Cyber Awareness Initiative Using Gamification

Industrial Internship
MSc Cybersecurity

Sabahath Rizwana Palappurath Showkath
Student ID: 21151474

School of Computing
National College of Ireland

Supervisor: Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Sabahath Rizwana Palappurath Showkath

Student ID: 21151474

Programme: MSc Cybersecurity **Year:** 2022

Module: Industrial Internship

Supervisor: Vikas Sahni

Submission Due Date: 06/01/2023

Project Title: Cyber Awareness Initiative Using Gamification

Word Count: 7091 **Page Count:** 20

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 bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Sabahath Rizwana Palappurath Showkath

Date: 06/01/2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

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

Cyber Awareness Initiative Using Gamification

Sabahath Rizwana Palappurath Showkath
21151474

Abstract

This research studies the effect of cybersecurity training on the incidents of phishing attacks on employees by using the concept of gamification and a cyber awareness quiz. The importance of using this concept is to encourage employees to actively partake in the cybersecurity measures taken by an organisation without making it a boring or stressful activity. The responses captured are mapped to points and transferred to a leader board to promote a healthy competition and the winner is rewarded with a gift-voucher as an incentive. The result of this research shows improved engagement by 40% in phishing reporting activities and 26.67% in overall performance of employees.

Introduction

Background

Due to the pandemic, the attack surface has grown drastically, and the hybrid mode of working from home and office is being exercised. This in turn has increased the challenge of monitoring the compliance of employees. There is always a possibility that individuals could be taken by surprise when at home and when they expect it least. Organisations from a variety of industries are investing more on cybersecurity each year as they become aware of the rising hazards as stated in PwC 2022 Global Digital Trust Insights[1]. Attackers with advanced skills are driven to identify weaknesses in the organisational networks and exploit them.

This research is inspired from the projects that identified the gaps in the cybersecurity practices of various organisations, especially in the field of training and awareness of employees which led to brainstorming how a particular cybersecurity training and awareness program could be incorporated into the work life organically.

Importance

The incident report of the Conti cyberattack on the Health Service Executive (HSE) in May 2021 explains how the attacker gained access to the hospital network when a staff viewed a file attachment[2] after clicking on a phishing email. Thus, it is crucial that all employees are aware of information security issues and follow the organisation's information security policy (ISP). Desolda *et al.* (2021) stated that a reliable system was dependent on its employees performing their duties adhering to the ISPs of the organisation. However, despite being aware of the security issues, Corradini (2020) mentioned that mishaps by employees may occur because of distractions like job pressure and that could result in security breaches. This highlights a crucial aspect of employee management which is emphasising on the welfare of the employees while implementing security awareness initiatives. Putting into

[1] https://riskproducts.pwc.com/resources/2022-global-digital-trust-insights

[2] https://www.hse.ie/eng/services/news/media/pressrel/hse-publishes-independent-report-on-conti-cyber-attack.html

consideration that not all employees across an organisation have the same level of cyber awareness, training costs which is reported by Aldawood and Skinner (2019) to be one of the major constraints, could be reduced by many strategies. A recent study has shown us that real world rewards, digital game elements such as points, leader boards and badges are a popular way towards professional training Mahat, Alias and Yusop, (2022).

Research Question

The research by Lévesque *et al.* (2018), which carried out a computer security clinical trial of anti-virus (AV) software with participants in a non-laboratory setting claimed that in real life, the protection provided by AV may be limited based on the type of users and how they configure their machines, and a single AV may not be best suited for all users. Furthermore, their research stated that network usage, the amount and types of web pages accessed, and other factors may all influence susceptibility to phishing. The reason why blacklisting may not be the best option was explained by Almomani (2018), stating that the given the short lifespan of phishing websites and the ease with which new phishing websites might be created, enormous work was put into maintaining the list. Williams and Li's (2017) research stated that leads and insights are needed to combine the technical as well as the human defences to effectively mitigate phishing. Hence, the question for this research is: *What is the effect of empowering employees via cybersecurity awareness?*

Limitations

The limitation faced in this research was the reluctance of the data protection team of the organisation to share the sensitive information such as phishing test results of employees.

Outline the structure of the report

The remainder of this paper is structured as follows: Section 2 discusses the Related Work, Section 3 discusses the Methodology, Section 4 discusses the Design Specification, Section 5 discusses the Implementation, Section 6 discusses the Evaluation, and finally Section 7 discusses Conclusion and Future Work.

1 Related Work

Numerous studies have offered insightful information about the worlds of cybersecurity, gamification, and human psychology, which helped in the formation of the methodology for this research by comprehending how these fields may be merged effectively. The majority of the research papers that contributed to the expansion of knowledge in the pertinent fields of cybersecurity and human psychology were systematic literature reviews or surveys. Limited research was conducted with practical applications involving voluntary participants which were employees of an organisation. This possibly could be due to the nature of data needed for such research where ethics, time, and general data protection regulations (GDPR) had to be given due diligence. However, with cybersecurity being one of the priorities of organisations across all industries today, a valuable contribution will be seen in the future.

This section is structured into the following subsections: Subsection 2.1 discusses social engineering, Subsection 2.2 discusses the importance and hurdles in information security compliance, Subsection 2.3 discusses human factors, Subsection 2.4 discusses prevailing trends in anti-phishing training and awareness, Subsection 2.5 discusses the gamification approach in cybersecurity training.

1.1 Social Engineering

Social engineering has been explained by Wang, Zhu and Sun (2021) as a cyber-attack by a threat actor where human vulnerabilities are exploited via persuasion, manipulation, or fear to acquire access to sensitive information or a restricted area. As it can be seen, there are several ways to achieve this and the capability of humans to come up with innovative ways to

do so is tremendous. The discussion here, offers the groundwork for comprehending the problem raised by the research question, as social engineering has been identified as the fundamental element in network intrusions or data breaches in organisations by Mansfield-Devin (2018).

The study by Hijji and Alam (2021) elaborated on the state-of-the-art and state-of-the-practice social engineering techniques in association with the attack methods that involved the generation of emails embedded with fake links.

Through their research Li *et al*. (2022) have clearly brought attention to the fact that there is a strong connection between information security, human vulnerabilities and social engineering and the need to update these connections from time-to-time. This is important to know because, to overcome new challenges posed by cyber-attacks, Aldawood and Skinner (2019) have suggested that the organisations need to take steps to inform employees about the latest attack techniques via cybersecurity training and awareness campaigns. These measures need to be taken because, "The human factor is truly security's weakest link" as stated by Mitnick and Simon (2003).

1.2 Information Security Compliance

Compliance is defined by Oxford University Press as "The practice of obeying rules or requests made by people in authority"[3]. The National Institute of Standards and Technology defines ISP as an "Aggregate of directives, regulations, rules, and practices that prescribes how an organisation manages, protects, and distributes information"[4]. In an organisation accommodating 1000s of employees, it could be challenging to improve employee compliance and thus, more research on effective solutions to solve these challenges must be addressed.

Choong and Theofanos (2015) through their research which examined employees' attitudes and experiences regarding compliance with organisational password policies noted that the stringent nature of the policies caused compliance to be thrown out of the doorway because maintaining multiple work-related passwords while adhering to rigorous criteria and change frequency was cognitively taxing, making it difficult for them to be fully compliant and have a positive attitude toward such policies. Furthermore, the study stated that the employees showed compliant behaviour only when they saw the policies in their favour or convenience thus bringing a positive attitude and proposed the development of effective policies that considered not just security but also usability for the employees.

In their study, D'Arcy and Teh (2019) mention that security related stress (SRS) caused frustrations and fatigue among employees. As a result of these emotions of frustration of following ISP at the organisation, employees gradually disregarded the violation of ISP which in turn showed a decrease in compliance to ISP. To overcome this challenge, D'Arcy and Teh (2019) proposed several solutions such as getting employee suggestions while developing policies, promoting positive coping strategies and adopting security education, training and awareness (SETA) programs. But the policies need to be updated; with the evolution of technology and promoting positive coping strategies come their own set of challenges and they do not seem to be practical.

The systematic literature review (SLR) by Ali *et al.* (2021) develops a model for transforming employee's non-compliant behaviour to compliant behaviour by addressing the core influential factors such as culture, motivation to protect, awareness of security, behaviour of the society and management of an employee's compliance towards ISP. A

[3] https://www.oxfordlearnersdictionaries.com/definition/english/compliance
[4] https://csrc.nist.gov/glossary/term/information_security_policy

process model has been proposed by Ali *et al.* (2021) to assist information security managers to understand the information security behaviour of their respective teams and make informed decisions while developing training and awareness programs. This study has contributed towards the methodology used in the current project where relevant parameters of real-world scenarios from the recommendations of Ali *et al.* (2021) have been considered.

1.3 Human Factors

This subsection provides a gist of the explanation of typical human behaviour thereby leveraging this understanding to curate a process for improving ISP compliance.

Social engineers successfully coerce victims into disclosing sensitive information[5] by using psychological manipulation. In addition to this, a recent study by Lambert-Mogiliansky and Calmettes (2021) concluded that human behaviour is affected or could get influenced in terms of making a rational decision or processing a given piece of information when subjected to distraction. Additionally, Lambert-Mogiliansky and Calmettes (2021) highlight the supplied information may quickly persuade people, and logical arguments against it would not be as effective, allowing the attacker to take advantage.

The importance of the study by Williams and Li (2017) is commendable because it explained that in a working environment, employees who were p reoccupied (or distracted) with work could easily be convinced to reveal essential information through the phishing email, which could result in identity theft, financial loss, and loss of intellectual property.

Furthermore, Levin and Milgrom (2004) explained the choice theory regarding preferences or choices made by humans irrespective of their beliefs (such as what is right or wrong) for a particular criterion and options available to them. This study also showed that generally humans were biased and in the presence of monetary choice, the most beneficial choice to them at that point of time was made by them whether the outcome was the expected one or favourable one in the bigger picture.

The study by Liu *et al.* (2022) provided yet another intriguing finding from survey-based research that, employees who adhered to ISPs were not influenced by rewards, incentives, or penalties and remained compliant as opposed to those who did not. Wiafe *et al.* (2020) recommended including a rewards and recognition system would help the organisation foster a security-conscious culture. These investigations gave a deep insight of human nature, which were used to create the project methodology.

1.4 Anti-Phishing Training and Awareness

Through the study of Williams and Li (2017) it was understood that there is a plethora of factors that can impact a person's circumstantial judgement towards social engineering. Williams and Li (2017) also highlighted that different people responded to a particular situation in their unique way and indicated that every individual has a unique thought process and thus concluded that for training to be relatively successful customisation needs to be brought into the prevailing methods.

The theoretical study by Chowdhury, Katsikas and Gkioulos (2022) included participants ranging from regular employees to the leadership during training method development and proposed a concept of using personalised learning where the training assessments and feedback of employees were gathered and processed to create their respective learning profiles but, this study did not have practical validations. In a practical world, involving the leadership in a limited time research has its limitations due to the sensitive nature of data collected.

[5] https://www.darkreading.com/operations/why-anti-phishing-training-isnt-enough/a/d-id/1340951

Furthermore, Jampen *et al.* (2020) stated that the security and phishing awareness training must be integrated to employees' work routines and further developed into a security culture such that, they do not feel burdened to do the training as an additional task. Considering the above factors and assessing the organisation security awareness training, the current research has proposed with a refreshed perspective where customisation is not employee oriented.

1.5 Gamification

In recent years, the concept of gaming in security awareness and training has gained popularity in research as it has been providing positive results. Sharif and Ameen (2020) through their extensive investigation concluded that the use of gamification as a tool for training overcame the challenge of training employees having varying knowledge in cybersecurity in an organisation.

By adopting a hybrid approach of passive and active learning, Franchina *et al.* (2021) has recommended creative engagement-based learning that can attain the security maturity an organisation is aiming for whilst remaining affordable and easily implementable.

Fujs, Vrhovec and Vavpotič (2022) proposed personalisation of information security training where the security training must be customised to the specific user to achieve intended learning outcomes and optimise cost. Although this proposal is innovative, this cannot be confirmed without analysing the results after putting it into practice and measuring the costs. For a company with large scale employees, a common platform must be developed to start user-engagement and make them realise where they are falling short. Then it is important to study further the proposed approach of Fujs *et al.* (2022), identifying user-specific training elements, user profiling, then building recommended systems for personalisation as the next step towards security awareness.

The gamification and leader board approach explained by Canham *et al.* (2022) would greatly assist in developing the security culture among participants which, in the long run, will achieve the goal for organisations to build the needed human firewall because as rightly said by Mitnick and Simon (2003), "Anyone who thinks that security products alone offer true security is settling for the illusion of security". This knowledge positively aided in the development of the methodology proposed.

Table 1 summarises the related work emphasising the strengths and weaknesses of the previous works. The objective of this project was to use gamification to merge the fields of psychology and cybersecurity and develop a novel method. The approach chosen needed to be organic yet reducing the strain on human error and allowing employees to be an asset rather than a liability.

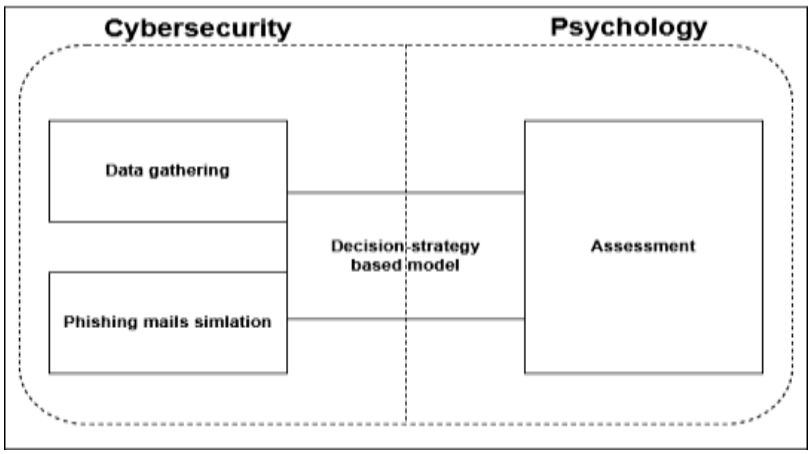
Table 1: Summary of Related Work

Authors	Strengths	Limitations
D'Arcy and Teh (2019)	Highlights the prevalence of SRS and neutralisation of ISP violation	Inability to affirm causality and inconsistency in the timing of survey invitations across time-zones
Jampen *et al.* (2020)	Recommended phishing training to be a recurrent process integrated naturally into employee work-life with possible customisation based on employees	Research and application of the recommendation to be done and validated in a real-world scenario. Also, mentioned about having missed some platforms while researching about all

		the available security/anti-phishing training platforms
Ali *et al.* (2021)	Proposed a process model to assist info-sec managers to develop customised security training programs based on the compliance level of the respective teams	Research and application of the proposal to be validated in a real-world scenario
Hijji and Alam (2021)	Latest phishing techniques during COVID-19	To provide initial level of training and awareness only which is the current scenario but it is not effectively reducing cyber-attacks or data breaches
Franchina *et al.* (2021)	A hybrid approach of initiative that combines engagement-based and less interactive method	Case studies were presented to address the benefits of the proposed hybrid approach
Liu *et al.* (2022)	Recommended positive feedback and recognition to improve ISP compliance	Survey based research which could have some limitations and has to be tested on a real-world scenario
Canham *et al.* (2022)	Gamification of online phishing training exercise of employees	A month-long experiment conducted due to limited budget

2 Research Methodology

This research combines the fields of human psychology and cybersecurity via gamification as the practice of identifying phishing mails and reporting them via the correct channels withing the organisation is expected to become a part of their regular work tasks.



1 - Methodology

2.1 Data Gathering

The participants' data were first collected and stored for analysis in the organisation's cloud storage. Their personally identifiable information (PII), which could be used to

categorise them into different groups based on defined criteria, was essentially present in the data which included location, whether they got phished, phished in the previous simulation, clicked link, and passed quiz. These groups would provide insights into the performance of participants individually and as a team.

The data were collected over the span of one week. The data points, as and when collected, were transferred into the organisation's Google Drive for storage using the services available. The utmost priority was given to ensure that the data gathered was with the consent of the participants, as well as the organisation's data protection team for the selected participants. All necessary security measures as per NCI's and the organisation's policy and guidelines were taken.

Furthermore, the participants were given a detailed explanation of the research such as what the research entails, that this research was conducted to monitor the responses of simulated phishing mails at the workplace and a reward awaited the top performers.

2.2 Phishing Mails Simulation

The phishing mails were generated by a dedicated team within the organisation. This ensured that the mails reached the participants as it could bypass the organisation firewalls. The responses were collected for the participating employees and used to perform further analysis. The analysis provided the insights about the percentage of participants who fell prey to the simulated phishing emails.

The responses to the phishing mails were logged by the data protection and security training departments of the organisation in which the responses of all participants who fell prey to the simulated phishing mail and of all the participants who did not fall prey were stored securely as per the protocols. The data of the participants that was essential to advance to the next stage were extracted, saved in a Google Sheet, and uploaded to the organisation's cloud storage and retrieved when needed.

2.3 Quiz

The awareness program was developed to make sure that all participants were aware of recent advances in social engineering and the ways in which phishing attacks could possibly occur. So, all participants were asked to participate in a '*Cyber Awareness Quiz'*; the questions for this were curated based on the significant advancements in the phishing and social engineering arena. Given the context, the participants, especially those who were not phished, needed to take this task seriously because, as Levin and Milgrom (2004) stated, once someone feels they have achieved something or won a competition, they tend to become careless and conceited. Hence, a reward of points was introduced to this task to keep all participants equally focused on the awareness program.

2.4 Decision-Strategy Based Model

The participants were divided into two groups, Phished and Not Phished, based on the information from the previous section.

Phished: The participants that were phished were subjected to security training videos by the dedicated team within the organisation. The videos provided the latest security-training on phishing, how it happens, what are the factors to investigate, how they could be disastrous to the individual and what are the possible implications of the same and how to report any suspicious mail received.

Not Phished: The participants were categorised into two. The first category being the one where the participants actively reported the simulated phishing mails to the organisation. The other category being the one where the participants did not report the mail or ignored the mail.

Points for Phished or Not Phished: The points proposed for this research were for participants that reported the phishing mail, that did not report the phishing mail but also did not click the link and for the phished participants to promote among participants a healthy competition, to win and be vigilant.

Points for Assessment: Leveraging the findings of Liu *et al.* (2022) and Levin and Milgrom (2004) that the employees in an organisation would be prone to work for monetary or recognition-based rewards shows no matter how important an event is for the safety of the employees or the organisation, it won't have the desired impact until the employees get something out of it. So, the topics for the quiz were published in the organisation's internal portal over the course of one month and a pass percentage of *80%* was set for the quiz.

Thus, points were allocated for the participants who passed the cyber awareness quiz, who failed the quiz points and who did not attempt the quiz.

3 Design Specification

The research incorporated a mechanism to strengthen compliance among employees of an organisation and build relevant training and security standards for them to not fall prey to phishing attacks.

To achieve this, data from employees of an organisation was collected by subjecting them to regular phishing simulations within the organisation, articles on trending cyber-attacks, and cyber awareness assessment and analysing their response. The proposed mechanism was designed to be recurrent in nature which could be deployed by the organisation across teams and locations to continually track the ISP compliance progress of the employees. The participants were allocated points as mentioned above based on their performance.

3.1 Data Collection

The research was launched by first performing analysis on the best mode and amount of data to be gathered as these could challenge the compliance measures at an organisational level. The next step was collection of consent from participants within the organisation to volunteer for this study. After this, the consent and request of the phishing simulation and data protection department of the organisation was obtained to release the required data. The data was stored in the organisation's Google Drive in a structured and organised format.

The PII that was collected from the participants was limited to name, location and email ID. Data for each participant was gathered by providing the phishing simulation team the name and email ID of the participants who agreed to take part in the research. When the results of simulated phishing mail responses were obtained from the team, the following data were stored:

- Name
- Email ID
- Location
- Date
- Got phished in the previous simulation

- Opened the phishing mail
- Clicked the link
- Reported the mail as a phishing mail

Furthermore, to ensure that the participants were well-informed regarding the project, the participants were given a detailed explanation of the research such as what the research entails, that this research was conducted to detect phishing at the workplace and an incentive was announced for the top performers based on their results. A cyber awareness quiz which was created using Google Forms was conducted as part of the research and the following data were obtained and stored:

- Email ID
- Date
- Quiz results
- Quiz answers
- Participant consent

3.2 Phishing Mails Simulation

The next step was to run simulation of phishing emails using the services of the dedicated team within the organisation. The content for the phishing email was decided by the team as well.

The responses of the participants whether phished or not as well as whether they opened the mail or not was provided by the team and the data were categorised accordingly. These data were further analysed to determine the points scored by the participants.

3.3 Phished

The phished participants were informed that they were phished and had to undergo a training session which was decided by the phishing mail simulation team. Critical research in the psychology domain had been evaluated to comprehend why humans make certain decisions in binary environments. As discussed in the related work section, Levin and Milgrom (2004) explained that choices made by humans were often regretted and a desire to change the same is pondered upon. However, in an environment where the choices presented did not have significance in the individual's life, there existed several other factors including distractions, carelessness, or desire to do something wrong that drove the humans to certain conclusion.

These factors could be hazardous to an organisation and helped determine the causality by which an individual would make a choice of clicking on the phishing link sent to them. When the participant clicked on the phishing mail, the action was recorded as "*opened phishing mail*" and when the participant clicked on the link in the email, the action was recorded as phished.

3.4 Cyber Awareness Program

Whether the participants got phished or not, the participants were apprised of the recent changes, technical advancements, and potential dangers to the organisation. To facilitate the same, the organisation conducted a cyber awareness program where every week one article on a cyber-attack topic was released in the internal portal for employees. The articles explained what the type of attack was and tips to stay safe and report to relevant teams within the organisation. In the modern era, where technology is developing at an exponential rate, it is essential that organisations employ precautions against cyber-attacks that keep up with the

advancement of the technologies as highlighted by Liu *et al.* (2022) and Aldawood and Skinner (2019) in their studies about the importance of updating the technologies and approaches towards prevention of phishing-based attacks with time. This awareness helps provide the necessary information to protect the personal and professional lives of the employees thereby also benefiting the organisation and validating the approach.

3.5 Cyber Awareness Quiz

This part of the research talks about the creation of a questionnaire using Google Forms which would be used to validate the of attention of employees towards the awareness program spoken about in the previous subsection. The questions were simple and entirely based on the awareness program conducted within the organisation. The quiz included questions of varying difficulty, starting from the definitions of the type of an attack to stating the tips to stay safe and approaches towards detecting the same, as these were elaborately discussed in the respective articles.

3.6 Research resources

This subsection summarises the resources that were collected, used, and stored for this project.

3.6.1 Human Resources

The participants were a group of employees from whom the least and appropriate of amount of data were collected to successfully complete this project. Data for each participant was gathered by providing the phishing simulation team the name and email ID of the participants who agreed to take part in the research. When the results of simulated phishing mail responses were obtained and a cyber awareness quiz was conducted as part of the research, the data mentioned above were collected and stored.

3.6.2 Cloud Storage Resources

Cloud services of the Google platform available in the organisation were used for the storage of the data, the drive was terminated which ensures that the data were purged without violating any ethical or privacy concerns.

3.6.3 Phishing Simulation Resources

The phishing simulation was done by a dedicated team within the organisation.

3.6.4 Cyber Awareness Articles

The articles were created by the team that is responsible for running the phishing simulation. Every week a new article was published in the organisation’s portal for a period of four weeks.

3.6.5 Cyber Awareness Quiz

At the end of publishing the articles, a quiz was created to measure the attention and understanding of the participants towards the articles using Google Forms.

3.6.6 Data Visualisation Resources

The participant data after responding to the test phishing mails and assessments were categorised and scored in terms of points stored in cloud using Google Sheets. The phishing results were divided into categories - phished, not phished, and ignored mail. Similarly, the

quiz results were also categorised as - passed, failed, and ignored quiz. This step helped to segregate the performances and identify the best participants among the lot.

The data from Google Sheets was loaded to the Microsoft PowerBI desktop application to visualise the data using various graphs, trend lines, tables, and pie charts.

4 Implementation

To achieve the objective of this research, data from 10 employees of an organisation with their consent was collected by subjecting them to regular phishing simulations within the organisation, articles on trending cyber-attacks, and cyber awareness assessment and analysing their responses. Furthermore, the consent and request of the phishing simulation and data protection department of the organisation was obtained to release the required data.

The proposed mechanism was designed to be recurrent in nature which could be deployed by the organisation across teams and locations to continually track the ISP compliance progress of the employees. To facilitate the same, the organisation conducted a cyber awareness program for a period of four weeks where each week one article on a cyber-attack topic was released in the internal portal for the employees.

The Personally Identifiable Information (PII) that was collected from the participants was limited to name, location and email ID. Data for each participant was gathered by providing the phishing simulation team with the names and email IDs of the participants who agreed to take part in the research. When the results of simulated phishing mail responses were obtained from the team, features such as name, email ID, location, date, got phished in the previous simulation, opened the phishing mail, clicked the link, and reported the mail as a phishing mail were stored for further analysis. Based on the articles published in the internal portal, a cyber awareness quiz created using Google Forms was conducted as part of the research and from this email ID, date, quiz results, quiz answers, and participant consent were obtained and stored.

Furthermore, to ensure that the participants were well-informed regarding the project, the participants were given a detailed explanation of the research such as what the research entails, that this research was conducted to detect phishing at the workplace and an incentive of 25 euros each was announced for the leading performers.

The points were allocated for each activity that was considered a response with respect to phishing mails or the quiz helping to differentiate the participants in the leader board based on their performance. Thus, as shown in table 2, the points proposed for this research were *+100* points for participants that reported the phishing mail and *+50* points for participants that did not report the phishing mail but also did not click the link and finally, *-50* points were allocated for the phished participants. This way, the participants would be engaged in a healthy competition, to win and be vigilant. The participants who passed the cyber awareness quiz were awarded a total of *+100* points. The participants who failed the quiz were awarded *0* points and finally, the participants who did not attempt the quiz were awarded *-20* points.

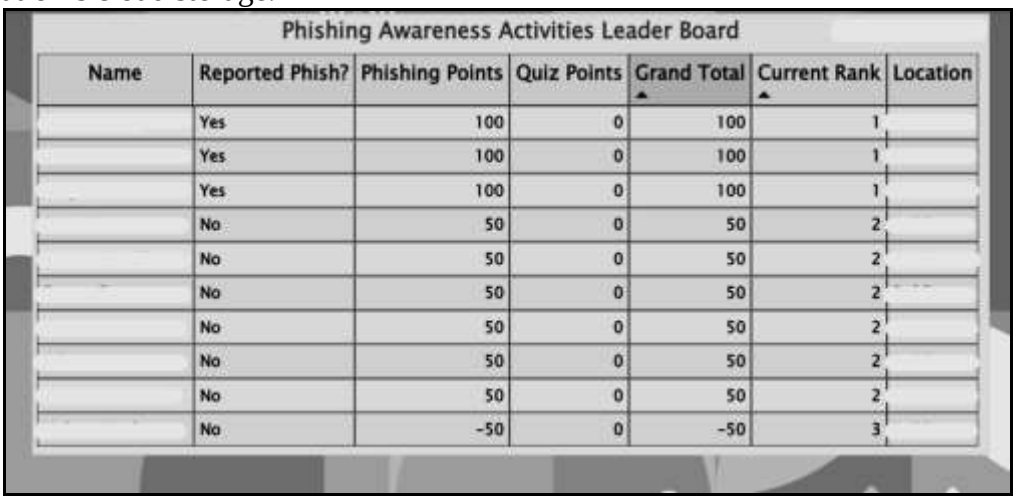
Table 2: Summary of Points

Phishing mail response points		**Quiz response points**	
Clicked on link	-50	Passed	+100
Ignored mail	-10	Failed	0
Reported mail	+100	Did not attempt	-20
Neither reported nor phished	+50		

Based on the points and categories, the participant data points were segregated and structured in the Google Sheet and were then loaded to Microsoft PowerBI desktop application to visualise the data using various graphs, trend lines, tables, and pie charts. Two dashboards were created for two groups of audiences.

1. The first one was for the participants who were shown a leader board visual which gave them an idea of who was performing the best and subtly alerting them to do better.
2. The second one was developed for the leadership within the organisation who could see the overall team performance and understand whether the training chosen for a particular team was bringing the desired results or not and much more.

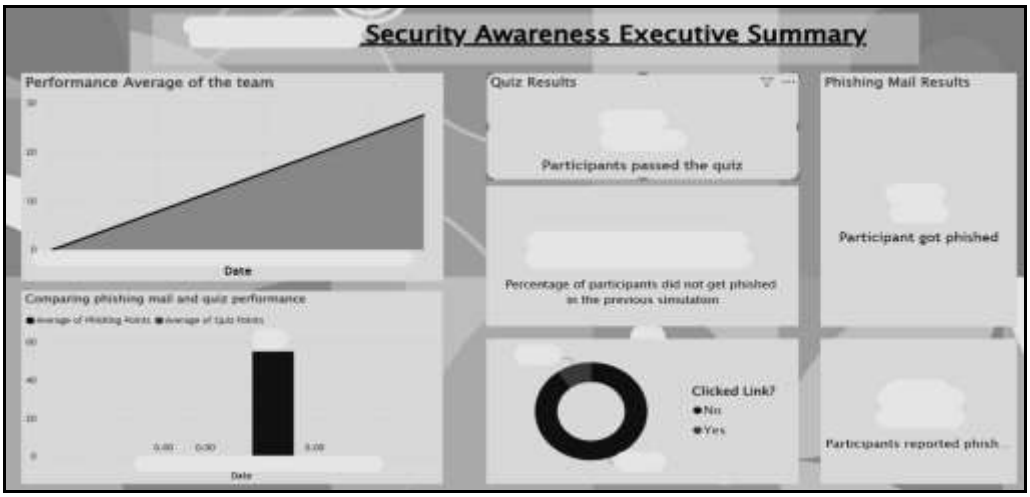
The Google Sheet containing raw data and dashboards were stored securely on the organisation's cloud storage.



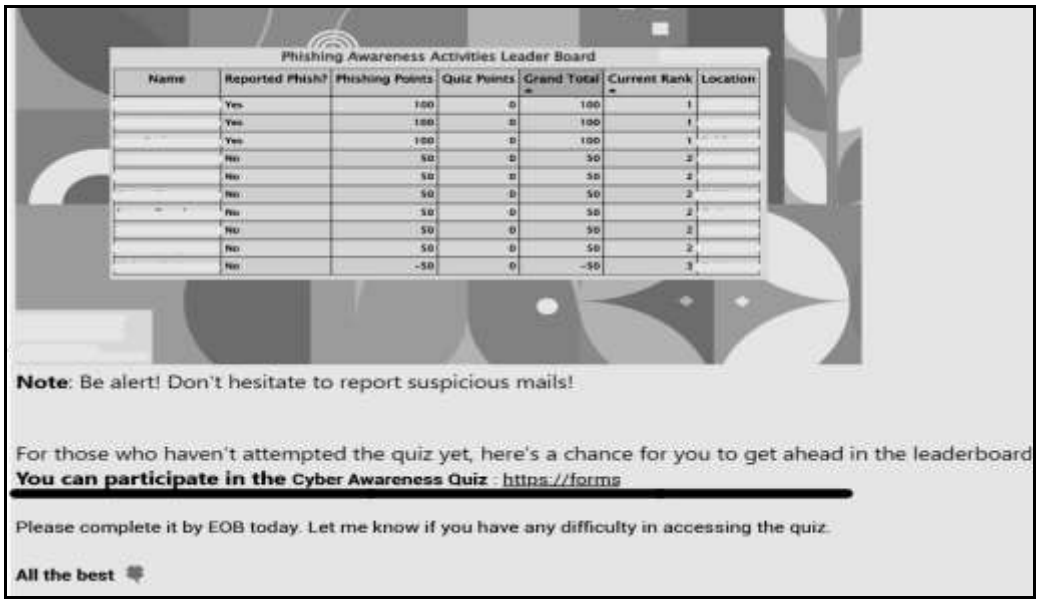
Phishing Awareness Activities Leader Board

Name	Reported Phish?	Phishing Points	Quiz Points	Grand Total	Current Rank	Location
	Yes	100	0	100	1	
	Yes	100	0	100	1	
	Yes	100	0	100	1	
	No	50	0	50	2	
	No	50	0	50	2	
	No	50	0	50	2	
	No	50	0	50	2	
	No	50	0	50	2	
	No	50	0	50	2	
	No	-50	0	-50	3	

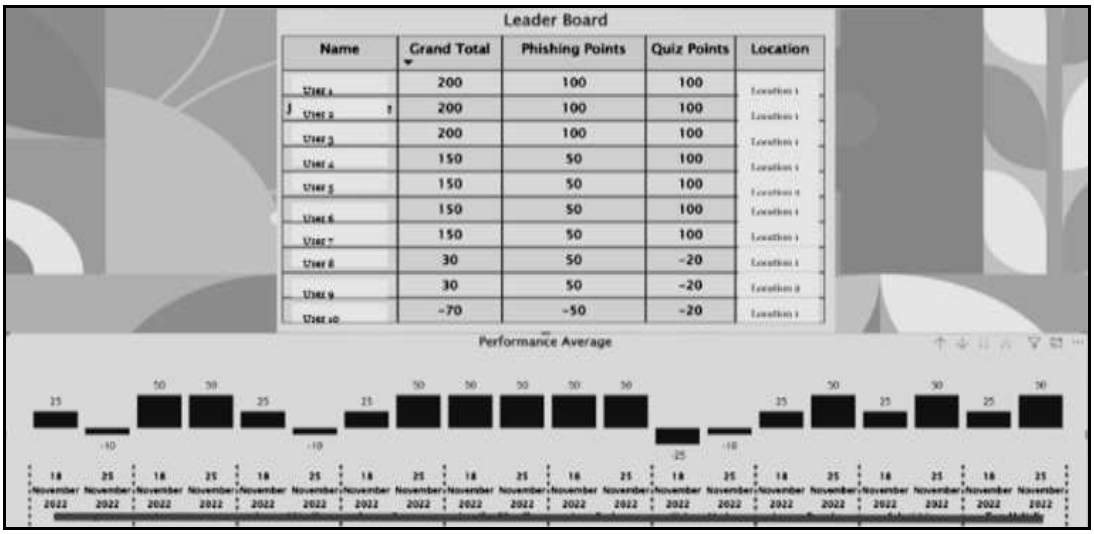
2 - Participant leaderboard after Experiment 1



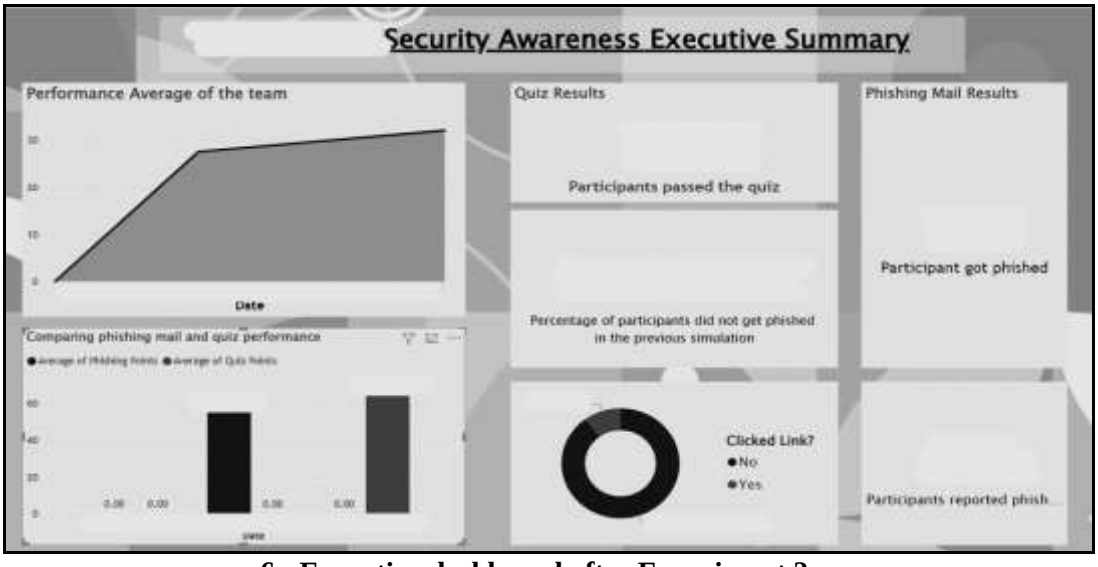
3 - Executive dashboard after Experiment 1



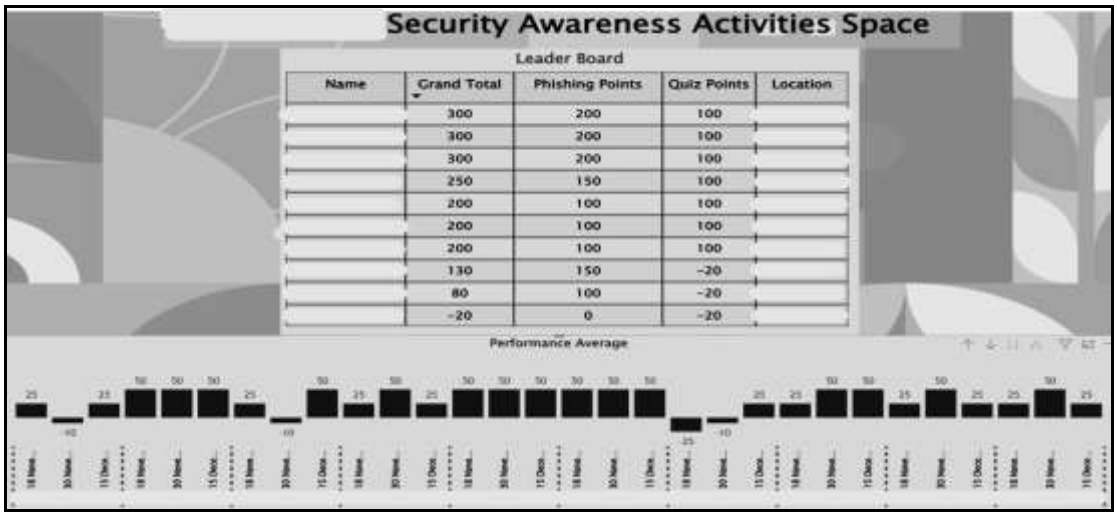
4 - Encouraging participants to attempt quiz (experiment -2)



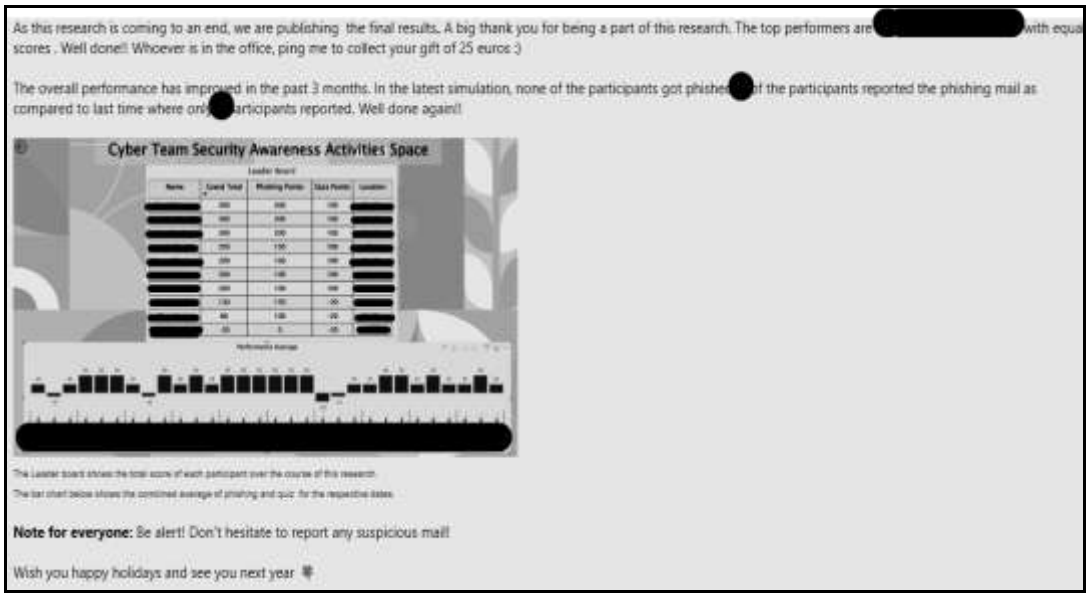
5 - Participant leader board Experiment 2



6 - Executive dashboard after Experiment 2



7 - Participant leader board Experiment 3



8 – Reporting to the participants their progress after Experiment 3

9 - Executive dashboard after Experiment 3

At the end of the research the top participants which was more than two in the leader board were given 25 euros each for their dedication and consistency in performance.

5 Evaluation

From the experiments conducted it was seen that the participant engagement and overall group performance has improved continuously.

In experiment 1 where a phishing simulation was run, it was noticed that not every participant reported the phishing mail. In experiment 2 where the quiz was conducted, there was an increase in participant engagement where the difference in overall results between the first and second experiment was indicated by a *14.01%* increase. In experiment 3, the difference in results between the second and third experiment showed *14.67%* increase in performance. Furthermore, if you particularly compare experiment 1 and experiment 3 which are the phishing simulation experiments, there has been *26.67%* increase in the overall performance and *40%* increase in the phishing reporting activity which were the objectives of this study.

5.1 Experiment 1

The first phishing simulation was run, and the results of the overall performance were calculated and recorded. A leader board indicating each participant's position was shown to the participants. At this stage, the executive dashboard did not have much to show.

5.2 Experiment 2

The cyber awareness quiz was circulated, and the results of the overall performance were calculated and recorded. The leader board with updated results based on the latest performance was shown to the participants. The executive dashboard showed key insights of this research such as who got phished, how many participants passed the quiz, who reported a phishing mail, and the variation in performance of the 10 participants in the group based on dates.

5.3 Experiment 3

The next phishing simulation was run, and the results of the overall performance were calculated and recorded. The leader board indicating each participant's position based on the latest performance was shown to the participants. The executive dashboard was updated with the latest details. The winners were awarded 25 euros each.

6 Conclusion and Future Work

This research studied the effect of cybersecurity training specifically on the simulation of phishing mails sent to employees by using the concept of gamification and monitoring the responses to the simulated phishing mails and cyber awareness quiz responses of participants. The responses captured were mapped to points and transferred to a leader board to promote a healthy competition and the winner was rewarded with a gift-voucher which was used as an incentive in this research. The result of this research showed improved engagement in phishing awareness activities and alertness of employees. Furthermore, an executive dashboard was developed to highlight the key findings in the data including the number of participants who reported a phishing mail, the number of participants that got phished in the previous simulation and the number of participants that passed the quiz. These findings

helped the management understand whether the measures taken for cybersecurity awareness were effective or not.

This model could be automated for improvement, with the points serving as the target variable of a machine learning model. The points earned could be used in a regression-based machine learning model to forecast the likelihood that a particular participant will be phished by producing a probability score. The ultimate system thus created must be able to raise the bar for employee compliance.

The response times recorded could be used as an advanced factor to compare and determine the social and mental engagement levels of an employee. Apart from using the response times to differentiate the participants in the leader board, they could contribute to a detrimental form for machine learning models to learn and understand the behaviour of an employee. Based on learning from historical data, the model must help in predicting if a participant would be more prone to being phished in the future.

In addition to improving the implementation technology-wise, this experiment can be expanded to a greater number of participants within an organisation and studied further.

References

Aldawood, H. and Skinner, G. (2019) 'Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues', *Future Internet*, 11(3), p. 73. doi: 10.3390/fi11030073.

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M. and Sohail, A. (2021) 'Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance', *Applied Sciences* 11(8), p. 3383. doi: 10.3390/app11083383.

Almomani, A. (2018) 'Fast-flux hunter: a system for filtering online fast-flux botnet', *Neural Computing and Applications* 29(7), p. 483–493. doi: 10.1007/s00521-016-2531-1.

Canham, M., Posey, M. C. and Constantino, M. (2022) 'Phish derby: Shoring the human shield through gamified phishing attacks', *Frontiers in Education*, 6, 807277. doi: 10.3389/feduc.2021.807277.

Choong, YY., Theofanos, M. (2015) 'What 4,500+ People Can Tell You – Employees' Attitudes Toward Organizational Password Policy Do Matter', In: Tryfonas, T., Askoxylakis, I. (eds) Human Aspects of Information Security, Privacy, and Trust: Third International Conference, HAS 2015, *Lecture Notes in Computer Science* vol 9190, pp. 299-310, *Springer, Cham*. doi: 10.1007/978-3-319-20376-8_27.

Chowdhury, N., Katsikas, S. and Gkioulos, V. (2022) 'Modeling effective cybersecurity training frameworks: A delphi method-based study', *Computers & Security* 113, 102551. doi: 10.1016/j.cose.2021.102551.

Corradini, I. (2020). 'Security: Human Nature and Behaviour', *Springer International Publishing*, pp. 23–47. doi: 10.1007/9783030439

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T. and Costabile, M. F. (2021) 'Human factors in phishing attacks: A systematic literature review', *ACM Computing Surveys* 54(8). doi: 10.1145/3469886

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

Franchina, L., Inzerilli, G., Scatto, E., Calabrese, A., Lucariello, A., Brutti, G. and Roscioli, P. (2021) 'Passive and active training approaches for critical infrastructure protection', *International Journal of Disaster Risk Reduction* 63, 102461. doi: 10.1016/j.ijdrr.2021.102461.

Fujs, D., Vrhovec, S. and Vavpotič, D. (2022) 'Towards personalized user training for secure use of information systems', *The International Arab Journal of Information Technology*, 19(3), pp. 307-313. doi: 10.34028/iajit/19/3/3.

Hijji, M. and Alam, G. (2021) 'A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: Challenges and prospective solutions', *IEEE Access* 9, pp. 7152–7169. doi: 10.1109/ACCESS.2020.3048839.

Jampen, D., Gür, G., Sutter, T. and Tellenbach, B. (2020) 'Don't click: Towards an effective anti-phishing training. A comparative literature review', *Human-centric Computing and Information Sciences* 10, p. 33. doi: 10.1186/s13673-020-00237-7.

Lambert-Mogiliansky, A. and Calmettes, A. (2021) 'Phishing for (quantum-like) phools—Theory and experimental evidence', *Symmetry* 13(2), p. 162. doi: 10.3390/sym13020162.

Lévesque, F. L., Chiasson, S., Somayaji, A. and Fernandez, J. M. (2018). 'Technological and human factors of malware attacks: A computer security clinical trial approach', *Association for Computing Machinery* 21(4). doi: 10.1145/3210311.

Levin, J. D. and Milgrom, P. R. (2004) *Introduction to choice theory*. Available at: https://web.stanford.edu/~jdlevin/Econ%20202/Choice%20Theory.pdf [Accessed 13 December 2022].

Li, T., Wang, X. and Ni, Y. (2022) 'Aligning social concerns with information system security: A fundamental ontology for social engineering', *Information Systems*, 104, 101699. doi: 10.1016/j.is.2020.101699.

Liu, C., Liang, H., Wang, N. and Xue, Y. (2022) 'Ensuring employees' information security policy compliance by carrot and stick: The moderating roles of organizational commitment and gender', *Information Technology & People* 35(2), pp. 802–834. doi: 10.1108/ITP-09-2019-0452.

Mahat, J., Alias, N. and Yusop, F. D. (2022) 'Systematic literature review on gamified professional training among employees', *Interactive Learning Environments*, pp. 1–21. doi: 10.1080/10494820.2022.2043910.

Mansfield-Devine, S. (2018). 'The ever-changing face of phishing', *Computer Fraud & Security* 2018(11), pp. 17–19. doi: 10.1016/S1361-3723(18)30111-8.

Mitnick, K. D. and Simon, W. L. (2003) *The art of deception: Controlling the human element of security*. Indianapolis, Indiana: John Wiley & Sons.

Sharif, K. H. and Ameen, S. Y. (2020) 'A review of security awareness approaches with special emphasis on gamification', in *2020 International Conference on Advanced Science and Engineering (ICOASE)*. Duhok, Iraq, 23-24 December 2020, pp. 151–156. doi: 10.1109/ICOASE51841.2020.9436595.

Wang, Z., Zhu, H. and Sun, L. (2021) 'Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods', *IEEE Access* 9, pp. 11895–11910. doi: 10.1109/ACCESS.2021.3051633.

Wiafe, I., Koranteng, F. N., Wiafe, A., Obeng, E. N. and Yaokumah, W. (2020) 'The role of norms in information security policy compliance', *Information & Computer Security*, 28(5), pp. 743–761. doi: 10.1108/ICS-08-2019-0095.

Williams, N. and Li, S. (2017) 'Simulating human detection of phishing websites: An investigation into the applicability of the Act-R cognitive behaviour architecture model', in *2017 3rd IEEE International Conference on Cybernetics (CYBCONF)*, Exeter, UK, 21-23 June 2017 pp. 1–8. doi: 10.1109/CYBConf.2017.7985810.