National College of Ireland

Using Phishing Simulation Testing to Analyse and Improve Efficacy of Security Awareness Training

MSc Research Project
MSc in Cybersecurity

Caroline Smyth
Student ID: 23183951

School of Computing
National College of Ireland

Supervisor: Dr. Raza Ul Mustafa

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Caroline Smyth……

Student ID: 23183951

Programme: MSc Cybersecurity **Year:** 23-24

Module: Internship/Practicum……

Supervisor: Dr. Raza Ul Mustafa……

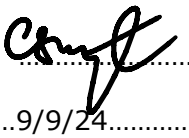
Submission Due Date: 9/9/24……

Project Title: Using Phishing Simulation Testing to Analyse and Improve Efficacy of Security Awareness Training

Word Count: …7751…… **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: 

Date: ……9/9/24……

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):	

Using Phishing Simulation Testing to Analyse and Improve Efficacy of Security Awareness Training

Caroline Smyth
23183951

Abstract

Phishing is a significant issue in cybersecurity, with an estimated 3.4 billion spam emails sent daily, and the prevalence of new phishing methods increasing year on year, with callback phishing, QR code use and smishing all of significance. Phishing is multifactorial and requires a multifactorial defence, employing both technical and social means, comprising both training and phishing simulation tests. Phishing simulation tests are a way to assess the effectiveness of training. Current research shows that security awareness is related to recency of training and familiarity with recognising phishing emails. The effect of training duration and recency of training was compared using training data and new and recent phishing simulation tests but was found to have no correlation with results. A QR code included was not scanned by any recipients. In two of the tests, failure of the test was found to have a dependence on recipient training language setting.

Keywords – Awareness, cybersecurity, phishing, simulation, training.

1 Introduction

Phishing is the practice of sending fraudulent emails in order to trick recipients into thinking they are sharing private data with a trustworthy contact, usually a company or government organisation. Revealing one's own email password can allow one's email to be used in business email compromise scams (BEC), masquerading as you with your colleagues and business contacts, in order to further compromise your network. Phishing ranges from simple generic emails with typographical errors and random sender addresses, sent to large groups of email addresses, to the more advanced, targeted towards single users (spear phishing), with spoofed addresses, or whaling, when a high-level figure is targeted, such as a senior executive. The threat actor's aim is to induce the recipient to download attachments, which either contain malware, or cause malware to be downloaded; or click a link to enter credentials or download malware.

Phishing represents the most prevalent threat in cybersecurity today, with an estimated 3.4 billion spam emails sent daily worldwide, and more than 83% of UK business affected in 2022 reporting phishing as the cause (Charles Griffith, 2024). In the last year, the incidence of "Quick-Response" (QR) codes sent by email has increased, being used in 22% of tests on a 600,000 user wide simulation test by Hoxhunt in October 2023, with only 36% of users able to identify the phish (Eliott Tallqvist, 2023; *Ultimate QR Code Phishing (Quishing) Prevention Guide: Here's What the Research Says - Hoxhunt*, 2024). Bleeping

Computer reported a phishing campaign actively targeting a “major US organisation” with QR codes via email (Bill Toulas, 2023). Callback phishing or vishing increased 625% from the first quarter of 2021 to the second quarter of 2022, according to KeepNet Labs (Keepnet Labs, 2024).

Phishing is situated in the Initial Access phase of the Mitre Attack framework and in the Delivery phase of the Cyber Kill Chain, and so efforts against phishing can stop attempts in these phases (Hutchins, Cloppert and Amin, 2010). As a result, organisations have a requirement to ensure that their security implements a Defence in Depth (DID) strategy. It is therefore imperative that employees are an integral component of this strategy, and have awareness of the various phishing methods, and can identify and alert of more sophisticated phishing attempts, to maintain security.

The subjects of my research provide consulting services in the healthcare and pharmaceutical area, and consists of two separate, but related, company structures of around 10,000 employees, and fewer than 900 respectively (named Com1 and Com2 in this report). Employees at all levels are presented with daily phishing emails, ranging from generic to more sophisticated attacks. Some use spear phishing and whaling techniques, involving impersonations of the CEO and other senior executives gleaned from newspapers and social media. Some attempts have included impersonations of third-party vendors. Third party vendors who have been the subject of BEC have been used for a more authentic appearing phishing attempt using a trusted email contact. To mitigate the susceptibility of our users, email security is extensive, and malicious links, including newly created websites, are blocked. However, it’s not feasible to block every email, which would interfere with business functions, so it’s essential for employees to approach email contacts with awareness of the potential for fraud.

Implementation of an annual Security Awareness Training program ensures that employees remain aware of their need to be vigilant when accessing email, and also presents the opportunity to highlight newly prevalent attack methods. Online interactive training videos allow employees to access the training on their own schedule, and at their own pace. Certain designated groups, such as those dealing with finances and invoices, also have directed live training to ensure they’re prepared for the finance and invoice specific types of phishing. However, prior to actually being compromised, how can an organisation assess the effectiveness of its security awareness program, and by extension, the effectiveness of its employees at recognising phishing emails? One option is the implementation of organisation wide phishing simulation tests.

The primary research question is: “Can Phishing Simulation Testing be used to Analyse and Improve Efficacy of Security Awareness Training”.

My primary hypothesis is that performance in phishing simulation testing (PSTs) is related to the security training previously done, and time taken to complete this training. Participation in PSTs also improves the user’s awareness of phishing emails, by becoming more familiar with phishes, which increases their speed and ease of recognition. This hypothesis can be tested by identifying whether failure to recognise a phishing email (“clicking”) is associated with fewer security training sessions completed. I further hypothesize that recency of training completed improves the speed and recognition of phishing emails and thus should show an improvement in recognition of phishing emails.

The running of PSTs and highlighting of phishing awareness is shown to improve performance on phishing simulation tests (McElwee, Murphy and Shelton, 2018). I would also like to investigate whether there's a correlation between time taken to complete training, with the hypothesis that time taken to complete training (and pass a test at the end) correlates with the ease of the user with recognising phishing emails, and thus should be a shorter time period for users who pass (or fail to click) the phishing test email. Most phishing emails (though not all) are written in English, with various levels of proficiency, so I will also investigate whether language is correlated with better performance on the PSTs. The simulation will be designed with reference to current phishing trends and intelligence within the organisations examined, and industry in general. It will be implemented by using a commercial tool (KnowBe4), which also performs as a security training platform. Training and phishing data will then be collated, anonymised and sorted for analysis. The data will be examined for statistically significant relationships, with significant results used to guide the focus of future training, training frequency, and future phishing simulation campaigns. It may also highlight areas of deficit in user awareness and training which can be mitigated in the next training campaign.

In the next section I'll highlight research and industry information which relates to this area and show where it guides my choices (where available). I'll then explain my research methodology in chapter 3, and design specification in chapter 4. I'll give an overview of implementation in chapter 5. My results are presented in chapter 6 and discussed in chapter 7.

2 Related Work

Phishing is a multifactorial issue, with technical and psychosocial factors being present, and so needs to be defended in a similar manner.

2.1 Research Trends

An examination of the trends in phishing in 2021 was useful to use as a basis for how a phishing email entices a user to click on it (Alkhalil *et al.*, 2021). They also include reference to the non-technical and confounding issues that can sometimes make users more susceptible to phishing, either at a particular time, i.e. when confused, busy or stressed, or based on personal characteristics such as obedience to authority or curiosity. Younger people are more susceptible to phishing, while older people tend to be less impulsive. This was useful as input to the design of the email to be sent and the various methods of deception which are used by groups.

A framework involving behavioural psychology was proposed which involves the gamification of security awareness, some components of which are available to use in KnowBe4 (Maqousi, 2023). Maqousi cites personalised training plans for security awareness and inclusion of incentives and leaderboards and competitive and fun aspects of learning to improve one's skills. This is an interesting aspect of awareness and use of leaderboards to show that one's team has completed more training than another can promote a healthy

competition but is unlikely to be seen as anything more than more work to be done in the guise of play. It doesn't impact our proposed study, but some aspects of the framework suggested could be integrated easily into our training program.

Ciupe and Orza (2024) used their phishing simulation as a method of identifying deficits in user knowledge by way of a large-scale phishing simulation test of 20,000 users in a university in Romania. They were able to then identify areas of deficits and focus on making users aware of them. This method is similar to that of (McElwee, Murphy and Shelton, 2018), and is one that could be adopted by our organisation regardless of results of this study.

Reinforcement and punishment were a feature of Yeoh et al.'s study by using operant conditioning to improve phishing awareness (Yeoh *et al.*, 2021). This is a dangerous path to follow as it can cause people to hide mistakes in real phishing incidents. An open policy of reporting phishing and reporting when one is taken in by a phish is the optimal policy.

2.2 Phishing Simulation Tests

McElwee, Murphy and Shelton (2018) assert that phishing employs both social and technical methods to attack organisations, and so both methods should be assessed for possible improvements in defensive methods. They performed testing over four years and found that both outcome-based controls and behaviour based controls are ideal for use with phishing simulation, with both serving to teach and engage users with measurable outcomes and incentives to achieve these. They found that incentives did not improve phishing susceptibility (relating bonuses to phishing targets). Their testing involved monthly generic simulation tests of 1,000 users, which could be considered to be a burden on the users if applied to Com1 and Com2. It would also likely require a full-time employee to run and analyse the output. However, they found that management encouragement regarding being phishing aware had a positive effect on their phishing detection. As they included a tool which collated phishing reports, it enabled them to have a tighter control on their results by including both active positive and negative findings.

PSTs also have an ethical concern as their implementation involves targeted deception of the end-user and can have a resultant negative effect either due to failure to recognise and report the phish, or feeling manipulated by the senders. Schwab *et al.* found that ensuring prior consent by the recipients improves user acceptance of the practice of phishing simulation tests (Schwab *et al.*, 2024). The organisation being investigated has a policy of open-ness regarding reporting phishing, whether or not users have been taken in by them, so consent to occasional phishing simulations is part of their security policy. Regardless, we must also weigh any negative impact of the tests against potential negative impact of falling for a real phishing email.

2.3 Cognitive Processing

Pietrantonio *et al.* used gaze analysis to analyse how different users processed or analysed suspicious emails, and their results are of interest to us in relation to how users with more experience with phishing emails tend to move confidently to the places they know will be able to tell them if an email is a phish or not (Pietrantonio *et al.*, 2024). They found computer science

experts' gazes would go to the email header and the sender address quickly then move to the body, while novices would look at the email body first, and take a longer time to process what they were seeing. This reinforces other research which shows that increased training correlates to increased awareness, and enforces the need to run phishing simulations, for users to put what they've learned into practice and continue to apply the principles. In our phishing email, the sender address is clearly not a legitimate one, though the email looks convincing otherwise. Thus, the computer expert will dismiss it immediately, while the novice will need to learn to examine the sender address initially.

2.4 Industry Intelligence

Industry intelligence is an important source of information regarding current trends in attack vectors and the methods of threat actors so must be referenced in any discussion of current trends and new directions for research.

In the last year, several outlets have identified increases in prevalences of newer forms of phishing, including QR code phishing, which doesn't appear to have been investigated in formal phishing research as yet (Bill Toulas, 2023; Eliott Tallqvist, 2023). Hoxhunt found that 22% of phishing emails in October 2023 used QR codes as their attack method (Eliott Tallqvist, 2023). In an almost 600,000 user strong phishing simulation they found only 36% of users were able to identify the QR email as a phish, with 5.5% actually scanning the code. Locally in our organisation, although Mimecast can defend against suspicious QR codes, some malicious ones have made it through and were later blocked by other software, so user awareness of the danger of physical and emailed QR codes is essential.

Callback phishing or vishing has shown an increase in prevalence over the past few years, with an increase of 625% from 2021 to 2022 (Keepnet Labs, 2024). The cost to UK businesses in 2020 just from callback phishing was £37.8 million.

My study intends to add to the data already available by including a QR code in one of the email templates. It also intends to assess whether increasing frequency of training (with a shorter duration might keep phishing in user's minds to improve their response to the phishing simulation.

3 Research Methodology

The research was performed by first investigating the previous phishing simulations that had been run in the organisation previously, and through investigating the related work and industry threat intelligence related to phishing in 2024.

Mimecast[1], the Email Security specialists, were consulted as their threat intelligence specifically impacts their Email Security business. Mimecast is used in Com1 to protect email security. In 2023 and 2024, QR code phishing increased in prevalence, with some coming into Com1's email system. Mimecast will filter emails with QR codes to quarantine, or hold them for administrator examination, if the URL is suspected to be malicious.

Smishing (sending a phishing SMS message) also increased in prevalence, along with increased incidence of spoofed emails supposedly from a senior colleague's private email address simply asking for the employee to send their mobile number for a WhatsApp message.

[1] https://www.mimecast.com

Callback or voicemail phishing wasn't seen within the organisation yet. This is where a user receives a voicemail enticing them to call back, e.g. that their order is being shipped and they'll be charged now, or that they owe money to the Internal Revenue Service of the US or UK. When the user calls, they can be enticed to give confidential information over the phone. Both callback or voicemail phishing (vishing) and smishing were considered as part of the phishing simulation. However, not all employees had a mobile phone or organisation phone number which could be targeted. KnowBe4 also recently discontinued their callback vishing simulation tests due to telecommunications regulations becoming more stringent.

The previous phishing email templates used were examined. They included a free two night's stay with the Marriott Hotel Chain, which was used in Q2 2024 for Com1 only. A screen shot is included in the configuration manual. This email was considered to have a difficulty level of 4 stars (out of 5) and resulted in a 10% failure rate, with almost 900 users clicking on the link in the email. Features of the email included an enticement of a free pillow set for completing a survey (though the subject line offered a voucher for a free stay). The domain the email came from was marriott-notifications.com.

In 2023, a "Message couldn't be delivered" email template purporting to be from Microsoft 365 had a difficulty level of 5/5 stars. It originated from messaging-micorsoft.com, a misspelled email domain. Both templates were provided by KnowBe4.

From an ethical standpoint, as part of this research, and as part of the implementation of the phishing simulation tests, ethical guidelines were written to ensure that the tests were designed fairly, and conformed with the expected level of phishing emails seen on a day-to-day basis (as mentioned previously, certain teams received extra training separately, which was not included in the general campaign specification). This included avoiding email types which could be construed as business related, either from HR, IT or other internal business (e.g. Microsoft/Teams/DocuSign). Similarly, known business partners and vendors should be avoided, where possible.

At the time planned for running the phishing simulation, Amazon's worldwide Prime day had just occurred, so an Amazon template was modified to offer late deals still available after Prime Day.

Phishing simulation tests can be implemented with open-source or commercial tools. Gophish.com[2] is an open-source offering, but their email templates are much less extensive and less polished than KnowBe4. KnowBe4 was the obvious choice to continue with in this study as it was previously used for both phishing and training for employees, and had data going back to 2022 to look for trends in. However, it was decided to limit the study to 2023, when campaigns, both training and phishing, were directed companywide, rather than to smaller groups of users. KnowBe4 includes notifications of mandatory training, allows users to do optional training if interested, and can include specific training related to one topic for a subset of users (e.g. to allow them exceptions to some security policies). However, KnowBe4 reports tend to be limited, and don't allow for multifactorial investigations. My study will improve access to the data learned while receiving the regular reports from KnowBe4. Reports from other companies produced in a similar format can also be analysed with some

[2] https://www.getgophish.com

modifications to the code based on the format of the data available, which allows for switching to other providers of phishing simulation tests in future.

I generated 35,000 separate entries of training information, with a similar amount of phishing information since 2023 for processing as part of my research, which included over 10,000 active users.

4 Design Specification

Based on the research done and papers read, it was decided that of the options available to us to implement, a QR code was the most relevant and could be implemented and assessed with the system we already used.

The phishing simulation was guided by new ethical guidelines this year to ensure that negative impacts of the deception were minimised. We avoided using any design that might be related to our business, including third party vendors, partners and internal departments, to ensure that users weren't overly impacted with suspicions in their regular day to day work.

The template to use was discussed with reference to the time of year this simulation was being run (end of July), the consideration of an international employee group, and worsened performance on the last simulation. Therefore, a mid-difficulty template offering late Amazon Prime day deals (Amazon Prime day, an annual event of reductions and discounts across Amazon, occurred the week before). This was based on a pre-existing Amazon Prime email and was updated to reflect the recent Prime day. The template included Amazon images, but a sender email address of deals@account-activity.com, and did not mention the recipient name, as it would normally do if coming from Amazon. For Com2, a QR code was added, in addition to the link already in the email, as a trial for future use.

The campaign was designed to send emails out during regular GMT time zone business hours over 3 days, then collect opening and clicking data for the next 4 weeks.

Following the campaign closure (and even before closure) a CSV file containing current results could be output for analysis.

A test campaign was also implemented in advance, to ensure that the emails weren't blocked as phishes. It was noted that as expected, the emails appeared marked with an "External" mark from our email system. Images didn't download automatically unless the sender was trusted (expected behaviour for external emails). The QR code for Com2 was found to appear similarly to an attached file and was visible at the top instead of the bottom of the email.

Prior to the campaign start the IT helpdesk were informed to send all phish related calls directly to the Information Security team, and to avoid blocking any suspicious behaviour.

5 Implementation

The design of the phishing simulation test described in the last chapter was implemented with KnowBe4 and data continued to be collected for a month after the last emails were sent. Following that, four CSV files were exported from KnowBe4, active user data from both companies investigated to ensure the outcome assessed current employees only, and all phishing and training activity recorded since the start of 2023.

A python script was created to initially preprocess and anonymise the data. This included dealing with changed email addresses between campaigns, and normalising different campaign names and information. Files output from this script were read into a second script for further processing and combination into one data frame with 11,060 unique user rows and 39 columns. Processing included changing dates and times to be able to compare and add them and discard irrelevant or unneeded data. Further difficulties included many of them having had an email change in the past 6 months, and thus a change of their data in KnowBe4, necessitating extra processing to ensure that historical information was available for comparison.

The data was then examined for correlations, dependents and relationships. Visualisations including bar charts, pie charts and histograms were produced and output.

User Reports were collated manually from the Information Security email inbox and reports sent through Outlook and Mimecast were output as csv files from Microsoft Defender and Mimecast systems. Related output from the IT helpdesk calls was also produced.

6 Evaluation

Data on 11,060 current users was collected and analysed to produce the following results. The results of 2 annual security awareness training programmes were included, and 3 sets of phishing simulation tests.

6.1 Phishing Test Performance

Figure 1 and Table I show the results of the last 3 phishing tests, performed in November 2023, April 2024 (Q2) and end of July 2024 (Q3) respectively. The 2024 Q3 phishing test performed resulted in a 0.9% phishing failure rate for Com1, and 0.45% for Com2, 0.86% combined. Com2 did not participate in the Q2 phishing test which showed a significant difference in performance, with a failure rate of 10% for Com1. Please note the different scale on the rightmost Com2-only bar chart, as Com2 has 10% of the number of employees of Com1. The failure rate is also calculated as clicked vs. opened, which indicates that the email was opened, either in preview or in full.

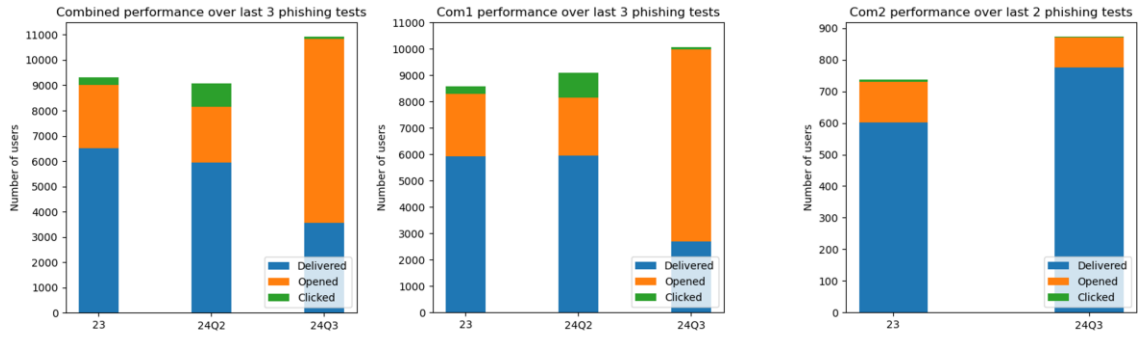


Figure 1: Performance on latest phishing tests

Table I shows this information in numeric format, with clicked, opened and delivered (received) shown, and performance on all. Failure rates on the tests have had varying results, which will be discussed further in the next section.

Table I: Phishing Test Data, including fail percentages

	Com1 (Pop. ~10,000)	Com2 (Pop. ~900)	Combined (Pop. ~11,000)
2024 Q3 (end July)			
Users Clicked (Failed)	91	4	95
Users Opened	7,371	99	7,470
Users Received (delivered)	10,060	874	10,934
Clicked vs. Delivered %	0.90%	0.45%	0.86%
Clicked vs. Opened %	1.23%	4.04%	1.27%
2024 Q2 (April)			
Users Clicked (Failed)	922	n/a	922
Users Opened	3,123	n/a	3,123
Users Received (delivered)	9,080	n/a	9,080
Clicked vs. Delivered %	10.15%	n/a	10.15%
Clicked vs. Opened %	29.52%	n/a	29.52%
2023 Q4 (November)			
Users Clicked (Failed)	285	8	293
Users Opened	2,656	137	2,793
Users Received (delivered)	8,567	738	9,305
Clicked vs. Delivered %	3.32%	1.08%	3.14%
Clicked vs. Opened %	10.73%	5.83%	0.49%

6.2 Training

Table II shows the training data for both organisations, which are visualised in Figure 2 and Figure 3. Both organisations time taken to complete training had significant outliers, both at the high and low end, with excessively high and low values (30 hours to complete around 30 minutes of assigned training, 0 hours spent to complete training). These values were found in the raw data also and weren't a result of data manipulation. I made the decision to disregard times higher than 65 minutes for 2024 training, and 120 minutes for 2023 training, as well as zero values for completed training. Correlations showed the same trend with outliers included but are not shown here. Pair plots were also generated for each of the phishing tests and their training data (not shown here), but no useful data was found as most relationships ended in a binary outcome, and correlating duration and recency of training is not a valid comparison.

Table II: Training Data

	Com1 (Pop. ~10,000)	Com2 (Pop. ~900)
2024 Q3		

2024 Training Complete	7,961	656
Both Training Complete	6,742	538
Days Since Training Complete		
Mean	93	91
Median	83	91
Stdev	52	
Max	188	156
Min	1	
Time Taken		
Mean Time Taken	24	23
Median	23	
Max (limited due to outliers)	65	65
Min	1	2
Stdev	11	
2023		
2023 Training Complete	7,801	640
Days Since Training Complete		
Mean	18	13
Median	21	91
Max	39	156
Min	4	1
Stdev	6	34
Days Since Training Complete		
Mean	33	36
Median	31	33
Max (limited due to outliers)	120	118
Min	1	4
Stdev	21	8.8

The Pearson Correlation Coefficient was calculated for the three phishing test results vs. the time since training was completed to assess if there was a linear relationship between any of the variables tested. The results are present below in Table III. Only 2023 PST and Q2 2024 had results of statistical significance, and both were almost zero, indicating likely no relationship, with a slight negative correlation for the data of users who completed both sets of training.

Table III: Pearson Correlation Results for training duration and recency

	Correlation Coefficient	P value	Correlation
2024 Q3 vs Days Since 2024 training	0.003954435706358139	0.7175217806686757	None
2024 Q2 vs Days Since 2024 training	0.007061274912209728	0.6868396791335853	None
2023 vs Days Since 2023 training	0.19787528121212852	0.003497889520972721	Very weak to none, significant
Q3 Fails vs time Training	0.013665327035304837	0.22965605122831237	None
Q2 Fails vs time Training	0.014264641819914617	0.20986631844528097	None
2023 Fails vs time Training	0.022333228440571846	0.04675975088466056	None, significant

Q3 vs total 23 + 24 training:	0.010588763244627507	0.40491512746142394	None
Q2 total 23 + 24 training	-0.06739603497091451	1.1143016006646748e-07	None, significant
Q2 total 23+24 training	0.014264641819914617	0.20986631844528097	None
Q3 vs training 24 done	0.020249831832407767	0.03509846748926144	none
Q2 vs training 24 or 23 done	0.03962538268869675	6.621744048684271e-05	None, significant
Q2 vs training 24 done	0.04475750048200036	0.000926146480031724	None, significant
23 vs training 23 done	0.0020099070477010666	0.8579905358869231))	None, significant

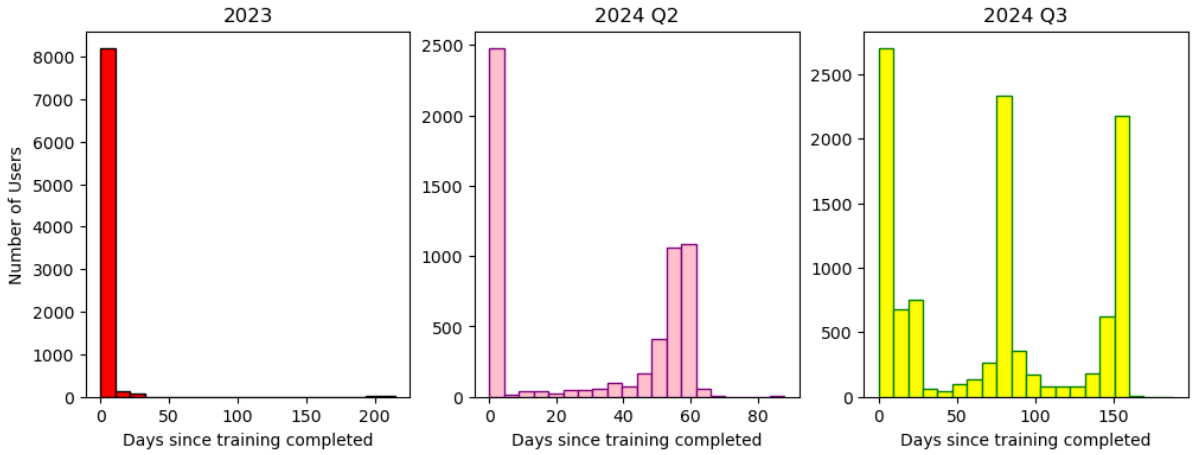


Figure 2: Days Since Training Completed prior to each Phishing Simulation

Recency of training (days since training completed) is displayed in Figure 2. This figure shows the distribution of the number of days since training before each of the three simulation tests. The peaks in the figures occur at the times reminders to complete training were sent to those who hadn't done it. Q2 and Q3 graphs represent the same training completion dates, with recency related to the date of the Q2 phishing test, if completed prior to the test, and if complete prior to the Q3 test. The peak at 60 days in Q2 was around the time of the launch and initial notifications to complete training, showing almost 2,000 users completed it very quickly. This peak becomes the 150-day peak seen in Q3, 5 months after the rollout of training. Peaks at 75 days and lower correspond to training reminders which were sent more consistently at that point.

In 2023, two separate training courses were offered, with the latest training completion date being taken as input to the days since training variable. Two peaks can be seen, prior to the phishing test, when a newer course was released, and reminders of the first course, and also 200 days prior, with the first course.

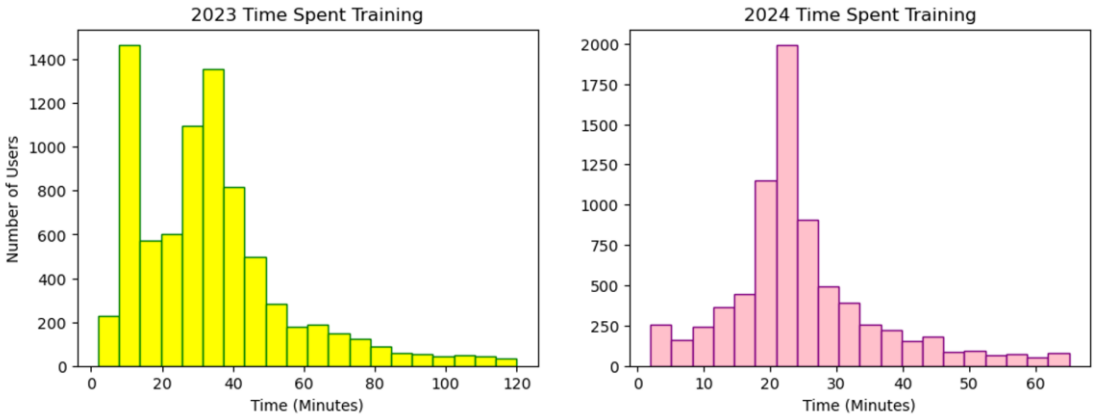


Figure 3: Time Spent on Training in 2023 and 2024

Figure 3 shows the duration of time spent on training. The peaks appear at the expected durations for the training completed. For 2023, this was either around 20 minutes duration, or if both sets of training were completed, around 35 minutes. Significant outliers were excluded, as mentioned previously.

6.3 Language

The Chi squared test was used to see there was a dependence between the user language chosen by the users who failed the phishing test, compared with the language selected by the users who had the phish delivered. Both the 2024 Q2 and 2023 tests showed that the Phish failure rate was a dependent variable based on the language chosen by the user.

Table IV: CHI squared result for languages for Clickers vs non-clickers

	P value	Result
2024 Q3	0.29640251311826765	independent
2024 Q2	7.53160774331795e-06	dependent
2023	0.02575922400965418	dependent

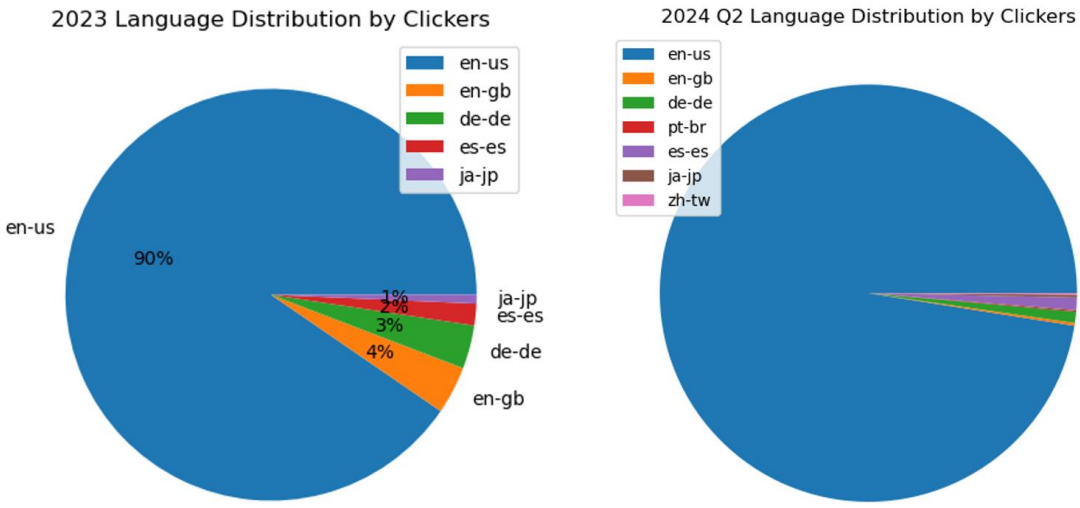


Figure 4: Language Distribution for 2024 Q2 and 2023 phishing tests

6.4 User Reports

User reports were collated through the various methods available. By the end of the phishing test, active user reports numbered 280 through 4 different methods of reporting, which represents 2.5% of users reporting the phish. This indicates active recognition and awareness of the phishing email, as well as awareness of the need to report all phishes, whether clicked or not. As collating these reports is a manual job, it's not possible to compare to previous results at this time.

6.5 Discussion

My hypothesis is unproven based on the data currently analysed. Failure rates on the phishing simulation tests have varied over the last three tests and are not correlated with training duration or recency. Training data didn't appear to have a non-linear relationship that could be correlated with the results seen. Pair plots were performed, but not included, to assess if there was a relationship between the numeric data. No relationships were found.

The different peaks in recency of training show us that although some users are quick to complete assigned training, others may forget about it, and if they don't complete it immediately, require a reminder to do so, with repeats as needed. One known issue is also that training in Com1 is usually assigned in a separate platform, with KnowBe4 still less well known, especially to new employees, though this has been improved, with a link to KnowBe4 installed in the usual learning platform. Increasing Awareness of Security Awareness training should improve KnowBe4 recognition, as well as the need for keeping up to date with training.

The peaks in duration of training also reflected the expected duration time, suggesting it was completed attentively. Outliers included duration times of zero, or as high as almost 30 hours for completed training. By formalising a consistent rollout and notification and follow-up of completion of mandatory training (and even shortening the training duration) I

anticipate that training duration results would have a lower variance and potentially a more linear relationship with the phishing outcomes.

The fail rate varies significantly between the 3 tests for Com1, with rates of 1%, 10% and 3% respectively, while for Com2 it was 0.45% and 1%. However, when the failure rate is presented as a percentage of the open rate, Com2 is between 4 and 6%. The opening rate in Com2 was just 100 opened the email, out of almost 900 who received it. As a QR code was included in this email it appeared at the top of the email similar to an attachment in preview. Receiving an email from an external source which appeared in such a way perhaps gave that group more indication that it was a phish, than compared to Com1, the larger group.

User reporting isn't collated automatically at this time, which reduces its use in analysis, and was shown previously to be of benefit with just 1,000 users being studied, although also ran three times more campaigns and training than this organisation (McElwee, Murphy and Shelton, 2018). With the next phishing test, it would be useful to have a central csv file which is updated from each report location with user information to ascertain if users are reporting in any of the ways suggested. This might give a better understanding of whether the phish was missed, ignored, or actively identified. 2.5% represents 2.5 times the number of users who failed to recognise the phish and is a positive number to use in promotion of training and phish recognition. If it can be associated with the reporting users' training and phishing data, then analysis can be performed. KnowBe4 do have an option to use the "Phish Alert Button" to collate data into their platform. This is a Microsoft add-in button that can be installed for most Outlook and Gmail client on Windows, Mac and mobile devices. It thanks the user for reporting simulated emails and confirms the simulation, and forwards non-simulated emails to the security team for investigation. However, as it's a separate download, it would require a rollout for all devices which users access their email on, so isn't a simple task to implement. In the meantime, encouraging reporting, especially using simple Outlook and Mimecast report buttons which already exist and results of which can be easily generated for input to the analysis to show positive identification of the phishes and perhaps be correlated with training duration and recency.

The Chi squared test suggests no correlation of language with phishing test performance in 2024 Q3 but was a dependent variable in 2023 and Q2 2024, which seems paradoxical. There are a few potential reasons for this difference, however. The language setting was sourced from the training language setting in KnowBe4 – the user can change this themselves, to choose which language they complete training in. The setting "en-us" is a default language for non-US locations as well as US locations for which a local language isn't set automatically. The majority of clickers used this language setting and there were increased numbers of clickers in 2023 and 2024 which may have allowed the dependence to be unveiled. Although it's a statistically significant relationship, it may just represent the fact that our phishing emails are sent in English, and 2 of the 3 topics were of interest to particularly US based users (though of international interest also). It would be interesting to see if this dependence continues in future simulation tests, and if language specific tests are used, whether it continues, or attracts more non-English speaking users.

Although KnowBe4 collects a lot of data, some of it is only collected on clicking the phishing email, so we only had data including location, operating system, and browser from the users who failed the test, meaning it could only show trends for clickers, and thus wasn't useful to analyse at this time.

7 Conclusion and Future Work

My research question and primary hypothesis “Can Phishing Simulation Testing be used to Analyse and Improve Efficacy of Security Awareness Training” is answered in the negative by this study. Future phishing tests may show a relationship with training, with more exact training data without significant outliers. The number of users who fail the phishing test may also have been too few in the most recent test (which is a positive outcome), which if that trend can be kept, will mean that my research question can’t be answered within this organisation’s ability. However, this and future data can be included in larger reviews taking in multiple similar phishing simulation tests in order to achieve a minimal meaningful number which can be used for correlations when failures are small, which would contribute to the published phishing research. Another option is to improve automated collation of user reports and track the positive outcome of the test also as an active pass, indicating that the phish was recognised and notified. 2.5% reports in the latest test might correlate to training duration and recency in a more specific manner as it uses a larger set of datapoints. With more time I would have been able to include the “reported” binary variable which at 280 users may have allowed a correlation to be seen.

The results of this research demonstrate the multi-modal nature of susceptibility to fraud and phishing. On a day-to-day basis, susceptibility to phishing in any format can have a number of causes, which cannot be accounted for, including the subject’s physical and mental status at the time of the phish (busy, tired, unwell, overloaded), as well as their awareness of phishing email recognition.

In our phishing simulation, we controlled several aspects of the attractiveness of the email including physical appearance, reward for clicking, and red flags which can indicate that perhaps it’s not a real email. However, we can’t control or know the psychological aspects of the user’s interaction with the email. The urgency or need to access the email however, was of a mild nature only (limited extended access to deals which might have been missed), and would not have been required to be accessed for business purposes, and thus should not have needed to be clicked at a busy or pressured time. This could indicate that users who opened, then clicked had been taken in by the phish.

A possible incentive to improve phishing outcomes is to target less training to users who consistently perform well, by streaming the users into levels of proficiency according to most recent passes or total amount of training done. The newest users can be assigned longer training while onboarding to ensure a better baseline awareness and potentially require less frequent training that they don’t want to do.

Location information was only collected for users who clicked on the email, which only allows us to see a spread of the failures and was based on the IP address they were logged in to at the time of clicking the phish link. Future improvements to allow for further analysis might include retrieval of location information from Active Directory for both companies and adding this to each user’s KnowBe4 profile.

The python code can easily be used to examine results of future phishing simulation tests, examine trends for users susceptible to phishing, and assess for changes in trends. As the tool is based on CSV data files, it can be used to analyse phishing simulation and training data from any source which can produce these files, with few modifications based on the data included. Specific information, such as knowledge of frequency and expected time spent training, and frequency of phishing simulations would be necessary for interpretation of the results. There is freedom to switch to another security awareness platform, whether commercial or open source, while retaining the data analysis implemented already.

Future research, for this data specifically, includes a requirement to analyse the passive aspects of the data: We can make conclusions based on active events recorded, including the time spent training, the number of phishing emails clicked, the number of users who report the emails. However, we can only make inferences regarding the users who didn’t either click or report the email. Did they log in to their email at that time and either ignore or

delete it, without reporting, or were they even accessing email at this time (a possibility with some employees who return for fixed contracts but whose user account remains open but inaccessible outside these contracts). Checking the email login access would help to exclude those users from tests, as their passive data skews the result to be better than it may actually be, and may mask relationships that exist with more active users. Similarly, distribution of browser use and operating system is available for users who have failed only, which doesn't allow us to check if a correlation is present within that population alone, or within the entire population who received the phish.

Formalising and automation of report tracking would allow the data to identify users who are actively engaged in phish simulation recognition and reporting, for targeted analysis of trends in their training and phishing performance to add to the dataset. The report data can also be augmented with the inclusion of non-simulation phishing email reports, allowing user engagement to be tracked, and potentially show a pattern of targeting (e.g. public information about one employee being used to contact other employees). Similarly, an awareness program regarding reporting of phishing emails can be implemented, with emphasis on the quickest methods to use when the user doesn't appear to have been directly targeted so that their work isn't impacted significantly by reporting phishes. To maintain user phish awareness, management highlighting information security training and phishing awareness (without informing them of an upcoming simulation campaign) might also improve engagement, reporting and awareness.

Future simulations can also consider streaming users into easier or more difficult phishing tests, depending on their performance. High phish simulation performers and active reporters could also be excluded from occasional tests, which could reduce any intra-team or department discussion of a current simulation that people should avoid, which can also skew results more positively. Further, considering the difference in performance in Q3 compared to Q2, it's essential to continue the momentum and track results over each quarter, as this may yield further data on phishing susceptibility throughout the year, e.g. with multiple packages being sent and received around the November/December holiday period, are users more likely to fall prey to delivery notification phishes? Or were more users on holiday or extended leave during this Q3 phishing simulation period?

Whether actively organising phishing simulation tests or not, all organisations have a responsibility and a duty to ensure that their employees are equipped with the knowledge and duty to actively avoid and report phishing emails. Phishing simulation tests are one way to monitor the efficacy of a security awareness program, before it becomes the subject of a successful phishing campaign.

References

Alkhalil, Z. *et al.* (2021) 'Phishing Attacks: A Recent Comprehensive Study and a New Anatomy', *Frontiers in Computer Science*, 3. Available at: https://doi.org/10.3389/fcomp.2021.563060.

Bill Toulas (2023) *Major U.S. energy org targeted in QR code phishing attack*, *BleepingComputer*. Available at: https://www.bleepingcomputer.com/news/security/major-us-energy-org-targeted-in-qr-code-phishing-attack/ (Accessed: 9 September 2024).

Charles Griffith (2024) *The Latest Phishing Statistics (updated June 2024) | AAG IT Support*, *AAG IT Support*. Available at: https://aag-it.com/the-latest-phishing-statistics/ (Accessed: 9 September 2024).

Eliott Tallqvist (2023) *Insights From the Hoxhunt Cybersecurity Human Risk Benchmark - Hoxhunt, HoxHunt.com*. Available at: https://www.hoxhunt.com/blog/insights-hoxhunt-cybersecurity-human-risk-benchmark-challenge (Accessed: 9 September 2024).

Keepnet Labs (2024) *Callback Phishing Explained: Protecting Your Data in 2024 - Keepnet, Keepnet Labs*. Available at: https://keepnetlabs.com/blog/what-is-callback-phishing-how-can-you-protect-your-business-against-callback-phishing-in-2024 (Accessed: 9 September 2024).

Maqousi, A.A. (2023) 'A Proposed Framework for User Cybersecurity Awareness', in *2023 24th International Arab Conference on Information Technology (ACIT)*. *2023 24th International Arab Conference on Information Technology (ACIT)*, Ajman, United Arab Emirates, pp. 1–6. Available at: https://doi.org/10.1109/ACIT58888.2023.10453904.

McElwee, S., Murphy, G. and Shelton, P. (2018) 'Influencing Outcomes and Behaviors in Simulated Phishing Exercises', in *SoutheastCon 2018*. *SoutheastCon 2018*, pp. 1–6. Available at: https://doi.org/10.1109/SECON.2018.8479109.

Pietrantonio, F. *et al.* (2024) 'A Gaze-Based Analysis of Human Detection of Email Phishing', in *2024 Silicon Valley Cybersecurity Conference (SVCC)*. *2024 Silicon Valley Cybersecurity Conference (SVCC)*, pp. 1–8. Available at: https://doi.org/10.1109/SVCC61185.2024.10637355.

Schwab, J. *et al.* (2024) 'What Makes Phishing Simulation Campaigns (Un)Acceptable? A Vignette Experiment on the Acceptance and Manipulation Intention Related to Phishing Simulation Campaigns'. Rochester, NY. Available at: https://doi.org/10.2139/ssrn.4737715.

Ultimate QR Code Phishing (Quishing) Prevention Guide: Here's What the Research Says - Hoxhunt (2024). Available at: https://www.hoxhunt.com/blog/quishing (Accessed: 9 September 2024).

Yeoh, W. *et al.* (2021) 'Simulated Phishing Attack and Embedded Training Campaign', *Journal of Computer Information Systems*, 62, pp. 1–20. Available at: https://doi.org/10.1080/08874417.2021.1919941.