Effectiveness of cybersecurity awareness training in lowering the risks of email-borne attacks for Irish SME

MSc Research Project
MSc in Cybersecurity

Hrvoje Jack Ascic
Student ID: x21181233

School of Computing
National College of Ireland

Supervisor: Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Hrvoje Jack Ascic		
Student ID:	x21181233		
Programme:	MSCCYBETOP	**Year:**	2023
Module:	MSc Industry Internship		
Supervisor:	Vikas Sahni		
Submission Due Date:	14/08/2023		
Project Title:	Effectiveness of cybersecurity awareness training in lowering the risks of email-borne attacks for Irish SME		
Word Count:	7602		
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: Hrvoje Jack Ascic

Date: 19/04/2023

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):	

Effectiveness of cybersecurity awareness training in lowering the risks of email-borne attacks for Irish SME

Hrvoje Jack Ascic
x21181233

Abstract

Phishing attacks pose a significant risk to businesses, particularly small and medium-sized enterprises (SMEs) with limited cybersecurity resources and expertise. This study looked into the effectiveness of cybersecurity awareness training in lowering the risks of email-borne attacks for Irish SME. According to the findings, ongoing training, and awareness programmes, such as the cybersecurity awareness workshop, can be effective in reducing SME's vulnerability to phishing attacks. The study sheds light on the importance of investing in ongoing training programmes to improve email security and make businesses less vulnerable to phishing attacks. The study emphasised the importance of businesses taking proactive measures to protect themselves from cyber threats.

The findings prove that the human factor as an attack vector can be lowered by 52% and highlight the significance of investing in cybersecurity resources and expertise in order to improve email security and reduce the risk of phishing attacks and to educate employees on the dangers of phishing attacks.

1 Introduction

The internet has transformed the way businesses operate, and while it has provided numerous benefits, it has also introduced new risks. Cybersecurity has emerged as a critical issue for businesses of all sizes, particularly small and medium-sized enterprises (SMEs), which are frequently more vulnerable due to limited resources and expertise. SMEs are facing a significant threat to their operations and reputation due to the rise of email-borne attacks such as phishing and business email compromise. SMEs must implement effective cybersecurity measures, including cybersecurity awareness training for their employees, to mitigate these risks.

This study looked into how Irish SME can use cybersecurity awareness training to reduce email-borne risks. The study's research question is:

How can Irish SMEs use cybersecurity awareness training to mitigate email-borne risks?

The research objectives are to identify the types of email-borne risks that SMEs face, assess the effectiveness of cybersecurity awareness training in mitigating these risks, and make recommendations for cybersecurity awareness training implementation in Irish SMEs. The study's hypothesis is that cybersecurity awareness training can reduce the likelihood and impact of email-borne risks in Irish SMEs significantly. The research hypothesis is that cybersecurity awareness training can significantly reduce the likelihood and impact of email borne risks in Irish SMEs. By investigating this hypothesis, this research aims to contribute to the scientific literature by providing evidence-based recommendations for SMEs to improve their cybersecurity posture.

This research makes an important contribution because it aims to provide practical recommendations to Irish SMEs on how to mitigate email-borne risks through cybersecurity awareness training. The study provides empirical evidence of the effectiveness of cybersecurity awareness training in Irish SMEs, and findings could help policymakers, SMEs, and other stakeholders improve cybersecurity practises in Irish SMEs. The study's practical implications could extend beyond Irish SMEs to other SMEs around the world facing similar cybersecurity challenges.

This report provides a comprehensive overview of the various aspects of the study. Section 2 presents a summary of the relevant research in the related subject. Section 3 discusses the research technique used and the various processes involved in reaching the study's conclusions. Section 4 proposes a framework for evidence collection that can be used as additional guidance during the audit process. Sections 5 and 6 contain detailed information on the framework's implementation and evaluation against the exploratory methodological approach. Section 7 presents the report's findings as well as any potential future employment opportunities.

2 Related Work

Email has established itself as a vital tool for business communication in the current digital era. However, this convenience has also made people significantly more susceptible to cyberattacks, especially Irish SMEs who might lack the funding for effective cybersecurity measures. Cybersecurity is an increasing concern for both the general public and businesses. As more and more operations and transactions take place online, leaving businesses and their customers open to cyberthreats like hacking, phishing, and malware, it is becoming more and more crucial for businesses. [1] Email threats like spam, business email compromise (BEC), spoofing, and phishing can seriously harm Irish businesses. These dangers may lead to monetary losses, reputational harm, and a decline in customer confidence. [2]

2.1 Email threats

Phishing is a type of fraud in which attackers use emails, instant messages, or bogus websites to obtain sensitive information from unsuspecting victims. Phishing attacks are becoming more common and sophisticated, posing a significant risk to individuals, businesses, and governments around the world. These attacks can cause financial loss, identity theft, and reputational harm to the victim. Khonji et al. [3] explore various phishing detection techniques, such as signature-based, behaviour-based, and machine learning-based approaches. By understanding the characteristics and tactics used by attackers, individuals and organizations can take necessary precautions to protect themselves from phishing attacks. Aleroud and Zhou [4] suggest a three-layered approach to combating phishing attacks, which includes technical controls, organizational controls, and individual controls. The survey heavily relies on secondary sources, which may result in some bias in the information presented. Furthermore, the paper's scope is relatively limited, and some critical aspects of phishing attacks may have been overlooked. Dhamija et al. [5] present an empirical study of the factors that contribute to the success of phishing attacks. They emphasise several factors that contribute to the success of phishing attacks, such as the persuasive design of phishing websites, the lack of visual cues to distinguish legitimate from fake websites, and Internet users' trust. However, because the study used a small sample size, the findings may not be generalizable to a larger population.

Email spoofing is another serious email threat. This is a technique used by attackers to deceive their victims by sending emails with a fake sender address. This is typically accomplished by changing the "From" field in the email header to make the email appear to have been sent from a legitimate source. Email spoofing can be used for a variety of purposes, including phishing, spamming, and malware distribution. Email spoofing is discussed in detail by Pandove et al. [6]. They recommend that users take preventative measures such as separating trusted and untrusted contacts into separate email accounts, deleting spam quickly, avoiding public terminals, scanning all attachments, using secure passwords, and encrypting emails with confidential information to avoid such attacks. The authors' discussion of countermeasures is limited to technical solutions, and additional information on user awareness training would have been beneficial. Hu and Wang [7] emphasise the high frequency of email spoofing attacks as well as the various methods employed by attackers, such as IP address spoofing and domain name spoofing. They recommend improvements to email authentication mechanisms such as SPF, DKIM, and DMARC. Their study is limited to analysing email headers and does not take into account the content of the emails or the behaviour of the recipients, nor does it take into account the impact of user education and awareness on the success of email spoofing attacks.

The method proposed by Bremler-Barr and Levy [8] is based on the observation that legitimate senders have a consistent pattern of behaviour, such as the frequency and timing of sending emails, whereas attackers have an inconsistent pattern of behaviour. This observation is used by the authors' method to determine the legitimacy of the sender's IP address. The authors do not provide a thorough assessment of the effectiveness of their proposed method. They only offer a proof-of-concept evaluation based on a small-scale dataset. The authors also fail to provide a thorough examination of the potential drawbacks of their proposed method, such as false positives or false negatives. Many researchers, such as A.C. Shuckers [9], recognise the lack of perfect efficiency in email filtering tools and highlight the importance of user awareness training and the need for users to be cautious when opening emails and clicking on links. In her paper she mainly focuses on technical solutions for preventing email spoofing attacks and does not provide a comprehensive analysis of user awareness training.

Another type of attack, BEC (Business Email Compromise), occurs when an attacker impersonates a senior executive or employee of the targeted organisation and sends a convincing email to another employee, supplier, or customer requesting a wire transfer or sensitive information such as login credentials or financial data. The emails frequently appear to be legitimate and may contain convincing details about the organisation or the executives involved, and they can dupe the recipient into actions that benefit the attacker, resulting in significant financial loss or data breaches. Cross and Gillet's [10] paper provides an in-depth analysis of the tactics used by attackers in BEC attacks, such as social engineering, email spoofing, and phishing. The authors offer insightful insights into the psychology of these attacks, emphasising the attackers' ability to manipulate victims into performing actions that benefit the attacker. The paper also discusses the prevalence of BEC attacks in various industries and breaks down the financial losses caused by these attacks. Cidon et al. [11] present a thorough examination of the BEC threat landscape, highlighting the limitations of existing detection methods. The authors contend that current rule-based and heuristic-based solutions are ineffective at detecting sophisticated BEC attacks that rely on social engineering and language manipulation. The proposed machine learning-based approach examines the sender, recipients, content, and other features of the email to identify patterns indicative of BEC attacks. However, the authors do not provide a comprehensive analysis of user awareness training and do not provide a detailed analysis of the potential drawbacks of their proposed approach, such as false positives or false negatives.

Bakarich and Baranek [12] present a case study of a fictitious company that is the victim of a BEC attack, as well as a step-by-step analysis of the attack, highlighting the attackers' tactics and the targeted organization's vulnerabilities. The authors also propose a set of best practises and recommendations that businesses can use to prevent and mitigate BEC attacks, such as using two-factor authentication, implementing email filters, and emphasising the importance of security awareness training for employees. The presented case study is fictitious and may not accurately reflect the complexities and nuances of real-world BEC attacks. Researchers like Mansfield-Device [13] recommend that businesses develop a clear incident response plan that includes regular testing and training. His determined that incident response planning and regular testing is particularly valuable, as it highlights the importance of being prepared for a BEC attack. Furthermore, the paper focuses on technical and procedural solutions rather than a comprehensive analysis of user awareness training.

2.2 Identifying the need for cybersecurity awareness training

Organizations commonly use email filtering tools to protect themselves against email-based threats such as phishing and malware. However, these tools are not impenetrable, and attackers are increasingly sophisticated in their methods of circumvention, such as social engineering and email spoofing. This highlights the importance of organisations implementing additional safeguards against these threats, such as cybersecurity awareness training for all employees. This training should cover topics such as email security best practises, identifying and reporting suspicious emails, and effectively using email filtering tools, and be repeated on a regular basis to ensure that employees are up to date on the latest threats and mitigation strategies.

When considering cybersecurity awareness training, organisations also need to consider the cost needed to implement such training. Zhang et al. [14] propose a cost-benefit analysis framework for assessing the efficacy and value of cybersecurity awareness training programmes, which includes the costs of developing and delivering training materials as well as the potential benefits of reducing security incidents and their associated costs. The proposed framework may not be applicable to all organisations because it does not consider the unique needs and vulnerabilities of each organisation. Furthermore, the paper focuses primarily on the financial costs and benefits of cybersecurity awareness training and does not provide a comprehensive analysis of the impact of training on employee behaviour and security attitudes.

Miranda [15] argues that a comprehensive phishing exercise approach to cybersecurity awareness training is more effective. The proposed method entails creating realistic phishing emails that mimic real-world attacks and using these emails to test employees' ability to detect and respond to phishing attempts. In order to improve their ability to recognise and respond to future phishing attempts, the author also emphasises the importance of providing feedback and follow-up training to employees who fail the phishing exercise. Sabillon at al. [16] present a detailed examination of the components of their proposed Cybersecurity Awareness TRAining Model (CATRAM), which consists of four stages: assessment, design, implementation, and evaluation. The model is intended to provide a structured approach to cybersecurity awareness training that includes the development of training materials, training delivery, and ongoing evaluation of the training program's effectiveness. From assessment to evaluation, the model provides a structured approach to training that includes all phases of the training process. Furthermore, the authors' emphasis on combining different training methods, such as classroom-based training and simulations, is especially valuable because it allows organisations to develop a training programme that meets the specific needs of their employees. Furthermore, the paper focuses primarily on the training process and does not provide a thorough examination of the impact of training on employee behaviour and attitudes towards security.

Researchers such as Dash and Ansari [17] would argue that a lack of cybersecurity awareness is one of the leading causes of security breaches, and therefore, organizations must prioritize cybersecurity awareness training for their employees. They propose a training model with four phases: assessment, planning, implementation, and evaluation, and provide a detailed analysis of each phase, emphasising the importance of conducting a thorough assessment of the organization's current security posture, developing a customised training plan, implementing the training plan via various methods, and evaluating the training program's effectiveness. The paper, however, could benefit from a more in-depth discussion of the specific training methods and tools used in each phase of the model. When it comes to cybersecurity awareness training, various assessment methods such as surveys, quizzes, interviews, and simulations are available. Rahim et al. [18] examine the strengths and weaknesses of each method and make recommendations for how they should be used. They also discuss the significance of selecting an appropriate method in light of factors such as the target audience, the level of knowledge required, and the assessment goals. They contend that a combination of methods is required to provide a holistic view of cybersecurity awareness within an organisation.

It is important to gauge the interest of employees when implementing the training. Proctor [19] investigates the effectiveness of cybersecurity awareness training programmes by surveying employees who have completed such training. While the training was generally well-received, he discovered that there were some areas that could be improved. Employees specifically reported a lack of engagement and interactivity in the training, and many felt that it did not adequately address the specific cybersecurity risks that they faced in their jobs. He recommends that cybersecurity awareness training programmes be tailored to the specific needs and risks of various job roles, and that interactive elements such as simulations and games be used to increase engagement. Jin et al. [20] White consider that cybersecurity awareness training should begin in school and have attempted to resolve the problem of gauging interest of high-school students by developing a Cyber Security Challenge game. When compared to those who did not play the game, students who played it showed a significant improvement in their understanding of cybersecurity concepts. The study's one limitation is that it was conducted with a small sample size of only 49 students. Furthermore, the study did not assess the game-based approach's long-term effectiveness. It is unclear whether the students' improved cybersecurity knowledge will last or deteriorate over time. Another study by Huynh et al. [21] promotes gamification in the training, and proposes Securipig, a game-based cybersecurity awareness training approach that aims to promote effective cybersecurity practises among employees. The authors created the game with the Security Culture Framework (SCF) as the training content. A user study with 32 participants was conducted to evaluate the game, and the results revealed that Securipig was effective in increasing participants' knowledge and awareness of cybersecurity threats and best practises. Furthermore, the game was found to be engaging, enjoyable, and simple to use by the participants.

2022 paper authors argue that traditional awareness training methods are often ineffective and propose an AI-based solution that combines natural language processing, machine and learning to provide personalized and engaging training to employees. Ansari et al. [22] concentrate on the use of artificial intelligence for cybersecurity awareness training in order to prevent phishing attacks. Their paper suggests using a phishing simulator to test the training's effectiveness and identify areas for improvement. Their findings suggest that AI-based cybersecurity awareness training could be a promising solution for organisations looking to improve their security posture by increasing employee awareness and decreasing the number of successful phishing attacks. In another one of her studies, Ansari [23] presents a quantitative study of the effectiveness of AI-based cybersecurity awareness training programmes. The study's goal was to compare the risk scores of participants before and after the training programme and to assess the training's effectiveness. The authors used a web-based game as a training platform, and the study included 243 participants. The results showed that the AI-based training programme was effective in lowering the risk scores of the participants. However, the sample size of the study is small, and more research is needed to validate the efficacy of AI-based cybersecurity awareness training programmes.

Gasiba et al. [24] discuss the creation of a cybersecurity awareness platform that enhances cybersecurity awareness training through the use of virtual coaches and automated challenge assessments. The platform's goal is to provide users with an interactive and engaging learning experience, allowing them to understand the risks and implement appropriate security measures to protect their systems and data. The platform generates personalised cybersecurity challenges for each user, which are then assessed automatically using machine learning algorithms. The researchers admit that more research is needed to assess the platform's effectiveness over time and in different user settings, as the technology leaves much to be desired. In a pilot study [25] with 40 participants, the same authors assessed the platform's effectiveness, finding that the personalised feedback and automated assessment engine have a significant impact on improving users' cybersecurity awareness. According to the study findings, participants' average risk score improved by 33.5% after using the platform.

Hijji and Alama [26] conduct a thorough review of the existing literature and empirical studies on cybersecurity training and awareness, and they propose a Cybersecurity Awareness and Training (CAT) Framework for remote workers. The CAT framework was created by researching existing frameworks and models, interviewing security experts, and conducting academic assessments to identify potential major levels and key practises. Following that, the proposed framework was evaluated using case studies that included demonstrations and statistical analyses. Post-case-study evaluations were also carried out in order to improve and enhance the framework in terms of usability, framework structure, and user satisfaction. The framework's limitations and potential challenges in different organisational settings could have been discussed in greater depth in their paper. [26]

Table 1 –Review Summary

Paper	Strengths	Limitations
Khonji et al.	Provides a comprehensive overview of phishing detection techniques	The paper's scope is relatively limited
Aleroud and Zhou | A.C. Shuckers	Focuses on technical solutions for preventing email spoofing attacks and acknowledges the importance of user awareness training	Does not provide a comprehensive analysis of user awareness training
Dhamija et al.	Presents empirical study on factors contributing to the success of phishing attacks	Small sample size limits generalizability of findings
Pandove, et al. | Hu and Wang	Provides detailed analysis of various email spoofing attack methods and recommends improvements to email authentication mechanisms	Limited to analysing email headers and does not account for impact of user education and awareness
Bremler-Barr and Levy	Proposes a novel method to determine the legitimacy of sender's IP address	Does not provide a thorough assessment of the method's effectiveness or potential drawbacks
Cidonet al. | Bakarich and Baranek | Cross and Gillet	Presents thorough examination of BEC threat landscape and proposes machine learning-based approach for detection	Does not provide comprehensive analysis of potential drawbacks of proposed approach or insightful insights into psychology of attacks
Mansfield-Device	Recommends businesses develop incident response plan with regular testing and training	Focuses on technical and procedural solutions rather than comprehensive analysis of user awareness training
Zhang et al.	Provides a cost-benefit analysis framework for evaluating cybersecurity awareness training programs	Focuses mainly on financial costs and benefits, may not be applicable to all organizations
Miranda | Sabillon et al. | Rahim et al.|	Proposes a structured approach to cybersecurity awareness training that includes assessment, design, implementation, and evaluation, as well as effectiveness of realistic phishing exercises, as well as importance of tailoring training programs to the specific needs	Focuses primarily on the training process and does not provide a thorough examination of the impact of training on employee behaviour and attitudes towards security
Dash and Ansari	Proposes a comprehensive training model with four phases: assessment, planning, implementation, and evaluation	Could benefit from a more in-depth discussion of specific training methods and tools used in each phase of the model
Ansari et al.| Ansari | Gasiba et al.| Hijji, Alam	Proposes an AI-based solution that combines natural language processing, machine learning, and a	Requires further research to validate the efficacy of AI-

	phishing simulator to provide personalized and engaging training	based cybersecurity awareness training programs

3 Research Methodology

The goal of this study was to look into the impact of cybersecurity awareness training on email-borne risks in Irish SME. Research methodology was designed to investigate this research question using a quasi-experimental design with a pre-test and post-test. Two phishing campaigns and a cybersecurity awareness training workshop were used in the study to assess participants' knowledge of email-borne risks and ability to detect phishing attacks. The sections that followed provided a detailed overview of this research project's research design, sample selection, data collection and analysis, ethical considerations, timeline, and limitations.

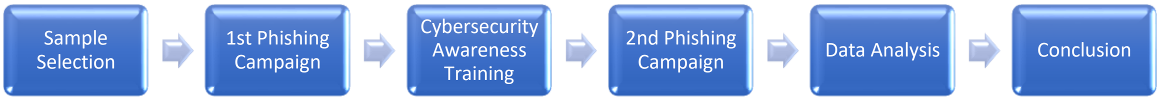


Figure 1 – Research Project Workflow

3.1 Research Design

This study used a quasi-experimental research design with a pre-test and post-test. Two phishing campaigns and an in-person training session were used to collect data. The two phishing campaigns were carried out to evaluate the effectiveness of the cybersecurity awareness training intervention. The first phishing campaign occurred prior to the training workshop, while the second occurred following the workshop. The simulated phishing emails were designed to look like real-world phishing emails and included links to fake login pages or malware attachments.

3.2 Sample Selection

The study targeted an Irish SME that communicates primarily via email. A power analysis was used to determine the sample size to ensure that the study had enough statistical power to detect significant differences. To take part in the study, 42 participants were recruited. Participants were drawn from various departments, including Recruitment, HR, Sales, Engineering, Marketing, and Facilities, and ranged in seniority from entry level roles to business owners. The sample selection process sought to recruit a diverse and representative sample of Irish SME in order to ensure that the study's findings were generalizable to the larger population. A sample size of 42 participants was deemed adequate for a quasi-experimental design and provided sufficient statistical power to detect significant differences.

3.3 Data Collection

Data was collected through two phishing campaigns. The first phishing campaign was conducted to establish a baseline measure of participants' susceptibility to phishing attacks.

The cybersecurity awareness training workshop followed and was designed to educate participants on email-borne risks, including phishing, spear-phishing, spoofing, and business email compromise attacks. The training included information on how to spot and report these attacks and how to protect sensitive information. Lastly, a second phishing campaign was conducted to assess any improvements in participants’ ability to spot and report phishing attacks.

3.4 Data Analysis

The data from the two phishing campaigns was analysed to see if there were any changes in participants' ability to detect and report phishing attacks following the cybersecurity awareness training intervention. Descriptive analysis was used to analyse the data. To summarise the data collected from the phishing campaigns, descriptive statistics such as frequency distributions and measures of central tendency were used. It was specifically looked at the number of people who clicked on links or opened attachments in each phishing campaign, as well as the devices they used to access the emails. Furthermore, thematic analysis was used to identify common themes and patterns in participants' responses to simulated phishing emails from the qualitative data collected from the phishing campaigns. The qualitative data revealed more about the participants' susceptibility to phishing attacks and their understanding of email-borne risks.

3.5 Ethical Considerations

Ethical considerations were a key component of the research project and were addressed throughout the study. Before participating in the study, the business owner was required to provide informed consent. All information gathered was kept private and anonymous. To protect their identities, participants were assigned unique identifiers, and the data collected was securely stored and only accessible to authorised members of the research team. Participants were told they could leave the study at any time without penalty. The use of simulated phishing emails was regarded as deception. However, after the study, participants were fully debriefed and given information on how to protect themselves from phishing attacks. Participants were chosen based on their willingness to participate, and there was no coercion or pressure to participate in the study. The information gathered was used solely for the research project and was not shared or used for any other purpose.

3.6 Timeline

The research was carried out over a three-week period. The first phishing campaign and pre-test survey were conducted in the first week, and the cybersecurity awareness training intervention was conducted in the second week. The second phishing campaign was carried out in the third week, respectively, and data analysis and write-up were carried out immediately after.

3.7 Limitations

The study's sample size was 42 employees from an Irish SME. While every effort was made to ensure that the sample was diverse and representative, the small sample size may limit the findings' generalizability to the larger population. The study relied on self-reported data, such as the number of people who clicked on links or opened attachments in phishing campaigns. Because self-report measures are susceptible to social desirability bias, participants may have provided socially desirable responses. The research project lasted three weeks, which may have been insufficient time to assess the long-term effectiveness of the cybersecurity awareness training intervention. To assess changes in participants' ability to detect and report phishing attacks, the study relied solely on phishing campaigns. While phishing campaigns are a valid and reliable method, other data collection methods, such as interviews or observations, were not used in the study to provide a more comprehensive understanding of participants' perceptions of cybersecurity.

4 Design Specification

In this section, design specifications are presented for the research project, which will look at the impact of cybersecurity awareness training on email-borne risks among Irish SME. This section identified and presented the techniques and requirements for the research project's implementation. Phishing campaign techniques and software requirements were specifically designed for the research project, the cybersecurity considerations involved in project implementation, and the training materials and resources used in the cybersecurity awareness training workshop. These techniques were chosen because they were relevant to the research question and could provide a comprehensive understanding of the impact of cybersecurity awareness training on email-borne risks among Irish SME.

Both the researchers and the participants needed computers and internet access for the research project. The phishing campaigns and cybersecurity awareness training intervention required participants to use their own devices. The researchers designed and delivered the training on their own laptops, as well as managed the data collected from the phishing campaigns. The research project required the use of several software applications. The simulated phishing tool, Proofpoint Essentials, was used to design and implement the phishing campaigns. The Proofpoint Essentials tool provided a reliable and valid method for measuring participants' susceptibility to phishing attacks, and the cybersecurity awareness training intervention provided participants with practical training on how to respond to email-borne risks. Microsoft PowerPoint was used to create the cybersecurity awareness training presentation, and Microsoft Teams was used for communication and collaboration with the research team and participants.

4.1 Phishing Campaigns

As part of the research project, two phishing campaigns were carried out. Proofpoint Essentials, a simulated phishing tool, was used to implement the campaigns. The first campaign used two types of phishing emails, one posing as a voicemail on Microsoft Teams and the other as a CV sent to the recruitment department. The second campaign used different types of phishing emails, but both groups received a phishing email about changing their email password. Each campaign had a total of 42 participants.

4.2 Cybersecurity Awareness Training

Participants received cybersecurity awareness training that was developed and delivered. The training was created in PowerPoint and delivered in-person to 25 participants. The training covered topics like detecting and responding to phishing attacks, identifying, and reporting suspicious emails, how to report BEC (business email compromise) attacks and general guidance on email security. The details and the content of the cybersecurity workshop is in the configuration manual.

4.3 Cybersecurity considerations

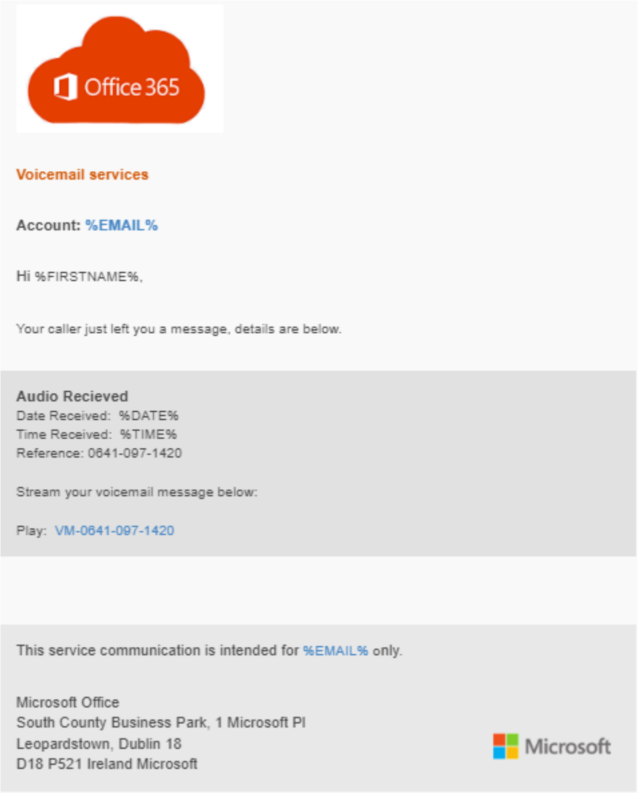
The information gathered from the phishing campaigns and the cybersecurity awareness training intervention was deemed sensitive and thus needed to be safeguarded. The data was encrypted, and only the research team had access to it. The data was securely stored in the cloud. The potential risks associated with the phishing campaigns and the cybersecurity awareness training intervention were explained to participants. They were given information on how to protect themselves and their data from phishing attacks, and they were told that they could leave the study at any time without penalty. For its security features, the Proofpoint Essentials tool used in the phishing campaigns was carefully selected and evaluated. The research team ensured that the tool was used in accordance with the vendor's instructions and that only authorised personnel had access to it.

5 Implementation

This research project was carried out in three stages: designing and deploying two phishing campaigns, as well as conducting a cybersecurity training workshop to increase user awareness of phishing emails.

5.1 First Phishing Campaign

The first phase of the project entailed creating and deploying a phishing campaign to all organisation users. Proofpoint Essentials was used to generate a convincing phishing email that appeared to be a legitimate request to check Microsoft Teams voicemail. 2nd group of participants received a CV for the open role advertised on the company website. The email contained a convincing-looking link that redirected users to a landing page where the number of users who clicked on the phishing email could be tracked. Furthermore, because access to the email server was available, data could be collected on how many users opened the email but did not take any further action. The campaign's results were closely monitored for analysis.



Voicemail services

Account: %EMAIL%

Hi %FIRSTNAME%,

Your caller just left you a message, details are below.

Audio Recieved
Date Received: %DATE%
Time Received: %TIME%
Reference: 0641-097-1420

Stream your voicemail message below:

Play: VM-0641-097-1420

This service communication is intended for %EMAIL% only.

Microsoft Office
South County Business Park, 1 Microsoft Pl
Leopardstown, Dublin 18
D18 P521 Ireland Microsoft

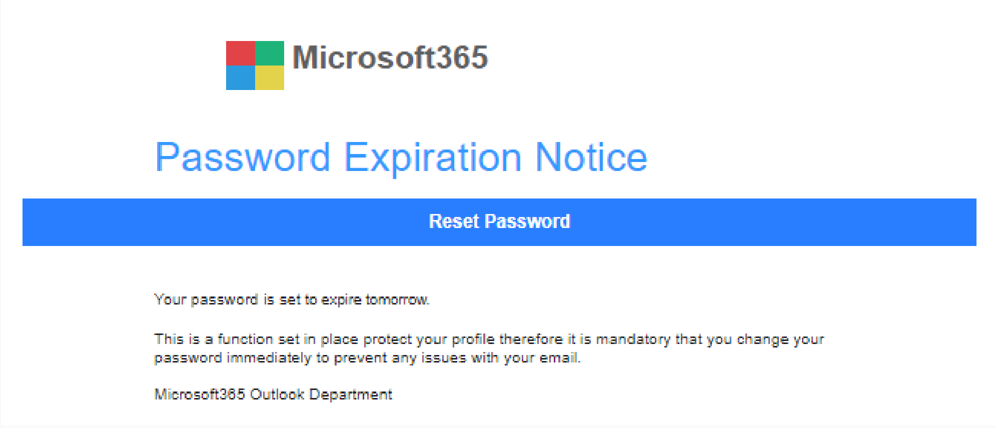
Figure 2 – 1st Phishing Email

5.2 Cybersecurity Awareness Workshop

The project's second phase included holding a training workshop to raise user awareness of phishing attacks. First, attendees were given an overview of the history of phishing emails, the motivations behind them, and the various types of attacks. A training programme covering topics such as identifying phishing emails, recognising social engineering tactics, and understanding the consequences of falling for a phishing attack was designed and built. The training was delivered in-person through a workshop with a select group of users from across the organisation. The workshop consisted of a mix of lecture-style presentations, hands-on activities, and group discussions. The training was designed to be engaging and interactive, with plenty of opportunities for participants to ask questions and receive feedback.

5.3 Second Phishing Campaign

Following the workshop, a second phishing campaign was carried out in the same manner as the first two campaigns. This campaign required users to change their Microsoft365 password within 24 hours or risk losing access to their account.



Microsoft365

Password Expiration Notice

Your password is set to expire tomorrow.

This is a function set in place protect your profile therefore it is mandatory that you change your password immediately to prevent any issues with your email.

Microsoft365 Outlook Department

Figure 3 – 2nd Phishing Email

6 Evaluation

This research project analyses the results obtained during the implementation phase. The project's goal is to evaluate the effectiveness of the proposed solution in raising user awareness of phishing attacks and lowering the risks associated with them. The results of the phishing campaigns and the cybersecurity training workshop are presented and discussed in this section. The findings were examined in light of the project's research questions and objectives. Only results statistics are provided, and no personal information such as names, email addresses, or company details are disclosed, ensuring the data's confidentiality.

6.1 1st Phishing Campaign Experiment

The first phase of the experiment involved creating and deploying a phishing campaign to all organisation users. The email was opened by 34 of the 42 participants, for an email open rate of approximately 81%. The phishing link was clicked on by 27 of the 34 participants who opened the email, for a 65% click-through rate. The email was not opened by eight participants, for a non-open rate of approximately 19%. The email was reported to the IT department by two participants.

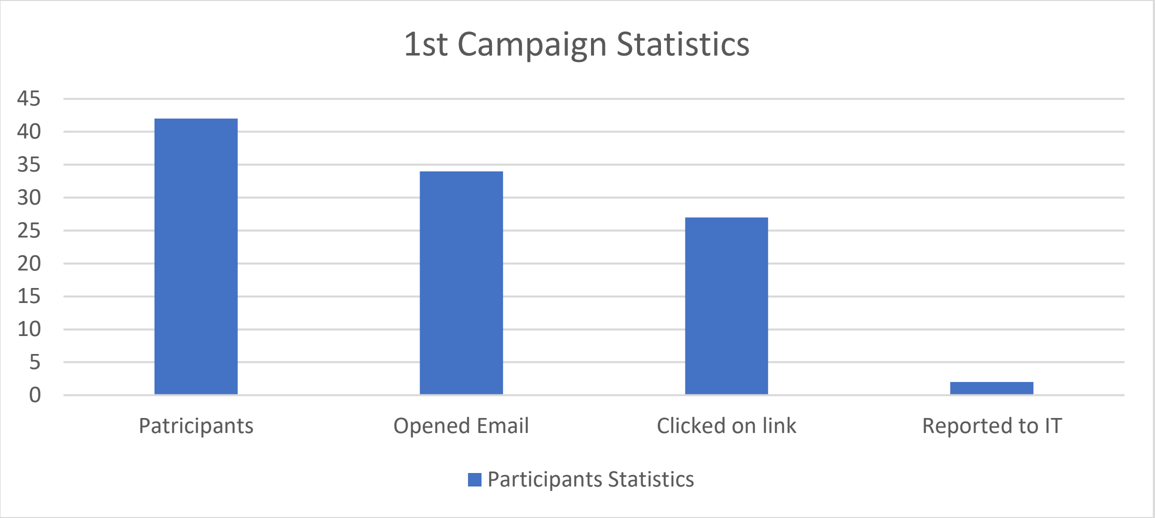


Figure 4 – 1st Phishing Campaign Statistics

The first phishing campaign's results reveal a significant vulnerability in the organization's email security. Because of the high email open and click-through rates, many users in the organisation may be unaware of the risks associated with phishing attacks. The fact that only two people reported the email to the IT department suggests that users aren't always aware of what to do when they receive a suspicious email. The non-open rate of about 19% suggests that some users in the organisation may be wary of opening emails from unknown senders. However, the successful phishing rate of approximately 74% highlights the organization's need for improved cybersecurity awareness training and email security measures.

6.2 Cybersecurity Awareness Workshop

The experiment's second phase involved holding a cybersecurity awareness workshop with 25 users from across the organisation. The workshop covered topics such as email's history and significance, its impact on business, why hackers use email and human error as attack vectors, and why hackers hack. Participants also learned about the evolution of phishing scams and watched a video of a phishing scam to better understand how these attacks work. During the workshop, participants examined several phishing emails and learned how to identify key details such as sender information, context, and content. They also examined five different emails to determine whether or not they were genuine. In addition, the participants evaluated five phishing-related statements to determine whether they were true or false.

The workshop concluded with six recommendations for how participants can protect themselves from phishing threats, including:

- using strong passwords
- never disabling multi-factor authentication
- avoiding unsecure and public Wi-Fi networks when accessing emails
- thoroughly examining every email
- never opening or replying to emails in a hurry
- reporting suspicious emails to the appropriate authorities.

6.3 2nd Phishing Campaign Experiment

Following the cybersecurity awareness workshop, the third phase of the experiment involved designing and deploying a second phishing campaign to all users in the organisation. The campaign targeted 42 participants in total. The email was opened by 13 of the 42 participants, resulting in an email open rate of approximately 31%. Only 5 participants clicked on the phishing link, resulting in a 12% click-through rate.

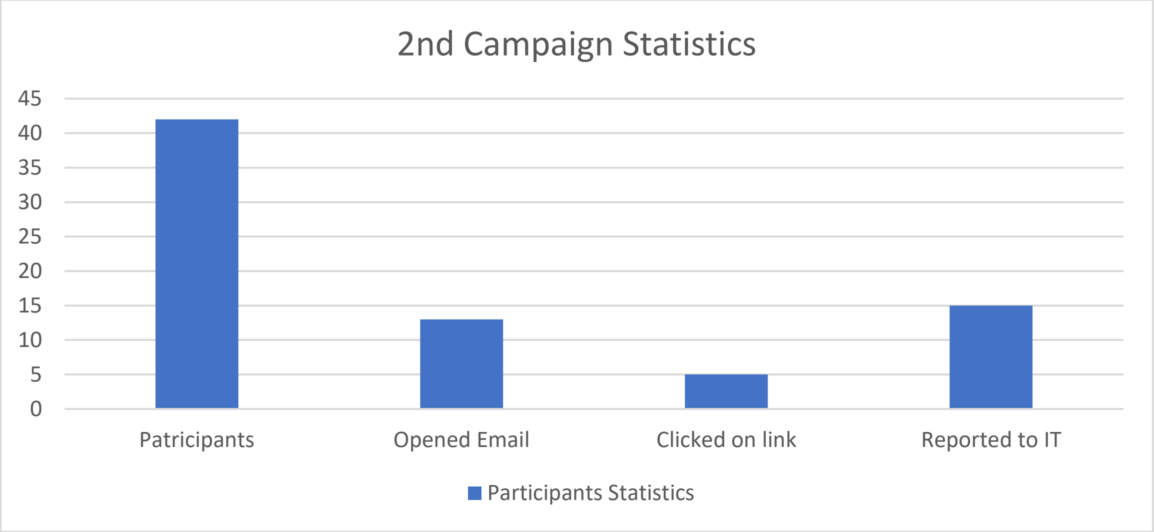


Figure 5 – 2nd Phishing Campaign Statistics

However, 15 participants reported the email to the IT department, indicating that the cybersecurity awareness workshop was successful in educating users about the dangers of phishing attacks and encouraging them to take appropriate action. The results of the second phishing campaign indicate that the cybersecurity awareness workshop was successful in reducing the organization's vulnerability to phishing attacks. It is worth noting that none of the workshop attendees clicked on the phishing link, demonstrating the effectiveness of the training programme in reducing user susceptibility to phishing attacks.

6.4 Discussion

The results of the two phishing campaigns provide valuable insights into the organization's vulnerability to phishing attacks and the effectiveness of the cybersecurity awareness workshop in reducing this vulnerability. The first phishing campaign yielded an 81% email open rate, indicating that many users in the organisation may be unaware of the risks associated with phishing attacks. The 65% click-through rate emphasises this vulnerability even more. The results of the second phishing campaign indicate that the cybersecurity awareness workshop was successful in reducing the organization's vulnerability to phishing attacks. The lower email open and click-through rates of approximately 31% and 12%, respectively, suggest that users are more aware of the risks associated with suspicious emails and are more likely to report them to the appropriate authorities. The fact that none of the workshop attendees clicked on the phishing link demonstrates the training program's effectiveness in reducing users' susceptibility to phishing attacks.

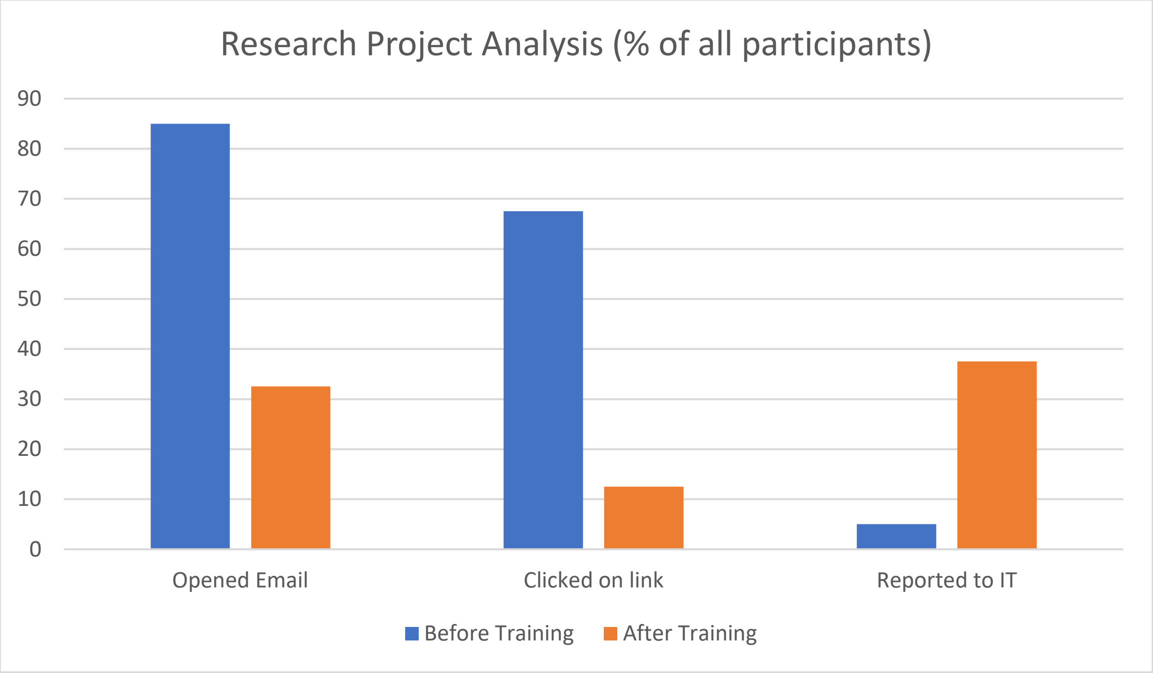


Figure 6 – Research Project Analysis

However, the non-open rate of approximately 69% in the second phishing campaign indicates that some users may still be vulnerable to phishing attacks, and additional efforts to improve cybersecurity awareness and email security measures in the organisation are required. This emphasises the importance of ongoing training programmes and phishing campaigns to reinforce the importance of email security and the dangers of phishing attacks.

The small sample size of participants is one limitation of the experiment design. The results may not be generalizable to the entire organisation or other organisations with different demographics or email security measures because there were only 42 participants. Future research could replicate this experiment with a larger sample size to ensure that the findings are generalizable. Another limitation is that the effectiveness of the cybersecurity awareness workshop was evaluated using only two phishing campaigns. While the results of the second campaign indicate that the workshop was effective, more research is needed to assess the training program's long-term effectiveness and the impact of ongoing phishing campaigns on user awareness and email security.

7 Conclusion and Future Work

The findings of the experiments and the cybersecurity awareness workshop provide important insights into the organization's vulnerability to phishing attacks and the effectiveness of training programmes in reducing this vulnerability. The first phishing campaign's high email open and click-through rates highlight the need for ongoing training and awareness programmes to educate users about the risks associated with suspicious emails. According to the results of the second phishing campaign, the cybersecurity awareness workshop was effective in reducing users' susceptibility to phishing attacks. The non-open rate in the second campaign, on the other hand, indicates that ongoing efforts are required to reinforce the importance of email security and the risks associated with phishing attacks.

To improve email security measures in the organisation, future work could include replicating the experiments with a larger sample size to ensure the findings are generalizable. Future research could also assess the long-term effectiveness of the cybersecurity awareness workshop as well as the impact of ongoing phishing campaigns on user awareness and email security. Furthermore, future training programmes could target specific vulnerabilities identified in the experiments, such as increasing user awareness of social engineering tactics and the appropriate actions to take when confronted with a suspicious email. This research project involved 42 participants and in future work, the number of participants could involve a significantly larger pool, so the research could be applied to general public.

Finally, the results of the experiments and the cybersecurity awareness workshop provide valuable insights into the organization's vulnerability to phishing attacks and the effectiveness of training programmes in mitigating this vulnerability. The findings indicate that the organization's cybersecurity awareness and email security measures require ongoing improvement. Future training programmes and phishing campaigns addressing specific vulnerabilities identified in the experiments could improve email security measures and lower the risks associated with phishing attacks in the organisation.

References

[1] S. Eftimie, R. Moinescu and C. Răcuciu, "Spear-Phishing Susceptibility Stemming From Personality Traits," in IEEE Access, vol. 10, pp. 73548-73561, 2022, doi: 10.1109/ACCESS.2022.3190009.

[2] A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg and E. Almomani, "A Survey of Phishing Email Filtering Techniques," in IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2070-2090, Fourth Quarter 2013, doi: 10.1109/SURV.2013.030713.00020.

[3] M. Khonji, Y. Iraqi and A. Jones, "Phishing Detection: A Literature Survey," in IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2091-2121, Fourth Quarter 2013, doi: 10.1109/SURV.2013.032213.00009.

[4] Ahmed Aleroud, Lina Zhou, Phishing environments, techniques, and countermeasures: A survey, Computers & Security, Volume 68, 2017, Pages 160-196, ISSN 0167-4048

[5] Rachna Dhamija, J. D. Tygar, and Marti Hearst. 2006. Why phishing works. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06). Association for Computing Machinery, New York, NY, USA, 581–590. https://doi.org/10.1145/1124772.1124861

[6] Pandove, K., Jindal, A. and Kumar, R., 2010. Email spoofing. International Journal of Computer Applications, 5(1), pp.27-30.

[7] Hu, H. and Wang, G., 2018, August. End-to-End Measurements of Email Spoofing Attacks. In USENIX Security Symposium (pp. 1095-1112).

[8] A. Bremler-Barr and H. Levy, "Spoofing prevention method," Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies., Miami, FL, USA, 2005, pp. 536-547 vol. 1, doi: 10.1109/INFCOM.2005.1497921.

[9] Schuckers, S.A., 2002. Spoofing and anti-spoofing measures. Information Security technical report, 7(4), pp.56-62.

[10] Cross, C. and Gillett, R., 2020. Exploiting trust for financial gain: An overview of business email compromise (BEC) fraud. Journal of Financial Crime, 27(3), pp.871-884.

[11] Cidon, A., Gavish, L., Bleier, I., Korshun, N., Schweighauser, M. and Tsitkin, A., 2019, August. High Precision Detection of Business Email Compromise. In USENIX Security Symposium (pp. 1291-1307).

[12] Bakarich, K.M. and Baranek, D., 2020. Something phish-y is going on here: A teaching case on business email compromise. Current Issues in Auditing, 14(1), pp.A1-A9.

[13] Mansfield-Devine, S., 2016. The imitation game: how business email compromise scams are robbing organisations. Computer Fraud & Security, 2016(11), pp.5-10.

[14] Zhang, Z., He, W., Li, W. and Abdous, M.H., 2021. Cybersecurity awareness training programs: a cost–benefit analysis framework. Industrial Management & Data Systems, 121(3), pp.613-636.

[15] Miranda, M.J., 2018. Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. International Management Review, 14(2), pp.5-10.

[16] 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.

[17] Dash, B. and Ansari, M.F., 2022. An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy. Int. Res. J. Eng. Technol.(IRJET), 9.

[18] Abd Rahim, N.H., Hamid, S., Kiah, M.L.M., Shamshirband, S. and Furnell, S., 2015. A systematic review of approaches to assessing cybersecurity awareness. Kybernetes, 44(4), pp.606-622.

[19] Proctor, W.R., 2016. Investigating the efficacy of cybersecurity awareness training programs (Doctoral dissertation, Utica College).

[20] Jin, G., Tu, M., Kim, T.H., Heffron, J. and White, J., 2018, February. Game based cybersecurity training for high school students. In Proceedings of the 49th ACM Technical Symposium on Computer Science Education (pp. 68-73).

[21] Huynh, D., Luong, P., Iida, H. and Beuran, R., 2017. Design and evaluation of a cybersecurity awareness training game. In Entertainment Computing–ICEC 2017: 16th IFIP TC 14 International Conference, Tsukuba City, Japan, September 18-21, 2017, Proceedings 16 (pp. 183-188). Springer International Publishing.

[22] Ansari, M.F., Sharma, P.K. and Dash, B., 2022. Prevention of phishing attacks using AI-based Cybersecurity Awareness Training. Prevention.

[23] Ansari, M.F., 2022. A quantitative study of risk scores and the effectiveness of AI-based Cybersecurity Awareness Training Programs. International Journal of Smart Sensor and Adhoc Network, 3(3), p.1.

[24] Gasiba, T., Lechner, U., Pinto-Albuquerque, M. and Porwal, A., 2020. Cybersecurity awareness platform with virtual coach and automated challenge assessment. In Computer Security: ESORICS 2020 International Workshops, CyberICPS, SECPRE, and ADIoT, Guildford, UK, September 14–18, 2020, Revised Selected Papers 6 (pp. 67-83). Springer International Publishing.

[25] Espinha Gasiba, T., Lechner, U. and Pinto-Albuquerque, M., 2020. Sifu-a cybersecurity awareness platform with challenge assessment and intelligent coach. Cybersecurity, 3, pp.1-23.

[26] Hijji, M. and Alam, G., 2022. Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. Sensors, 22(22), p.8663.