National College of Ireland

National College of Ireland

Project Submission Sheet

Student Name:	Sailaja Midde		
Student ID:	24112666		
Programme:	MSc in Cybersecurity	**Year:**	2025-2026
Module:	Practicum		
Lecturer:	Mosab Mohamed		
Submission Due Date:	01-08-2025		
Project Title:	The Role of Human Factors in Phishing Attacks: Behavioural Cybersecurity Study		
Word Count:	3435		

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

	Sailaja Midde
Signature:	…… ……
	01-08-2025
Date:	…… ……

PLEASE READ THE FOLLOWING INSTRUCTIONS:

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.
3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**
5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a fail.**

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

AI Acknowledgement Supplement

[Practicum]

[The Role of Human Factors in Phishing Attacks: Behavioral Cybersecurity Study]

Your Name/Student Number	Course	Date
Sailaja Midde	MSc in Cybersecurity	01-08-2025

This section is a supplement to the main assignment, to be used if AI was used in any capacity in the creation of your assignment; if you have queries about how to do this, please contact your lecturer. For an example of how to fill these sections out, please click here.

AI Acknowledgment

This section acknowledges the AI tools that were utilized in the process of completing this assignment.

Tool Name	Brief Description	Link to tool
NA	**NA**	**NA**
NA	**NA**	**NA**

Description of AI Usage

This section provides a more detailed description of how the AI tools were used in the assignment. It includes information about the prompts given to the AI tool, the responses received, and how these responses were utilized or modified in the assignment. **One table should be used for each tool used**.

[NA]	
[NA]	
[NA]	[NA]

Evidence of AI Usage

This section includes evidence of significant prompts and responses used or generated through the AI tool. It should provide a clear understanding of the extent to which the AI tool was used in the assignment. Evidence may be attached via screenshots or text.

Additional Evidence:

[Place evidence here]

Additional Evidence:

[Place evidence here]

TABLE OF CONTENTS

THE ROLE OF HUMAN FACTORS IN PHISHING ATTACKS: A BEHAVIORAL CYBERSECURITY STUDY

Sailaja Midde
X24112666
Programme Code – Research in Computing CA2
National College of Ireland

Abstract

Phishing is a prevailing cyberattack mode of entry as the attackers seek to use human rather than the technical components of the target. This proposal focuses on the role cognitive biases, stress, multitasking, and digital literacy play on being prone in the context of the organization. It documents background research in the identification of gaps, objectives to quantify the behavioral drivers and training effects, a mixed-methods solution consisting of longitudinal simulated-phishing campaigns and contextualized afterwards followed by training with boosters. The approach monitors click-through and reporting rates, biases and stress scales, demographic or role factors, which are examined using ANOVA in approximating the differences and relations. The anticipated results are the integrated behavioral model of phishing risk, justification of good reinforcement cadence, human-factor metrics validity, and practitioner recommendations regarding just-in-time feedback that supplements technical measures and decreases the incidents with strong ethical protections.

Keywords: Phishing, Human Factors, Cybersecurity Training, Cognitive Biases, Behavioral Cybersecurity

1. Introduction

1.1 Problem Statement

The research problem focuses on the continuing success of phishing attacks despite the widespread adoption of advanced cybersecurity technologies. It is human behavior that these attacks are based on and people represent the weakest point in the security of organizations. The resulting imbalance renders organizations susceptible to breaches, leading to financial losses, reputation damage, and data loss (Labrecque *et al.,* 2021). This paper aims to explore the relationship between these psychological and behavioral factors in terms of their contribution to phishing susceptibility, which can shape constructive human-based approaches to cybersecurity on a larger scale of digital defense.

1.2 Importance of the Study

The research targets the human layer, the main adversarial vector of effective phishing, and operationalizes behavioral insights into prioritized training, policy, and interface nudges to mitigate breaches and expenses and augment technical controls.

General findings from the literature: Authority and signs of urgency have been shown to raise click-through; perceived stress, time pressure, and multi-tasking undermine scrutiny. This has training builds but, without reinforcement, fades; demographics and digital literacy confer variable benefits; and life-like simulations and just-in-time feedback demonstrate a measurable increase in resilience.

1.3 Research Questions

● How do cognitive biases (eg, authority bias and urgency) affect the chances of a person falling victim to phishing attacks?

● To what extent does stress and multitasking make a person more vulnerable to phishing in a work context?

● Does previous cybersecurity training lower a working professional's vulnerability to phishing?

● To what extent do demographics (eg, age, digital literacy, and job role) correlate with phishing vulnerability?

1.4 Motivation and Importance

The phishing attack has been a dominant breach channel but security ends up being technologically overweight against human behavior (Kheruddin*et al.,* 2024). Authority/urgency cues, stress, time pressure, and multitasking increase risk, and training effects deteriorate without refreshing. There are gaps in evidence: hardly any studies combine cognitive biases with workload and demographics, there are not so many field experiments, and there is inadequate standardization of measurements. The purpose of the research is to develop a testable framework and assessment plan of human-centered countermeasures to complement technical controls and be applicable to hybrid, remote, and onsite work environments.

1.5 Proposed Solution and Contributions

Proposed Solution: The study offers a mixed-methodology that includes longitudinal simulated-phishing campaigns and comprehensive surveys of cognitive biases, stress levels, workload, and digital literacy. It will combine A/B testing of training interventions with reinforcement boosters which will look at their long-term effects (Sabillon *et al.,* 2021). Multivariate and causal modelling methods will be utilised to discover mediators and moderators of phishing susceptibility, and just-in-time feedback mechanisms will be created to enhance user awareness and minimise vulnerability in the real-world environment.

Contributions: The research will provide a synthesized behavioral model of phishing risk with associations of both the psychological and situational and the demographic factors. It will offer causal evidence of the relationship of stress and multitasking effects on susceptibility and quantify the degradation of training status over time, providing guidelines on the optimal strengthening schedule (Ibrahim*et al.,* 2025).

1.6 Structure of the Document

1. Introduction: Context, problem, questions, contributions.

2. Literature Review: Critically contrast biases, stress/workload, training, demographics; expose gaps/niches.

3. Research Method and Specification: Solution, design steps, tools/data, evaluation metrics, ethics, Gantt.
4. References: Harvard style; CORE rankings/citation counts.

2. Literature Review

2.1 Introduction to Previous Work and Key Arguments

Earlier studies of phishing have highlighted issues of humanity as key predisposing factors. Available literature has provided a synthesis of evidence on cognitive, social, and contextual motivators/drivers and other works have charted areas including authority and urgency indicators, workload, and training efficiencies. Reporting intentions and intervention design in empirical research are yet another area which studies have been conducted. The review compares and contrasts these strands to answer the research questions of cognitive biases, stress and multitasking, training effectiveness, and demographic or digital-literacy impacts, as well as to determine the research niche that the study will occupy.

2.2 Cognitive Biases and Phishing Vulnerability

According to (Al-Hazwani*et al.*, 2024), authority, urgency, and familiarity biases can lower users' scrutiny when Research indicates that authority, urgency, and familiarity bias, must be used to reduce scrutiny by the users when given potentially harmful information. Additional studies point to the role of social and organizational clues in shaping intentions to act, indicating that biases also work in combination with norms. According to (Pagan *et al.*, 2023), certain work gives general classifications of various types of biases, others give more detailed explanation of decision pathways. The results also show that bias effects can be organizational or culturally sensitive and that there is a need to test the bias and situational effects.

Conclusion & link: Prejudices are central pivoting factors in phishing vulnerability, yet the extent to which they integrate with the organizational environment is ambiguous. The second subsection discusses the possibilities of contextual moderators of stress and multitasking.

2.3 Stress, Multitasking, and Work Environment

According to (Xi et al., 2023),Time pressure and high workload have been shown to inhibit users in their capacity to deliberate thoroughly, and cognitive overload may compound errors. In some studies, it is stated that organizational climate may play a mediating role in determining the authentication or escalating of suspicious emails in a stressed situation. According to (Ibrahimet*et al.*, 2025), These findings give more detailed explanations of environmental pressures on vulnerability as compared to the general accounts of human factors risk.

Conclusion & link: The relationship between stress and multitasking and vulnerability is there, however the strength of the relationships and the pathways involved is still unclear. The following subsection will discuss whether awareness programs and training can assist in curbing such risks.

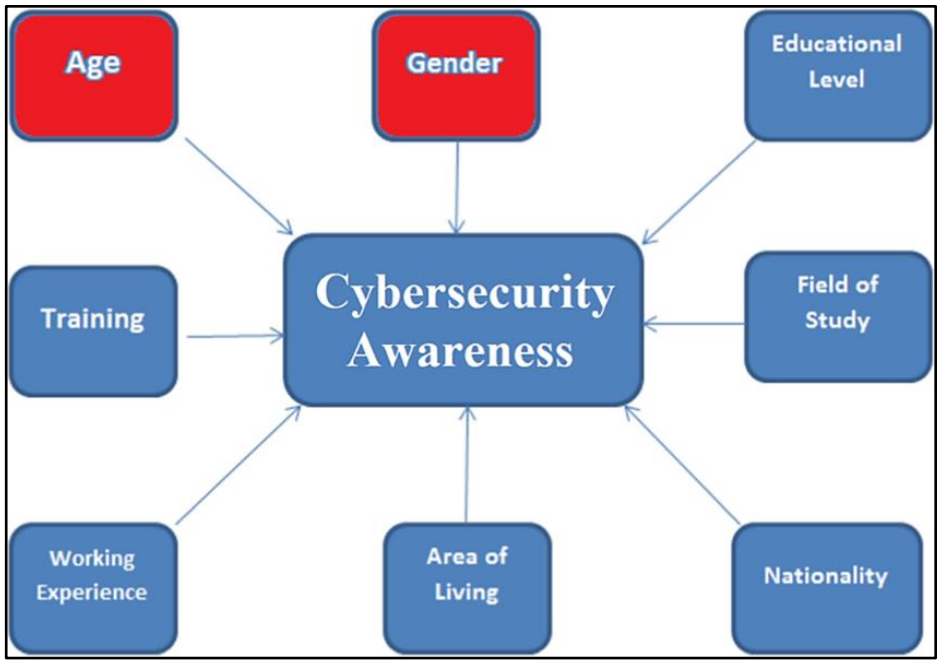

Figure 1: Cybersecurity Awareness

(Source: TherdpongDaengsi, 2021)

2.4 Cybersecurity Training and Awareness Programs

According to (Sabillon *et al.*, 2021), In some research it has been found that there is more knowledge gained through generic training, although there is no guarantee that this training will lead to safer behavior. According to (Nasir, 2023), there also have been other studies which have indicated that interventions based on reporting norms and feedback provision is best. It is generally accepted that awareness campaigns that are single that lack follow-up appear to lose their steam, whereas the use of simulations and continuous learning has a more positive outcome in the context of programs. These results suggest that the training should be contextualized, repeated, and reinforced on a real-time basis to prove the most effective.

Conclusion & link: Training can be effective though it is subject to certain conditions. The following section examines the question of whether demographic and literacy variables can inform more specific and efficacious interventions.

2.5 Demographics and Digital Literacy

According to (Terlizzi *et al.*, 2021), the results on the demographic issue (age and job position) are inconclusive. Other reports indicate that older workers could be the ones who are more susceptible, whereas digital literacy and experience appear to be more significant. According to (Saivasan and Lokhande, 2022), this discrepancy signifies that demographics cannot be used as the sole risk indicators. The studies also indicate that the demographic variables have not been rigorously studied, lending uncertainty to their significance. e.

Conclusion & link: Responses to demographic questions are inconclusive and most probably influenced by literacy and exposure through occupations. These insights are combined in the final subsection that defines the research niche.

2.6 Identifying the Research Niche

According to (Alluqmani et al., 2025), the broad areas of consensus in this review are that cognitive biases, stress and training factors contribute to phishing vulnerability and that training is more effective with reinforcement. According to (Iqbal and Yusof, 2024), there is limited research on the desirable training design that can keep up with these factors or the reduction of training over time, measured in the granularity of many studies are not complex or systematic enough to take into account. The strategy will produce validated behavioral measures and direct interventional actions that supplement current technical controls.

3. Research Method and Specification

3.1 Proposed Solution

This research adopts a behavioral cybersecurity approach that combines simulated phishing training activities with response-based data analysis. The experiment will start at the point of baseline phishing simulation to randomly distribute participants in a working environment and this will gauge the initial susceptibility level (Greitzer *et al.*, 2021). Subsequently, participants will be entered into structured surveys that will examine cognitive biases (e.g., authority and urgency), stress, multitasking, digital literacy and demographics. To measure the resulting behavior change in terms of detection and reporting of phishing, additional post-training phishing simulations will be used. This assignment is a primary quantitative study because it gathers original data via phishing simulations and surveys. It has been analyzing measurable variables with statistical methods to assess patterns with relationships and training effectiveness.

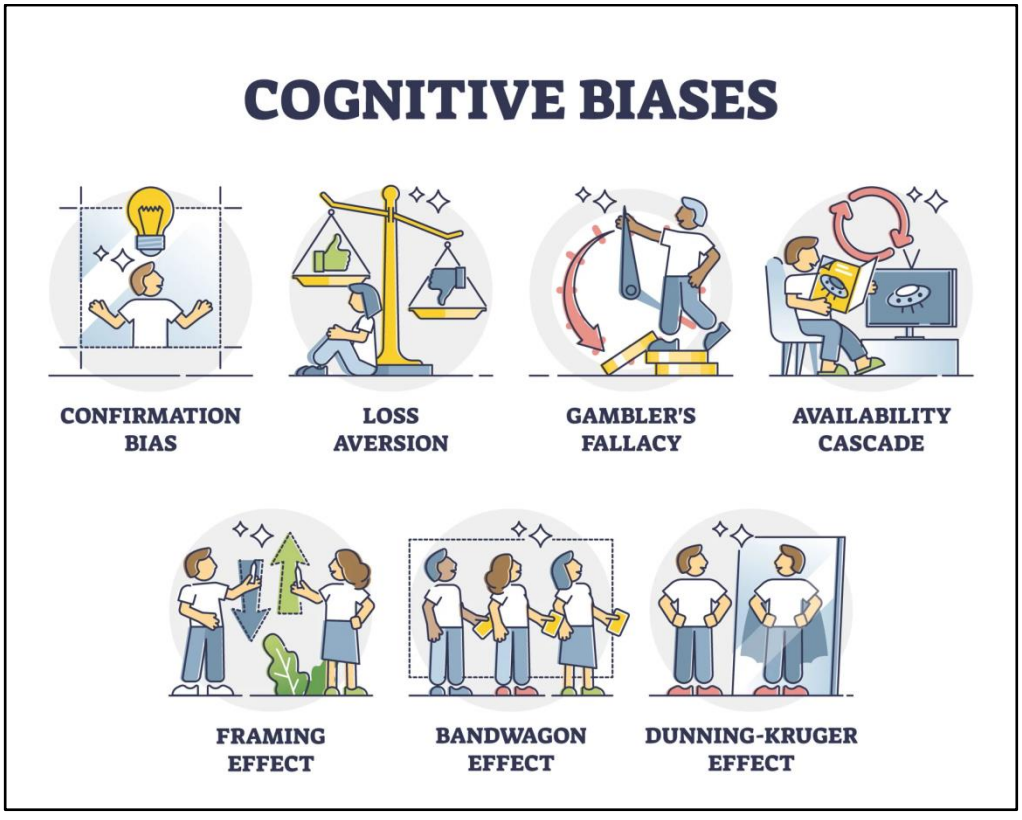

Figure 2: Cognitive Biases

(Source: Ruhl, 2023)

3.2 Project Plan and Gantt Chart

Table 1: Project Plan (Step-by-Step Activities)

Step	Activity	Description	Dependencies
1	Literature Refinement	Finalize review of studies on biases, stress, and training	None
2	Survey & Simulation Design	Develop phishing emails and structured survey instruments	Step 1
3	Baseline Data Collection	Conduct initial phishing simulations and administer surveys	Step 2
4	Training Implementation	Deliver standard or enhanced training to participants	Step 3
5	Post-Training Simulations	Run follow-up phishing simulations to evaluate training effects	Step 4
6	Data Analysis	Analyze collected data using Python and ANOVA for statistical significance	Step 5
7	Evaluation & Reporting	Summarize findings and prepare final report with recommendations	Step 6

Table 2: Gantt Chart (Tasks, Dependencies, Timescale)

Task	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9	Week 10	Week 11	Week 12
Literature Refinement												

Survey & Simulation Design												
Baseline Data Collection												
Training Implementation												
Post-Training Simulations												
Data Analysis												
Evaluation & Reporting												

The table shows good progress with the Literature Refinement is complete (green). Survey & Simulation Design remains incomplete (red), and Baseline Data Collection is half complete (blue). Remaining tasks has been included: Training with Post-Training Simulations, Data Analysis and Reporting, are planned (yellow) but yet to start.

3.3 Tools and Test Data

Python will be the most prominent data analysis tool because it allows processing large sets of data and can perform complex statistical modeling (Lafuente *et al.*, 2021). Phishing tests will be carried out using an organisational email system designed to create project specific tracking to determine click through rate and report activity. The surveys will be given through secure online forms, and data will be stored on the encrypted drives. ANOVA tests will also be carried using Python to find differences across training groups and to determine whether any predictor significantly predicts phishing susceptibility.

3.4 Evaluation Strategy

The assessment process will be done in terms of addressing the research questions by quantifying the changes in the behavior and the study of relationships with determinants of behavior concerning phishing vulnerability. This study is a primary, quantitative research project as it collects original data through phishing simulations and surveys. It has been focusing on measurable variables and using statistical analysis to evaluate relationships and outcomes (Kheruddin et al., 2024). Statistically significant decrease of click-through rates and increase of reporting rate among the participants who underwent the enhanced training as compared to those who underwent the standard training will be used as the success criteria. The statistical libraries of

Python will be used to analyze the data, employing ANOVA to detect differences among the groups and correlations to test the relationships between behavioral factors and susceptibility. The survey will be used in combination with the observational evidence gained during the phishing simulations to create a more thorough assessment.

3.5 Ethical Considerations

Strict guidelines will be followed to uphold ethical integrity during the study. The purpose of the study will be detailed by means of a consent form in which the participants will be informed of their options to withdraw, at any time, and without penalty. Data will be anonymous at the collection point and stored in encrypted devices; only the research team will have access to the data. The phishing tests themselves will not be distressing; clicking on simulated links will cause no actual damage (Pagan *et al.,* 2023). Prior to initiating the collection of data, ethical approval will be sought by the responsible institutional review board. Moreover, the results will be reported in an aggregate form to guarantee that no single person can be identified. Data protection laws will also be observed and retention rules enforced so that at the end of the research venture, data is destroyed securely.

4. References

Al-Hazwani, I., Ahmed, N., El-Assady, M. and Bernard, J., 2024, October. Towards Personal Explanations for Recommender Systems: A Study on the Impact of Familiarity and Urgency. In Adjunct Proceedings of the 2024 Nordic Conference on Human-Computer Interaction (pp. 1-8).

Alluqmani, K., Karrar, A.E., Alhaidari, M., Alharbi, R. and Alharbi, S., 2025. Assessing the Efficacy of Security Awareness Training in Mitigating Phishing Attacks: A Review. International Journal, 14(3).

Greitzer, F.L., Li, W., Laskey, K.B., Lee, J. and Purl, J., 2021. Experimental investigation of technical and human factors related to phishing susceptibility. ACM Transactions on Social Computing, 4(2), pp.1-48.

Ibrahim, H.M., Ahmad, K. and Sallehudin, H., 2025. Impact of organisational, environmental, technological and human factors on cloud computing adoption for university libraries. Journal of Librarianship and Information Science, 57(2), pp.311-330.

Iqbal, F. and Yusof, Z.B., 2024. Efficacy of Cybersecurity Awareness Training in Reducing Phishing Vulnerabilities in Organizations. Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures, 8(12), pp.10-21.

Kheruddin, M.S., Zuber, M.A.E.M. and Radzai, M.M.M., 2024. Phishing attacks: Unraveling tactics, threats, and defenses in the cybersecurity landscape. Authorea Preprints.

Labrecque, L.I., Markos, E., Swani, K. and Peña, P., 2021. When data security goes wrong: Examining the impact of stress, social contract violation, and data type on consumer coping responses following a data breach. Journal of Business Research, 135, pp.559-571.

Lafuente, D., Cohen, B., Fiorini, G., García, A.A., Bringas, M., Morzan, E. and Onna, D., 2021. A Gentle introduction to machine learning for chemists: an undergraduate workshop using python notebooks for visualization, data processing, analysis, and modeling. Journal of Chemical Education, 98(9), pp.2892-2898.

Nasir, S., 2023, July. Exploring the effectiveness of cybersecurity training programs: factors, best practices, and future directions. In Proceedings of the Cyber Secure Nigeria Conference (pp. 151-160).

Pagan, N., Baumann, J., Elokda, E., De Pasquale, G., Bolognani, S. and Hannák, A., 2023, October. A classification of feedback loops and their relation to biases in automated decision-making systems. In Proceedings of the 3rd ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization (pp. 1-14).

Ruhl, C. (2023). What is cognitive bias? Simply Psychology. [online] Available at: https://www.simplypsychology.org/cognitive-bias.html.

Sabillon, R., Serra-Ruiz, J. and Cavaller, V., 2021. An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. In Research anthology on artificial intelligence applications in security (pp. 174-188). IGI Global.

Saivasan, R. and Lokhande, M., 2022. Influence of risk propensity, behavioural biases and demographic factors on equity investors' risk perception. Asian Journal of Economics and Banking, 6(3), pp.373-403.
Terlizzi, V., Claut, L., Tosco, A., Colombo, C., Raia, V., Fabrizzi, B., Lucarelli, M., Angeloni, A., Cimino, G., Castaldo, A. and Marsiglio, L., 2021. A survey of the prevalence, management and outcome of infants with an inconclusive diagnosis following newborn bloodspot screening for cystic fibrosis (CRMS/CFSPID) in six Italian centres. Journal of Cystic Fibrosis, 20(5), pp.828-834.
TherdpongDaengsi (2021). Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. [online] Available at: https://www.researchgate.net/figure/Related-factors-for-cybersecurity-awareness_fig2_356235704.
Xi, N., Chen, J., Gama, F., Riar, M. and Hamari, J., 2023. The challenges of entering the metaverse: An experiment on the effect of extended reality on workload. Information Systems Frontiers, 25(2), pp.659-680.