022; Enisa, 2018).

In addition, to analyze human susceptibility to phishing under time limits, the questionnaire was designed to consider usability aspects. In order to ensure this, the number of questions was limited to 5 in total about phishing, and the questionnaire can be accessed on any digital device with an internet browser and access. So participants do not get overloaded with the unnecessary overhead of volunteer work (Frandsen-Thorlacius, Hornbæk, Hertzum, & Clemmensen, 2009).

5.7 Societal and Ethical Contribution

This research has contributed to the existing body of knowledge by giving a structured approach with a future roadmap for the research community. This study's literature, methodology, results, and discussion are based on facts, and nothing is concealed. Therefore, this study is entirely adaptable and verifiable. All content is appropriately referred to existing research, and other people's contribution to this research is acknowledged (Govil, 2013).

This study's aims and objectives are independent of personal biases and racism. The research work positively impacts individuals and society by providing and understanding people's needs in CSA and identifying reasons for making solutions adaptable for all.

Socially, the study provides valuable insights into how time pressure affects individuals' cybersecurity behavior and susceptibility to phishing attacks. By investigating this aspect, the research helps raise awareness among individuals about the potential risks and vulnerabilities associated with time-constrained situations. This knowledge can contribute to empowering users to make informed decisions, adopt safer practices, and protect themselves against phishing attempts. Ultimately, this contributes to the overall cybersecurity awareness of individuals, fostering a more secure digital environment for everyone.

Ethically, the study demonstrates a commitment to ensuring the well-being and privacy of participants. The utilization of a scenario-based phishing questionnaire allows for a controlled and ethical exploration of participants' responses and behaviors in simulated phishing situations. This approach prioritizes the protection of participants' personal information and provides an ethical approach to studying and understanding cybersecurity behavior. By adhering to ethical research practices, the study upholds the principles of respect, privacy, and informed consent, ensuring that participants' rights and well-being are safeguarded.

In summary, the research study on the “Effect of Time Pressure on Human Cybersecurity Behavior”, employing a scenario-based phishing questionnaire, contributes socially by enhancing cybersecurity awareness and empowering individuals to make informed decisions. Ethically, the study upholds the principles of privacy and participant well-being, setting a responsible example for conducting research in the field of cybersecurity.

6 Conclusion

This section of the report concludes the study and suggests future work.

The main aim of this study was to identify factors that affect human cybersecurity behavior. Therefore, to limit the scope of the study, the impact of time pressure on human cybersecurity behavior regarding the ability to detect phishing was initially investigated. The study used quantitative research and developed a questionnaire comprising interactive phishing email scenarios distributed online to 3 anonymous random groups with 03-time limits (No time, Perceived time, and Actual Time). The study's result shows a slight change in user behavior under time pressure, and the impact is either positive or negative, showing that the time pressure factor slightly improves or decreases an individual's ability to detect phishing scenarios. However, the results are not statistically significant for all demographic groups. Therefore, the NULL hypothesis is not rejected.

Moreover, the result of the study also reflects that more than 50% of the participants are prone to phishing attacks, and their ability to detect phishing is deficient. In addition, keeping in view the importance of individuals in cybersecurity, this study investigated dichotomized demographics to see if there exists any impact of time pressure on males compared to females, older people versus young people, level of education, and IT competency. The results show no statistical significance.

The study has contributed to assessing factors that affect human cybersecurity behavior and how time pressure can influence human behavior in detecting phishing attacks. In addition, the method and literature described in this study highlight how time pressure affects human ability and how a similar approach can be reused to measure the impact of time on other cybersecurity threats.

The design of awareness and training programs considering and adding phishing exercises is essential to improve the human ability to detect phishing. The study results reflect the necessity of training people about phishing and cue to identify such attempts. The study does not suggest ignoring individual differences but recommends framing awareness and training programs according to their needs. One fit for all approach is not a viable, sustainable solution in any cybersecurity context.

6.1 Future work

The findings of this study present a different perspective than previous research, which identified time pressure as a significant influencing factor. However, it is essential to acknowledge the limitations of the existing methodology and sampled data, as they introduce biases and may not accurately represent the entire population.

To address these limitations and further advance the understanding of the impact of time pressure on cybersecurity behavior regarding phishing susceptibility, several future research directions can be considered:

1. **Controlled Experimental Setup:** Conduct the study in a controlled laboratory environment to minimize random user responses and increase control over variables. This controlled setting would allow more precise manipulation of time pressure conditions and provide more reliable data.

2. **Expanded Questionnaire:** Expand the questionnaire by incorporating additional questions and response options, including a "do not know" option. This would allow participants to indicate their lack of awareness or knowledge about specific phishing contexts, reducing potential bias and providing a more accurate assessment of their decision-making processes.

3. **Broader Participant Sampling:** Extend the study to include a larger and more diverse population to ensure a representative sample. This would involve recruiting participants from various demographics and backgrounds to understand how time pressure affects cybersecurity behavior comprehensively.

4. **Comparative Analysis:** Compare the responses and behaviors of participants under different time pressure conditions, including variations in time limits. This would involve retesting the study with modified time limits for actual time pressure to examine if there is a significant variation in responses and susceptibility levels.

5. **Qualitative Analysis:** Supplement the quantitative findings with qualitative research methods, such as interviews or focus groups, to gain deeper insights into participants' perceptions, experiences, and decision-making processes related to time pressure and phishing susceptibility.

6. **Longitudinal Study:** Conduct a longitudinal study to investigate the long-term effects of time pressure on cybersecurity behavior. This would involve tracking participants' behaviors and susceptibility to phishing attacks over an extended period to understand how time pressure impacts their decision-making consistently.

By pursuing these future research directions, the study can enhance its validity, provide more nuanced insights, and contribute to a more comprehensive understanding of the role of time pressure in human cybersecurity behavior regarding phishing susceptibility.

References

Abd Rahim, N. H., Hamid, S., Kiah, M. L. M., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*.

Alqahtani, M. A. (2022). Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences, 12*(5), 2589.

Aslam, M., Khan Abbasi, M. A., Khalid, T., Shan, R. u., Ullah, S., Ahmad, T., . . . Ahmad, R. (2022). Getting Smarter about Smart Cities: Improving Data Security and Privacy through Compliance. *Sensors, 22*(23), 9338.

Ayyagari, R., & Crowell, A. (2020). Risk and demographics' influence on security behavior intentions. *Journal of the Southern Association for Information Systems, 7*(1), 1.

Bhagavatula, S., Bauer, L., & Kapadia, A. (2021). *What breach? Measuring online awareness of security incidents by studying real-world browsing behavior.* Paper presented at the European Symposium on Usable Security 2021.

Buchanan, E. A., & Hvizdak, E. E. (2009). Online survey tools: Ethical and methodological concerns of human research ethics committees. *Journal of empirical research on human research ethics, 4*(2), 37-48.

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal of Cybersecurity, 8*(1), tyac006.

Chowdhury, N. H., Adam, M. T., & Skinner, G. (2018). *The impact of time pressure on human cybersecurity behavior: An integrative framework.* Paper presented at the 2018 26th International Conference on Systems Engineering (ICSEng).

Chowdhury, N. H., Adam, M. T., & Skinner, G. (2019). The impact of time pressure on cybersecurity behaviour: a systematic literature review. *Behaviour & Information Technology, 38*(12), 1290-1308.

Chowdhury, N. H., Adam, M. T., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. *Computers & Security, 97*, 101931.

Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. *Telematics and Informatics, 35*(6), 1770-1780.

Countries by GDP. (2023). Retrieved from https://www.populationu.com/gen/countries-by-gdp

Egelman, S., Harbach, M., & Peer, E. (2016). *Behavior ever follows intention? A validation of the Security Behavior Intentions Scale (SeBIS).* Paper presented at the Proceedings of the 2016 CHI conference on human factors in computing systems.

Egelman, S., & Peer, E. (2015). *Scaling the security wall: Developing a security behavior intentions scale (sebis).* Paper presented at the Proceedings of the 33rd annual ACM conference on human factors in computing systems.

Ehizibue, D. (2022). *Investigation of individuals' behavior towards phishing attacks using the health belief model.* University of Twente.

Eisinga, R., Grotenhuis, M. t., & Pelzer, B. (2013). The reliability of a two-item scale: Pearson, Cronbach, or Spearman-Brown? *International journal of public health, 58*, 637-642.

Enisa. (2018). Cybersecurity culture guidelines: behavioural aspects of cybersecurity. *European Union Agency for Network and Information Security*.

Fertig, T., & Schütz, A. (2020). About the measuring of information security awareness: a systematic literature review.

Fertig, T., Schütz, A. E., & Weber, K. (2020). *Current Issues Of Metrics For Information Security Awareness.* Paper presented at the ECIS.

Frandsen-Thorlacius, O., Hornbæk, K., Hertzum, M., & Clemmensen, T. (2009). *Non-universal usability? A survey of how usability is understood by Chinese and Danish users.* Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

GDP by Country. (2023). Retrieved from https://wisevoter.com/country-rankings/gdp-by-country/

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems, 18*(1), 2.

Govil, P. (2013). Ethical considerations in educational research. *International journal of advancement in education and social sciences, 1*(2), 17-22.

Hammer, M. J. (2017). Ethical considerations for data collection using surveys. *Number 2/March 2017, 44*(2), 157-159.

Hazari, S., Hargrave, W., & Clenney, B. (2008). An empirical investigation of factors influencing information security behavior. *Journal of Information Privacy and Security, 4*(4), 3-20.

Ikhsan, M. G., & Ramli, K. (2019). *Measuring the information security awareness level of government employees through phishing assessment.* Paper presented at the 2019 34th international technical conference on circuits/systems, computers and communications (ITC-CSCC).

Kävrestad, J., Hagberg, A., Nohlberg, M., Rambusch, J., Roos, R., & Furnell, S. (2022). Evaluation of contextual and game-based training for phishing detection. *Future Internet, 14*(4), 104.

Kritzinger, E., Da Veiga, A., & van Staden, W. (2022). Measuring organizational information security awareness in South Africa. *Information Security Journal: A Global Perspective*, 1-14.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*.

LimeSurvey. (n.d-a). Limesurvey. Retrieved from https://www.limesurvey.org/en/

LimeSurvey. (n.d-b). Limesurvey Privacy Policy. Retrieved from https://www.limesurvey.org/en/privacy-policy

McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M., & Lillie, M. (2018). The effect of resilience and job stress on information security awareness. *Information & Computer Security*.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69*, 151-156.

Mujinga, M., Eloff, M. M., & Kroeze, J. H. H. (2017). A socio-technical approach to information security.

Ngoqo, B., & Flowerday, S. V. (2015). Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users. *Computers & Security, 53*, 132-142.

Nunes, P., Antunes, M., & Silva, C. (2021). Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions. *Procedia Computer Science, 181*, 173-181.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security, 66*, 40-51.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security, 42*, 165-176.

Pilette, C. (2021). Digital generations: The technology gap between seniors, parents, and kids. Retrieved from https://us.norton.com/blog/how-to/digital-generations#

Rocha Flores, W., Holm, H., Nohlberg, M., & Ekstedt, M. (2015). Investigating personal determinants of phishing and the effect of national culture. *Information & Computer Security, 23*(2), 178-199.

Scholl, M., Leiner, K., & Fuhrmann, F. (2017). *Blind spot: Do you know the effectiveness of your information security awareness-raising program?* Paper presented at the Proceedings of the 21st World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2017).

Skinner, G., & Parrey, B. (2019). *A literature review on effects of time pressure on decision making in a cyber security context.* Paper presented at the Journal of Physics: Conference Series.

Suter, W. N. (2011). *Introduction to educational research: A critical thinking approach*: SAGE publications.

Ten Berge, J. M., & Sočan, G. (2007). The set of feasible solutions for reliability and factor analysis *Handbook of latent variable and related models* (pp. 303-320): Elsevier.

Urbach, N., & Ahlemann, F. (2010). Structural equation modeling in information systems research using partial least squares. *Journal of Information Technology Theory and Application (JITTA), 11*(2), 2.

Van Griethuijsen, R. A., van Eijck, M. W., Haste, H., Den Brok, P. J., Skinner, N. C., Mansour, N., . . . BouJaoude, S. (2015). Global patterns in students' views of science and interest in science. *Research in science education, 45*, 581-603.

Voigt, P., & Von dem Bussche, A. (2017). The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing, 10*(3152676), 10-5555.

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security, 88*, 101640.

Williams, E. J., & Joinson, A. N. (2020). Developing a measure of information seeking about phishing. *Journal of Cybersecurity, 6*(1), tyaa001.

Witsenboer, J. W. A., Sijtsma, K., & Scheele, F. (2022). Measuring cyber secure behavior of elementary and high school students in the Netherlands. *Computers & Education, 186*, 104536.

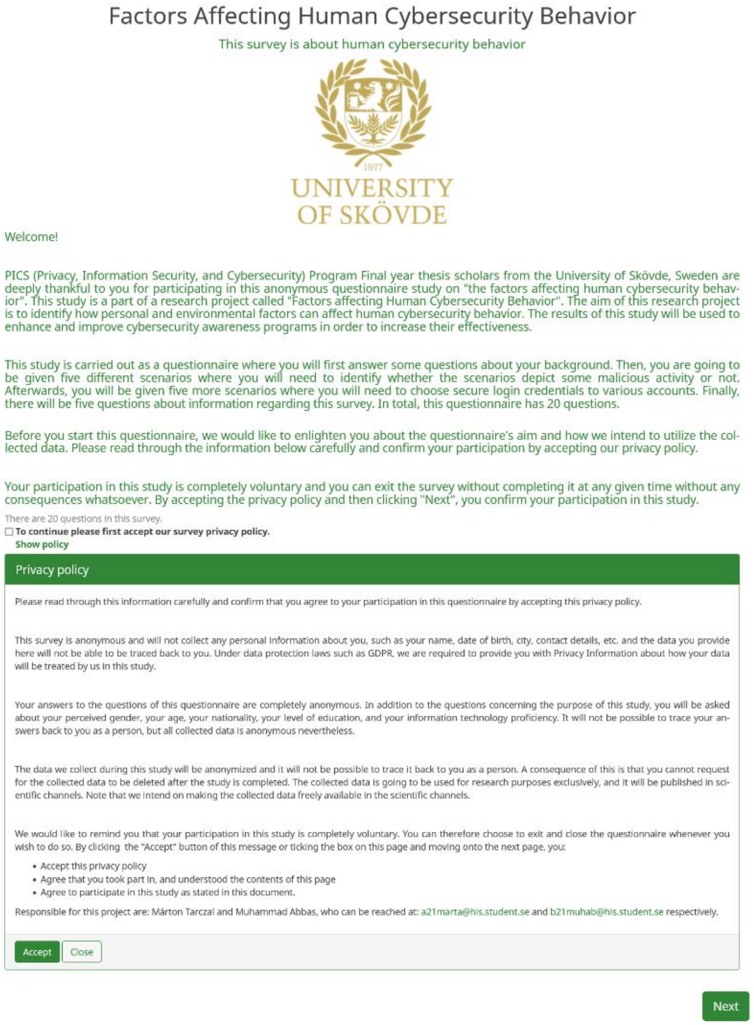
Yang, R., Zheng, K., Wu, B., Li, D., Wang, Z., & Wang, X. (2022). Predicting user susceptibility to phishing based on multidimensional features. *Computational Intelligence and Neuroscience, 2022*.

Zhang, X., Yao, Z., Qunchao, W., & Tsai, F.-S. (2022). Every coin has two sides: the impact of time pressure on employees' knowledge hiding. *Journal of Knowledge Management, 26*(8), 2084-2106.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: a comparative study. *Journal of Computer Information Systems, 62*(1), 82-97.

Appendix 1

COMPLETE QUESTIONNAIRE



Factors Affecting Human Cybersecurity Behavior

This survey is about human cybersecurity behavior

Welcome!

PICS (Privacy, Information Security, and Cybersecurity) Program Final year thesis scholars from the University of Skövde, Sweden are deeply thankful to you for participating in this anonymous questionnaire study on "the factors affecting human cybersecurity behavior". This study is a part of a research project called "Factors affecting Human Cybersecurity Behavior". The aim of this research project is to identify how personal and environmental factors can affect human cybersecurity behavior. The results of this study will be used to enhance and improve cybersecurity awareness programs in order to increase their effectiveness.

This study is carried out as a questionnaire where you will first answer some questions about your background. Then, you are going to be given five different scenarios where you will need to identify whether the scenarios depict some malicious activity or not. Afterwards, you will be given five more scenarios where you will need to choose secure login credentials to various accounts. Finally, there will be five questions about information regarding this survey. In total, this questionnaire has 20 questions.

Before you start this questionnaire, we would like to enlighten you about the questionnaire's aim and how we intend to utilize the collected data. Please read through the information below carefully and confirm your participation by accepting our privacy policy.

Your participation in this study is completely voluntary and you can exit the survey without completing it at any given time without any consequences whatsoever. By accepting the privacy policy and then clicking "Next", you confirm your participation in this study.

There are 20 questions in this survey.

□ **To continue please first accept our survey privacy policy.**

Show policy

Privacy policy

Please read through this information carefully and confirm that you agree to your participation in this questionnaire by accepting this privacy policy.

This survey is anonymous and will not collect any personal information about you, such as your name, date of birth, city, contact details, etc. and the data you provide here will not be able to be traced back to you. Under data protection laws such as GDPR, we are required to provide you with Privacy Information about how your data will be treated by us in this study.

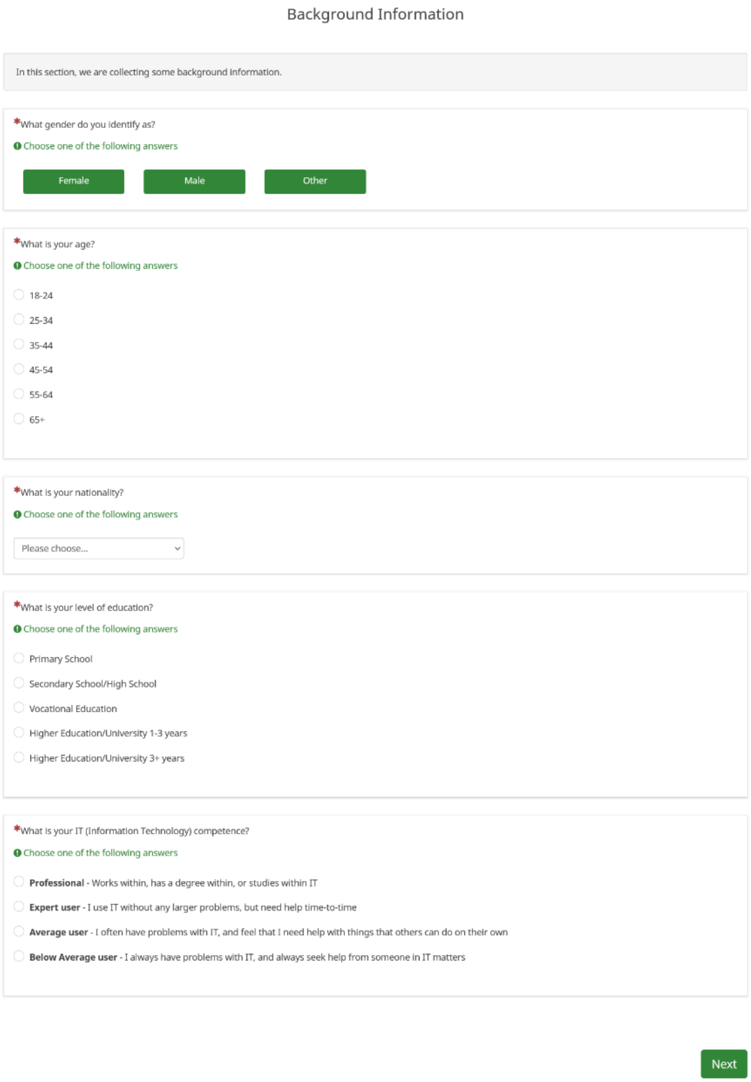
Your answers to the questions of this questionnaire are completely anonymous. In addition to the questions concerning the purpose of this study, you will be asked about your perceived gender, your age, your nationality, your level of education, and your information technology proficiency. It will not be possible to trace your answers back to you as a person, but all collected data is anonymous nevertheless.

The data we collect during this study will be anonymized and it will not be possible to trace it back to you as a person. A consequence of this is that you cannot request for the collected data to be deleted after the study is completed. The collected data is going to be used for research purposes exclusively, and it will be published in scientific channels. Note that we intend on making the collected data freely available in the scientific channels.

We would like to remind you that your participation in this study is completely voluntary. You can therefore choose to exit and close the questionnaire whenever you wish to do so. By clicking the "Accept" button of this message or ticking the box on this page and moving onto the next page, you:

- Accept this privacy policy
- Agree that you took part in, and understood the contents of this page
- Agree to participate in this study as stated in this document.

Responsible for this project are: Márton Tarczal and Muhammad Abbas, who can be reached at: a21marta@his.student.se and b21muhab@his.student.se respectively.



Background Information

In this section, we are collecting some background information.

*What gender do you identify as?

Choose one of the following answers

*What is your age?

Choose one of the following answers

○ 18-24
○ 25-34
○ 35-44
○ 45-54
○ 55-64
○ 65+

*What is your nationality?

Choose one of the following answers

Please choose...

*What is your level of education?

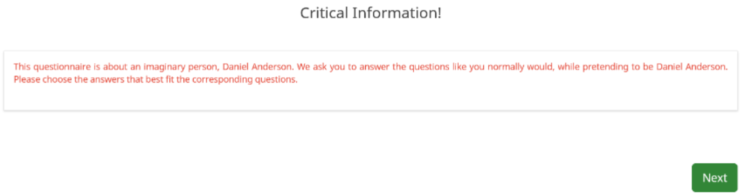
Choose one of the following answers

○ Primary School
○ Secondary School/High School
○ Vocational Education
○ Higher Education/University 1-3 years
○ Higher Education/University 3+ years

*What is your IT (Information Technology) competence?

Choose one of the following answers

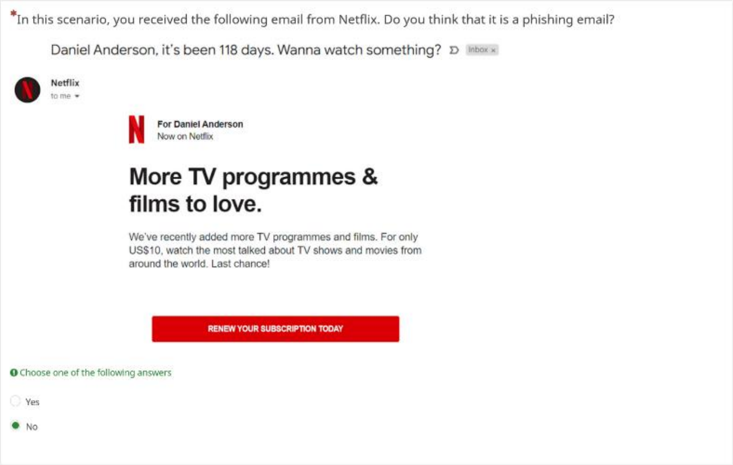
○ **Professional** - Works within, has a degree within, or studies within IT
○ **Expert user** - I use IT without any larger problems, but need help time-to-time
○ **Average user** - I often have problems with IT, and feel that I need help with things that others can do on their own
○ **Below Average user** - I always have problems with IT, and always seek help from someone in IT matters



Critical Information!

This questionnaire is about an imaginary person, Daniel Anderson. We ask you to answer the questions like you normally would, while pretending to be Daniel Anderson. Please choose the answers that best fit the corresponding questions.

Question 1



*In this scenario, you received the following email from Netflix. Do you think that it is a phishing email?

Daniel Anderson, it's been 118 days. Wanna watch something?

Netflix
to me

For Daniel Anderson
Now on Netflix

More TV programmes & films to love.

We've recently added more TV programmes and films. For only US$10, watch the most talked about TV shows and movies from around the world. Last chance!

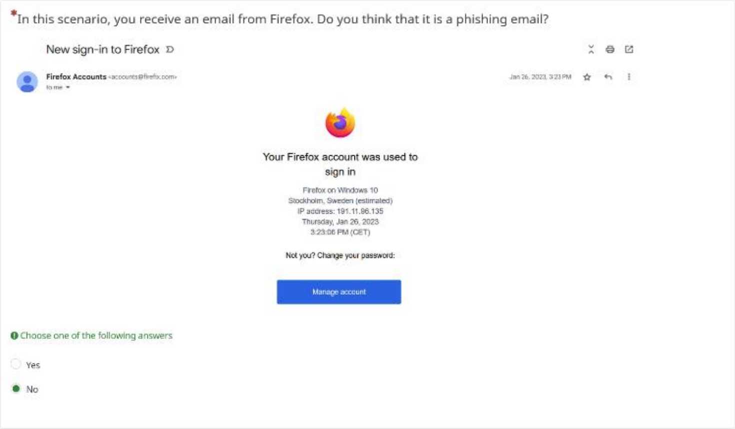
Choose one of the following answers

○ Yes

● No

Next

Question 2



*In this scenario, you receive an email from Firefox. Do you think that it is a phishing email?

New sign-in to Firefox

Firefox Accounts <accounts@firefox.com>
to me

Jan 26, 2023, 3:23 PM

Your Firefox account was used to sign in

Firefox on Windows 10
Stockholm, Sweden (estimated)
IP address: 191.11.86.135
Thursday, Jan 26, 2023
3:23:06 PM (CET)

Not you? Change your password:

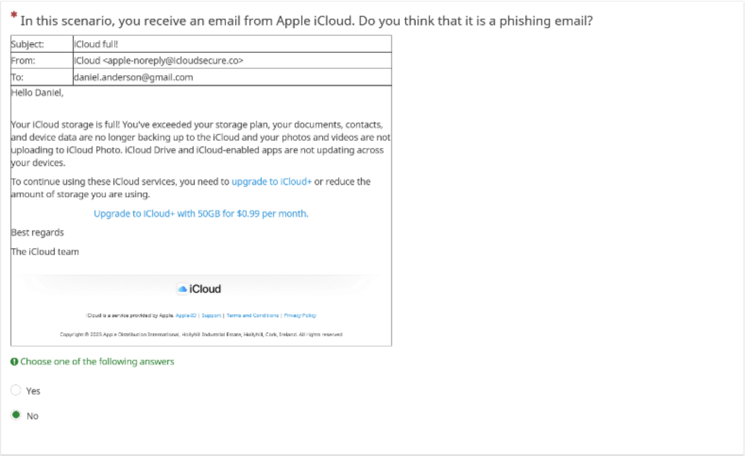
Choose one of the following answers

○ Yes

● No

Next

Question 3



* In this scenario, you receive an email from Apple iCloud. Do you think that it is a phishing email?

Subject:	iCloud full!
From:	iCloud <apple-noreply@icloudsecure.co>
To:	daniel.anderson@gmail.com

Hello Daniel,

Your iCloud storage is full! You've exceeded your storage plan, your documents, contacts, and device data are no longer backing up to the iCloud and your photos and videos are not uploading to iCloud Photo. iCloud Drive and iCloud-enabled apps are not updating across your devices.

To continue using these iCloud services, you need to upgrade to iCloud+ or reduce the amount of storage you are using.

Upgrade to iCloud+ with 50GB for $0.99 per month.

Best regards

The iCloud team

iCloud

iCloud is a service provided by Apple. Apple-ID | Support | Terms and Conditions | Privacy Policy

Copyright © 2023 Apple Distribution International, Hollyhill Industrial Estate, Hollyhill, Cork, Ireland. All rights reserved.

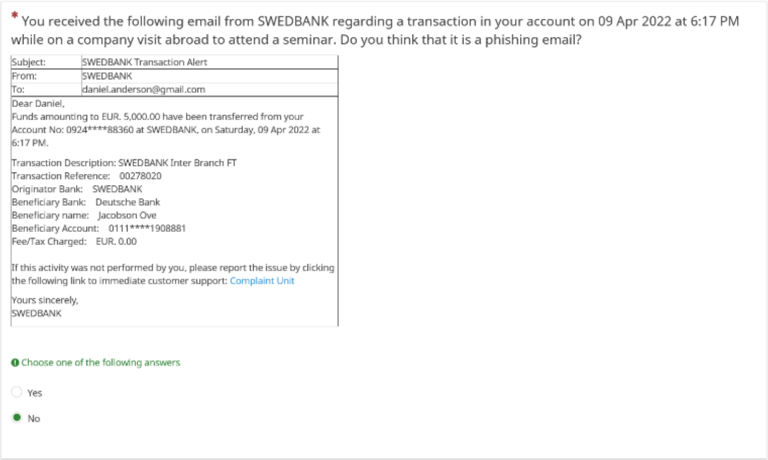
Choose one of the following answers

○ Yes

● No

Next

Question 4



* You received the following email from SWEDBANK regarding a transaction in your account on 09 Apr 2022 at 6:17 PM while on a company visit abroad to attend a seminar. Do you think that it is a phishing email?

Subject:	SWEDBANK Transaction Alert
From:	SWEDBANK
To:	daniel.anderson@gmail.com

Dear Daniel,
Funds amounting to EUR. 5,000.00 have been transferred from your Account No: 0924****88360 at SWEDBANK, on Saturday, 09 Apr 2022 at 6:17 PM.

Transaction Description: SWEDBANK Inter Branch FT
Transaction Reference: 00278020
Originator Bank: SWEDBANK
Beneficiary Bank: Deutsche Bank
Beneficiary name: Jacobson Ove
Beneficiary Account: 0111****1908881
Fee/Tax Charged: EUR. 0.00

If this activity was not performed by you, please report the issue by clicking the following link to immediate customer support: Complaint Unit

Yours sincerely,
SWEDBANK

Choose one of the following answers

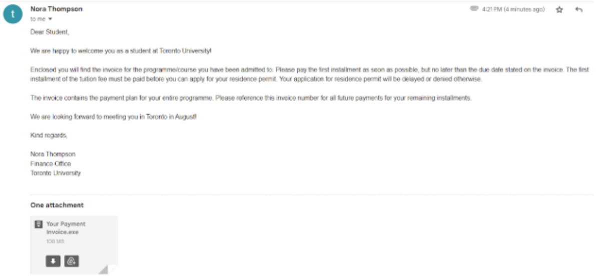
○ Yes

● No

Next

Question 5

*In this scenario, you are an applicant who just applied for admission at Toronto University with a scholarship. You get the following email from the Finance Office. Do you think that it is a phishing email?



Nora Thompson
to me

4:21 PM (4 minutes ago)

Dear Student,

We are happy to welcome you as a student at Toronto University!

Enclosed you will find the invoice for the programme/course you have been admitted to. Please pay the first installment as soon as possible, but no later than the due date stated on the invoice. The first installment of the tuition fee must be paid before you can apply for your residence permit. Your application for residence permit will be delayed or denied otherwise.

The invoice contains the payment plan for your entire programme. Please reference this invoice number for all future payments for your remaining installments.

We are looking forward to meeting you in Toronto in August!

Kind regards,

Nora Thompson
Finance Office
Toronto University

One attachment

Your Payment Invoice.exe
108 MB

Choose one of the following answers

○ Yes

● No

Next

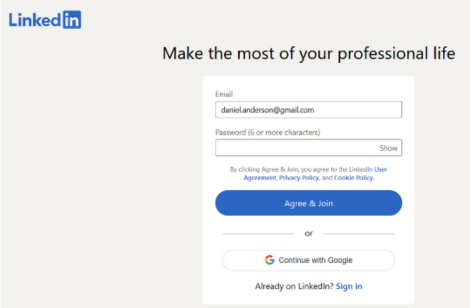
Critical Information!

The following 5 questions will be about password creation and handling. In each of these scenarios, you will be presented with four different passwords. Your task is to choose the password that you think is the closest in structure to a password that you would use for that account.

Next

Question 6

*Please select the password from the list below that is most similar to a password that you would use when creating this jobsite account:



Make the most of your professional life

Email
daniel.anderson@gmail.com

Password (6 or more characters)
Show

By clicking Agree & Join, you agree to the LinkedIn User Agreement, Privacy Policy, and Cookie Policy.

Already on LinkedIn? Sign in

Choose one of the following answers

○ aZtG@497$/#

○ 1986March8!

○ Password123!

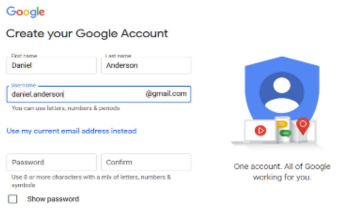
○ 1YellowCatCrossedTheRoad?

○ KYbeR1&

Next

Question 7

*Please select the password from the list below that is most similar to a password that you would use when creating this Google Account:



Google

Create your Google Account

First name: Daniel

Last name: Anderson

Username: daniel.anderson@gmail.com

You can use letters, numbers & periods

Use my current email address instead

Password

Confirm

Use 8 or more characters with a mix of letters, numbers & symbols

□ Show password

One account. All of Google working for you.

Choose one of the following answers

○ KYbeR1&

○ Password123!

○ aZtG@497$/#

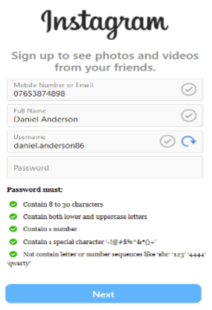
○ 1986March8!

○ 1YellowCatCrossedTheRoad?

Next

Question 8

*Please select the password from the list below that is most similar to a password that you would use when creating this Instagram account:



Instagram

Sign up to see photos and videos from your friends.

Mobile Number or Email: 07653874898

Full Name: Daniel Anderson

Username: daniel.anderson86

Password

Password must:

- ✓ Contain 8 to 30 characters
- ✓ Contain both lower and uppercase letters
- ✓ Contain 1 number
- ✓ Contain 1 special character '-!@#$%^&*()+'
- ✓ Not contain letter or number sequences like 'abc' '123' '4444' 'qwerty'

Next

Choose one of the following answers

○ KYbeR1&

○ 1YellowCatCrossedTheRoad?

○ Password123!

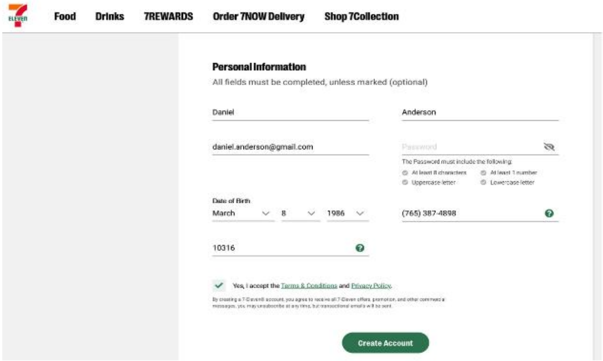
○ aZtG@497$/#

○ 1986March8!

Next

Question 9

*Please select the password from the list below that is most similar to a password that you would use when creating this 7-Eleven account for food shopping:



Personal Information

All fields must be completed, unless marked (optional)

Daniel | Anderson

daniel.anderson@gmail.com | Password

The Password must include the following:
- At least 8 characters
- At least 1 number
- Uppercase letter
- Lowercase letter

Date of Birth
March 8 1986

(765) 387-4898

10316

✓ Yes, I accept the Terms & Conditions and Privacy Policy.

By creating a 7-Eleven® account, you agree to receive all 7-Eleven offers, promotion, and other commercial messages. you may unsubscribe at any time, but transactional emails will be sent.

Create Account

Choose one of the following answers

○ 1986March8!

○ KYbeR1&

○ aZtG@497$/#

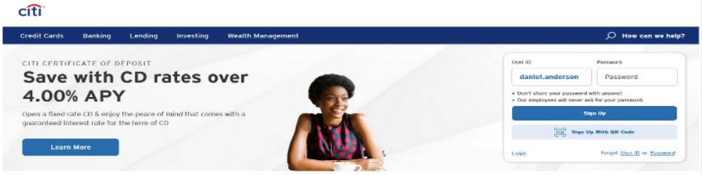
○ Password123!

○ 1YellowCatCrossedTheRoad?

Next

Question 10

*Please select the password from the list below that is most similar to a password that you would use when creating this bank account:



CITI CERTIFICATE OF DEPOSIT

Save with CD rates over 4.00% APY

Open a fixed-rate CD & enjoy the peace of mind that comes with a guaranteed interest rate for the term of CD

Learn More

User ID: daniel.anderson

Password: Password

- Don't share your password with anyone!
- Our employees will never ask for your password.

Sign Up

Sign Up With QR Code

Login

Forgot User ID or Password

Choose one of the following answers

○ 1986March8!

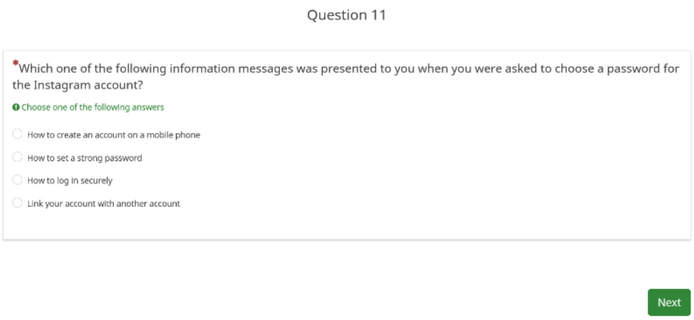
○ Password123!

○ 1YellowCatCrossedTheRoad?

○ aZtG@497$/#

○ KYbeR1&

Next



Question 11

*Which one of the following information messages was presented to you when you were asked to choose a password for the Instagram account?

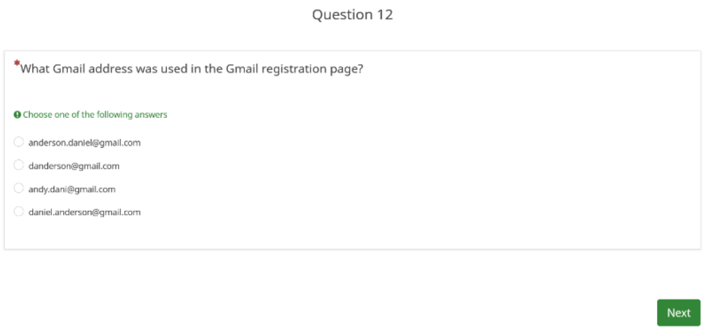
Choose one of the following answers

○ How to create an account on a mobile phone

○ How to set a strong password

○ How to log in securely

○ Link your account with another account



Question 12

*What Gmail address was used in the Gmail registration page?

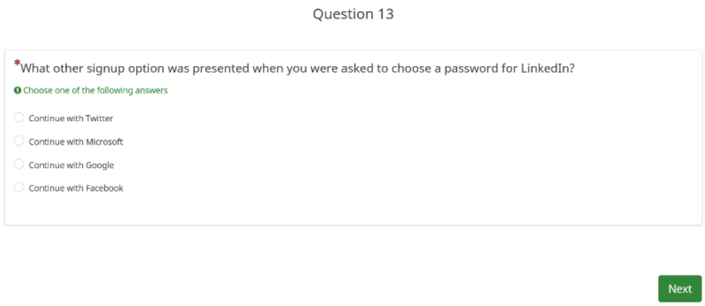
Choose one of the following answers

○ anderson.daniel@gmail.com

○ danderson@gmail.com

○ andy.dani@gmail.com

○ daniel.anderson@gmail.com



Question 13

*What other signup option was presented when you were asked to choose a password for LinkedIn?

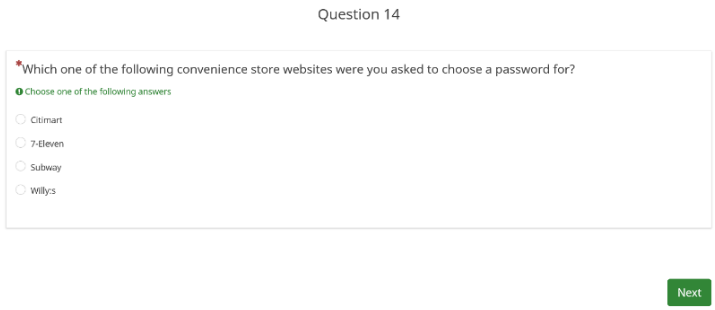
Choose one of the following answers

○ Continue with Twitter

○ Continue with Microsoft

○ Continue with Google

○ Continue with Facebook



Question 14

*Which one of the following convenience store websites were you asked to choose a password for?

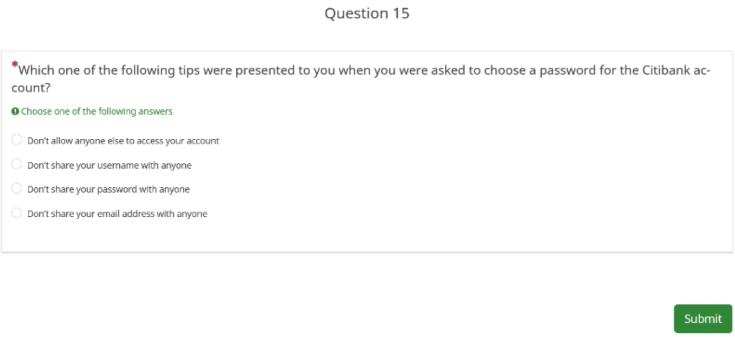
Choose one of the following answers

○ Citimart

○ 7-Eleven

○ Subway

○ Willy:s



Question 15

*Which one of the following tips were presented to you when you were asked to choose a password for the Citibank account?

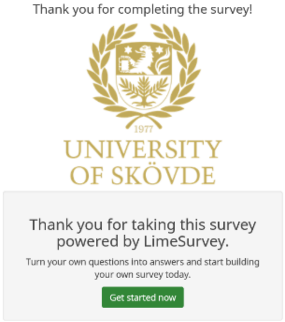
Choose one of the following answers

○ Don't allow anyone else to access your account

○ Don't share your username with anyone

○ Don't share your password with anyone

○ Don't share your email address with anyone



Thank you for completing the survey!

1977

UNIVERSITY OF SKÖVDE

Thank you for taking this survey powered by LimeSurvey.

Turn your own questions into answers and start building your own survey today.