



# Creating an Educational Tool for Phishing Awareness

CM3203

Emma Hall | C1738719

**Supervisor:** Amir Javed

**Moderator:** Federico  
Liberatore

## **Abstract**

The focus of this project is on the creation of an anti-phishing interactive educational tool. Information on the importance of phishing education resources is noted within the introduction and the resource limitations are described within the background research, alongside phishing email common identifiers and existing teaching methodologies that impact a user's learning. The design of the tool is explained and justified against e-learning principles explored in the research stage, alongside the reference emails used to construct the example phishing emails. Additionally, the implementation was completed unifying JavaScript, HTML and CSS to create a responsive mailbox for users to operate. The project was successful in the creation of an interactive anti-phishing educational tool however was tested on applicability and not tested by participants and as such, there has been no concrete evidence that this tool improves a user's learning. This factor is described in the future work section which details recommended uses of the tool for future development.

## **Acknowledgements**

I would like to thank my supervisor Amir Javed for their ongoing support and guidance throughout this project. I would also like to extend a thank you to my family and friends who have continued to support and encourage me throughout the duration of my time at university.

# 1 Table of Contents

1	Introduction.....	7
1.1	Preface.....	7
2	Aims and Objectives.....	7
2.1	Main Project Aim.....	7
2.2	Core Objectives.....	8
2.3	Desirable Objectives .....	8
3	Research.....	9
3.1	Phishing Attack Examples and Categories .....	9
3.1.1	Emotive Emails .....	9
3.1.2	Legal and Financial .....	11
3.1.3	Authoritative .....	13
3.2	Phishing Email Indicators.....	14
3.3	Anti-Phishing Resource Limitations .....	15
3.4	E-Learning Design Principles.....	18
3.5	Design Research for Mailbox interfaces .....	20
3.5.1	Mailbox layouts:.....	20
3.5.2	Mailbox Features:.....	22
4	Design and Approach Specifications .....	23
4.1	Anti-Phishing Educational Tool Requirements .....	24
4.1.1	Non-functional Requirements:.....	24
4.1.2	Functional Requirements:.....	25
4.2	Concept User Interface Design .....	26
4.2.1	Main homepage Design .....	26
4.2.2	Quiz page Design .....	27
4.2.3	Response Submitted (Interface after phishing/non-phishing selection) Design.....	30
4.2.4	Quiz Review page Correct/Incorrect Phishing Email Design.....	31
4.2.5	Results page Design .....	32
4.2.6	Help Page Design.....	34
4.3	Design of Emails.....	35
4.3.1	The Scenario: .....	36
4.3.2	The Emails:.....	36
4.4	Cite Map.....	47
4.5	Risk Assessment .....	47
5	Implementation.....	48
5.1	Homepage.....	49
5.1.1	Username input .....	49

5.2	Quiz Page .....	50
5.2.1	Email Changes .....	52
5.2.2	Phishing and Not Phishing categorisation & classification .....	53
5.2.3	End of Quiz Alert .....	56
5.2.4	Interactive Links/Attachments and popups.....	56
5.2.5	Help Page.....	57
5.2.6	Correct/Incorrect Display (Quiz Review html page).....	58
5.2.7	Results page .....	60
5.3	Implementation Constraints/Challenges.....	63
6	Applicability Testing .....	63
6.1	Evaluation of Requirements .....	63
6.1.1	Non-Functional Requirements .....	63
6.1.2	Functional Requirements .....	64
6.2	Evaluation of Functionality (Test Cases) .....	65
6.2.1	Test Case 1: Input name and Begin Quiz.....	65
6.2.2	Test Case 2: Input null name - negative test case.....	65
6.2.3	Test Case 3: Selecting email from main quiz page .....	66
6.2.4	Test Case 4: Selecting Help Page and Return to Quiz buttons.....	67
6.2.5	Test Case 5: Selecting phishing button when the email is phishing.....	68
6.2.6	Test Case 6: Selecting phishing button when the email is not-phishing.....	69
6.2.7	Test Case 7: Selecting not-phishing button when the email is phishing.....	70
6.2.8	Test Case 8: Selecting not-phishing button when the email is not a phishing email....	71
6.2.9	Test Case 9: Hover over link/attachments .....	73
6.2.10	Test Case 10: Navigating Next and Previous.....	74
6.2.11	Test Case 11: Using view results button.....	75
6.2.12	Test Case 12: Returning to Homepage .....	76
7	Future Work .....	76
8	Conclusions.....	78
9	Appendix.....	81
	Figure 1 - Microsoft Phishing email [34] .....	10
	Figure 2 - COVID-19 Phishing scam alert [33] .....	10
	Figure 3 - Fake Charity COVID Scam [35].....	10
	Figure 4 - Berkley HR Phishing example [46].....	12
	Figure 5 - Berkley Phishing HR example [14].....	12
	Figure 6 - GlobalPay Phishing Example [16] .....	12
	Figure 7 - Boss Phishing example [45].....	13
	Figure 8 - Berkley Chancellor phishing Example [47].....	13
	Figure 9 - Screenshot showing Gmail mailbox layout [28] .....	20

Figure 10 - Screenshot showing Protonmail mailbox layout [29].....	21
Figure 11- Screenshot showing Outlook mailbox layout [30] .....	21
Figure 12 - Screenshot showing typical inbox structure [28] .....	22
Figure 13 - Screenshot showing typical message pane structure [28].....	22
Figure 14 - Screenshot showing typical navigation menu [28].....	22
Figure 15 - Screenshot showing typical conversation side panel [28] .....	23
Figure 16 - Homepage Interface design.....	26
Figure 17 - Official Quiz page Interface Design .....	27
Figure 18 - Response Submitted Interface Design .....	30
Figure 19 - Correct Answer Email Review Interface Design .....	31
Figure 20 - Incorrect Answer Email Review Interface Design .....	32
Figure 21 - Results page Interface Design .....	33
Figure 22 - Help page Interface Design.....	35
Figure 23 - Security Notice Berkley Phishing Example [42].....	37
Figure 24 - Email 1 Design.....	37
Figure 25 - Email 2 Design.....	38
Figure 26 - YouTube IS THIS YOU scam example [26] .....	39
Figure 27 - Email 3 Design.....	39
Figure 28 - Email 4 Design.....	41
Figure 29 - Email 5 Design.....	42
Figure 30 - Delay in Payroll Phishing Example [44] .....	43
Figure 31 - Email 6 Design.....	44
Figure 32 - Email 7 Design.....	45
Figure 33 - Email 8 Design.....	46
Figure 34 - Cite Map Showing Connectivity between Webpages.....	47
Figure 35 - Homepage displaying Input Name alert .....	49
Figure 36 - Homepage after Implementation .....	49
Figure 37 - Screenshot of Code for Inputting name into Tool .....	50
Figure 38 - CSS snippet showing flex property to scale DOM objects .....	51
Figure 39 - Quiz Page after Implementation.....	51
Figure 40 - Quiz page Email 1 Layout .....	52
Figure 41 - Screenshot of JavaScript code used to interchange emails on quiz page.....	52
Figure 42 - HTML code used to interchange emails on quiz page.....	53
Figure 43 - Screenshot of code which counts answer as correct.....	54
Figure 44 - Snippet of email_display function to show correct/incorrect text boxes on Review webpage.....	54
Figure 45 - Screenshot of code which counts answer as Incorrect.....	55
Figure 46 - Screenshot of HTML code with parameters for Incorrect & Correct answers.....	55
Figure 47 - Screenshot of show_stats() function to set variables ready for cross site access .....	56
Figure 48 - Screenshot of quiz interface at the end of the quiz.....	56
Figure 49 - Screenshot of Contacts list popup Example.....	57
Figure 50 - Screenshot of Link/Attachment popup Example.....	57
Figure 51 - Screenshot of JavaScript used to hide and show popups .....	57
Figure 52 - Help page after implementation .....	57
Figure 53 - Correct Answer Example for Not Phishing Email after Implementation .....	58
Figure 54 - Incorrect Answer for Phishing Email after Implementation .....	59
Figure 55 - Screenshot of Function for view results button.....	59
Figure 56 - Preview of View Results button on Interface after Implementation .....	60
Figure 57 - Snippet of code used to make bar charts for results page .....	61
Figure 58 - Snippet of code used to summarize total indicators per category .....	61

Figure 59 - Snippet of code used to insert data into bar charts for results page..... 61

Figure 60 - Screenshot of results page interface ..... 62

Table 1 - Table of Phishing Indicators ..... 14

Table 2 - Table of Usability Heuristics..... 18

Table 3 - Table of Non-functional Requirements for Project ..... 24

Table 4 - Table of Functional Requirements for Project ..... 25

Table 5 - Design Justifications for Homepage Interface ..... 26

Table 6 - Design Justifications for Quiz main Interface ..... 28

Table 7 - Design Justifications for Response Submitted Interface..... 30

Table 8 - Design Justifications for Quiz Review Interface ..... 32

Table 9 - Design Justifications for Results Interface..... 33

Table 10 - Design justifications for Help Interface ..... 35

Table 11 - Design for Microsoft Security Alert Phishing email ..... 36

Table 12 - Design for Teams Meeting Invite Not-Phishing email ..... 38

Table 13 - Design for No Subject IS THIS YOU scam Phishing email ..... 39

Table 14 - Design for Message from HR Phishing email ..... 40

Table 15 - Design for Charity Scam Phishing email ..... 41

Table 16 - Design for Payslip Error Phishing email..... 43

Table 17 - Design for Message from CEO Phishing email..... 44

Table 18 - Design for IT Company Newsletter Not-Phishing email ..... 46

Table 19 - Table showing Non-Function Requirement Testing Results..... 64

Table 20 - Table showing Functional Requirements Testing Results ..... 64

Table 21 - Input name and Begin Quiz (Test Case 1) ..... 65

Table 22 - Input null name - negative test case (Test Case 2) ..... 66

Table 23 - Selecting email from Main Quiz page (Test Case 3)..... 66

Table 24 -Test results for Test Case 3 - Selecting emails on emails 1-8 ..... 67

Table 25 - Selecting Help Page and Return to Quiz buttons (Test Case 4) ..... 67

Table 26 - Test results of Test Case 4 Selecting Help Page and Return to Quiz ..... 68

Table 27 - Selecting Phishing button when the email is Phishing (Test Case 5) ..... 68

Table 28 - Test results against Test Case 5 Phishing page ..... 69

Table 29 - Selecting Phishing button when not Phishing (Test Case 6)..... 70

Table 30 - Test results for Test Case 6 on emails 2 and 8 ..... 70

Table 31 - Selecting Not-Phishing when Phishing (Test Case 7)..... 71

Table 32 - Test results for Test Case 7 ..... 71

Table 33 - Selecting Not-Phishing when Phishing (Test Case 8)..... 72

Table 34 - Test results for Test Case 8 on emails 2 and 8 ..... 72

Table 35 - Test results for Phishing combinations using a mixture of Test Cases 5,6,7 and 8 ..... 73

Table 36 - Hover over link/attachments (Test Case 9) ..... 73

Table 37 - Test results for Test Case 9 on Links/Attachments per email ..... 74

Table 38 - Test results for Test Case 9 on popups per profile pictures ..... 74

Table 39- Navigating using next and previous buttons (Test Case 10) ..... 74

Table 40 - Test results on each email for Test Case 10 ..... 75

Table 41 - Using View Results Button (Test Case 11)..... 76

Table 42 - Returning to Homepage (Test Case 12)..... 76

# 1 Introduction

## 1.1 Preface

Phishing attacks on organisations have risen since 2016 and become one of the most prevalent threats on the internet. It is recognised that over 70% of data can be lost to even one successful attack on an organisation<sup>[1]</sup>. As well, the cost of these attacks can be significant with a single data breach averaging at approximately £3.86 million<sup>[2]</sup>. Subsequently, it is vital that people take sufficient precautions and implement security measures in order to protect themselves and their institutions from a phishing attack. The organisational impact for phishing can be catastrophic with many companies incurring substantial damage and loss to their sensitive/confidential data.

Whilst in many years' security measures like anti-virus and anti-malware tools that protect a company's internal infrastructure from the impact of phishing has seen a substantial growth and development, it is employees that appear to be a significant factor in an organisational susceptibility to a phishing attack<sup>[19][64]</sup>. Employees have been recognised by multiple companies as one of the biggest risks to their security measures. Access controls without proper classification can give employees administrative privileges that enable them to freely disable security features on their computer<sup>[3]</sup>. This opens their device up to exploitation, including all devices connected on the same network, and can be detrimental to an organisation if a breach occurs. User's behaviour, including a blasé attitude towards security, can be contributed to an individual's awareness of online threats including but not limited to malware, trojan horses, worms, viruses and of course, phishing.

As users can pose a prominent risk to an organisation, phishing is often most effective within organisations as it exploits the user vulnerability relying on their trust and responsiveness to spread and compromise/corrupt internal data. Anti-phishing educational resources are important to keeping an organisation secure and mitigate human error when it comes to their behaviour online. Existent online educational resources for phishing and phishing awareness are deemed an effective means of mitigating the vulnerability that humans possess. With appropriate tools and materials, users are more aware of phishing and can respond appropriately with more self-awareness and confidence.<sup>[4]</sup> As a result, it is essential that people within the workplace are taught to recognise these attacks to prevent them from causing unintentional harm to company and personal resources and sensitive data. Often times we find that people learn better through experiences and by "doing". This would mean that someone would need to be faced with a phishing email and have responded incorrectly to then be able to learn from that experience. Needless to say this is not the safest method of education and as such, a tool is required to simulate these emails in a safer environment but that is still similar to a person's standard email mailbox to effectively learn by "doing".

This project surrounds the creation of an anti-phishing educational tool which teaches how to identify phishing emails within a professional context. The tool is essentially a simulation of a standard mailbox whereby a user determines if an email presented is likely to be phishing or not phishing. Once all emails have been categorised by the user, they are presented with feedback showing if they were correct or incorrect in their choice as well as shown the elements within the phishing emails that indicate its nature. This report explains the implementation journey of this tool from research to conclusions, discussing any future work or adaptations that could be done as an extension of the project.

## 2 Aims and Objectives

### 2.1 Main Project Aim

Aim: Create an interactive educational tool using JavaScript and HTML that can be deployed online to companies.

**a.** The tool will be a phishing awareness quiz which will display phishing emails to a user, take in their responses, and generate on screen feedback after each question(email).

**b.** At the end of the awareness quiz, the tool should present the user with a final (on screen) report which identifies which emails the user is most likely to be susceptible to, and indicators misses of these phishing emails. This information should be shown on each particular email they are more likely to be susceptible to explaining any identifying techniques the user should be aware of. This area should be used to educate the user in identifying phishing emails.

## 2.2 Core Objectives

1. Establish an understanding of phishing
  - a.** complete research into phishing and typical phishing identifiers to ultimately ascertain a publicly available dataset to use as reference for my phishing email examples.
2. Understand the limitations of current anti-phishing resources.
  - a.** explore the limitations of anti-phishing educational resources and explain how the tool will be addressing these
3. Understand educational tools and learning styles
  - a.** complete research into existent design and usability traits of various phishing tools and educational tools which can be used in design.
4. Create a list of functional and non-functional requirements
  - a.** from the research regarding the tools and phishing, define a list of non-functional and functional requirements of the tool. Make sure to list the purpose and why each requirement meets usability, applicability and functionality traits.
5. Create user journey and test cases
  - a.** create test cases for the project to test the tool against for evaluation purposes
  - b.** create user journey to depict the activity flow of how the quiz pages link together, and how the user will progress through the tool.
6. Create concept design of tool
  - a.** Create user interface designs showing the aesthetic of each website frame.
  - b.** Include justification within the design of each interface and explain any design principles utilized
7. Code the tool
  - a.** Using JavaScript and HTML code the tool which should meet the design specifications and functional/non-functional requirements defined prior to implementation.
  - b.** The quiz should have a feedback report which shows what types of emails the user is likely to be susceptible to.
  - c.** The feedback should also include a summary of phishing indicators found within the example phishing emails that the user has missed.
8. Evaluate the tool against defined criteria and test cases
  - a.** Using the criteria defined, I will evaluate how the tool meets each criteria and record how well it functioned.

## 2.3 Desirable Objectives

1. Create graphical representations of users results

- a. Create a graph out of the user's responses that is displayed at the end of the session showing how well they did.
2. Level variations depending on company requirements
  - a. Depending on the company using the tool, create levels which each user should pass in order to meet the companies determined level of phishing awareness
3. Statistical Analysis based on the emotional response of the user to be used by the manager/security team to determine the success of a phishing email.

### **3 Research**

In order to understand what makes an effective online educational tool and the elements that need to be considered within the tool, research has been completed into e-learning methodologies and anti-phishing resource limitations. Below discusses the existing gaps within educational resources most of which the tool aims to address and will aid in the justification of specific features within said tool. Additionally, phishing attack examples and indicators are discussed which will help to determine the indicators that are going to be focused on when constructing a feedback report for a user, as well as be used as a reference when creating the examples that are to be included within the tool.

#### **3.1 Phishing Attack Examples and Categories**

A significant factor in developing an anti-phishing educational tool to be deployed in an organisation is to include examples of phishing attacks that people are likely to be faced with. Whilst there are a number of attacks that have a possibility of being performed on an organisation, and it is important to include a variety, it should also be ensured that email examples used are relevant and emulate those which are likely to appear in an employee mailbox. This tool will contain 8 emails 6 of which are phishing emails. There are a couple of reasons behind this choice of email quantity one of which being time scale of the project: due to the time constraints of the project it has been deemed best to focus on creating a small number of quality phishing email examples than introducing an overwhelming number. Additionally, as the tools aim was to help the user to distinguish between likely phishing emails and non-phishing, it was considered important to add in a select few non-phishing emails. It has been decided that 2 non-phishing emails are to be used within the tool as this would allow more focus on a wider set of phishing emails to be displayed. The more emails the user can be exposed to, the broader their perspective will be on phishing emails enabling them to identify them better in numerous conditions outside the tool.

Additionally, to be able to draw relevant and useful statistics from the tool, the emails need to be separated into categories. For this anti-phishing tool, only a few phishing types are going to be used for quantifying user phishing susceptibility:

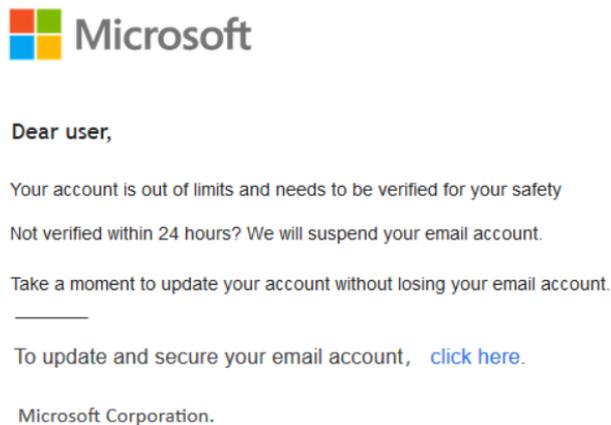
- Emotive - sad, urgent/shocking and happy
- Legal and financial emails
- Authoritative - managerial/ hierarchical

##### **3.1.1 Emotive Emails**

Emotive emails has been chosen as one of the phishing categories as studies have shown that emotion plays a part in users' susceptibility to phishing emails<sup>[31]</sup>. The idea behind this is that typically our decision making process is driven by our emotions and many attackers will take advantage of this fact by attempting to invoke an emotional response from a person that leads them to sharing sensitive/personal data. This has been highlighted significantly during the COVID-19 pandemic where buzz words such as "quarantine", "mask", "COVID" have been referenced within phishing emails all in

an attempt to invoke panic within a person and get them to click on the attaching medium<sup>[32]</sup>. Typical emotive phishing emails can be emails alerting the employee that their account is being deactivated, credit card compromised, a promotion or job offering announcement, or an urgent request from a colleague to help on a task of some nature. Emotive emails can also be separated in the emotional response they attempt to attain from the recipient. Common emotional categories that will be being used are happy, sad, angry, and shock.

Emotive Email Examples:



UPDATE NOW

Figure 1 - Microsoft Phishing email [34]

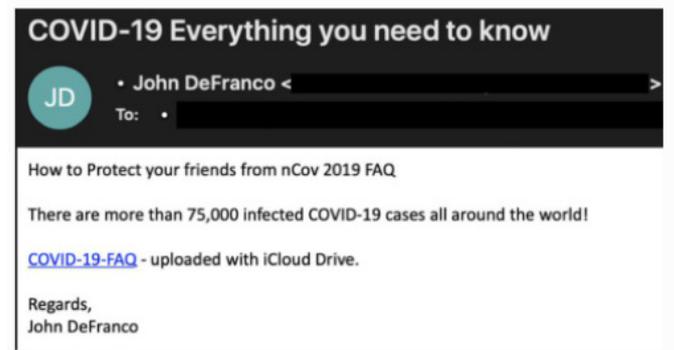


Figure 2 - COVID-19 Phishing scam alert [33]

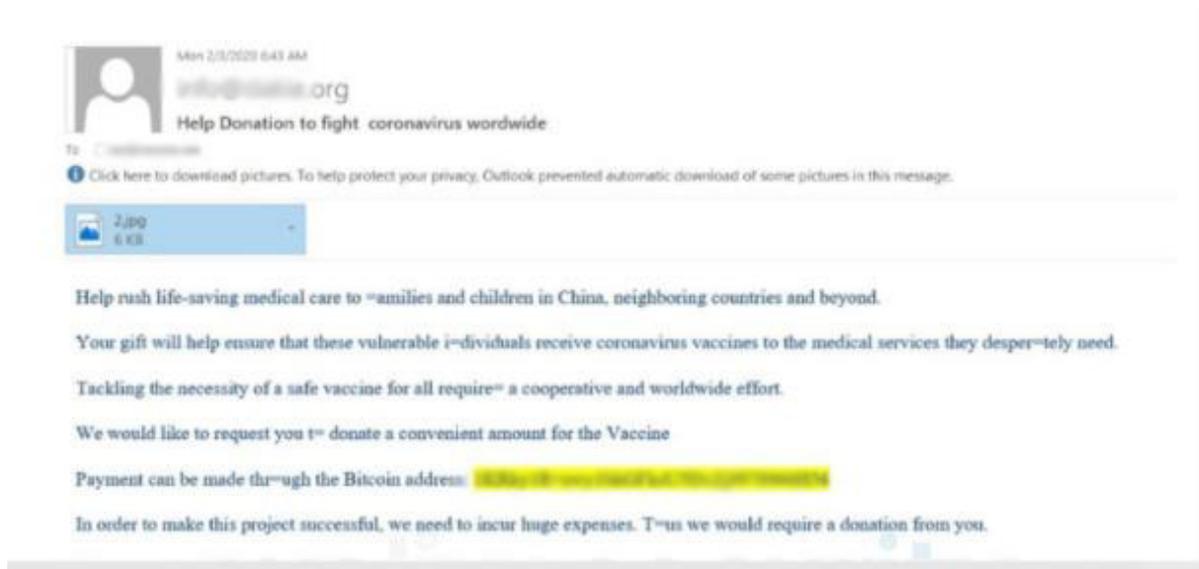


Figure 3 - Fake Charity COVID Scam [35]

The emails above I have deemed as an example of emotive emails due to the language and words used. The words used in the Microsoft security alert such as "suspend", "safety", and "losing" all connote feelings of danger and failure. I feel that the language used invokes a sense of urgency within the user as it states that without action, the recipient will become unsafe. Additionally, the COVID-19 email example from John DeFranco<sup>[33]</sup> utilizes a similar technique by playing on people's fears of getting COVID. The language here uses phrases like "protect your friends" and "75,000 infected" implying again the sense of urgency to follow the link within the email. As well, the email attempts to manipulate the user by pulling on their moral obligations to protect their friends: through not clicking on the link provided, they are doing the opposite of what has been stated within the email which is to protect their friends. Language and tone play a significant part in phishing emails and is an important indicator which will be displayed in the example phishing emails within the tool.

As studies have shown that emotions play a significant part in phishing emails, it has been decided to use 3 emotive emails within the 6 phishing ones that will be implemented. Due to the commonality of emotive emails within phishing attacks, I felt that it was best to add in more emails of this category as it would better reflect the emails users are more likely to receive in real life cases.

### **3.1.2 Legal and Financial**

Legal and financial has also been chosen as a phishing email category as phishing emails surrounding money requests or employee payment failures have been prevalent within my research. These emails encompass those that ask for financial details or request the recipient to click on an invoice/attached notice to view financial information on their account. They can be very convincing when they appear to emanate from people who work alongside the recipient or from the correct department thus, having a few example emails within the anti-phishing tool would better highlight how to indicate them. As It had been decided to provide 6 phishing examples 3 of which resided in the emotive category, it was deemed necessary to provide 2 legal and financial emails. Likewise with emotive emails, phishing emails requesting the recipient look at a link for financial/legal reasons were a common occurrence hence the need to display more than 1 within the anti-phishing tool. Additionally, with 2 examples of legal and financial emails, the sophistication of the emails could vary which would better highlight their convincing nature and display the ways to determine their illegitimacy despite this.

## Legal and Financial Email Examples:

From: "HR@berkeley.edu" <HR@berkeley.edu>  
Subject: Message from human resources  
Date: April 13, 2017 at 9:29:54 PM PDT  
To: XXXXX@berkeley.edu

Dear XXXXX@berkeley.edu

An information document has been sent to you by the Human Resources Department.

[Click here](#) to Login to view the document. Thank you!

Berkeley University Of California HR Department  
© 2017 The Regents of the University of California. All rights reserved.

CONFIDENTIALITY NOTICE: This email and any attachments may contain confidential information that is protected by law and is for the sole use of the individuals or entities to which it is addressed. If you are not the intended recipient, please destroying all copies of the communication and attachments. Further use, disclosure, copying, distribution of, or reliance upon the contents of this email and attachments is strictly prohibited.

**Figure 5 - Berkley Phishing HR example [14]**

To: xxxxxx@berkeley.edu  
From: ADP PORTAL <director.stics@boyaca.gov.co>  
Date: Tue, 24 Jan 2017 13:31:49  
Subject: Update Portal

The Human Resources/Payroll Department has completed the final paystub changes for 2017 tax year.  
To view the changes to your paystub information and view/download your W-2 forms (2014 - 2016 tax years), go to: [Adp Portal](#)

We hope you find the changes to your paystub information useful and welcome any comments you may have.  
Yours Sincerely,  
Danielle Carrel.

**Figure 4 - Berkley HR Phishing example [46]**

From: GlobalPay <VT@globalpay.com>  
Subject: Restore your account  
Date: February 7, 2014 3:47:02 AM MST  
To: David

1 Attachment, 7 KB Save Quick Look

Dear customer,

We regret to inform you that your account has been restricted.  
To continue using our services please download the file attached to this e-mail and update your login information.

© GlobalPaymentsInc

 [update2816.html \(7 KB\)](#)

**Figure 6 - GlobalPay Phishing Example [16]**

The above emails are examples of financial and legal emails as the attacker is attempting to obtain sensitive information from the recipient by acting as a reputable financial company/entity. One convincing feature of the top-left email is the confidentiality notice which supports the look of a legitimate professional email. It is these features which will be added to an example phishing email in order to show how even with this element, an email can still be phishing. With the bottom example, there is a good phishing indicator present in the shape of a generic greeting<sup>[16]</sup>. It has been identified that generic greetings such as "dear customer", "hello user" etc. are often an element of a phishing email as they can be sent out to more than one recipient in bulk thus increasing the chance of someone clicking on the attachment or link. That said, the absence of one can also be an indicator of a phishing email as the top-right example displays.

There can be multiple techniques that aid in determining the legitimacy of legal/financial phishing emails including following the methods that the company provide financial and legal information or requests. Typically, no organisation will request sensitive information such as credit card numbers or account information through email. Furthermore, 2 emails will be included in the tool that cover

financial/legal email examples and include the use of the greeting indicator as a way of identifying them.

### 3.1.3 Authoritative

Authoritative emails aim to get a recipient to interact with its contents through mimicking an authoritative figure within the company's email. This could be a manager, director or CEO of a company. This technique works best targeting companies as it utilizes the reputability and stature of the "sender" to get people to trust that the content of the email is safe and legitimate: often employees are less likely to question an email coming from their boss or seniority especially when they are told to hurry with a request<sup>[65]</sup>. As this type of attack is more likely to occur within a workplace, it was considered best to add in an example into the simulation which would expose the user to such a case where a higher authority is requesting help or action from them.

Authoritative Email Examples:

**From:** Your Boss <yourboss@fakeyourcompany.com>  
**Sent:** 09 October 2018 11:06  
**To:** Your Company Finance <finance@yourcompany.com>  
**Subject:** IMPORTANT: Fund Transfer Done Today

Hi Gwen,

Could you do me a favour? There's a pending invoice from one of our providers and because I'm on holiday I need you to take care of it for me because I can't access the accounts from here.  
They contacted me and I told them to send through the email to you as well (check spam filter incase it's accidentally blocked!)  
Just click on the link in their email and transfer the amount to the account they specify.

This needs to be done TODAY so make it high priority.

If you do this for me it would be a huge favour.

Any questions then reply to this email. I can't take calls right now so just stick to replying to this email.

Thanks,  
Your Boss

**Figure 7 - Boss Phishing example [45]**

From: Nicholas B. Dirks <penweltm@miamioh.edu>  
Date: Wed, Dec 14, 2016 at 8:55 AM  
Subject: Important Announcement from Chancellor Nicholas B. Dirks  
To:  
  
Good Morning Berkeley Family,  
  
Please read attached for an important announcement from Chancellor Nicholas B. Dirks  
  
Thanks,  
Nicholas B. Dirks  
*Chancellor*  
  
1 attachment: shared Document.pdf

**Figure 8 - Berkley Chancellor phishing Example [47]**

The above emails are examples of an attacker emulating a managerial/authoritative entity like a chancellor. The top example is a very sophisticated email which actually uses the name of the recipient attained from harvested social networks<sup>[39]</sup>. This method has become more used which means that people need to rely on other identifying elements than a greeting indicator. Of course, it does depend

on how you communicate with your manager so it is important to note that what indicators the individual uses to identify the emails will somewhat change: this factor will be highlighted within the explanation section of certain emails remarking what makes each email phishing. In addition, the top email also does not come with a link/attachment but is actually a preface for another phishing email. The idea for this is that the recipient will trust the next email which has an unauthorised link/attachment regardless of errors since the initial one references it and, emanates from a trusted source: ultimately the less time attackers will need to refine the succeeding phishing email.

For these examples there are a few indicators that could be used to identify them as phishing. One point to make is that the top email requests a money transfer. It is suspicious that an immediate money transfer would be requested without giving further context of who the provider is and why it is needed on the day the email has been sent. Another aspect of the email includes the request to only reply to that email. A good way to determine if this is legitimate is to compose a new email and send it to the account that you have in your contacts for the true sender in order to validate its real: the request to only communicate on that email thread is strange in this circumstance. Additionally, the language used in the bottom email is also suspicious. The sender essentially refers to the document being sent in the third person which is an odd grammatical choice for someone of such stature as a chancellor<sup>[16][17]</sup>. Again, both language and grammar are indicators which will be included in the anti-phishing tool as identifiers for phishing emails.

### 3.2 Phishing Email Indicators

Having observed many emails to determine what types of emails exist nowadays, what indicators existed and how they were to be included in the example phishing emails was established. Below are a list of indicators which have been discovered in multiple sources that are prevalent within phishing emails to date<sup>[16][17][23][55]</sup>.

**Table 1 - Table of Phishing Indicators**

Indicator	Description
Grammatical & Spelling Errors <sup>[51][52][16]</sup>	Phishing emails often have numerous grammatical or spelling errors. Be sure to check the grammar within professional and company emails.
Language and Tone <sup>[17][53]</sup>	Language indicators are things such as the tone of the email, as well as emotional cues that aim to trick you into sending money because you are shocked or sad about the message content. It is important to examine the language used in the email and make sure that what is being said reflects what you would expect from the sender.
Fake Domain/ Email Addresses <sup>[16][17][12]</sup>	Domain indicators are things such as Legitimate companies contacting you through a @gmail or @hotmail account. Emails can also be faked and whilst at first glance look similar to a contact, may be misspelled or not match in another way.

	An attacker can spoof an email address as well to make them appear legitimate - other indicators are necessary in this case to identify the phishing email.
Suspicious Links or Attachments <sup>[17][54][55]</sup>	Legitimate companies will refrain from requesting money or asking for sensitive information through a linked attachment. The links can also point to arbitrary html pages/sites that do not match the URL of the company they are pretending to be from.
Generic Greeting <sup>[16][17][56]</sup>	Legitimate companies typically will address you via your actual name. Be cautious of emails that have a very generic greeting such as 'hello user, dear valued customer, dear employee etc.' These can be indicators of a phishing email

The above indicators will be used in the tools example phishing emails differing how many are used per email and then quantifying how many are on each email. This will display to the user what types of indicators they are less attuned to in perceiving phishing emails and as such, what they should be aware of in the future.

### 3.3 Anti-Phishing Resource Limitations

Through the research conducted, it was discovered that many resources online for anti-phishing education were identified as "textbook" courses with limited resources found that provide an immersive simulative experience<sup>[63]</sup>. Many online phishing resource hubs<sup>[57][58][61]</sup> often signposted to these courses which were a mixture of video, poster, pamphlets and test mediums that attempted to communicate the concepts and theories behind phishing and susceptibility. Whilst these resources are beneficial in teaching these concepts, they are often constrained in their approach to teaching and aren't as effective at influencing user behaviour online. Moreover, upon searching for phishing and anti-phishing educational resources existent within today's climate, search engines typically showed websites that provided resources like anti-phishing software and reporting tools<sup>[59][60]</sup>, instead of an abundance of educational resources, that addressed phishing on a technical level. These software's, although imperative as a remediation measure for security breaches and phishing attacks, do not address the human component that is predominant in phishing and as such, do not fully mitigate susceptibility to phishing.

Ultimately, the lack of education surrounding phishing and awareness of it can contribute to people's online safety and susceptibility to phishing emails thus, there is a need to bridge this educational gap. In order to do this, tools need to be created to help effectively educate people on seeing phishing emails and recognising them in a safe environment. The tool aims to address this educational gap through creating my anti-phishing simulation tool which will include a statistical summary of phishing categories and indicators within each email that have been identified. This will not only help tackle phishing attacks but also provide a basis on understanding why they were successful. Simulation e-learning can help to increase retention of these concepts and theories through user experience.<sup>[7][15]</sup> They can provide a more immersive experience in which users are able to practice the act of responding or recognising phishing emails. In turn, users can better apply their knowledge in real world environments that reflect the ones they were faced with in the simulation. As phishing relies on a user's online behaviour, a simulation tool is most effective as it attempts to attune a user's behaviour by employing

kinesthetics learning<sup>[8]</sup>. In addition, a study conducted in 2020 determined that visual and interactive measures for phishing education proved to have more of an impact on the information retained by participants<sup>[9]</sup>. Subsequently, resources need to have much more inclusion of interactive elements such that are likely to be present in simulations in order to aid users in memorizing the content being shown. This interactive property is the basis for the tool and the support behind the theory.

Some recourses are existent within large companies who are able to provide anti-phishing courses and training to their employees regularly. However, this doesn't necessarily mean that phishing attacks and the problem of human awareness is fully combatted. In fact, putting aside the immediate problem of SME's budgetary constraints and the prominent expense of educational resources, there are other limitations existent tools pose. Many resources don't provide an effective enough personalisation or implement the story based instruction principle which allows a resource to simulate each company's corporate environment<sup>[5][21]</sup>. Without this inclusion, resources and tools can be ineffective in teaching individuals anti-phishing principles. The tool aims to address this factor in my tool including a personalization element to help engage the user and improve the simulation further to reflect their mailboxes. The personalization element will likely be applied through the use of the user's name. The plan for the tool is to have a section in which a person can type in their name which is then stored temporarily by the tool to be inputted into various email elements. These elements will include such this as the greeting of an email i.e. Dear [username] and be used in the "to" line within an email header emulating that of an email that has been sent to that individual. The story based principle explains that an effective form of teaching is allowing users to progress through a simulation or course following a story. In this case, this principle will be applied within the tool by providing a brief scenario to the user which will essentially immerse them in this fictional environment. The scenario will explain the fictional company they work for alongside what they need to do to traverse through the emails. Whilst the user journey will not be directly following a lengthy story, it will provide the concept through immersion and by creating the idea that they are a part of the story. Consequently, this will positively impact the user's retention of the information provided by the tool by being engaging and immersive.

In conjunction with this, anti-phishing resources are limited by what they can use in respect to company logos, personnel names, emails etc., and as such, these tools are unable to capture a lot of phishing examples in which these factors are utilized in an attack. Without authorisation it is very difficult to achieve enough of the aforementioned personalisation within an educational tool. Phishing has become sophisticated, and hackers aren't generally concerned with legality including stealing company logos or any personal data to perform a phishing attack whereas, developers for these types of tools are bound by company policies that restrict the use of these. This is a limitation with anti-phishing educational resources as without a company's authorization, the tool cannot use their logos or data that might breach privacy policies. Subsequently, the tools lack personalisation when it comes to fully simulating their workplace environment i.e. email interface. The aim of this project and the tool being created is to combat the problem of personalisation. Whilst likewise the tool cannot include a company's specific logo during the implementation phase of this project, the aim is to create a tool which uses other personalization techniques in order to combat this limitation and make the simulation reflect that of one's personal inbox. These features will likely include using the users name in certain phishing email examples and developing the interface to closely resemble the appearance of existing mailboxes such as Gmail and outlook. The existing design structure of these mailboxes will be utilized when designing the tool so that certain features are located in familiar places to the user. This familiarity will help the usability of the tool as well as support the immersive experience of the simulation.

Another limitation of existent anti-phishing tool is that there isn't enough consideration to demographic factors. Factors such as age, gender and educational and employment play a significant part in how a user will behave online<sup>[6][24]</sup>. Whilst all demographic factors play a role in one's online behaviour, it is however important to note that tools should not attempt to meet every demographic as this will

ultimately make the tool much more complex and difficult for every person to use. It is vital then that developers simply focus on a few demographics in order to refine a target audience and thereby better consider the critical attributes of those people that can be accommodated in the tool. The employment demographic will be focused upon for the structure and context of the phishing emails which will ultimately encompass the age demographic typically found within the workplace. This is because the tool is intended to be deployed in a professional environment and as such, a major consideration for the email structure needs to surround the demographic of employment. The biggest part about simulating the design of a mailbox is that there is not a significantly large range of typical design elements on existing mailboxes that pertain to specific demographics being often designed universally with each in mind. Subsequently, the design of the mailbox will be in line with the universal nature of existing mailboxes incorporating neutral colour palettes, font types, and displayed icons. In order to be unbiased within the tool and not be specific to a certain company, one aim is to create an email box and emails based upon a fictional workplace that whilst is reflective of a typical workplace that includes communication via emails, is not representative of any one specific company. This will improve the inclusivity of who can use the tool alongside incorporating the method of the mentioned story based principle by providing a fictional scenario for the user to follow alongside whilst learning. When considering the demographic of age within the workplace, learning methods have been explored briefly within the e-learning design principal section below in order to identify confirmed and effective techniques which can be utilised within the tool. As the main premise of the tool is to teach, it is important that the tool adhere to appropriate learning methods that align with the mentioned focused demographic of age. Whilst the demographics in designing the tool and creating the example phishing emails will be considered, these will not be used for statistical purposes. As the core objective of the tool is to teach people in identifying phishing emails with a reflective review of the types of emails they are more likely to be susceptible to, it is not in the scope of the project to provide a way to analysis the susceptibility of phishing in relation to gender, age or educational background. That said, It is encouraged to adapt the tool in such a way to provide this capability if this would help in future studies of phishing.

Furthermore, courses and resources can often be time-consuming and attempt to fill as much information as possible into the program. Many resources, especially written/readings ones, do not consider the integration of phishing courses into employee workflow. This is important as employees can become demotivated by lengthy courses that take them away from their productivity at work for a considerable amount of time. There is a lack of anti-phishing resources that require a short period of time from each user to complete<sup>[18][22]</sup>. That said, with the abundance of phishing attacks existent, it is difficult to meet this desirability without feeling as though the resource cuts out too much information, and hence why many resources opt for a lengthier completion time to ensure they cover everything. Ultimately, the posed solution here is to develop a tool which requires less of a user's time to be completed, or at least maintains user engagement regardless of time. As factors such as physical environment are less easy to control through a virtual educational tool, the focus for the resource needs to be on employee engagement and how to engage and tailor the resource to maintain it. Whilst there will not be studies or evaluation conducted upon how well the tool integrate within employee workflow, usability heuristics will be considered within the design. This will help to ensure the tool is user friendly which will inevitably contribute to efficiency of use and therefore provide an insight into how well it could integrate within a typical workflow.

With educational resources you want to be able to not only educate but also pull statistics from the tool in order to identify gaps or information that could help in an organisation. With existent anti-phishing resources, there isn't any identifiable tools or courses that provide this external feature or analytic capability. Through having the capability to record and assess the capabilities of its employees, the organisation can see any major gaps in their organisational knowledge that need to be addressed further. For example, the organisation can put more focus on further staff training for a specific topic or put

efforts into building a technical solution for gaps where human error is likely to be substantial. This would require an external database and storage of user data and is a current limitation which the tool aims to address as a desirable objective. This means that as it is not a fundamental component of the tool, work will only be conducted upon it if time permits it within the project.

### 3.4 E-Learning Design Principles

There are many capabilities and benefits through e-learning materials including the global accessibility of information, scalability, adaptability, and more. Designing these recourses for optimal learning is integral to ensure the resource is suitable for the topic it covers and its intended audience learning style. There are many principles which dictate how developers should design e-learning materials and what is to be considered<sup>[10]</sup>. Consequently, research on usability design principles has been conducted which will be utilized in the construction of the anti-phishing tool documented in the coming chapters.

For the design of web and interaction tools, websites and applications, Jakob Nielsen formulated 10 usability design principles. These principles are referred to as 'heuristics' and whilst they are not concrete guidelines for creating an interface, they are typically recognised as the best practices for doing so<sup>[11]</sup>. As such, I feel it important to align with these heuristics during the design phase and as such, each interface design will refer to them. As the general best practice of evaluating usability and conducting a heuristic evaluation is having the tool examined by subject matter experts in the field of HCI (human computer interaction), testing the tool against the principles after implementation will not be conducted. That said, the heuristics are still being utilized within the design process being considered upon each interface design in order to aid in increasing usability of the tool.

**Table 2 - Table of Usability Heuristics**

Heuristic	Description
Visibility of system status & feedback	The system should always inform the user of its current state and what is required of them to use it. Appropriate feedback should be given upon an action in order to inform the user that their action has been completed successfully or unsuccessfully depending on the response. <sup>[11][41]</sup>
Match between system and real world. (natural mapping)	The design should explicate information in a human readable manner. Words, phrases and terms should be communicated to the user that are familiar to them. Concepts, images and icons should be displayed in natural and logical order. <sup>[40]</sup> This principle also refers to having a clear relationship between tool controls and the effect they have on the application <sup>[43]</sup> .
Consistency and standards	Refers to similar operations and similar elements for achieving similar tasks <sup>[41]</sup> . various elements should be consistent in their structure and function. Colour palettes should be consistently used within the application and industry conventions should be followed when constructing familiar elements. Meet user expectations by following industry standard positioning of buttons and messages.

Recognition rather than recall.	This is the relationship between what something looks like and how it's used. The functionality of all elements should be intuitive to the user. In addition, elements can be given signifiers which are any perceivable indicator that communicates appropriate behaviour to a person <sup>[41]</sup> Often times this can be a simple text label. to display what the element does.
Error Prevention & Constraints	Limit the range of interaction possibilities to simplify the interface <sup>[40]</sup> . Remove any elements that are unnecessary to the design of the tool and could potentially contribute to error.
User control and Freedom	Make the interface flexible by allowing users to undo an action where necessary. Exit buttons are examples demonstrations of this principle as they allow the user control of the system feeling less entrapped if they can manipulate it in such a way as navigating away from a page <sup>[40]</sup> .
Flexibility and Efficiency of user	The device should accommodate a variety of users regardless of experience. This means that whilst the system should provide helpful tips to novice users, it can be adapted to accommodate those who are regular users. These methods could be personalization capabilities for more technical users to amend their settings based on preferences <sup>[41]</sup> .
Aesthetic and minimalist design	The interface should not contain any information that isn't essential to the functionality or purpose of the device. Every piece of information should be justified in its existence <sup>[41]</sup> .
Help users recognise, diagnose and recover from errors	Enable user's chances to understand and error they may have caused and to remediate it. Whenever an error occurs, notify the user of this error and explain a way to avoid it <sup>[40]</sup> .
Help and documentation	Help areas within the system should be implemented to give hints and tips to the user whenever they are stuck. Information on how buttons function or what the tool is requiring the user to do should be explained clearly and visible <sup>[40]</sup> .

Since the premise of this project is focused on helping people identify phishing and not an in depth look into examples of how heuristics are used in real life applications, anyone who wishes to conduct further reading into this topic area is encouraged to do so starting with references 49 and 50 documented in the reference section.

A vital rule within the collection talks about the need for feedback. In this case feedback refers to showing the user when an action has been completed however, feedback has also been recognised as the need for users to receive a critical feedback concerning their progress. For adult and young adult learning in the workplace it is important to consider this principle enabling them opportunities for

critical reflection<sup>[36]</sup> and as such, the tool will have clear pages for feedback showing if the user is correct or incorrect depending on how they categorise phishing/non phishing emails. Alongside evaluating my tool on its functionality, it will be tested against the principles discussed above to ensure it aligns with confirmed effective HCI (human-computer interaction) practices. Ultimately, this should then support some of the usability validation: as usability is not being tested with physical participants, there needed to be a way to attain some perspective in how effective the tool would be in real world applications.

### 3.5 Design Research for Mailbox interfaces

In order to determine how the tools interface would be constructed, research was conducted on how existing mailboxes are already structured. As usability is important within an online education tool, as mentioned in the above section, the tool design will follow the layout of specific features so that users are better immersed in the experience. The familiarity of the environment can better increase the chances of a user's recall on the information learnt<sup>[25]</sup> and thus, help the users better identify phishing emails in real world scenarios.

#### 3.5.1 Mailbox layouts:

Below are some typical mailbox layouts that will be utilized in the design processes. The references included Gmail, Outlook and another mailbox called Protonmail all of which follow a similar structure and are commonly used in the real world.

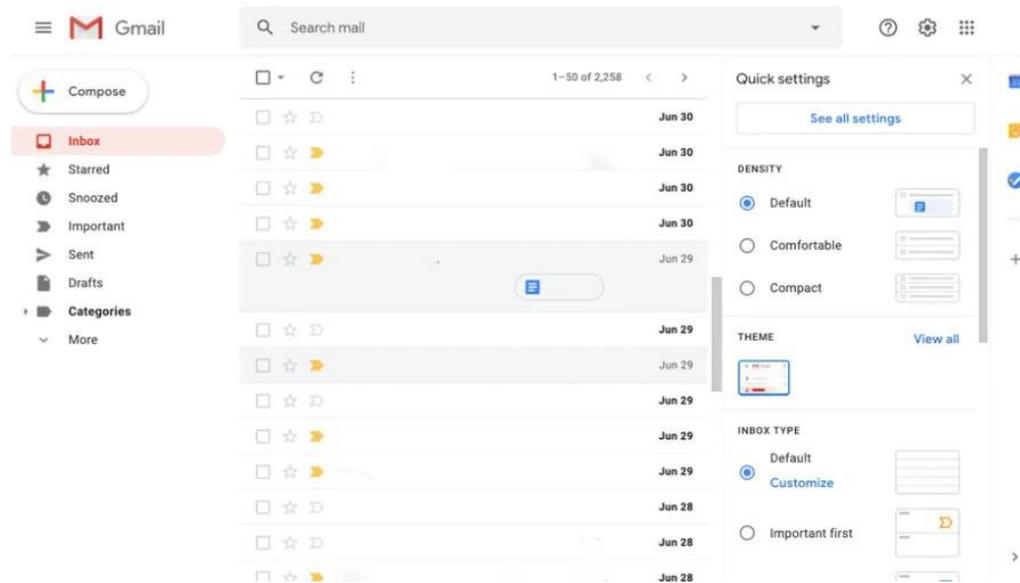


Figure 9 - Screenshot showing Gmail mailbox layout [28]

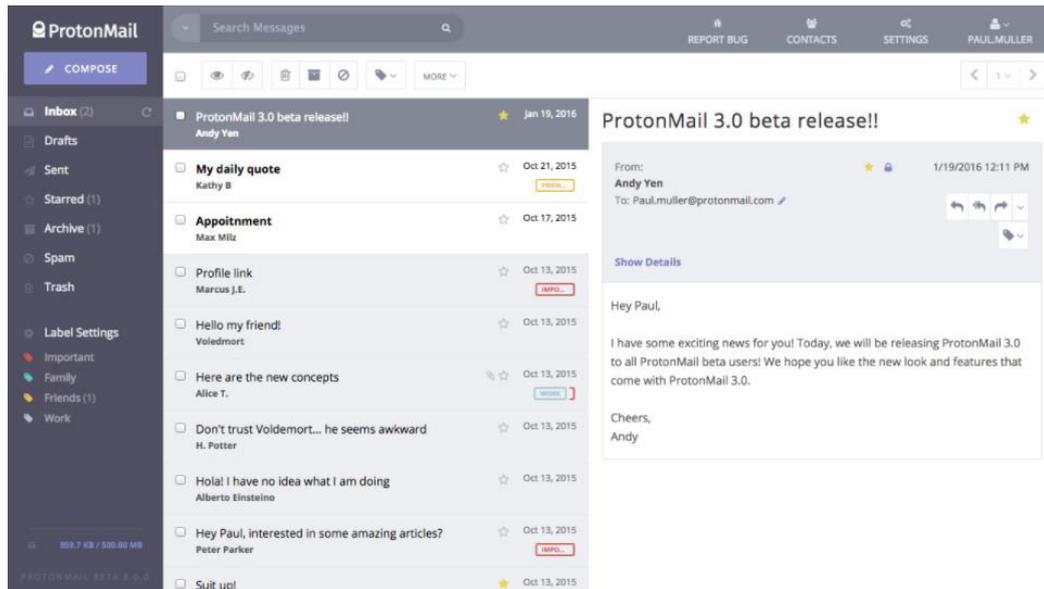


Figure 10 - Screenshot showing Protonmail mailbox layout [29]

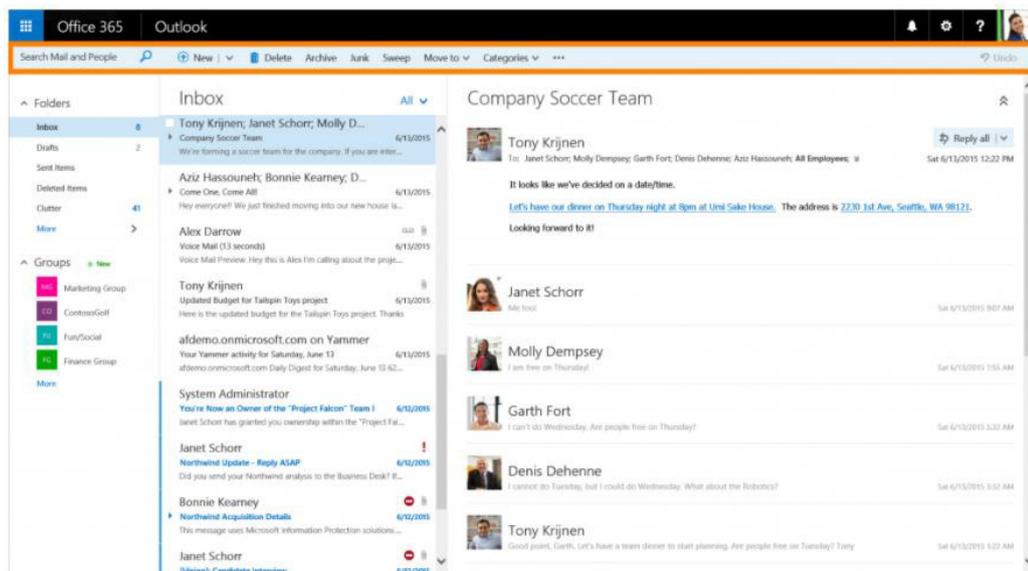


Figure 11- Screenshot showing Outlook mailbox layout [30]

### 3.5.2 Mailbox Features:

<input type="checkbox"/>			<b>Facebook</b>	<b>Getting back onto Facebook</b>	<b>Jun 29</b>
<input type="checkbox"/>			<b>Google</b>	<b>New sign-in from Samsung</b>	<b>Jun 28</b>
<input type="checkbox"/>			<b>Olenna Mason</b>	<b>Hey girl!</b>	<b>Jun 24</b>
<input type="checkbox"/>			<b>Grace Ellington</b>	<b>Volunteer Opportunity - I W</b>	<b>Jun 21</b>
<input type="checkbox"/>			<b>Olenna Mason</b>	<b>Lakestone student art exhi</b>	<b>Jun 21</b>

Figure 12 - Screenshot showing typical inbox structure [28]

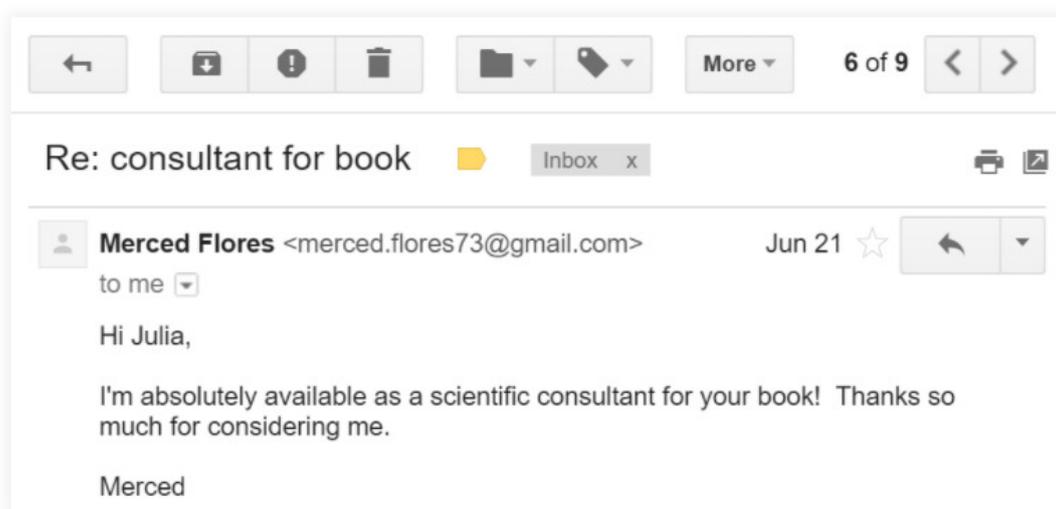


Figure 13 - Screenshot showing typical message pane structure [28]

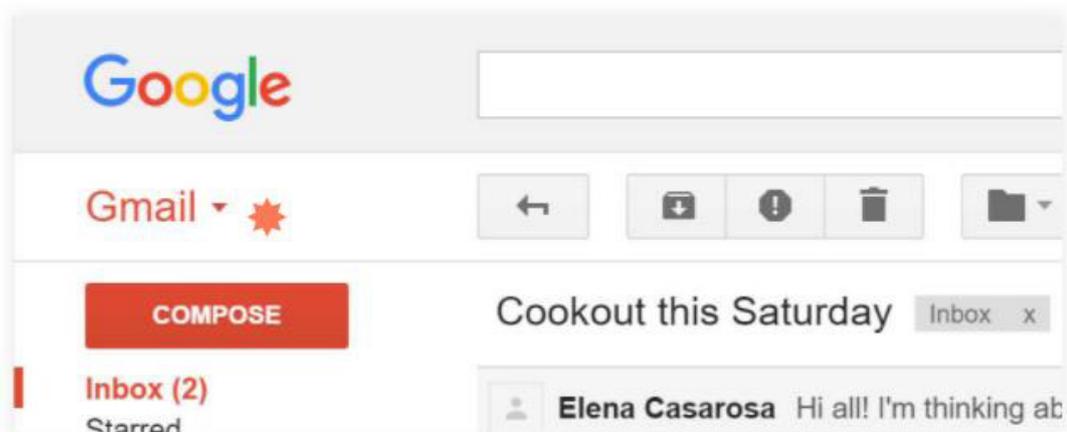


Figure 14 - Screenshot showing typical navigation menu [28]

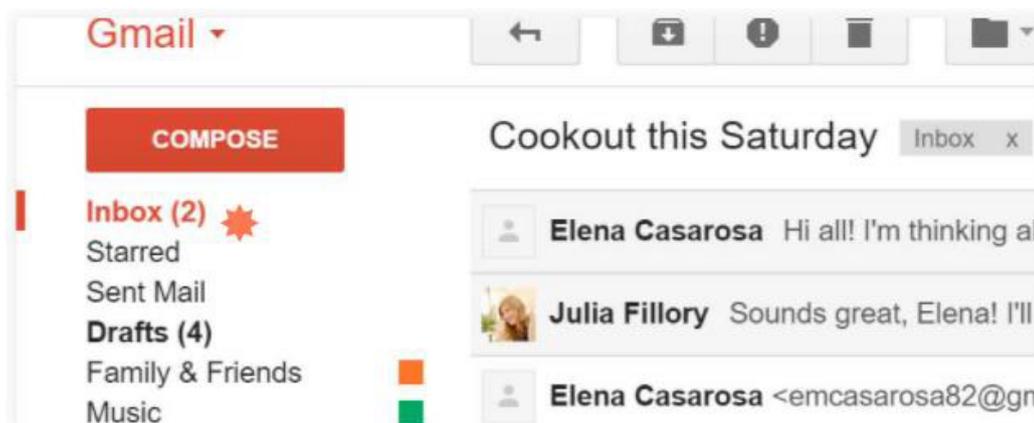


Figure 15 - Screenshot showing typical conversation side panel [28]

Whilst familiarity within the tool is important, it is stressed that the main purpose of the tool is to aid people in identifying phishing emails by first quizzing them on how well they currently recognise phishing emails, and also informing them on the various indicators of phishing emails. This means that not every feature described on a mailbox will be responsive in the tool. These features will be things like search bar and compose button which will only be included for aesthetic purposes as they will not be providing any additional support to the functionality of the tool. It has been decided to follow the common structure of the mailboxes represented above and have 3 columns for the page: a side bar with a contacts list on, a mini preview panel of the emails received, and a bigger column showing the message pane structure. Not only will this be in line with the aforementioned common structure of mailboxes, but this structure in which all elements and interactive components are displayed on a single interface will help with the visibility and discoverability of the tool: each option is shown to the user which makes it easier to use<sup>[11]</sup>.

## 4 Design and Approach Specifications

Below the design of the tool has been documented. This includes the system requirements, concept interface designs, email designs and a risk assessment. The implementation stage should follow the design that has been planned and depicted below unless a specific aspect of the plan cannot be implemented properly. In these cases, changes or alterations to the design will be highlighted within the implementation section of the report. For this project, the programming languages being used are HTML, JavaScript and CSS to construct an interactive anti-phishing educational tool. The aforementioned languages are being used as they are notably compatible with one another and have been said to be easier to interpret and become familiar with. In addition, there has been some prior experience in designing an interconnected website using HTML and CSS so this will allow me to design the tool to closely resemble a real life email inbox. In conjunction with this, JavaScript has been recognised as an easier language to learn and implement than other programming languages existent today, and as it works client-side, it can run functions immediately within the user's browser contributing to quick load up times of the tool. Since there is a time constraint on the project, JavaScript in combination with HTML and CSS was deemed the best option as manipulation and creation of the tool would be simpler to do so with than other languages which may require an extended time frame to accommodate the learning curve.

## 4.1 Anti-Phishing Educational Tool Requirements

Non-functional requirements (NFRs) determine the operational requirements of the system rather than any specific behaviours of said system. These are often recognized as 'quality attributes' which are used to evaluate the systems performance. See table 3 for details.

### 4.1.1 Non-functional Requirements:

Table 3 - Table of Non-functional Requirements for Project

Num	Requirement	Acceptance Criteria
1.	Tool should not hold any sensitive information to align with privacy regulations.	<ul style="list-style-type: none"> <li>No information relating to the person i.e. their name should be stored in the tool after the tool has been closed</li> </ul>
2.	Tool should be scalable and compatible with window sizes and browsers.	<ul style="list-style-type: none"> <li>Tool must work properly on following browsers: <ul style="list-style-type: none"> <li>Safari</li> <li>Google Chrome</li> <li>Firefox</li> <li>Microsoft Edge</li> </ul> </li> <li>Tool must change size dynamically to fit within different window sizes.</li> </ul>
3.	Every possible action should support testing and evaluation and be tested accordingly.	<ul style="list-style-type: none"> <li>Testing should be done and work on all interactive features including buttons and username input features.</li> </ul>
4.	Webpages should load promptly and efficiently	<ul style="list-style-type: none"> <li>Each webpage should not exceed a loading time of 5 seconds with the exception of cases where internet connection is poor.</li> </ul>
5.	All interactive elements on the webpages should be responsive and complete in a timely manner	<ul style="list-style-type: none"> <li>Each element should respond almost immediately and carry out a set action properly.</li> </ul>
6.	The tool should be easy to use and understand for all users	<ul style="list-style-type: none"> <li>Tool should be simple and easily understandable for first time users.</li> <li>Tool interface should be designed aligning with usability heuristics to improve usability</li> </ul>
7.	Final Report should be true to user's performance	<ul style="list-style-type: none"> <li>I will carry out a variety of tests for different cases where I purposely get certain emails incorrect/correct and determine if the final results reflect my performance.</li> </ul>

Functional requirements are those which describe what the system/application should do. These are the behaviour of the system not the operational requirements. See table 4 for details.

#### 4.1.2 Functional Requirements:

Table 4 - Table of Functional Requirements for Project

Num	Requirement	Acceptance Criteria
1.	The user must be able to input their name into the name field upon entering the quiz	<ul style="list-style-type: none"> <li>The user must be able to type in their name into the input field and then have their name accepted and reflected in specific and appropriate areas of the quiz.</li> </ul>
2.	Tool must display emails to user and allow them to select either "phishing" or "no phishing" as a response.	<ul style="list-style-type: none"> <li>Phishing and non-phishing buttons should be fully functional in each email. The user should be allowed to select either as an option.</li> </ul>
3.	User must be able to navigate to help page when they are stuck on the official quiz page. They should also be able to navigate away from the help page and return to the state of the quiz that they left it in prior to viewing the help page.	<ul style="list-style-type: none"> <li>User should be able to select "help" and be sent to a help page whereby they are shown explanations of how each interactive element functions.</li> <li>User should be able to select "return to quiz" and be transported back to the quiz in the state they left it in.</li> </ul>
4.	Users must be able to navigate from their current answer to their previous one. They will not be allowed to change what they have submitted but will be able to view the information on the previous page if necessary.	<ul style="list-style-type: none"> <li>User must be able to navigate to and from the email they are on using the previous and next buttons.</li> </ul>
5.	Users must be able to view results at the end of the quiz and scroll through information relating to phishing emails they have just seen.	<ul style="list-style-type: none"> <li>User must be able to view their performance based on each email after the quiz stage. They should be able to navigate back and forth these like they had done previously.</li> </ul>
6.	The user must not be able to navigate to review page until all emails have been categorised.	<ul style="list-style-type: none"> <li>The user will only be allowed to move to their final performance result webpage once they have navigated through all the emails again displaying whether they were correct or incorrect in their previous choice.</li> </ul>

## 4.2 Concept User Interface Design

In the following section, the concept interface design for the anti-phishing educational tool has been detailed. These mock-up designs have been completed in PowerPoint using their shapes features. Not all aspects such as the colour of each element is set and is subject to change upon implementation if a certain aesthetic better mimics the look of a real email inbox. Each element has been explained and depicted on the designs and justify the elements' purpose on each page. Elements that are similar on multiple interfaces have only been documented once within a design unless the function of the element changes on another interface.

### 4.2.1 Main homepage Design

**Purpose:** This homepage is required as a prerequisite for the quiz. It shall be used as a way to attain the users name for personalization purposes and to provide a brief explanation of what phishing is to help support the users initial understanding. See table 5 for justification of elements for Homepage.

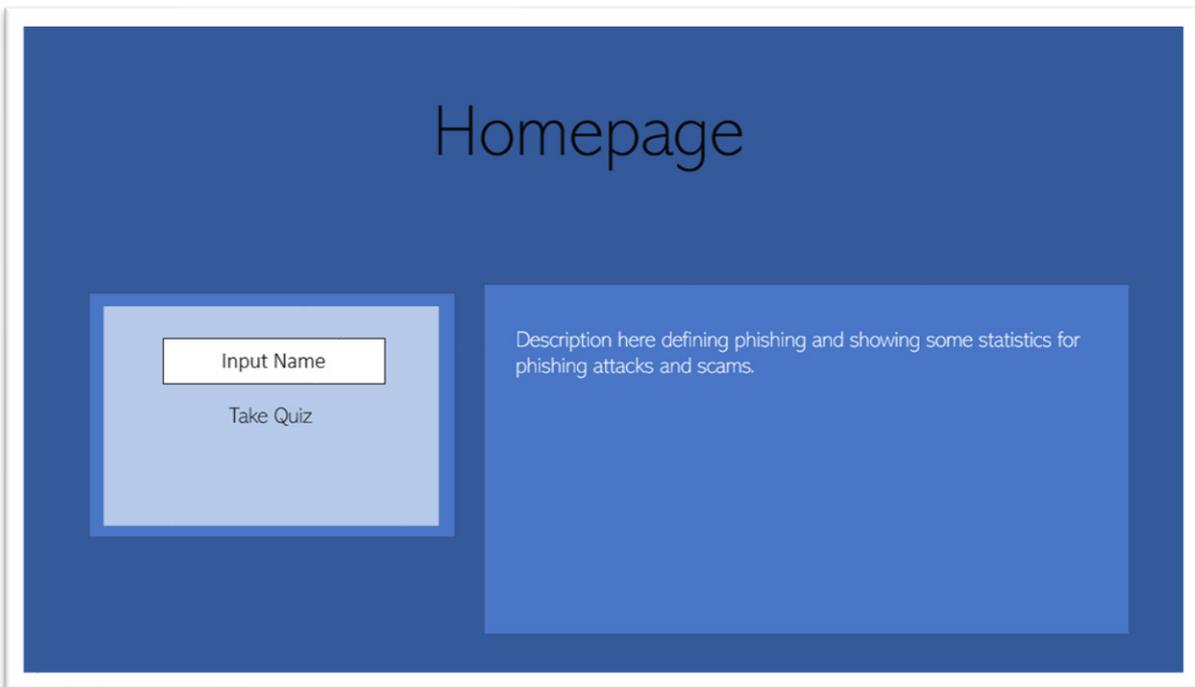


Figure 16 - Homepage Interface design

Table 5 - Design Justifications for Homepage Interface

Element	Justification
Input Name	This feature lets the user input a name in order for certain emails to contain the users name in the greeting message. The name will also be used in the "to" line within the email header. This is a personalization feature which will help simulate the user's usual inbox better. The username will not be stored in a database but in the session storage.

	Upon exiting the quiz, this name should be removed for privacy purposes.
Take Quiz button	Button to direct user to the Quiz page.
Phishing Description	Explanation of what phishing is and how it is carried out. This is to highlight to the user the subject they will be being tested on and provide a brief supporting definition of phishing for their initial understanding.

**Design Heuristic Considerations**

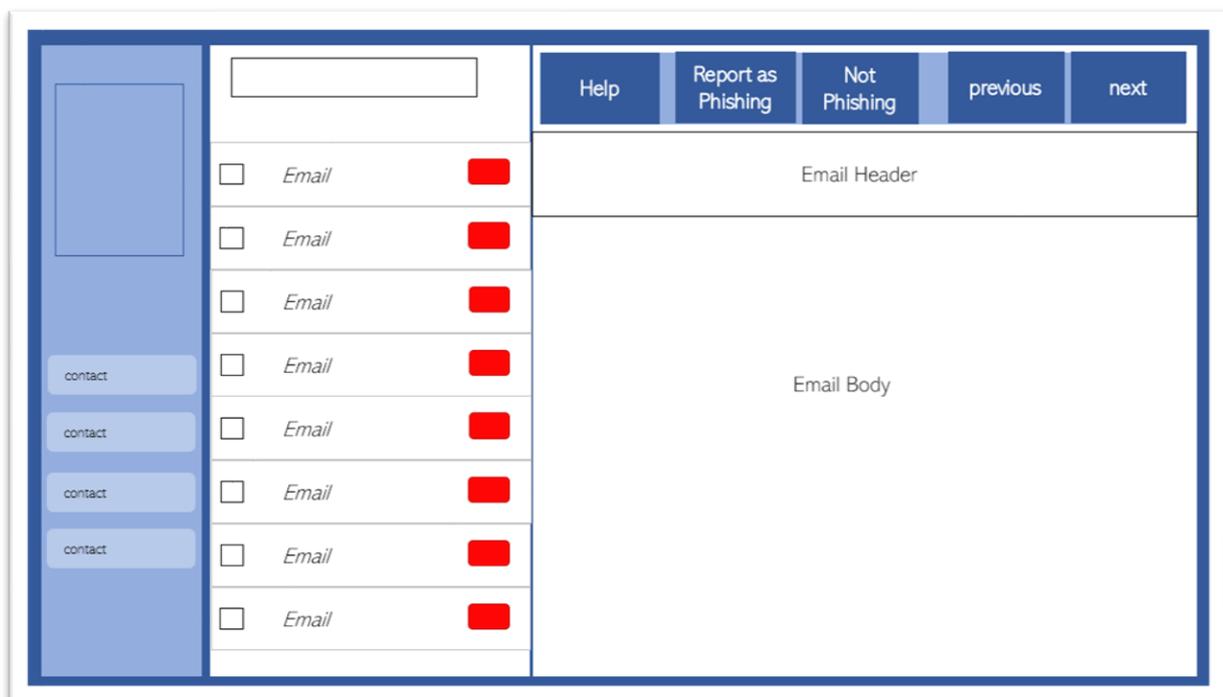
Simplistic aesthetic of the homepage design with minimal interactive elements: there are no redundant elements on this page and each element is necessary to the tools function. In addition, the number of actions a user can take is constricted with only two interactive elements being functional leaving little room for error. Likewise, all options are visible to the user aligning well with the visibility heuristic.

**Additional comments:**

Upon a user entering their name and clicking on the "take Quiz" button, the site will navigate to the main Quiz page in which they can carry out the quiz selecting either phishing or not-phishing depending on the email.

**4.2.2 Quiz page Design**

**Purpose:** This page is the foundation for the quiz. It is where each email will be displayed to the user which they will categorise by selecting either phishing or not-phishing. See table 6 for justification of elements for the quiz main page interface.



**Figure 17 - Official Quiz page Interface Design**

Table 6 - Design Justifications for Quiz main Interface

Element	Justification
Contact List	This list is located on the side bar of the interface. It is to be implemented as a pop up list whereby users can hover over each contact to view extra details about them like job position and email. As some phishing emails can look to come from peoples own trusted contacts, it is an important element to add into this simulation as it will highlight some key phishing indicators for people to remember in real life situations. These contacts will fit in with the scenario that will be explained to the user when they initially start the quiz.
Email Preview	This will show part of the email body alongside the sender's name and subject line. This element is required to further mimic the appearance of a common mailbox. This element should also be clickable in that once a user does click on it, it should then navigate that user to the email it previews. Again, this is to further emulate a mailbox to further immerse the user in the simulation. Additionally, the email previews will be written in bold and once the user selects one, this font weight will change to normal with the background also changing to a light grey. This will provide feedback to the user and show that their actions have been completed.
Email	The email content will be shown in the standard format of an email. The elements of the email will include the header, subject line, and "to" line. This area is the vital part of the tool as it will display the main email message for the user to view.
Help button	This button allows the user to navigate to a help screen which will explain how each button works and highlight where to find it. This element is useful to clarify the functionality of the tool to the users limiting frustration caused by a gap in user understanding.
Report as Phishing button	This button is one of the two options the user has for deciding whether an email shown is or isn't phishing. Once selected, the response should be stored and used to calculate the users overall score (how many emails they classified correctly or incorrectly).
Not Phishing button	Similar to the above, this button will be clicked upon by the user if they deem the email they are being shown as not phishing. Again, once clicked on, the response should be stored on top of this in order for the users total score to be calculated and presented back to them at the end of the quiz.
Previous	This button links to the previous email within the mailbox. This is another option available for users to navigate to the different emails. This type of navigational feature can be found on existing email mailboxes like Gmail and outlook, so I think it is best to apply this in the tool.
Next	Likewise to the previous button, this allows the user to proceed to the next email in the mailbox. It enables the user to traverse sequentially through the emails if they are used to doing so in real life. The

	positioning in relation to the previous button copies that of how most applications position next and previous buttons i.e. a keyboard has left and right arrows which can also be used to navigate back and forth in a text document. The buttons positioning apply the HCI principle of mapping in that its familiar positioning corresponds to its intended purpose: essentially back and forth is denoted as previous and next in this case.
New Icon	The new icon represented in this design as a red box should disappear as soon as a user clicks on a specific email. This is to provide feedback that the users action of selecting the email had been completed. It also allows the user to keep track of what emails they have observed and which they have yet to, as well as mimicking the appearance of a real life email inbox in which either an icon saying "new" will be displayed for any new emails or, the writing is bolder suggesting a new email has been received.
Check box	This is another element which will be used to provide feedback for the user. Once the user has selected an email, the box will be checked showing that their action has been completed and that they are now being shown a new email.

### Design Heuristic Considerations

A significant part about this interface is that it has been designed as a reflection of a real world mailbox and as such, this aligns with the 'match between system and real world' heuristic. Additionally, elements such as the email preview and emails themselves are designed in such a way that its functionality is intuitive to the user: as the interface reflects a mailbox they would be familiar with using, they are attuned to navigating through the emails in the way the tool is designed for navigation. Moreover, the user can clearly see the help button in the control panel which should quickly subdue any user confusion providing them with an understanding of how each button works if they are ever stuck; the help and documentation heuristic has also been adopted as part of the tool. Furthermore, the way in which this page works gives the user freedom in how they wish to navigate through the emails. They have options to either use the next and previous buttons or freely choose any email they wish in the email panel.

### Additional Comments:

For clarity purposes, the majority of the buttons for the tool are located at the top of the screen. Each element within this bar will be spaced clearly so that all buttons are clear to the user. The emails will exist all on the same webpage but be shown and hidden according to the email the user wishes to view. Once the user has completed the quiz, they should be directed to another page which shows them if they were correct or incorrect depending on their decision. This should not be done until all responses are submitted else it may influence someone's decisions. For example, if someone were to know what indicators were present on one email before they proceeded with the next, their mindset would then be attuned to look for the mentioned indicators and this may not reflect their original ability to identify phishing emails. It is desired that users complete the quiz as best they can without accidental influence or assistance so that the ending results will accurately reflect the user's abilities. The tool can then better highlight specific and correct improvement areas or knowledge gaps the user need to improve upon.

### 4.2.3 Response Submitted (Interface after phishing/non-phishing selection) Design

**Purpose:** This is the design for the interface upon a user selecting the button phishing or non-phishing. The screen should remove the phishing and non-phishing buttons and then show them a sign that their action has been saved hence, the response submitted box is displayed. See table 7 for justification of elements for the response submitted interface design.

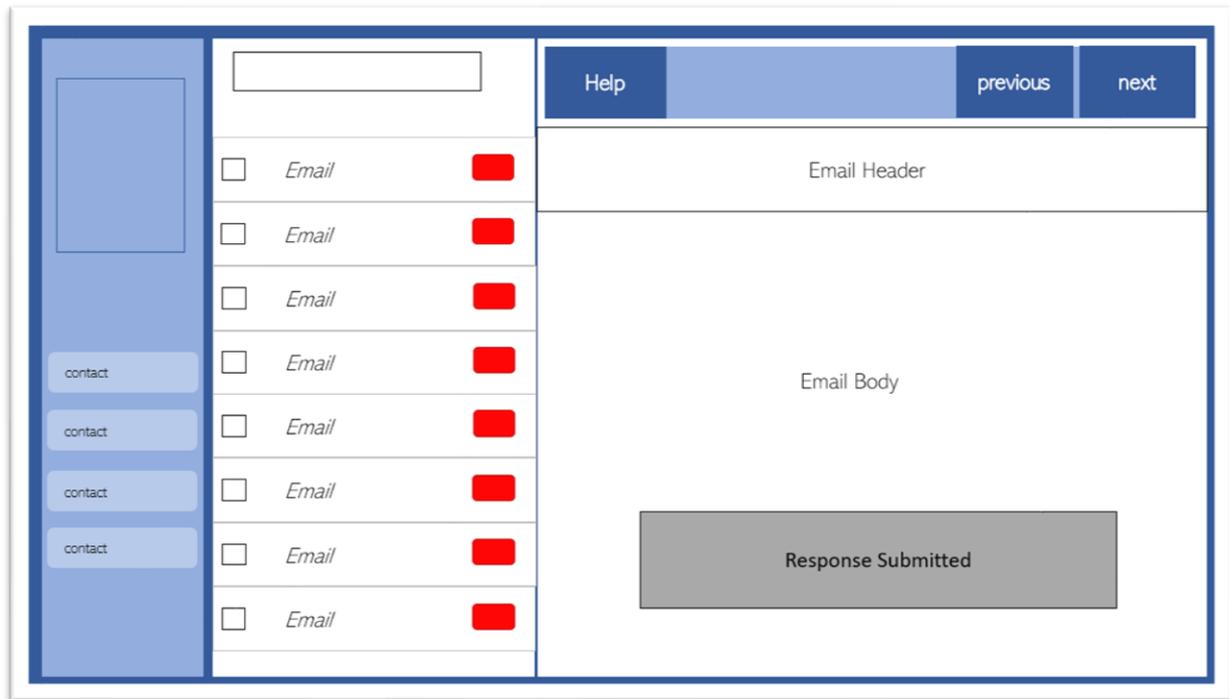


Figure 18 - Response Submitted Interface Design

Table 7 - Design Justifications for Response Submitted Interface

Element	Justification
Absent Non-phishing/phishing button	The phishing and non-phishing buttons should both be removed from the interface as it will ensure the user cannot select an option twice impacting their results.
Response Submitted text-box	The response submitted text box enables the user to clearly see that their choice and action has been recorded. This provides a feedback feature that is discussed within the design principles above.

#### Design Heuristic Considerations

The error prevention heuristic is adopted within this interface in reference to the disappearance of the phishing and not phishing buttons. This removes the user's ability to select more than one answer which if not prevented would cause problems when calculating the user's performance. As well, the feedback heuristic has been considered when design this interface as the response submitted text box is shown after they select an answer. The heuristics discussed in the previous interface designs are also reiterated here as the interface is essentially a reflection of a real world email inbox.

#### 4.2.4 Quiz Review page Correct/Incorrect Phishing Email Design

**Purpose:** below shows the design of how the interface will look upon the user finishing the quiz. This is a review stage whereby the user can traverse through the emails they categorised as phishing and non-phishing, and then see if they were correct in their decisions. See table 8 for justification of elements for the quiz review page interface.

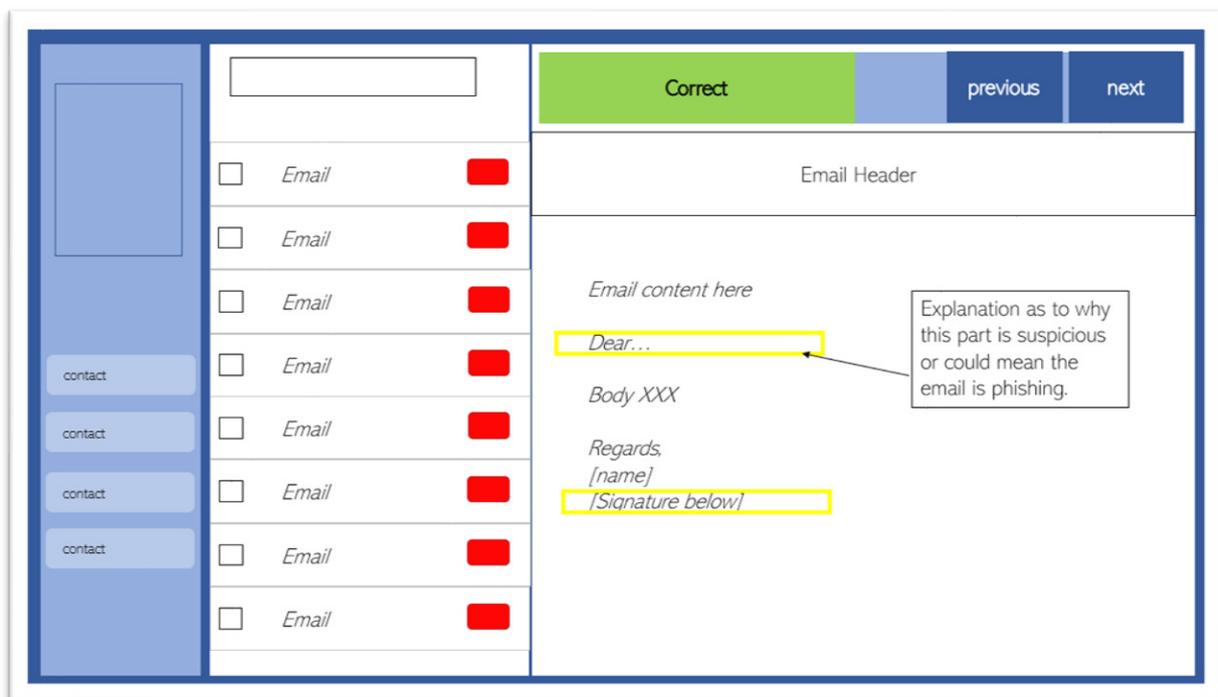
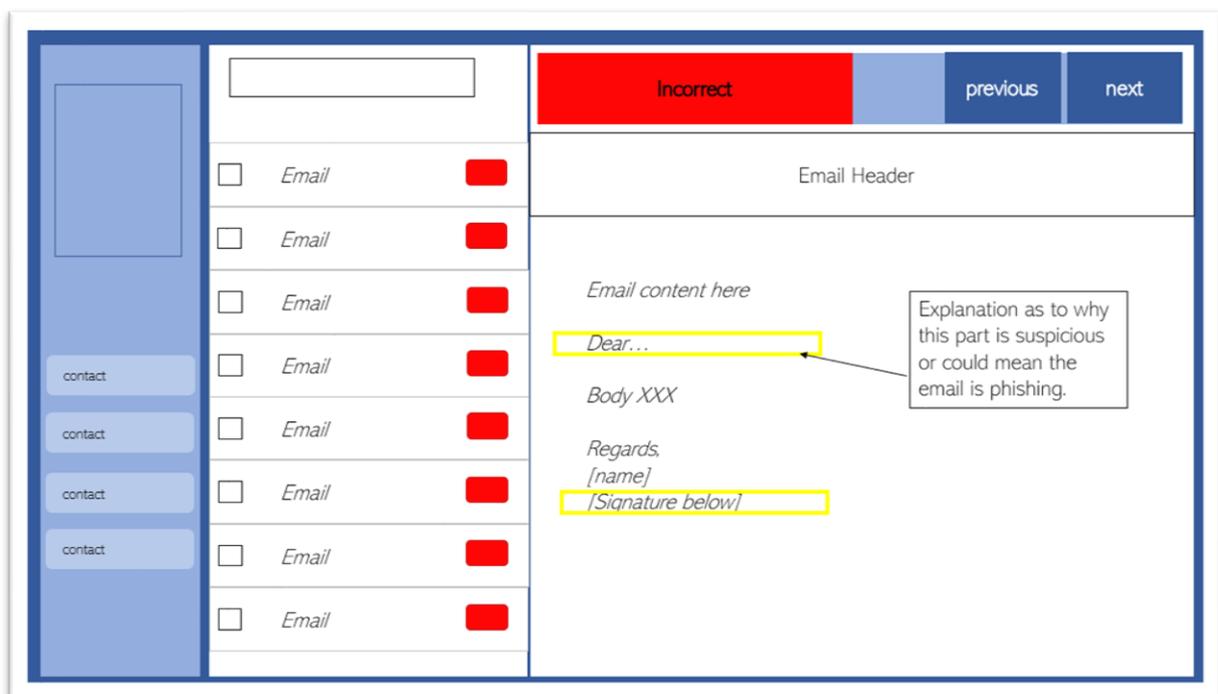


Figure 19 - Correct Answer Email Review Interface Design



**Figure 20 - Incorrect Answer Email Review Interface Design**

**Table 8 - Design Justifications for Quiz Review Interface**

Element	Justification
Incorrect/Correct Message	This box should appear in the top bar where the phishing and non-phishing buttons were. This clearly shows whether the user was correct or incorrect in their decision.
Highlight boxes	In both cases whether the user was correct or not, the areas which were indicators of phishing will be highlighted regardless. This allows the user to clearly identify the area to be aware of when identifying these types of emails in real life or confirm their original suspicions.
Explanation text box	As above, the explanation box will be given in order to explain why an area of the email is an indicator of phishing.

**Design Heuristic Considerations**

The user can recognise the control buttons 'next' and 'previous' from the previous page to immediately understand how to use them. In addition, the buttons that are no longer required are removed from the interface design in order to reduce redundancy and align with the minimalistic design heuristic. In conjunction with this, this interface is also designed to provide an initial email explaining what the user should do in order to move to the next page upon loading which provides sufficient documentation for the user to follow: this brief would likely impact the efficiency of the quiz and process as the user wouldn't require extra time in order to understand their objectives.

**Additional Comments:**

The initial email the user should be faced with is an introductory email explaining what this page is to be used for and then how to navigate to the next one. Once the user has traversed through each email and reviewed the information provided on them, a view results prompt/alert needs to appear on the screen which will navigate the user to their final statistics page. This prompt/alert should only appear once the user has gone through each email to ensure that they acknowledge each email and why specific ones have been deemed phishing.

**4.2.5 Results page Design**

**Purpose:** This page is included to show the users results at the end of the quiz. See table 9 for justification of elements for the results page interface design.



Figure 21 - Results page Interface Design

Table 9 - Design Justifications for Results Interface

Element	Justification
Incorrect/Correct percentage graph	This graph shows a visual representation of correct to incorrect answers the user gave overall. This includes both phishing and non-phishing emails to provide an overall perspective on how well the user distinguished phishing from non-phishing emails.
Phishing category percentage graph	This graph shows, for the phishing emails they could not identify correctly, which type of email they were. This is where the above defined categories are displayed: authoritative, emotive, and legal/financial. The graph should allow the user to understand what type of email they are more likely to be susceptible to and thus this awareness may help them attune their online behaviour.
Overall scores correct (num)	This is a number representation which shows how many correct answers the user gave overall. The number representation is useful in clearly defining their overall score and accommodates individuals who may not be accustomed to perceiving data on a pie chart.
Overall phishing correct score (num)	This is a number representation of how many phishing emails were correctly identified by the user. This highlights just the phishing emails so the user can have a clear image of how well they can identify these emails independently of the legitimate ones.
Phishing categories (num)	This is a number representation of how many phishing emails were incorrectly identified put into different categories. This element exists to

	support the category graph and accommodate those who many are not accustomed to perceiving data on a pie chart.
Phishing indicators Incorrect	This element shows a bar chart in which each phishing email that has been incorrectly identified Is split up into specific bars on the X axis, and the number of indicators within the email is represented in the Y axis. This allows the user to view what phishing indicators they may be overlooking and which to keep aware of in the future.
Phishing indicators Correct	Similar to the element, this bar chart shows all the phishing emails that have been correctly identified alongside how many indicators were present per email. Again, this is to bring to attention the number of indicators within each email and can be used to compare against the incorrectly identified emails to highlight focal improvement areas for the user. As well, these statistics can be used to understand if the quantity of indicators within an email can a factor be in whether a user can identify the email as phishing.
Description of Indicators found	This is a supporting text area which explains how many indicators in total (per indicator category) were found within the emails. This text area will be split into two showing supporting information for both the correct and incorrect bar charts above it. This information will also explain a brief summary of what the indicators are likely to be in a broad sense to help raise awareness of them in the future.
Return to Homepage button	This button allows the user to leave the results page and return to the main homepage.

### Design Heuristic Considerations

This page has clear documentation and explanation of each graph or visualisations presented on screen. As well, the graph/charts have been accompanied by a numerical representation of the data to accommodate a variety of users who may or may not be comfortable with interpreting data on a graph or chart. Furthermore, the number of visual representations on the screen panders to people who may just want to quickly see what their score was overall without diving deeper into any explanations or further information. This quality accommodates a variety of users who may have different times set to complete the quiz. Following on from this, the positioning of the explanations is effective and fits in with the usability heuristics as each element that is linked i.e. correct/incorrect graph and correct/incorrect textbox, is closely situated together to make it clear that the entities are related.

#### 4.2.6 Help Page Design

**Purpose:** This page enables users to get help in understanding how the quiz works and the functionality of each button. The user will be able to return to quiz at any point where they left it upon selecting the "help" button. See table 10 for justification of elements for the help page interface design

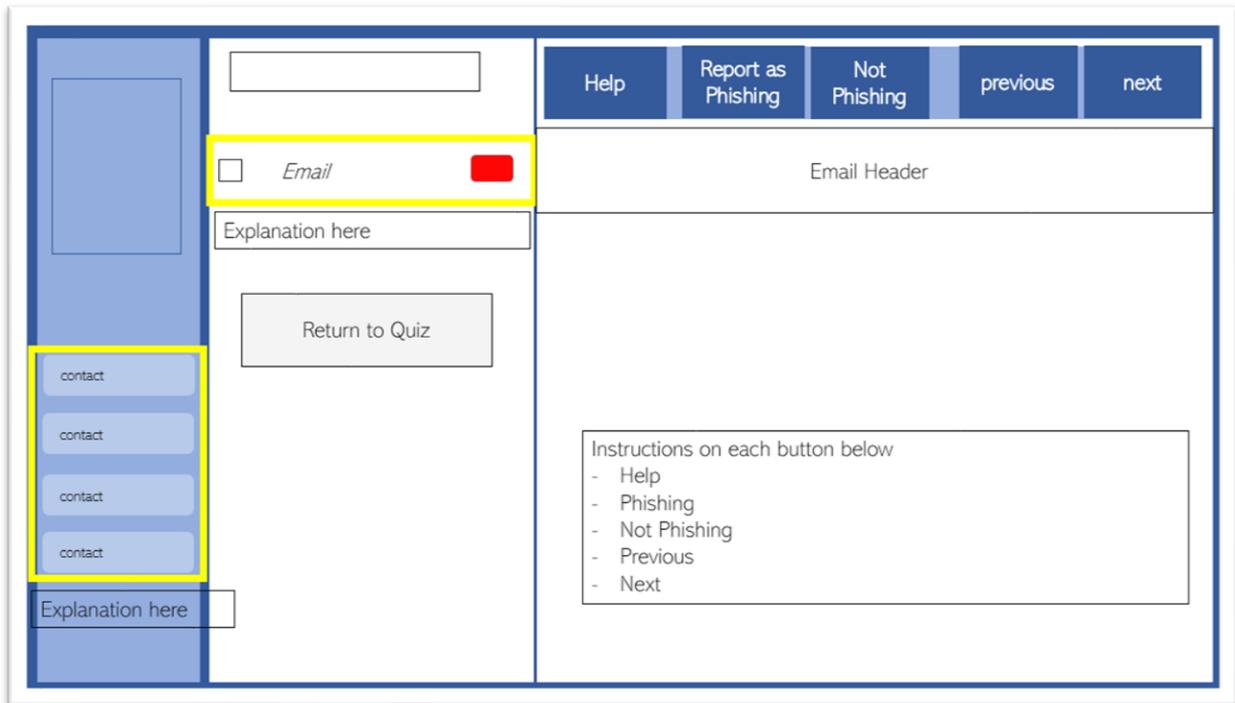


Figure 22 - Help page Interface Design

Table 10 - Design justifications for Help Interface

Element	Justification
Highlighted boxes	Boxes will appear around certain elements in order to make visible any interactive features.
Return to Quiz button	This button enables the user to return to the quiz and back to the state they left it in.
Explanation boxes	These boxes provide supporting information explaining the interactive features and how to interact with them.
Button Instruction area	This area explains each button shown in the top panel and how they work so the user can fully understand the options available to them.

### Design Heuristic Considerations

The main heuristic depicted within this design is help and documentation. The page provides sufficient information explaining how each interactive element is meant to be interacted with. Each highlighted area emphasises and clearly outlines which particular elements, aside from the control panel, is usable.

### 4.3 Design of Emails

Below I have designed the emails I will be implementing in my tool alongside their reference emails. Additionally, I have designed a scenario to support the quiz and the environment it simulates, as well as determined how many indicators will be present per email.

#### 4.3.1 The Scenario:

In order to reflect a professional workplace, and to not be bias to any specific company, a brief scenario has been developed that the user will be 'acting' in. A fictional bank was created and chosen to be the basis for the work environment called OXBanking whereby the user will be asked to act as one of their employees. There will not be a large amount of context provided in what type of job the user has or how long they have been there for as these are unnecessary details, and their absence should not affect the user's performance or tools effectiveness: an overwhelming amount of detail given within the scenario may confuse the user which will inevitably negatively impact their judgement and performance.

Alongside the scenario brief, a contact list will be provided displaying the names of trusted contacts the user can reference when looking through the emails. This is needed as some of the emails will emanate from a trusted source and as it is impossible to change the emails to actually reflect that of a user's real life contacts, creating a set that links to the scenario is a good alternative. A random name generator was used to generate some names for fake employees of the company that was created and each one was arbitrarily assigned job roles.

##### Contact list:

- Amy Palmer - Sales Executive
- Robert Walker - CEO
- Claire Pickett - Human Resources
- Andrew Graham - IT
- Kelly Reid - Customer Services.

Each of the contacts will have an email as such: firstname.lastname@OXBanking.com. This format resembles that of many business emails and subsequently is the reason the emails will be structured this way.

#### 4.3.2 The Emails:

Below details each design of the emails that are to be included within the anti-phishing educational tool. Each table identifies a reference email used to construct the email included in the tool, the category which it has been labelled under for type of phishing, as well as an explanation of indicators used per email.

Email index:

- Table 11 - Microsoft Security Alert
- Table 12 - Teams Meeting Invite
- Table 13 - IS THIS YOU scam email
- Table 14 - Message from HR
- Table 15 - Fake Charity Scam
- Table 16 - Payslip Error
- Table 17 - Message from CEO
- Table 18 - IT Company Newsletter

**Table 11 - Design for Microsoft Security Alert Phishing email**

**Email 1 - Microsoft Security Alert (Phishing)**

<p><b>Reference Email(s)</b></p>	<p>Figure 1 from page 8 (right)</p>
<p>----- Forwarded Message -----                  &gt; Subject: UPDATE EMAIL: Don't lose access to your account!!                  &gt; Date: 19 Feb 2021 05:37:51 -0800                  &gt; From: <a href="mailto:berkeley.edu@support">berkeley.edu@support</a>                  &gt;                  &gt;                  &gt; Security Notice!                  &gt;                  &gt; Dear XXXX,                  &gt;                  &gt; Our security system has detected some irregular activity connected to your                  &gt; account. you will be unable to send and recieve emails until this issue has                  &gt; been resolved                  &gt;                  &gt; CLICK HERE TO VALIDATE NOW                  &gt;                  &gt;                  &gt; To prevent further irregular activity we will restrict access to your                  &gt; account within 72 hours if you did not validate your account.                  &gt; *Note:* Mail Administrator will always keep you posted of security                  &gt; updates. Mail Admin                  &gt;                  &gt; <a href="mailto:berkeley.edu@2021">berkeley.edu@2021</a> Secured Service.                  &gt;</p>	 <p><b>Dear user,</b></p> <p>Your account is out of limits and needs to be verified for your safety</p> <p>Not verified within 24 hours? We will suspend your email account.</p> <p>Take a moment to update your account without losing your email account.</p> <p>_____</p> <p>To update and secure your email account, <a href="#">click here</a>.</p> <p>Microsoft Corporation.</p> <p>JUPDATE NOW</p>

**Figure 23 - Security Notice Berkley Phishing Example [42]**

<p><b>My Email:</b></p>	<p><b>Category:</b> Emotive</p>
<p>M &lt;@Microsfot.com&gt;</p> <p>Subject: URGENT: restore your account!</p> <hr/> <p>Dear user,</p> <p>We have noticed some iregular activity on your accountt. You will be unable to access it until this is resolved.</p> <p><a href="#">CLICK HERE TO VALIDATE NOW</a></p> <p>Failure to do so will result in <u>permanent</u> account deactivation.</p> <p>Yours Sincerely,</p> <p>Security Team</p> <div data-bbox="236 1599 699 1666" style="border: 1px solid black; padding: 5px; width: fit-content;">                 &lt;Microsoft Logo here&gt;             </div> <div data-bbox="991 1503 1369 1603" style="border: 1px solid black; padding: 5px; width: fit-content;">                 Link popup:                  \$payME12.html             </div>	

**Figure 24 - Email 1 Design**

<p><b>Indicators used</b></p>	<ul style="list-style-type: none"> <li>• <b>Language:</b> Tone of the email is very threatening. The subject line uses an exclamantion mark and the term "URGENT" to invoke panic in the recipient.</li> <li>• <b>Link &amp; attachment:</b> Suspicious link that doesn't go to a legitimate URL.</li> <li>• <b>Greeting:</b> generic user greeting.</li> </ul>
-------------------------------	---

	<ul style="list-style-type: none"> <li>• <b>Spelling &amp; Grammatical Errors:</b> incorrect spelling of Microsoft in the header and, incorrect spelling of irregular and account.</li> <li>• <b>Fake Domain/email address:</b> Microsfot.com is incorrect.</li> </ul>
<b>Additional Comments</b>	It was decided that the tool would include a security alert as a phishing email as it has been identified as a common type that many people can fall for. Since security alerts connote the feeling of unsafeness, and the email on first glance appear to emanate from a reputble company, this type of email is very effective at receiving a response.

Table 12 - Design for Teams Meeting Invite Not-Phishing email

Email 2 - Meeting Invite from Colleague (Not Phishing)	
<b>My Email:</b>	<b>Category:</b> N/A
<p>A &lt;@amy.palmer@Oxbanking.com&gt;</p> <p>Subject: FW: Sales Annual Meeting Invitation (9:00am) <span style="border: 1px solid black; padding: 2px;">Paper clip icon</span></p> <hr/> <p>Hi [user name],</p> <p>Hope you are well,</p> <p>I'm just forwarding you an email invitation for the meeting that is being held on Monday at 9:00am. Having looked over the meeting agenda I through your input would be useful.</p> <p>Please can you let me know if you can make it by accepting the invite ASAP.</p> <p>All the best,</p> <p>Amy Palmer</p> <div style="border: 1px solid black; padding: 5px; width: fit-content; margin-top: 10px;">                     &lt;Amy Signature here&gt;                 </div> <div style="border: 1px solid black; padding: 5px; width: fit-content; margin-top: 10px; position: absolute; left: 500px; top: 100px;">                     Link popup: Microsoft_Teams_Sales_invite.ics                 </div>	
<b>Indicators used</b>	N/A
<b>Additional Comments</b>	An email that is less likely to be phishing was created which included having features like the sender of the email being a trusted contact (both email addresses in the contact list and on the email match). Also a popup link that relates to the Teams meeting the email references has been inlcuded as a supporting not phsihing indicator, as well as providing an employee signature and non generic salutaion to the user. The 9:00am detail added is also another indicator that it is less likely to be phishing as this could easily be disproved by any team member in the department. When it does come to reviewing the not-phishing emails a disclaimer will however be applied explaining how in this case it is not phishing yet the user should always keep their eyes peeled for similar

Figure 25 - Email 2 Design

	looking emails showing various indicators which will be explained within the disclaimer.
--	--

Table 13 - Design for No Subject IS THIS YOU scam Phishing email

**Email 3 - No Subject Email from colleague (Phishing)**

Reference Email(s)

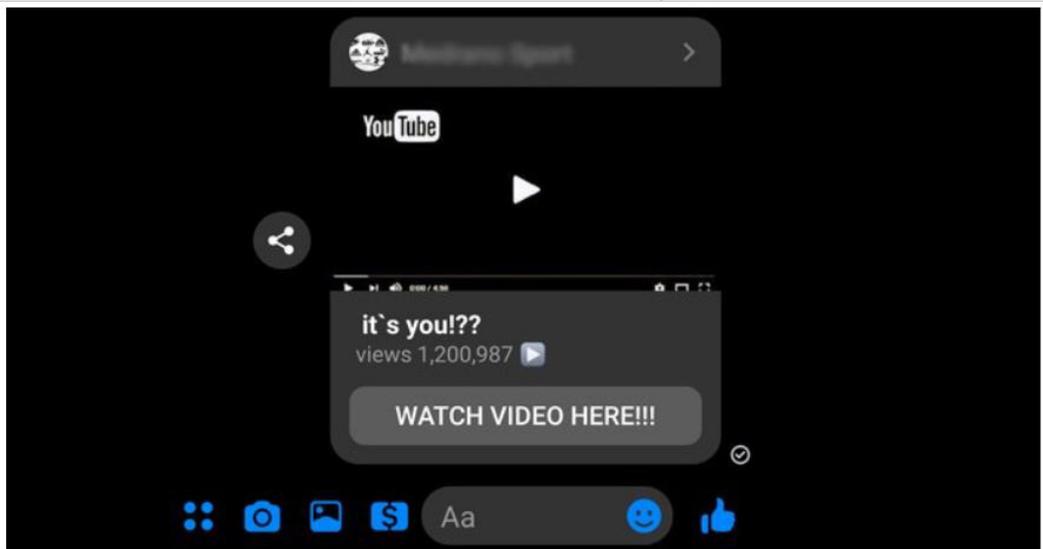


Figure 26 - YouTube IS THIS YOU scam example [26]

**My Email:** **Category:** Emotive

KR <@kelly.reid@Oxbanking.com>

Subject: No subject

[IS THIS YOU?!](#)

<Kelly Signature here>

Link popup:  
gfstsshsgebhbhe.com

Figure 27 - Email 3 Design

<b>Indicators used</b>	<ul style="list-style-type: none"> <li>• <b>Language:</b> The absence of email content/context is a red flag. Language has been identified here as an indicator through the absence of it within the body. It can also be an indicator through the "IS_THIS_YOU?!" phrase on the link as it attempt to invoke panic within the user and entice them into clicking the click to check they are not being referenced somewhere else online.</li> <li>• <b>Link &amp; attachment:</b> Suspicious link that doesn't go to a legitimate URL.</li> </ul>
------------------------	--

	<ul style="list-style-type: none"> <li> <b>Greeting:</b> Similar to Language, the absence of a greeting from a colleague is suspicious within this case. Of course, this depends on how interactions typically occur within each persons workplace but for the majority of professional interactions, an absent greeting alongside the other indicators is a red flag for phishing.         </li> </ul>
<b>Additional Comments</b>	<p>This email is a play on the IS THIS YOU! facebook scam<sup>[26]</sup>. Because of the scams prevalence within todays climate, it was important to implement a version of this within the phishing email simulation. It hopefully then can be used as a reference for people who get targetting by the social media scam enabling them to recognise the message as phishing. A part of this scam is an act of spoofing<sup>[12]</sup> whereby the message appears to emanate from a trusted source within your contact list. This factor has been used in the design of this email to have it appear as though it originates from a person within the conatcts list.</p>

**Table 14 - Design for Message from HR Phishing email**

<b>Email 4 - Message from HR (Phishing)</b>	
<b>Reference Email(s)</b>	Figure 14 from page 9
<div style="border: 1px solid #ccc; padding: 10px;"> <p>From: "HR@berkeley.edu" &lt;HR@berkeley.edu&gt;            Subject: Message from human resources            Date: April 13, 2017 at 9:29:54 PM PDT            To: XXXXX@berkeley.edu</p> <p>Dear XXXXX@berkeley.edu</p> <p>An information document has been sent to you by the Human Resources Department.</p> <p><a href="#">Click here</a> to Login to view the document. Thank you!</p> <p>Berkeley University Of California HR Department            © 2017 The Regents of the University of California. All rights reserved.</p> <p>-----</p> <p>CONFIDENTIALITY NOTICE: This email and any attachments may contain confidential information that is protected by law and is for the sole use of the individuals or entities to which it is addressed. If you are not the intended recipient, please destroying all copies of the communication and attachments. Further use, disclosure, copying, distribution of, or reliance upon the contents of this email and attachments is strictly prohibited.</p> </div>	
<b>My Email:</b>	<b>Category:</b> Legal/Financial

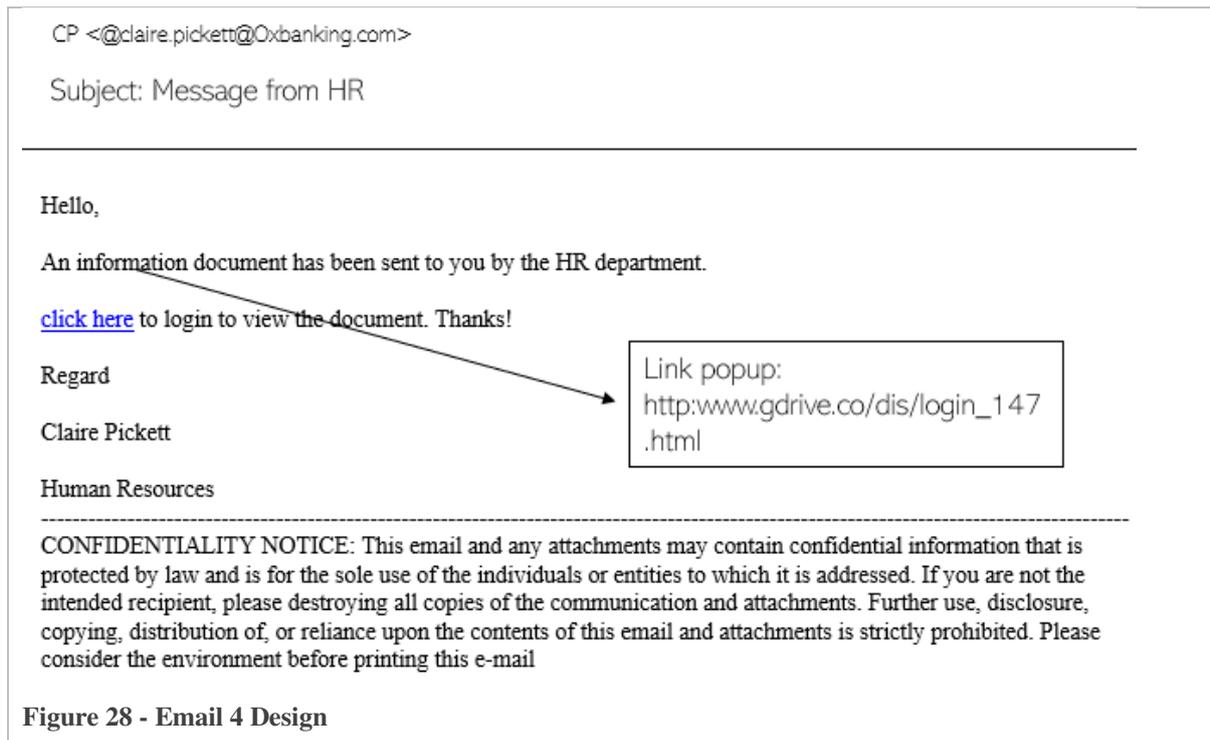
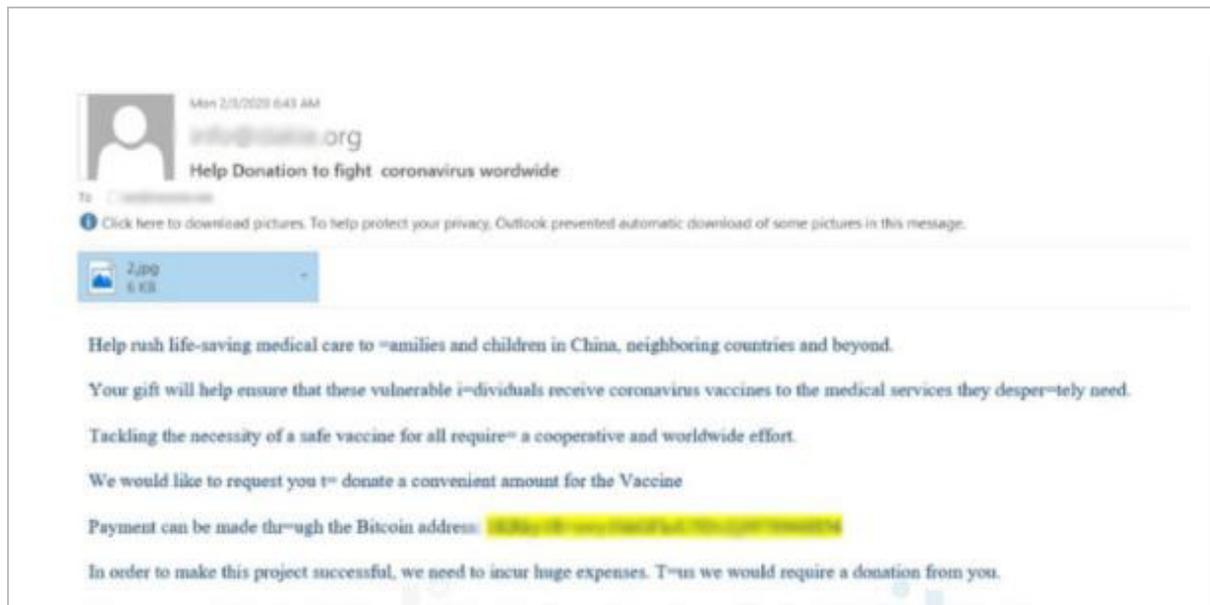


Figure 28 - Email 4 Design

<b>Indicators used</b>	<ul style="list-style-type: none"> <li>• <b>Language:</b> Language is very professional but vague and doesn't provide much context into what document the user is receiving.</li> <li>• <b>Link &amp; attachment:</b> Suspicious link that doesn't go to a legitimate URL. There is an partial top level domain (drive.co) which is suspicious as legitimate links aren't shaped this way.</li> <li>• <b>Greeting:</b> There is a generic greeting that would be unusual for colleagues communicating within a workplace.</li> </ul>
<b>Additional Comments</b>	<p>This email is one of the sophisticated emails as it uses some convincing techniques to fool the user. Not only does it spoof the sender, it also uses a confidentiality notice which is not typically considered as an element that would appear in a phishing email. This email is useful as it allows user to attune themselves into identifying factors of a phishing email that indicate its nature and not be misled by the convincing elements.</p>

Table 15 - Design for Charity Scam Phishing email

Email 5 - Charity Scam (Phishing)	
<b>Reference Email(s)</b>	Figure 3 from page 8



**My Email:**

**Category:** Emotive

LG <mailing.list\_OLifeOfGivingFoundation@gmail.com>

Subject: Your donation could help save a life!

For 30 years we have been helping to save lives through your donations but we still have a way to go! Your support and kindness will help people give vulnerable children the support and care they desperately need during these unforgivable times. To help save a life today follow the link below to donate. We thank you greatly for your kindness.

Save a life today!

Donate

Link popup:  
http://give.pc.com

If you wish to not receive further emails please [unsubscribe](#) by clicking unsubscribe.

Link popup:  
http://webpages.org/cas/ltd/paypal.com

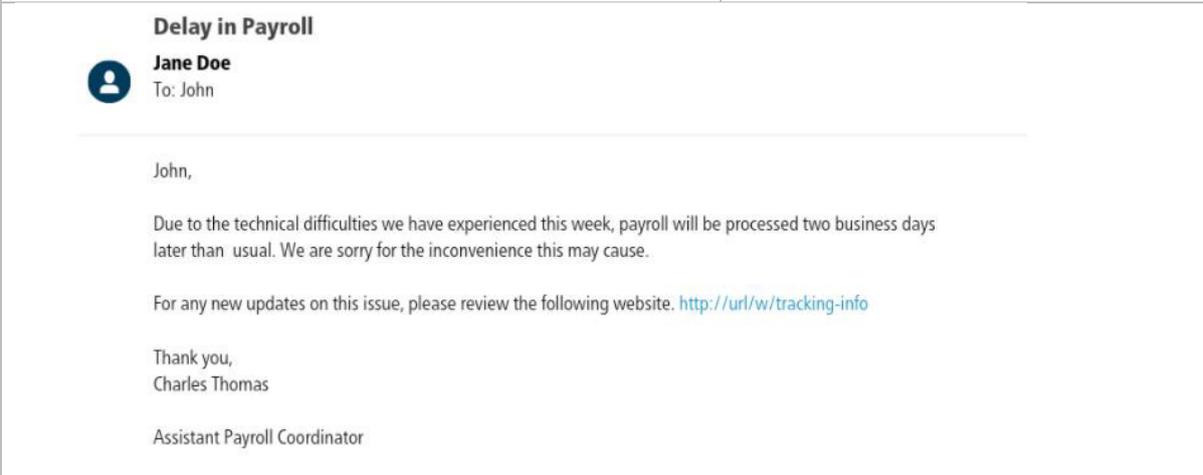
Figure 29 - Email 5 Design

**Indicators used**

- **Language:** Language is very vague and doesn't provide much context into what charity is or does.
- **Link & attachment:** Suspicious links that don't go to a legitimate URL. One goes to a paypal account which doesn't match an unmailing list and the other goes to an insecure link that again does not reflect the website of the "lifeOfGivingFoundation" charity.

	<ul style="list-style-type: none"> <li>• <b>Fake Domain/email address:</b> Legitimate companies will typically not send emails out to people under a gmail account.</li> </ul>
<b>Additional Comments</b>	<p>A fake charity was created for this email which attempts to draw the recipient in by pulling on their proverbial heartstrings. Essentially, this email attempts to invoke an emotional response from the recipient to make them feel as though they have an obligation to help the children referenced within the charity summary. Whilst this type of email is likely to be blocked by a company's anti-phishing software, it is important to emphasize the significance emotion plays within phishing attacks and as such, display this to a user. This email differs from the other emotional emails by trying to invoke a sense of sadness or sympathy as opposed to shock and panic. It is essential to implement this email type due to this difference in order to cover a wider set of emotions invoked by phishing emails.</p>

Table 16 - Design for Payslip Error Phishing email

Email 6 - Payslip error (Phishing)	
<b>Reference Email(s)</b>	Figure 6 from page 10 (bottom)
 <p><b>Delay in Payroll</b>  <b>Jane Doe</b>          To: John</p> <p>John,</p> <p>Due to the technical difficulties we have experienced this week, payroll will be processed two business days later than usual. We are sorry for the inconvenience this may cause.</p> <p>For any new updates on this issue, please review the following website. <a href="http://url/w/tracking-info">http://url/w/tracking-info</a></p> <p>Thank you,          Charles Thomas</p> <p>Assistant Payroll Coordinator</p>	
<p><b>Figure 30 - Delay in Payroll Phishing Example [44]</b></p>  <p>From: <b>GlobalPay &lt;VT@globalpay.com&gt;</b>  <span style="float: right;">Hide</span>          Subject: Restore your account          Date: February 7, 2014 3:47:02 AM MST          To: David</p> <p style="text-align: right;">1 Attachment, 7 KB <span>Save</span> <span>Quick Look</span></p> <p>Dear customer,</p> <p>We regret to inform you that your account has been restricted.          To continue using our services please download the file attached to this e-mail and update your login information.</p> <p>© GlobalPaymentsInc</p> <p>  <a href="#">update2816.html (7 KB)</a></p>	
<b>My Email:</b>	<b>Category:</b> Legal/Financial

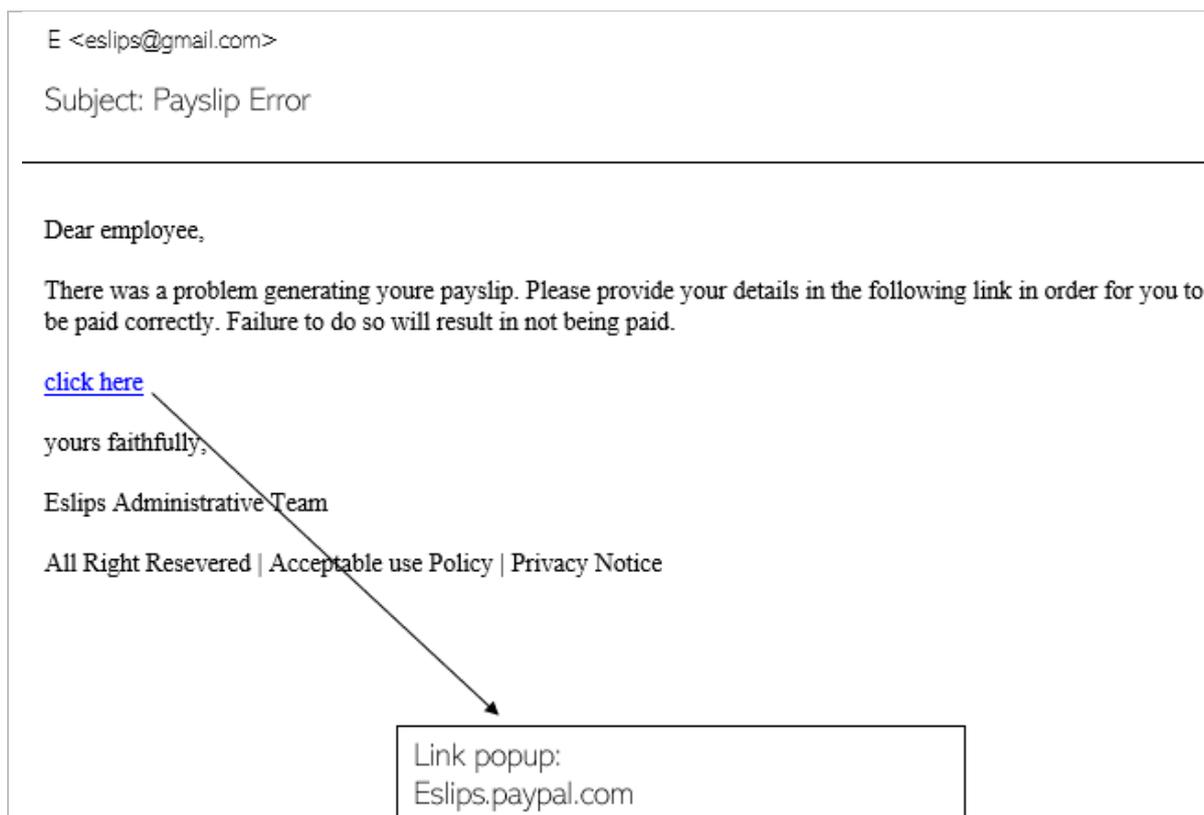


Figure 31 - Email 6 Design

<p><b>Indicators used</b></p>	<ul style="list-style-type: none"> <li>• <b>Link &amp; attachment:</b> Suspicious link that goes to a random paypal account.</li> <li>• <b>Grammatical and Spelling Errors:</b> There is grammatical errors present within the body of the email (reserved and you're is spelt incorrectly). As well, the sentence does not flow well not reflecting the professional emails you'd expect to receive from a payslip company.</li> <li>• <b>Fake Domain/email address:</b> Legitimate companies will typically not send emails out to people under a gmail account.</li> <li>• <b>Greeting:</b> The greeting is very generic which wouldn't be usual for a payslip company contacting an employee.</li> </ul>
<p><b>Additional Comments</b></p>	<p>This email attempts to utilize the reputation of a fictional payslip company in order to convince users of its legitimacy. This email is written similar to the Microsoft security alert email as it could enable the tool to provide an insight into whether the financial aspect/entity of the email would be more of a convincing factor than one that lacks this but is similar in structure.</p>

Table 17 - Design for Message from CEO Phishing email

<p><b>Email 7 - Message from CEO email (Phishing)</b></p>	
<p><b>Reference Email(s)</b></p>	<p>Figure 7 from page 11</p>

<p><b>From:</b> Your Boss &lt;yourboss@fakeyourcompany.com&gt;  <b>Sent:</b> 09 October 2018 11:06  <b>To:</b> Your Company Finance &lt;finance@yourcompany.com&gt;  <b>Subject:</b> IMPORTANT: Fund Transfer Done Today</p> <p>Hi Gwen,</p> <p>Could you do me a favour? There's a pending invoice from one of our providers and because I'm on holiday I need you to take care of it for me because I can't access the accounts from here. They contacted me and I told them to send through the email to you as well (check spam filter incase it's accidentally blocked!) Just click on the link in their email and transfer the amount to the account they specify.</p> <p>This needs to be done TODAY so make it high priority.</p> <p>If you do this for me it would be a huge favour.</p> <p>Any questions then reply to this email. I can't take calls right now so just stick to replying to this email.</p> <p>Thanks, Your Boss</p>	
<b>My Email:</b>	<b>Category:</b> Authoritative
<p>RW &lt;robert.walker@OXbanking.com&gt;</p> <p>Subject: IMPORTANT: Transfer Needed TODAY</p> <hr/> <p>Hi [user name],</p> <p>I need you to do me a favour. There is a pending invoice to one of our providers and as i am on holiday i cannot access the accounts from here. I have told them to send through their email to you with their account link and the amount of money they require (check spam folder in case accidentally blocked!). Just click on link in their email and transfer the amount they have requested.</p> <p>This needs to be done TODAY as a high priority.</p> <p>Any questions, please reply to this email. I cannot take calls right now so reply to the email instead.</p> <p>Thanks,</p> <p>Robert Walker</p>	
<b>Indicators used</b>	<ul style="list-style-type: none"> <li>• <b>Language:</b> Language is very vague and doesn't provide much context into what the provider is that the sender is referring to. Additionally, it is very informal for how you would expect a CEO to be communicating to an employee. The language used also is an attempt to invoke panic from the recipient by capitalising words like "IMPORTANT" and "TODAY" to emit a sense of urgency.</li> <li>• <b>Fake Domain/email address:</b> The sender address is similar to the email address of the legitimate sender in the person's contact list however, the banking.com part of the address has an extra n in. This element is not noticeable on first glance so requires users to properly examine the email contents and be aware of subtleties like this.</li> </ul>
<b>Additional Comments</b>	<p>This email is the only authoritative email that will be implemented in the tool. This uses the reputation of a CEO to get people to respond and it is useful to include in the tool due to this aspect. This email inclusion ensures people are aware that just because the sender appears to be a credible and reputable source does not mean it is legitimate. It is also useful as it does not have a link or attachment present. In conjunction, it is necessary to have this</p>

	email structured as such to highlight that certain emails can be prefaces for additional phishing emails: this is a sophisticated method in decieving the recipient and one that will be highlighted with its inclusion within the tool.
--	--

Table 18 - Design for IT Company Newsletter Not-Phishing email

Email 8 - IT Company Newsletter (Not Phishing)	
<b>My Email:</b>	<b>Category:</b> N/A
<div style="border: 1px solid black; padding: 10px;"> <p>AG &lt;andrew.graham@OXbanking.com&gt;</p> <p>Subject: Annual IT Newsletter Available!</p> <hr/> <p>Hi all,</p> <p>A quick reminder that the annual IT newsletter is now available. I think its really important everyone reads it to find out the latest IT news. You can either access the newsletter <a href="#">here</a> or pick a copy up at the front desk.</p> <p>Happy reading!</p> <p>Kind Regards,</p> <p>Andy</p> <div style="text-align: center; margin-top: 20px;">  <div style="border: 1px solid black; padding: 5px; display: inline-block;">                     Link popup:  <a href="http://OXbanking/Newsletters/IT.sharepoint.com">http://OXbanking/Newsletters/IT.sharepoint.com</a> </div> </div> </div>	
<b>Figure 33 - Email 8 Design</b>	
<b>Indicators used</b>	N/A
<b>Additional Comments</b>	This email is the second of the two non-phishing emails. The aim here was to try and use an email that contained a link to highlight how some links will match the site it is likely to be from. The link that will be used is directing users to the company sharepoint where the IT annual newsletters reside. The URL looks correct and the message also contains another indication that this email is likely to be legitimate. This feature is the area in which the sender says "pick a copy up at the front desk", a phrase which would unlikely be used in a phishing email as it is easily disproved if not real.

#### 4.4 Cite Map

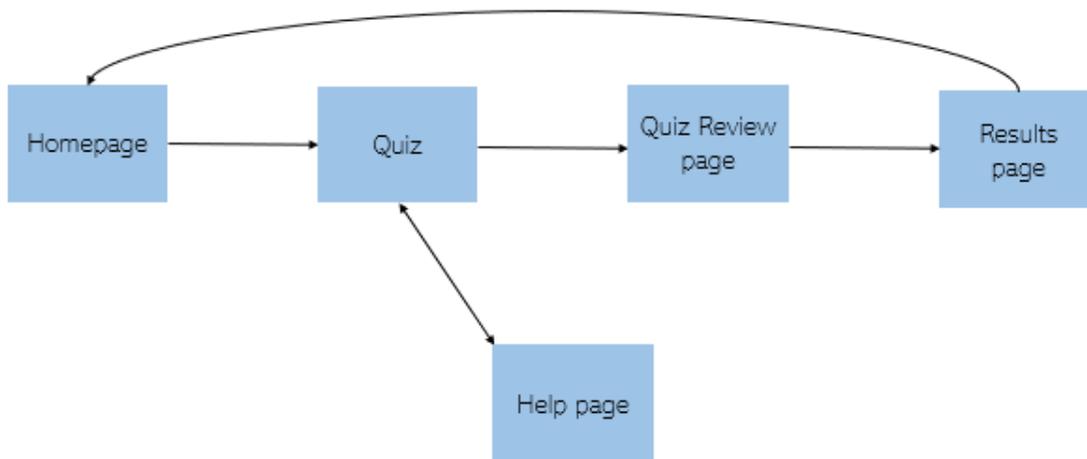


Figure 34 - Cite Map Showing Connectivity between Webpages

Above is a simple structure of the webpages that will exist within the tool. The arrows indicate linking webpages. Where an arrow is pointing in both directions it means that the user will be able to traverse to and from a specific page else, if the arrow is depicted only pointing in one direction, this means that the user can only navigate from a certain page to the succeeding one. In the above diagram, the user is only able to navigate to and from the help page whilst on the official quiz page, as at that stage it is important the user is able to get assistance with the tool so they can complete the quiz accurately. The user's journey will progress thusly:

- The user will begin at the homepage where they will input their name into a name field and select "take quiz"
- The user will then complete the quiz deciding whether an email shown to them is phishing or not phishing; once this has been completed
- The user will be prompted with an alert which navigates them to the quiz review page where they will traverse through the emails they had observed prior, and see if they were correct/incorrect in their decisions
- Finally, the user will navigate to the results page where they will be able to view their statistics and performance and reminded about the indicators that help in identifying phishing emails.
  - The final page will have a "return home" button whereby the user can navigate back to the homepage when they are finished with the tool.

#### 4.5 Risk Assessment

Before implementation, a few risks were documented that could occur during implementation of the tool. This is so preparation could take place for any eventuality that may negatively impact the projects progression and have a mitigation technique ready to be actioned in these cases. This will hopefully aid in allowing me to complete the project to the best of my abilities with little setbacks. Below this set of potential risks have been documented:

Risk	Risk Severity	Likelihood	Mitigation Action
Illness affecting timeline of tasks and their completion	Medium	Medium	Ensure there is plenty of time to complete specific sections of the tool to accommodate unforeseen spells of illness
Change in project scope	High	Low	continuous reviews and documentation required in order to keep track of work and progress. Document challenges so that any changes are dealt with and managed effectively.
Data loss	High	Low	Continuous backups of data to be done at frequent intervals. Save data on two platforms both on laptop and in the cloud so it is accessible in one area if another becomes inactive.
Limited background knowledge of using JavaScript to implement an educational tool	Medium	High	Additional times has been given for implementation of the tool in order to accommodate for any experimental stages of designing the tool using JavaScript allowing me to familiarise myself with the language.
unexpected obligations interrupting the initial workflow timeline	Medium	Medium	Additional time has been provisioned in order to accommodate for any unexpected events that may remove myself from the project for a period of time. This includes academic work obligations as well as external work responsibilities that may temporarily impede my ability to complete certain tasks in the desired timeframe.

## 5 Implementation

The following section will specify how the tool has been implemented. Here the main functionalities of the tool have been explained and highlight how the critical interactive elements work in accordance with the tool's main objective. Any challenges that have occurred during the implementation phase of my project have been detailed, alongside any remediation methods or alterations that have been made to overcome them.

To ensure I developed and practiced by coding skills through this project, I tried my best to keep to best coding practices. This meant that as the coding commenced attention would be given to the following guidelines: use comments to define each section of code so each section's purpose was known, keep code clean through clear formatting ensuring elements that belonged inside specific tags were indented correctly within the tag, try to reduce duplicating code where possible and instead attempt to create functions which similar actions could call from, and try to give appropriate names to variables within my code. The last goal, however, was harder to achieve as when more of the tool was implemented the number of variables being used grew in relation to make certain elements function. This led to some variable names being less refined than others and is an area that needs to be addressed in future practices. During the project, a clean file structure was maintained in that certain elements of the project were organised in separate folders: images used were kept in an image folder, the stylesheet enclosed in a CSS folder, the JavaScript file contained within a script folder, and all other HTML pages that made up the tool were kept in a main application folder. This ensured that all important documents for the project were centralised and easy to locate thereby minimizing time spent finding and working on them.

## 5.1 Homepage

Below are screenshots of the final implementation of the homepage to the tool. This section was the easiest to code in comparison to the other pages however, changes were made to the design partially upon implementation. This change is discussed further below.



Figure 36 - Homepage after Implementation

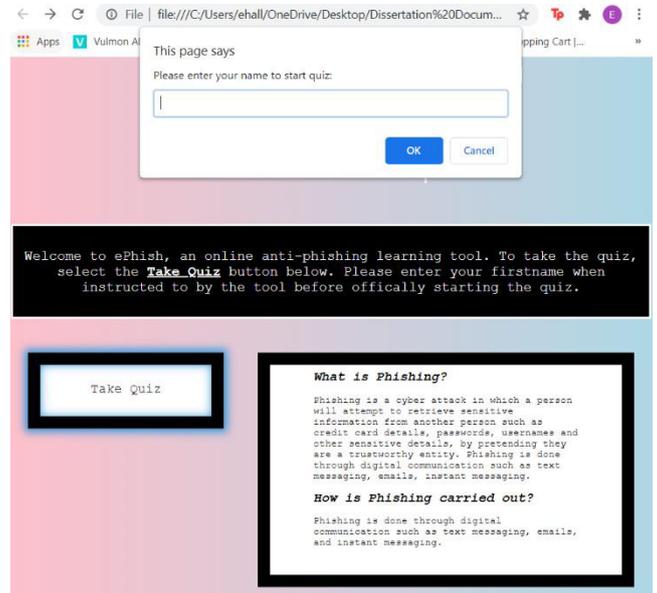


Figure 35 - Homepage displaying Input Name alert

### 5.1.1 Username input

In order for the user to input their name into the tool, and it be inserted into specific areas of the HTML page that displays the main quiz, an alert box was used that requests the user to input a name upon selecting the "take Quiz" button. Implementation of this capability using as a standard input box, as originally designed within the webpage, proved difficult as the username would not save in session storage once It had been validated in a JavaScript form. Subsequently, an alert box was used as an alternative approach which was easier to implement and that appears once the user has selected the mentioned quiz button: this allowed the name to be saved in the session as desired and used in the show\_name() function explained below. Saving the name to session storage meant that once the browser is closed or upon the user returning back to the homepage, the storage would be cleared ensuring no identifiable information about the user was kept on the system. In figure 37, you can see that I have used appropriate prompts to let the user know they need to input a name within the input box displayed.

```

function name_input() {
  var txt;
  var person = prompt("Please enter your name to start quiz:", );
  sessionStorage.setItem(person_temp, person);
  if (person == null || person == "" ) {
    document.location = "Main.html";
  } else {
    document.location = "Quiz.html";
  }
}

// Show user name in boxes

function show_name(){
  var test = sessionStorage.getItem(person_temp)
  var y = document.getElementsByClassName("person_name");
  var i;
  for (i = 0; i < y.length; i++) {
    y[i].innerHTML = test;
  }
}

```

Figure 37 - Screenshot of Code for Inputting name into Tool

The show\_name() function is called using an "onload" parameter within the body of the quiz page. Upon the quiz loading, the name of the user is extracted from the session storage and inputted into any tag that has been classified as "person\_name" using the innerHTML property. This allowed the user's name to be inserted in a variety of areas within the tool all at once i.e. an email greeting that reads "Hi [username],".

## 5.2 Quiz Page

The quiz page was a little harder to implement during the implementation phase. Originally the concept of having each email on a separate page was experimented with however, this method was found to be more complex when it came to interlinking various elements across different HTML pages. In addition, having multiple pages for each email was thought to most likely result in having an exceptional amount of duplicated code that would be required across the tool which was not considered as part of the best coding practices.

Subsequently, it was decided that all emails within the quiz would interchange on the same page. This meant that JavaScript needed to be used to manipulate the DOM (Document Object Model) objects using style properties to hide and display them depending on desired state of the quiz. Unexpectedly, this section took a significant time to test as in order to ensure the elements appeared and disappeared accordingly, each email needed to be continuously selected and deselected to check that the function at the time worked appropriately. In conjunction, a non-functional requirement of the tool surrounded the need for each element on the screen needed to fit into various window sizes. This area also took a while to implement as the window needed to be resized every time a new element was added into the webpage, or altered in anyway, in order to ensure it resized appropriately. In order to do this the display property was used within the CSS stylesheet to display the majority of elements within a "flex" container. This meant that the elements would resize upon changes to the window sizes. As well, the unit "vw" (viewport width) was used when assigning width and height to various objects which also contributed to the tool's effective scalability. Figures 39 & 40 display the layout used to recreate the image of a typical email inbox which was constructed using the example mailbox design references identified in the research area. Figure 39 also shows the scenario and instructions email that the user is shown on initial entry of the webpage, and figure 40 depicts the style and implementation of email 1: a Microsoft security alert phishing email. To see a preview of the rest of the emails please see Appendix A-G.

```
.body_container{
display: flex;
flex-direction: column;
}
```

Figure 38 - CSS snippet showing flex property to scale DOM objects

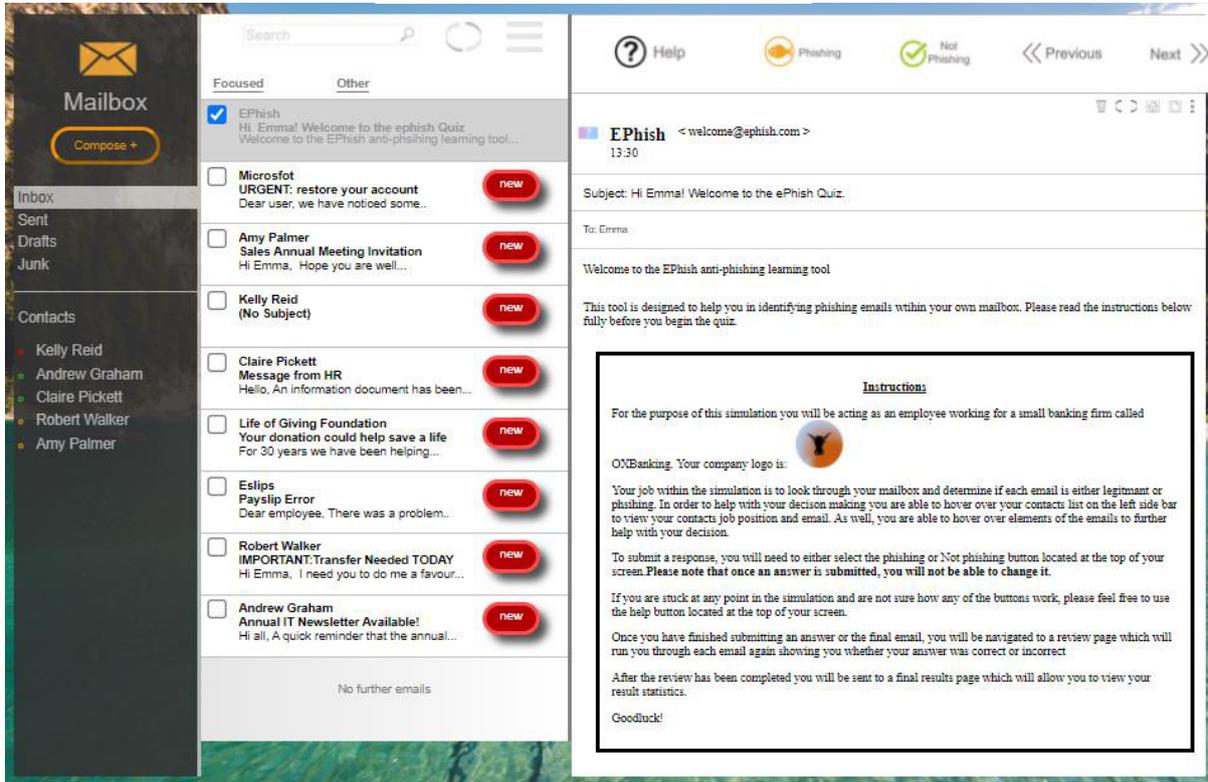


Figure 39 - Quiz Page after Implementation

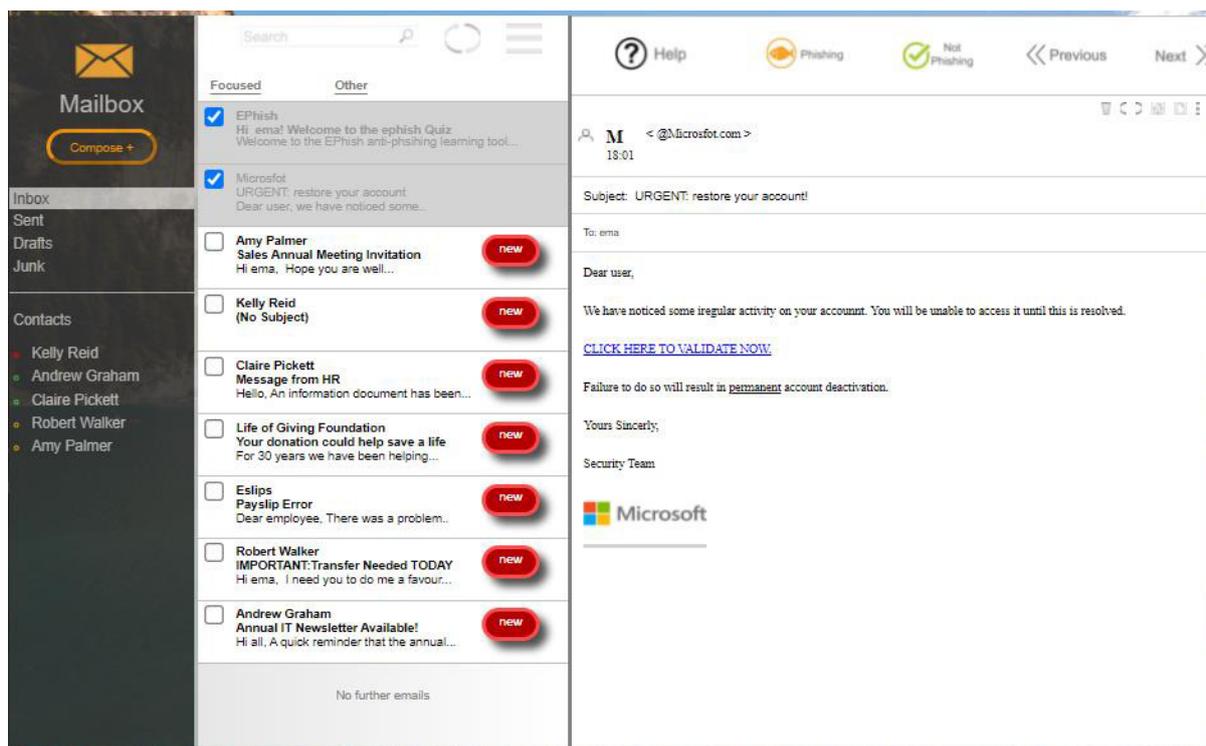


Figure 40 - Quiz page Email 1 Layout

In order to make add into the design certain images like the fake search bar and the icons situated next to it, as well as the icons on top of the email header, Microsoft PowerPoint was used. With the program, the shapes tool was utilized to create and sculpt the aforementioned elements changing their colour, size and position to emulate elements found on a standard email inbox. Additionally, a fake company logo and signature for certain employees was created for the tool in the same way using PowerPoint. You can see the logo that was created displayed within figure 39 and employees' signature which is shown in emails 2 and 3 displayed in Appendix A and B. The images which could not be created on PowerPoint such as the Microsoft logo was simply found on google and referenced within the code.

### 5.2.1 Email Changes

This section details the implementation of how the emails changed in and out of view depending on which email the user clicks on. As all emails follow the same structure in relation to how they interchange on screen, only a snippet of code has been displayed below that shows how one email changes. When a user clicks on a specific email, or selects the "next" button on screen, the function email() is called.

```
function email(email, head, preview, check, icon, id, nav){
    document.getElementById(email).style.display = 'initial';
    document.getElementById(head).style.color='#999999';
    document.getElementById(head).style.fontWeight='normal';
    document.getElementById(preview).style.color='#999999';
    document.getElementById(preview).style.fontWeight='normal';
    document.getElementById(id).style.background='lightgrey';
    document.getElementById(check).checked = "checked";
    document.getElementById(icon).style.visibility = 'hidden';

    var elems = document.getElementsByClassName('navigation');
    for (var i=0;i<elems.length;i+=1){
        elems[i].style.display = 'none';
    }

    document.getElementById(nav).style.display = 'initial';
}
```

Figure 41 - Screenshot of JavaScript code used to interchange emails on quiz page

This function requires specific parameters to work and as such, each email calling the function has different parameters affixed to it. For example, email 1 (which I have named in accordance with the email 1 design depicted in the above design specification section) has the parameters displayed in figure 41 set to the email function.

```

<!-- first_email -->
<div id="email1" class="email" onclick="email('First_email_content', 'head1
', 'preview1', 'check1', 'new_1', 'email1', 'email_1')">
<input id="check1" type="checkbox" class="check">
<div class="container">
  <p id="head1" class="header">Microsfot<br>URGENT: restore your
  account
  </p>
  <p id="preview1" class="preview">Dear user, we have noticed some..
  </p>
</div>
<div id="new_1" class="new_icon"><span class="new">new</span></div>
</div>

```

Figure 42 - HTML code used to interchange emails on quiz page

As you can see, various elements have been assigned that belong to email 1 a number 1 to their id name. This method has been repeated in the succeeding emails in which the parameters have the same number applied on the end of their names in order to maintain some consistency in the code. Here the DOM objects are being manipulated within JavaScript to change the appearance of the elements onclick of the main email preview object. Each element id that is being passed into the function is being altered for instance, the preview section of the email on the middle panel, changes background colour to light grey and the font weight becomes normal instead of bold. The code shown in figure 39 is used to show the email through making the element classed as "navigation" visible using the "initial" styling feature. The function iterates through each of the emails defined within a container called "navigation" and hides all but the email that is specified after the loop referred to by the parameter "nav".

### 5.2.2 Phishing and Not Phishing categorisation & classification

To be able to calculate whether a user categorised each email as phishing/not phishing correctly, the functions depicted in figures 43 and 44 have been used. As a subsidiary aim of the implementation phase was to keep to best coding practices, two separate functions were used to calculate whether the user was correct or incorrect depending on their answer. This was to minimize code repetition hence the quantity of parameters needed within the function: this means that instead of the function being replicated 8 times to suite each email, the HTML code can simply change the parameter values for each email which reduces code repetition. Figure 42 shows the function that is used to set a user's answer to correct and works for all emails including those that are not phishing. However, in order to calculate a total summary of phishing emails that have been correctly identified, an additional parameter is required in the function that increments the variable p\_correct (representing correct phishing emails) if a value is passed through it. As you can see in figure 46 email 1 is phishing and therefore if a user selects the phishing button, the value correct will be passed through the phish\_correct parameter. For emails that are not phishing, no value is passed through the parameter and is therefore identified as a null value which does not get counted in the total number of phishing emails correctly identified calculation. This feature enables users to establish how well they identified phishing emails independently of the entire email set.

```
function phish_correct(pid, npid, response, email_correct_id, email_incorrect_id, hb_correct, phish_correct){
    correct++;
    if(phish_correct!=null){p_correct++;}

    document.getElementById(pid).style.visibility = 'hidden';
    document.getElementById(npid).style.visibility = 'hidden';
    document.getElementById(response).style.display = 'initial';
    sessionStorage.setItem(email_correct_id, JSON.stringify(1));
    sessionStorage.setItem(email_incorrect_id, JSON.stringify(0));
    sessionStorage.setItem(hb_correct, JSON.stringify(1));

    // set correct
    if (correct+Incorrect == 8){
        show_stats();}
}

```

Figure 43 - Screenshot of code which counts answer as correct

The parameters which are taken in include: the pid and npid which are id's of the phishing and not phishing buttons specific to each email that get hidden upon being selected by a user, the response text box which is shown when the user submits their answer by clicking a preferred button, the email\_correct\_id and the email\_incorrect\_id which are set to either 1 or 0 depending on whether the user's response is correct or not, the hb\_correct parameter which likewise is set to either 1 or 0 depending on the users response, and finally the phish\_correct parameter which is only required in the phish\_correct function to determine how many correct phishing emails the user has identified.

Moreover, the email\_correct\_id and the email\_incorrect\_id change depending on the email. As shown in figure 46, I have set the parameter values to email\_1\_correct and email\_1\_incorrect for email 1: the middle number differs depending on the email number. This is so the tool can keep a record of each email and which text box to display in the next webpage that allows the user to review their performance. The different ids are assigned a value of either 1 or 0 which is then parsed through an if statement shown in figure 44. This then displays either the correct or incorrect textbox on the matching email residing on the succeeding quiz review webpage. Whilst the quiz page saves the variables to session storage, the actual function is only called using the "onload" HTML attribute within the body object of the aforementioned review webpage

```
function email_display(){
    var e = sessionStorage.getItem('email_1_correct');
    var e2 = sessionStorage.getItem('email_2_correct');
    var e3 = sessionStorage.getItem('email_3_correct');
    var e4 = sessionStorage.getItem('email_4_correct');
    var e5 = sessionStorage.getItem('email_5_correct');
    var e6 = sessionStorage.getItem('email_6_correct');
    var e7 = sessionStorage.getItem('email_7_correct');
    var e8 = sessionStorage.getItem('email_8_correct');

    if(e ==1){
        document.getElementById('correct_1').style.display = 'initial';
    }else{
        document.getElementById('incorrect_1').style.display = 'initial';
    }
}

```

Figure 44 - Snippet of email\_display function to show correct/incorrect text boxes on Review webpage

The hb parameter shown in figure 43 and 45 is used in a succeeding function within the results webpage which creates a bar chart based on whether or not the phishing email was identified correctly. It is

named thusly because hb is an acronym for 'head and body' as the variable is used primarily to show the indicators found in both the head and body of the emails. The function to create the chart and use the variable is discussed more in the coming result page implementation section.

```
function phish_incorrect(c, pid, npid, response, email_correct_id, email_incorrect_id, hb_correct){
  Incorrect++;

  document.getElementById(pid).style.visibility = 'hidden';
  document.getElementById(npid).style.visibility = 'hidden';
  document.getElementById(response).style.display = 'initial';
  sessionStorage.setItem(email_correct_id, JSON.stringify(0));
  sessionStorage.setItem(email_incorrect_id, JSON.stringify(1));
  sessionStorage.setItem(hb_correct, JSON.stringify(0));

  // set incorrect
  if (correct+Incorrect == 8){
    show_stats();}

  // Classify Email
  if(c == 'emotion'){
    emotive++;
  } else if(c == 'finance'){
    legal_financial++;
  }else if (c == 'auth'){
    Authoritative++;
  }
}
```

Figure 45 - Screenshot of code which counts answer as Incorrect

At the end of the function depicted in figure 43 and in the middle of 45, an if statement is used which counts how many correct and incorrect answers the user has given. Once the summation of the correct and incorrect variables gets to 8, this means that every email has therefore been answered since there is only 8 emails in total to view. Upon the user finishing the quiz, the show\_stats() function is called whereby specific variables such as correct and incorrect is set to session storage: this allows another html page to access the variables and use them in functions called by said page. Only in the phish\_incorrect() function do I use an if statement in order to classify a particular phishing email.

```
<button id="pb1" class="p_button" onclick="phish_correct('pb1', 'npb1', 'response_1',
  'email_1_correct', 'email_1_incorrect', 'hb_1_correct', 'correct')"></button>

<button id='npb1' class="np_button" onclick="phish_incorrect('emotion','pb1', 'npb1',
  'response_1', 'email_1_correct', 'email_1_incorrect', 'hb_1_correct')"></button>
```

Figure 46 - Screenshot of HTML code with parameters for Incorrect & Correct answers

The classification if statement shown in figure 45 is used in each case where a specific button, if selected, would result in the user not having correctly identified a phishing email. This information is required in order to collect data on how many phishing emails were incorrectly identified by the user and therefore, which type of phishing emails the user is likely to be susceptible to. As shown in figure 46, the value 'emotion' is parsed through as a parameter within the phish\_incorrect function. The if statement then compares the value being parsed through the function with the term's emotion, finance and auth each referring to a specific type of email. Upon the value matching a specific term, a respective variable is incremented by 1. The value parsed differs per email depending on what I originally

determined the email category to be within my design stage. Furthermore, this information is then saved to session storage, like many others, in order to be utilized within a graph displayed on the results page.

### 5.2.3 End of Quiz Alert

Once the user has finished the quiz and answered all 8 emails, an alert is provided notifying the user that they are finished with the main quiz and they are free to review their results. When the `show_stats()` functions called multiple variables are set to the session storage. Each variable is given a key in order for following webpages to access it and use it in functions within that page. Incorrect and Correct variables are stored to be used when calculating the users overall score, and each category i.e. emotive and authoritative, are set to independent variables. These are then used when creating a pie chart as mentioned in the above section. Once the user selects the "ok" button on the alert, they are transported to the next webpage which shows them whether or not they identified each email correctly accompanied by information relating to the phishing indicators found on each email.

```
function show_stats(){
    alert("End of Quiz, click ok to view your results");
    window.sessionStorage.setItem('final_correct', JSON.stringify(p_correct));
    window.sessionStorage.setItem('Legal', JSON.stringify(legal_Financial));
    window.sessionStorage.setItem('Emotion', JSON.stringify(emotive));
    window.sessionStorage.setItem('Auth', JSON.stringify(Authoritative));
    window.sessionStorage.setItem('Correct', JSON.stringify(correct));
    window.sessionStorage.setItem('Incorrect', JSON.stringify(Incorrect));
    document.location="Quiz_Answers.html";
}
```

Figure 47 - Screenshot of `show_stats()` function to set variables ready for cross site access

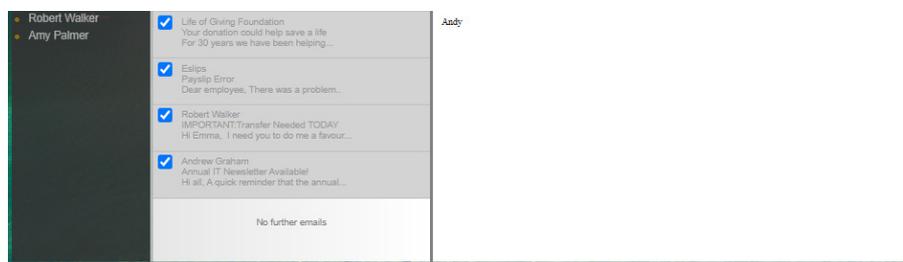


Figure 48 - Screenshot of quiz interface at the end of the quiz

### 5.2.4 Interactive Links/Attachments and popups

In order to provide an interactive element to the emails, especially for links and attachments implemented within various emails, a simple in and out function was used that was called using the "onmouseover" and "onmouseout" HTML attributes. This meant that when a user hovers their cursor over a HTML object calling the `popupIn()` function, another element is displayed as a popup: the element becomes hidden again upon a user removing their cursor off of the main HTML object. Whenever this function was called, the parameter would change depending on the element id name given to the HTML objects. The example displayed in figure 49 uses the id "popup1" to display the popup. This function was used for all popups that were implemented within the tool.



Figure 49 - Screenshot of Contacts list popup Example

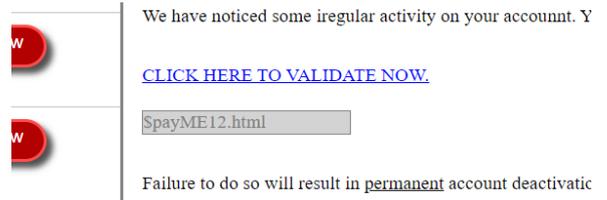


Figure 50 - Screenshot of Link/Attachment popup Example

```
function PopupIn(id) {
    document.getElementById(id).style.display = 'block';
}

function PopupOut(id)
{
    document.getElementById(id).style.display = 'none';
}
```

Figure 51 - Screenshot of JavaScript used to hide and show popups

### 5.2.5 Help Page

To provide helpful information regarding how each button worked within the tool, a help page was designed and implemented. This was implemented similar to how the emails interchanged on the main quiz page. When a user selected the help button, the different objects on the quiz HTML page were alerted. As you can see in figure 52, the contact list and introductory email preview have had their borders increased in thickness and changed to yellow. This was done by using JavaScript and the style property much like the way the DOM objects were alerted in figure 41. Upon a user selecting the "click here to return to Quiz" button, these elements were reset to their original style defined in the CSS stylesheet, and any newer elements like the written instructions were hidden from view.

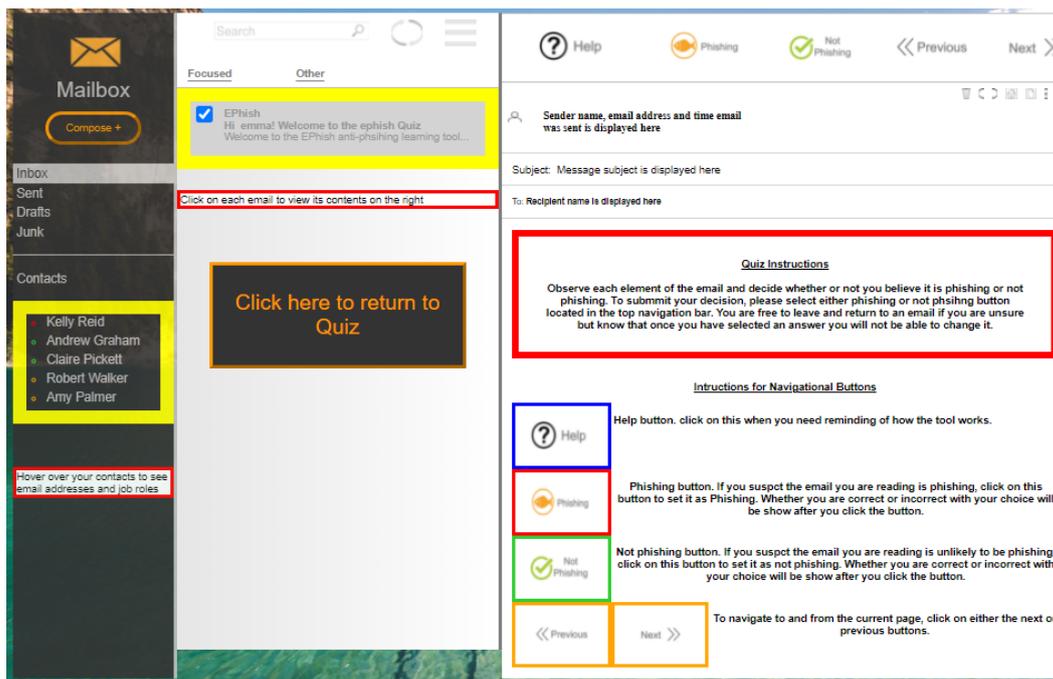


Figure 52 - Help page after implementation

### 5.2.6 Correct/Incorrect Display (Quiz Review html page)

When the user is finished with the main quiz portion of the tool, they are navigated to the review section. The main function of this webpage is to display the correct and incorrect textbox in the top bar as shown in figures 53 and 54. As the areas needed to be shown regardless of whether the user was correct or incorrect, the elements that were altered on each email were kept the same regardless of the correct or incorrect textbox that was shown. Each element that was an indicator of phishing with an email had their borders changed to yellow and thickened, and an explanation of that indicator written in blue next to the element. On the other hand, when the emails were not phishing, a written disclaimer was put below the email. This disclaimer informs users that whilst the email in this case is not deemed phishing, the user should always be vigilant for phishing indicators listed underneath it.

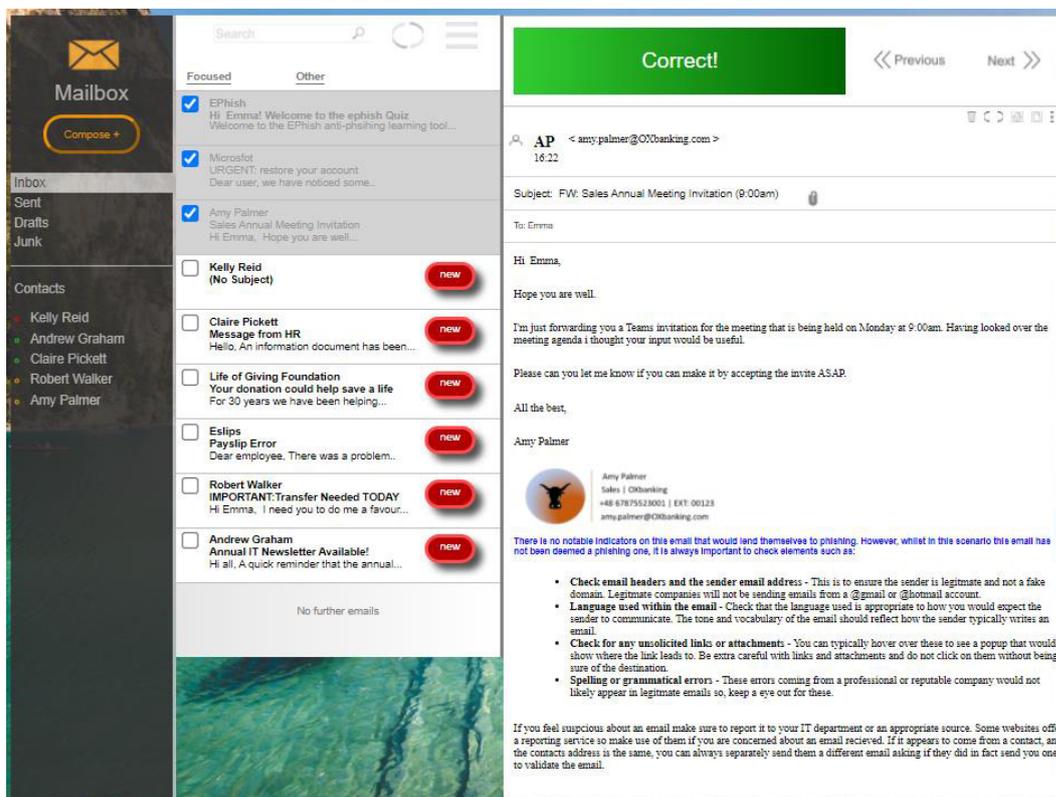


Figure 53 - Correct Answer Example for Not Phishing Email after Implementation

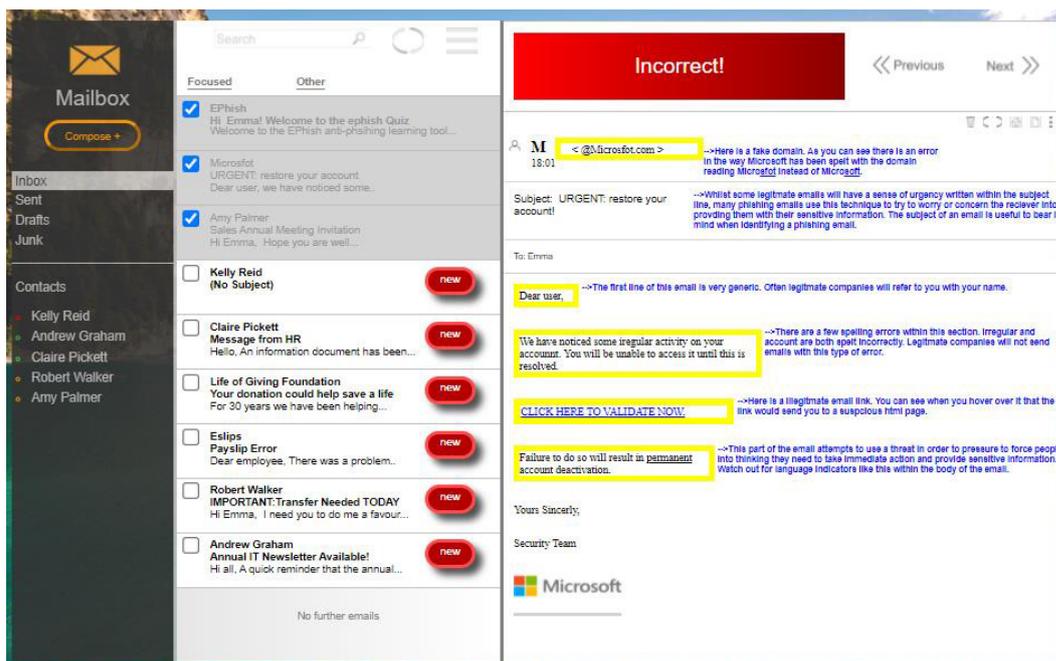


Figure 54 - Incorrect Answer for Phishing Email after Implementation

In order for the user to navigate away from this review stage and then to the final results page an alert or button needed to be implemented to notify the user that they were being transported to the succeeding page. Initially, this view results button was planned to be implemented as an alert which would action when the user selects all emails in the set and prompt them to proceed to the next webpage. However, this did not work well in practice as the alert would immediately pop up on the window freezing it in its state at the time. This meant that the user could not return to an email to review it if they needed more time to absorb the information and as such, the premise and objective of the review page would be redundant. Subsequently, the view results button was implemented as an alternative to enable users to review each email in their own time. Additionally, it does not become active until all emails have been traversed through ensuring the users take sufficient time to see which emails they may have misjudged or identified correctly. Figure 55 shows the simple code used to implement this button. Each email is parsed through a count function which assigns the email the number 1 if the user has selected it. Upon all email count variables being assigned 1, the button becomes active else an alert is presented prompting the user to navigate through the emails before clicking the button again.

```
function final_page(){
    if(
        email_count_1 == 1
        &email_count_2 == 1
        &email_count_3 == 1
        &email_count_4 == 1
        &email_count_5 == 1
        &email_count_6 == 1
        &email_count_7 == 1
        &email_count_8==1){
        document.location='results.html';
    }else{
        alert("Please review all the emails before navigating to final results");
    }
}
```

Figure 55 - Screenshot of Function for view results button

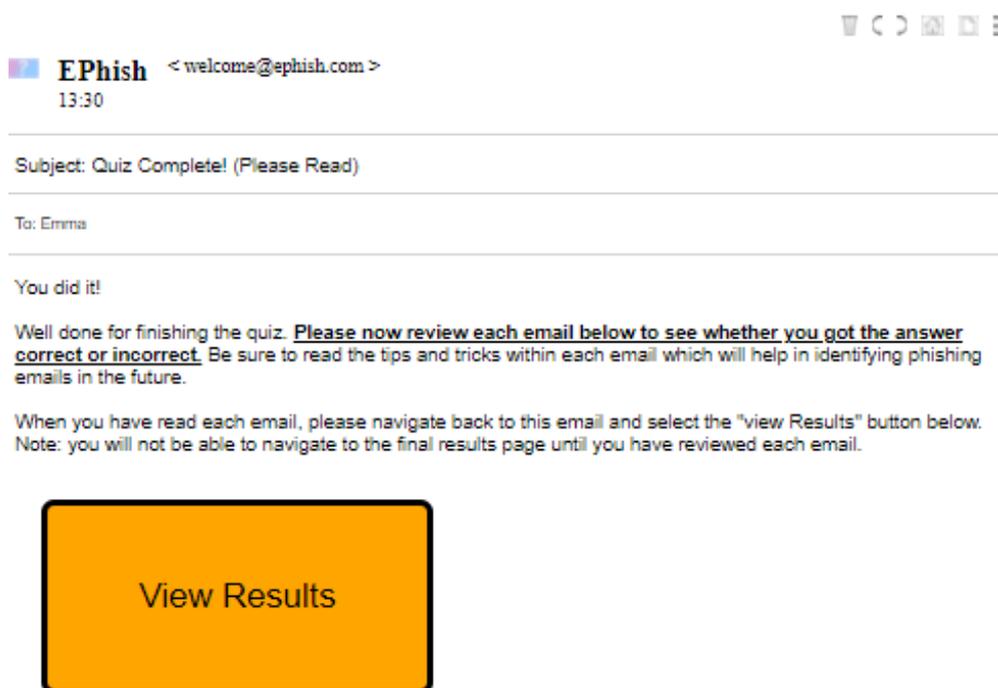


Figure 56 - Preview of View Results button on Interface after Implementation

### 5.2.7 Results page

The final page in my tool is the results page showing a statistical representation of the user's performance. The implementation of this page closely aligned with the original design with only minor adjustments in relation to the positioning of a few elements to make the page as a whole more aesthetically pleasing. In order to make the pie charts and bar charts the HTML5 and JavaScript charting library Canvas.js<sup>[48]</sup> was utilized. For each bar chart depicted in figure 60, a function such like the one shown in figure 57 is used. This example is used to represent the number of phishing indicators present on emails that were incorrectly identified. New variables for the indicators are instantiated within the function in order to calculate the overall number of indicators detected by the user per category: the categories are as stated in previous sections, language, links, fake domains, spelling, and greetings. This function is where the hb parameter that was earlier discussed in a prior section is utilized. The value gets passed through an if statement where it is compared with either 1 or 0. If the numbers correspond, then the data for the particular email the hb value has emanated from is inserted into the graph; the indicators linked to the email in question is set as well to help quantify the total indicators per email. There are two functions which make the bar charts: one for correct answers and the other for incorrect. The only section that differs is the if statements which compare the hb parameter value to 1 or 0 as well as the following if statements which are used to display information relating to the indicators below the charts.

```

var language = 0;
var links = 0;
var fake_domain = 0;
var Spelling = 0;
var greeting = 0;

var email_1 = sessionStorage.getItem('hb_1_correct');
var email_2 = sessionStorage.getItem('hb_2_correct');
var email_3 = sessionStorage.getItem('hb_3_correct');
var email_4 = sessionStorage.getItem('hb_4_correct');
var email_5 = sessionStorage.getItem('hb_5_correct');
var email_6 = sessionStorage.getItem('hb_6_correct');
var email_7 = sessionStorage.getItem('hb_7_correct');
var email_8 = sessionStorage.getItem('hb_8_correct');

var chart = new CanvasJS.Chart("chartContainer4", {
  animationEnabled: true,
  title: {
    text: "Indicators in Phishing Emails Incorrectly Identified"
  },
  axisY: {
    title: "Number of Indicators on email",
    includeZero: true,
  },
  axisX: {
    labelFontSize: 5.4,
  },
  data: [{
    type: "column",
    showInLegend: true,
    name: "Header",
    color: "darkred",
    dataPoints: [
    ]
  }
]
}

```

Figure 57 - Snippet of code used to make bar charts for results page

```

if (language!=0) chart.render();
var textnode = document.getEle
document.getEle if (email_1==0){
chart.data[0].addTo("dataPoints", {y:2, label: "Email1"});
chart.data[1].addTo("dataPoints", {y:4, label: "Email1"});
}

```

Figure 58 - Snippet of code used to summarize total indicators per category

```

Spelling ++;
links ++;
greeting ++;
fake_domain ++;
}

```

Figure 59 - Snippet of code used to insert data into bar charts for results page

The if statement shown in figure 58 checks if the indicator variable instantiated at the start of the function is empty or not and if it isn't, then the tool displays a message showing how many in total indicators within a particular category i.e. language indicators the user "missed" or "found" depending on the correctness of their answer. This line is repeated within the function per indicator category so that the appropriate text is represented below each of the bar charts. Moreover, the inner.HTML property is once again utilized to input the messages into the appropriate HTML object tags. Whilst I strived to reduce the amount of duplicated code within my tool, in the bar charting functions there had to be a lot of repetition. There were a few reasons for this one of which being that I wanted to create two bar charts similar in style to keep consistency within the visualisations. The other purpose for the repeated code is that it was vital that, no matter whether the user was correct or incorrect in their guess,



Figure 60 - Screenshot of results page interface

they were still presented with the same information explaining what indicators to be aware of and what they encompass. This ensures that all users were educated or reminded about phishing and nothing was bias or provided unfairly to a particular group: all information the tool could provide was unbiasedly provided to everyone. In contrast to the above charts, Canva.Js's pie charting capability has been utilized to construct the pie charts shown in figure 59. This function is structured similarly to the charting function in figure 58 but with a few minor changes to the way the data portion is structured. For the pie charts, the data type is changed to "doughnut" not "column" which is recognised by the Canva.Js library API as a pie chart. To see a full view of the pie chart function see Appendix H. An additional feature that was implemented is that if the user scores less than half in either the total overall score or the overall phishing score, the number is shown as red however, if they score half or over, the number turns lime green. This choice was made as it emphasises improvement areas better. Red connotes danger or in this case poorer performance and is therefore used to emphasise troubling areas to be aware of and work to improve. The usage of the colour green was also idealised in a similar way in order to emphasize an area that went well. I thought to use the halfway mark of the total numbers as

a threshold as typically half or 50% is considered a pass in a lot of quizzes and courses. Subsequently, if the user was able to "pass" the quiz or attain a score above this area it should be displayed in green. The colours green and red, as you can see in figure 60, were also utilized for the bar charts as green and red are also used in element designs to indicate correct and incorrect. Essentially, industry conventions and consistency heuristics were utilized to determine the colours that would represent positive and negative data. In relation to this, the pastel tones of the chart representing phishing categories were matched with those representing the same data in a numerical state. Again, this was to provide consistency within the interface and use good object mapping practices.

### **5.3 Implementation Constraints/Challenges**

During my implementation phase there was a little time to attempt a backend analysis capability on the tool. This meant that user results could be stored within a database and then extract this information on a statistics page which could be viewed by a manager or organisational lead. The aim of this was to attempt to provide further insight into an organisations knowledge gap and identify any areas that need improvement. Unfortunately, this task was not as simple as has been originally thought to be and as such, the capability was not implemented fully. As JavaScript works client-side it does not support cross origin resource sharing for security purposes and therefore, my code could not directly communicate to a database. Whilst a variety of methods were experimented with to resolve this problem such as attempting to incorporate Node.js into my existing code, it appeared that due to the completeness of my tool, extra libraries and languages that were being used were not simple to integrate and would require more in-depth expertise and time provisioned that was not currently accommodated for.

As mentioned, trying to make the tool scalable was one challenge which arose during implementation. I had previously not known how to make the content flexible and responsive to window changes and therefore it took some time to understand how the "flex" attribute worked and could be manipulated. In conjunction, to ensure each element was correct, the window needed to be resized every time an element was changed or inserted. This meant that the implementation stage took longer in order to learn this technique and appropriately set the elements on the page. In reference to learning curves, the more prominent challenge was my lack of experience with JavaScript. Whilst it was one of the easier languages to interpret, it did still take me some time to get used to creating functions and interlinking these with specific webpages. Furthermore, the learning curve, as expected, extended the implementation time.

## **6 Applicability Testing**

In order to test the applicability of the tool it was assessed under requirements that were predetermined in the design stage of the project, as well as the overall functionality of the tool using test cases.

### **6.1 Evaluation of Requirements**

In order to review how well the implementation measured in relation to the predefined requirements, testing was done on each of them displaying how each one was or was not met and then a reasoning behind this. See tables 19 and 20 to view the testing outcomes for non-functional and functional requirements for this project.

#### **6.1.1 Non-Functional Requirements**

**Table 19 - Table showing Non-Function Requirement Testing Results**

Requirement	Pass/Fail	Justification
1.	pass	No information is stored from the user. Name of user is temporarily stored but deleted after window closes.
2.	pass	Tool is dynamically resizable, and each interface aesthetically matches across all browser types. The functionality of the tool also meets expectations across these browser types.
3.	pass	Each action supported testing and evaluation.
4.	pass	Each webpage load up time was below 5 seconds
5.	pass	All interactive elements responded promptly
6.	pass	Interfaces designed and implemented using usability heuristics
7.	pass	Final report when tested within test cases generated correct report to user performance.

### 6.1.2 Functional Requirements

**Table 20 - Table showing Functional Requirements Testing Results**

Requirement	Pass/Fail	Justification
1.	pass	User could insert name into input box, and it was then displayed in various correct elements within the HTML pages.
2.	pass	Phishing and not phishing buttons were clickable and worked correctly (evidence in test cases 5-8)
3.	pass	Navigation from help to main quiz was a success (evidence in text case 4)
4.	pass	All navigation ability functioned correctly whether it was using next and previous buttons or selecting a specific email. (evidence in test cases 3 & 10).
5.	pass	results were displayed at the end of the quiz and review stage correctly.

6.	pass	user was not able to navigate away from review page until all emails had been traversed through (evidence in test case 11).
----	------	---

## 6.2 Evaluation of Functionality (Test Cases)

The test cases below have been used to test each interactive element of the tool and ensure that any functionality implemented works as desired. Each test case has an overall pass or fail mark depending on whether each step within the case was successful.

### 6.2.1 Test Case 1: Input name and Begin Quiz

#### Description

Test case to validate the application accepts username input and navigates user to quiz. See table 21 for steps and results of case.

#### Pre-conditions for this test case

All files used for application i.e. CSS, JavaScript and HTML should be linked correctly.

Table 21 - Input name and Begin Quiz (Test Case 1)

test Case ID: 1			Name: Input name and Begin quiz		
Steps	Step Description	Expected Result	Actual Result (if different from expected)	pass/fail	Test comments
1	Launch Application	Application opens and displays homepage.	N/A	pass	
2	Type name into name box	Application accepts input - shows email in field	N/A	pass	
3	Press enter	Name should be accepted, and user should be taken to quiz	N/A	pass	
		<b>Test Case Status</b>	<b>Pass</b>		

### 6.2.2 Test Case 2: Input null name - negative test case

#### Description

Test case to validate that the application does not navigate to next page unless name is inputted into username section. See table 22 for steps and results of case.

#### Pre-conditions for this use case

All files used for application i.e. CSS, JavaScript and HTML should be linked correctly.

**Table 22 - Input null name - negative test case (Test Case 2)**

test Case ID: 2			Name: Input null name - negative test case		
Steps	Step Description	Expected Result	Actual Result (if different from expected)	pass/Failed	Test comments
1	Launch Application	Application displays login page.	N/A	pass	
2	Leave name field empty and press enter	Application remains on main page and does not navigate to the quiz.	N/A	pass	
		<b>Test Case Status</b>	Pass		

### 6.2.3 Test Case 3: Selecting email from main quiz page

#### Description

User should be able to select any one of the emails that appear on the mailbox screen. Once selected, the site should navigate to the relevant email. See table 23 for steps and results of case, and table 24 to view test results from additional testing using this case.

#### Pre-conditions for this test case

User must have entered their name into application and have been navigated to main mailbox page from the "Take Quiz" button.

**Table 23 - Selecting email from Main Quiz page (Test Case 3)**

test Case ID: 3			Name: Selecting email from main quiz page		
Steps	Step Description	Expected Result	Actual Result (if different from expected)	pass/Failed	Test comments
1	Select an email from the email panel previewing emails.	Email should be clickable - application takes user to the relevant email the preview was showing.  Email preview style changes: <ul style="list-style-type: none"> <li>• New icon should have been removed</li> <li>• The check box should be ticked</li> <li>• Email preview background should be light grey</li> </ul>	N/A	pass	

		<ul style="list-style-type: none"> <li>Email preview font style should not be in bold</li> </ul>			
2.	Select introduction email from the email previewing panel.	Email should be clickable - application takes user to relevant email.	N/A	pass	
		<b>Test Case Status</b>	<b>Pass</b>		

This test case was completed against emails 1-8 recorded in the below table:

**Table 24 - Test results for Test Case 3 - Selecting emails on emails 1-8**

Email number	pass/fail
1	PASS
2	PASS
3	PASS
4	PASS
5	PASS
6	PASS
7	PASS
8	PASS

#### 6.2.4 Test Case 4: Selecting Help Page and Return to Quiz buttons

##### Description

User should be able to select help page and be navigated to the help page. Once completed, the user should then be able to return to the main quiz page in the state they had left it in. . See table 25 for steps and results of case, and table 26 to view test results from additional testing using this case.

##### Pre-conditions for this test case

User must be completing the quiz on the main quiz page.

**Table 25 - Selecting Help Page and Return to Quiz buttons (Test Case 4)**

test Case ID: 4			Name: Selecting Help Page and Return to Quiz buttons		
Steps	Step Description	Expected Result	Actual Result (if different from expected)	pass/Failed	Test comments
1	Select help button	Application navigates to help page	N/A	pass	

2	Select 'Return to Quiz' button	Application navigates back to main quiz page in state the user left it in.	N/A	pass	
		<b>Test Case Status</b>	Pass		

The above test case was tested against 6 scenarios displayed in the below table. This shows what email the help button was selected on; how many emails had been seen prior to selecting help and then whether or not the test passed the above test case:

**Table 26 - Test results of Test Case 4 Selecting Help Page and Return to Quiz**

Email number upon selecting help	Number of emails previously seen	pass/fail
1	4	PASS
2	2	PASS
3	0	PASS
4	3	PASS
5	0	PASS
6	3	PASS

### 6.2.5 Test Case 5: Selecting phishing button when the email is phishing

#### Description

Test case to validate the application displays the correct response for phishing emails that the user has classified as "phishing". See table 27 for steps and results of case, and table 28 to view test results from additional testing using this case.

#### Pre-conditions for this test case

User must be on a selected email which has been deemed a phishing email by tool.

**Table 27 - Selecting Phishing button when the email is Phishing (Test Case 5)**

test Case ID: 5			Name: Selecting phishing button when the email is phishing		
Steps	Step Description	Expected Result	Actual Result (if different from expected)	pass/Failed	Test comments
1	Select "phishing" button from the top menu within the email.	"response submitted" text box should appear underneath the email contents.	N/A	pass	

2.	Navigate to review page	Review webpage shows a correct textbox on top of each phishing email that was selected as phishing.	N/A	pass	
3.	Navigate to results page	Results page should show the total correct phishing emails accurately and display on correct/Incorrect pie chart. Email number and accurate linking indicators should also be shown on 'correct' bar chart.	N/A	pass	
<b>Test Case Status</b>			<b>Pass</b>		

The above test case was tested against 1,3-6 emails which are phishing emails. This data is shown in the below table:

**Table 28 - Test results against Test Case 5 Phishing page**

<b>Email number</b>	<b>pass/fail</b>
1	PASS
3	PASS
5	PASS
6	PASS
7	PASS

### 6.2.6 Test Case 6: Selecting phishing button when the email is not-phishing

#### **Description**

Test case to validate the application displays the correct response for non-phishing emails that the user has classified as "phishing". See table 29 for steps and results of case, and table 30 to view test results from additional testing using this case.

#### **Pre-conditions for this test case**

User must be on a selected email which has been deemed a non-phishing email.

**Table 29 - Selecting Phishing button when not Phishing (Test Case 6)**

test Case ID: 6			Name: Selecting phishing button when the email is not-phishing		
Steps	Step Description	Expected Result	Actual Result (if different from expected)	pass/Failed	Test comments
1	Select "phishing" button from the top menu within the email.	"response submitted" text box should appear underneath the email contents.	N/A	pass	
2.	Navigate to review page	Review webpage shows a Incorrect textbox on top of each phishing email that was selected as phishing.	N/A	pass	
3.	Navigate to results page	Results page should show the total number of incorrect emails on pie chart for correct/Incorrect summary.	N/A	pass	
		<b>Test Case Status</b>	<b>Pass</b>		

The above test case was tested against 2 and 8 which are not phishing emails. This data is shown in the below table:

**Table 30 - Test results for Test Case 6 on emails 2 and 8**

Email number	pass/fail
2	PASS
8	PASS

### 6.2.7 Test Case 7: Selecting not-phishing button when the email is phishing

#### Description

Test case to validate the application displays the correct response for phishing emails that the user has classified as "non-phishing". See table 31 for steps and results of case, and table 32 to view test results from additional testing using this case.

#### Pre-conditions for this test case

User must be on a selected email which has been predefined as a phishing email.

**Table 31 - Selecting Not-Phishing when Phishing (Test Case 7)**

test Case ID: 7			Name: Selecting not-phishing button when the email is phishing		
Steps	Step Description	Expected Result	Actual Result (if different from expected)	pass/Failed	Test comments
1	Select "not-phishing" button from the top menu within the email.	"response submitted" text box should appear underneath the email contents.	N/A	pass	
2.	Navigate to review page	Review webpage shows a Incorrect textbox on top of each phishing email that was selected as phishing.	N/A	pass	
3.	Navigate to results page	Results page should show the total Incorrect phishing emails accurately displayed on correct/Incorrect pie chart. Email number and accurate linking indicators should also be shown on 'Incorrect' bar chart.	N/A	pass	
		<b>Test Case Status</b>	<b>Pass</b>		

The above test case was tested against 1,3-6 emails which are phishing emails. This data is shown in the below table:

**Table 32 - Test results for Test Case 7**

Email number	pass/fail
1	PASS
3	PASS
5	PASS
6	PASS
7	PASS

**6.2.8 Test Case 8: Selecting not-phishing button when the email is not a phishing email.**

**Description**

Test case to validate the application displays the correct response for non-phishing emails that the user has classified as "non-phishing". See table 33 for steps and results of case, and tables 34 and 35 to view test results from additional testing using this case.

**Pre-conditions for this test case**

User must be on a selected email which has been deemed a non-phishing email.

**Table 33 - Selecting Not-Phishing when Phishing (Test Case 8)**

test Case ID: 8			Name: Selecting not-phishing button when the email is not a phishing email.		
Steps	Step Description	Expected Result	Actual Result (if different from expected)	pass/Failed	Test comments
1	Select "not-phishing" button from the top menu within the email.	"response submitted" text box should appear underneath the email contents.	N/A	pass	
2.	Navigate to review page	Review webpage shows a correct textbox on top of each phishing email that was selected as phishing.	N/A	pass	
3.	Navigate to results page	Results page should show the total number of correct emails properly and on pie chart for correct/Incorrect summary.	N/A	pass	
		<b>Test Case Status</b>	<b>Pass</b>		

The above test case was tested against 2 and 8 which are not phishing emails. This data is shown in the below table:

**Table 34 - Test results for Test Case 8 on emails 2 and 8**

Email number	pass/fail
2	PASS
8	PASS

Testing was carried out for different combinations of correct and incorrect phishing and not-phishing emails. This was to ensure all graphs and results shown on the results page were accurate and reflected the true performance of the user. The scenarios tested are documented in the below table

Test Number.	Phishing correct	Phishing Incorrect	Not-Phishing correct	Not-Phishing Incorrect	Pass/Fail
1.	1	5	0	2	PASS
2.	2	4	1	1	PASS
3.	3	3	2	0	PASS
4.	4	2	0	2	PASS
5.	0	6	0	2	PASS
6.	6	0	2	0	PASS

Table 35 - Test results for Phishing combinations using a mixture of Test Cases 5,6,7 and 8

### 6.2.9 Test Case 9: Hover over link/attachments

On moving cursor over link or attachment, a pop up should appear. On removing the cursor, the popup should disappear. See table 36 for steps and results of case, and tables 37 and 38 to view test results from additional testing using this case.

#### Pre-conditions for this test case

User should be on the quiz main page or review page.

Table 36 - Hover over link/attachments (Test Case 9)

test Case ID:9			Name: Hover over link/attachments		
Steps	Step Description	Expected Result	Actual Result (if different from expected)	pass/Failed	Test comments
1	Hover cursor over link section	Pop up for link appears	N/A	pass	
		<b>Test Case Status</b>	Pass		

All popups were tested against the above test case recorded in the below table:

**Table 37 - Test results for Test Case 9 on Links/Attachments per email**

Email number with link	Pass/Fail
<b>1.</b>	<b>PASS</b>
<b>2.</b>	<b>PASS</b>
<b>3.</b>	<b>PASS</b>
<b>5.1</b>	<b>PASS</b>
<b>5.2</b>	<b>PASS</b>
<b>6.</b>	<b>PASS</b>

**Table 38 - Test results for Test Case 9 on popups per profile pictures**

Contact profile	Pass/Fail
Kelly	<b>PASS</b>
Andrew	<b>PASS</b>
Amy	<b>PASS</b>
Claire	<b>PASS</b>
Robert	<b>PASS</b>

5.1 and 5.2 refer to the two links found in email 5 - the fake charity email.

#### **6.2.10 Test Case 10: Navigating Next and Previous**

Application should let the user navigate back and forth via the next and previous buttons to appropriate emails. See table 39 for steps and initial results of case, and table 40 to view test results from additional testing using this case.

#### **Pre-conditions for this test case**

User should be on the review page or the main quiz page.

**Table 39- Navigating using next and previous buttons (Test Case 10)**

<b>test Case ID:10</b>	<b>Name: Navigating Next and Previous</b>
------------------------	---

Steps	Step Description	Expected Result	Actual Result (if different from expected)	pass/Failed	Test comments
1	Select 'next' button	Email should be displayed that is the next email in the email review panel sequence.	N/A	pass	
2.	Select 'previous'	Email should be displayed that is previous to the current email in the email review panel sequence.	N/A	pass	
		<b>Test Case Status</b>	<b>Pass</b>		

This test case was completed against emails 1-8 recorded in the below table:

**Table 40 - Test results on each email for Test Case 10**

Email number	pass/fail
1	PASS
2	PASS
3	PASS
4	PASS
5	PASS
6	PASS
7	PASS
8	PASS

### 6.2.11 Test Case 11: Using view results button

Application should alert the user if they select 'view results' before they have traversed through all emails. See table 41 for steps and results of case.

#### Pre-conditions for this test case

User should be on review page of the tool.

Table 41 - Using View Results Button (Test Case 11)

test Case ID:11			Name: Using view results button		
Steps	Step Description	Expected Result	Actual Result (if different from expected)	pass/Failed	Test comments
1	Select 'view results' without looking through any email	alert should pop up informing user to look through every email before selecting 'view results'.	N/A	pass	
2.	Traverse through emails and then select 'view results'	View results button becomes active and navigates user to results page.	N/A	pass	
		<b>Test Case Status</b>	<b>Pass</b>		

### 6.2.12 Test Case 12: Returning to Homepage

Application should return user to homepage when "return to homepage" button is selected. See table 42 for steps and results of case.

#### Pre-conditions for this test case

User should be on their results page.

Table 42 - Returning to Homepage (Test Case 12)

test Case ID:12			Name: Returning to Homepage		
Steps	Step Description	Expected Result	Actual Result (if different from expected)	pass/Failed	Test comments
1	Select "Return to Homepage" button	Application navigates user to main homepage	N/A	pass	
		<b>Test Case Status</b>	<b>Pass</b>		

**Summary of Results:** Overall the testing concluded that the tool was a success. Each non-functional and functional requirement was met, and the tool worked as desired; It was able to keep track of a user's performance and accurately relay the information to said user.

## 7 Future Work

Whilst the project met its core objectives, there is still significant work that could be done to improve the tool implemented. The desirable objectives documented in the beginning of this report discussed

additional features/capabilities of the tool that would be useful to implemented if time permitted. These capabilities encompassed using the tool for analysis purposes. In order for this tool to further help organisations in understanding phishing and identifying knowledge gaps in their estate, the tool would require a backend analysis system whereby, each employee's performance is stored in a database and then collated in a final feedback report that organisational managers or seniority could review. This report could then show specific areas of susceptibility that they need to address within their organisation for example, if multiple employees are typically more vulnerable to emotive emails, further training in relation to these emails could be administered to improve this susceptibility. The increased visibility into an organisation's estate would enable them to make changes or improvements that would increase their security and prevent data breaches brought on through phishing.

As this desirable objective was kept in mind throughout the project, all variables that are required for this backend analysis capability are in fact present within the tool currently. Each variable necessary, such as number of phishing emails incorrectly identified per phishing email type, is already being saved in the session storage. As such, the variables required can be transferred to a database for permanent storage before being cleared from the session. Whilst there has been some attempted work made towards this, as discussed in the implementation chapter, creating a database connection to a JavaScript file poses a lot of challenges as it cannot directly communicate with a server side application or database. Many sources online discuss the use of Node.js which is a JavaScript library that can handle this type of connection and is one of the libraries I attempted to utilize in the construction of the backend analysis capability. Unfortunately, as stressed, the time frame of the project was a major obstacle which impacted how much time could be provisioned for learning the concepts and functions within a new library: especially how the library integrated with the existent code of the tool. Consequently, one objective for future work is to spend time implementing this capability utilizing libraries such like Node.js in order to provide organisations with an insight into their overall phishing susceptibility. Additionally, another capability will need to be implemented that authenticates the name of a user. As I implemented it as an alert box it has no validation mechanism surrounding it that ensures the name being used is a viable one and doesn't contain numbers or letters. Whilst work produced assumed that users would enter in appropriate names since the tool was built to be deployed in professional environments, it would be good to implement a function that validates this if the names in later practices are required to evidence each employee's performance.

Moreover, another future work objective is to apply this tool in real life in order to observe if it is effective as an educational tool. Whilst usability heuristics have been considered during the design of the tool, this does not concretely prove that the tool is effective in real world application. Subsequently user testing needs to be conducted against the tool to prove its effectiveness and encourage the usage of it. Likewise, as there was no testing done on the actual heuristics, since following best practices this would require an industry expert, an evaluation needs to be conducted in this area as well. Both of these evaluations would help in identifying any major gaps within the tool which impact how well it is able to educate people on phishing. Since this is a major application component of the tool, it is necessary to get feedback on how well it performs before being deployed in any environment.

When discussing future work on the tool there has also been consideration made on some future applications of it. One future usage of the tool could be within physiological studies. An example of a useful experiment is giving participants a questionnaire which asks them about their educational background, age, gender etc. Once they have completed this questionnaire, they should then be presented with the tool which they use as in intended. The performance report derived from this could then provide insight into the correlation between phishing susceptibility and certain demographics. Of course, this would require a backend analysis capability which is also a part of future work as discussed above.

An aspect of the tool is that it categorises emails based on what phishing types they fall into: emotive, authoritative, and legal and financial. Phishing emails have not been specifically categorised and as such, for the purpose of this tool, the categories were determined based on my research and opinion derived from said research. As these categories are useful when observing user susceptibility to certain features of a phishing email, I do feel that my opinions need to be further supported. Whilst the research conducted helped to strengthen my decision for how to categorise the emails, I feel it would be useful to complete more research and reach out to industry experts to further support the decision made. In conjunction with this, when determining the nature of each example email used I found that certain emails overlapped. For example, a particular email used emotive language to invoke panic from the recipient however, the message emanated from an authoritative figure thus it was categorised as such. The next step in developing the tool would be to have variables that keep track of emails that come under a combination of the categories defined. When the final feedback report is generated, there needs to be a capability that lets the user see what combinations of phishing emails they are more likely to be susceptible to. For example, taking the mentioned email as a reference, a user can determine whether the authoritative sender was a key factor in how susceptible they were to the email, or if the emotive aspect contributed to this more.

Moreover, to enable the introduction of more categories or combinations of categories, more emails will be required to be implemented that cover a wider basis. This can also be seen as a future work objective. Following on from this, as newer phishing incidents arise and become more sophisticated, the tool will need to develop in conjunction. This means that the emails will inevitably have to be alerted to some extent or additional emails will need to be implemented alongside the existent ones to help people identify them in a safer environment. I believe this will greatly improve its effectiveness in the real world as it covers more phishing cases and exposes users to them before they experience them in real life.

## 8 Conclusions

The main intention of the project was to create a resource that could be deployed in organisations that would educate users about phishing and ways to identify these types of emails. This idea was derived from research surrounding the prevalence of phishing<sup>[1][2]</sup> and the need for new anti-phishing educational resources to improve people's awareness of phishing in a safe environment: especially within organisations who are a significant target for this type of attack. Through the examination of the project aims and objectives, there is sufficient evidence to conclude that the project was a success. As you can see upon revisitation, the main aim of the project was to create an interactive tool that quizzed users on phishing emails and then provided them with an accurate feedback of their performance. Conclusively this aim has been achieved following the evidence located in the implementation and testing phase. The tool does indeed require users to categorise emails and decide whether they are phishing or not phishing such as a quiz would do, and then provides information within a feedback section which reflects how well they distinguished between the email set provided by the tool. Whilst there is no validation that the tool is effective in teaching users about phishing or or improving their existent knowledge, this validation was not an original aim or objective and as such remains out of the project scope. That said this area has been considered and in order to work towards aligning with usability techniques that would contribute to the tool's effectiveness, each interface has been designed with usability heuristics in mind. Nevertheless, I feel it would be necessarily to complete heuristic evaluation to confirm the application of heuristics within the design has been helpful and contributes to the effectiveness of the tool. In addition, for the effectiveness of the tool to be validated, evaluations need to be conducted upon it that introduce real life participants. These evaluations will help to prove its effectiveness and encourage its usage in the real world. Whilst the project was successful overall,

there are still many expansions and future work that can be done on improving it. A main area of future work is to develop a backend analysis tool which would help organisations identify large knowledge gaps within their estate and work towards improving this to reduce human error caused by phishing susceptibility, and ultimately improve their cybersecurity as a result.

## **8.2.Reflection and Learning**

Throughout the project I was able to gain some invaluable insights into how I worked and managed a large individual project. Whilst I feel that the project was successful overall, I have learnt many things throughout my journey that will undoubtedly remain with me in the future. A significant part of the project was in fact the initial plan. Whilst initially I kept to the intended project timeframe as best I could, external obligations continued to be a prominent challenge. Despite ensuring extra time was provisioned to complete certain aspects of the project, my inexperience with such a large project was evident and I felt that I was too optimistic with how I initially provisioned time. I feel as though I spent too much time at the start of the project researching phishing and covering areas that weren't pivotal to the project or deliverable. As a result, the implementation phase got a bit delayed meaning that the time to complete it was shorter than originally provisioned which ultimately, was accompanied by significant stressors. Whilst I managed to construct the tool and have it function as intended in the newly shortened time scale, this was definitely an area that I will be focusing on in future projects. As mentioned, since I had not undertaken such a large individual project, I could not gauge accurately how much time I would take to complete certain sections. After this project I now feel much more entuned with my working style and how long specific project areas will likely take. This will undoubtedly be useful when I begin my career in the industry.

Whilst I made a few mistakes during the project and have since learnt from these, I am also very proud of what I created. Having little experience with JavaScript, I was really pleased with how I managed to create a functional tool from scratch. I did not consider myself to be a strong coder however, this project has allowed me to develop my web application skills and technical knowledge within this area. During implementation I made mistakes, experimented with some coding techniques and conducted a lot of debugging which has really helped to broaden my knowledge surrounding JavaScript, HTML and CSS. That said, the biggest lesson I have learnt from using this programming language is how, despite its notable usage in web application, it is not the best language to use if you want a database to accompany your tool. As mentioned, this can be done however, it would require a lot more experience and knowledge into JavaScript and server side application which I do not currently possess.

Furthermore, when revisiting my aims and objectives prior to the project fully commencing, I did make some changes. Within the initial plan objective 2 was originally to establish factors that pertain to phishing susceptibility. Whilst this is important in understanding the concept behind why a person is more likely to fall victim to phishing, the main aim of the project is first and foremost to create an interactive tool that helps educate people how to identify phishing emails and therefore, does not require an in depth exploration into the motivations that surround phishing susceptibility. As a result, this aim was changed to exploring the limitations of current anti-phishing resources which better supports the main aim of the project. This area is vital to research in order to create an effective educational tool that provides capabilities which current tools do not. The amended objective, however, should be considered if the tool were to be used for psychological studies to confirm or explore existing theories of email susceptibility pertaining to various demographics, which has been highlighted as an objective in future work.

Fundamentally, I have had both positive and negative experiences with this project. Overall I am very proud of what I created and how the project turned out. As I am pursuing a career path in cybersecurity,

I really enjoyed constructing a tool that surrounded phishing and preventing these attacks from being successful. Human error is always going to be a large vulnerability within an organisation but nevertheless, I feel that the tool would help to mitigate some of this. Having completed a large project now I know how to provision time more appropriately and realistic to my work pattern. This knowledge will inevitably be very useful in the future.

## 9 Appendix

### A. Email 2 - Employee Teams Invite (Not Phishing)

The screenshot displays an Outlook mailbox interface. On the left, there is a navigation pane with 'Mailbox' (Compose +), 'Inbox', 'Sent', 'Drafts', 'Junk', and 'Contacts'. The 'Contacts' list includes Kelly Reid, Andrew Graham, Claire Pickett, Robert Walker, and Amy Palmer. The main area shows a list of emails under 'Focused' and 'Other' tabs. The selected email is from Amy Palmer (AP) with the subject 'FW: Sales Annual Meeting Invitation (9:00am)'. The email body contains a Teams invitation for a meeting on Monday at 9:00am. A signature block for Amy Palmer is visible at the bottom of the email.

**Mailbox**  
Compose +

**Inbox**  
Sent  
Drafts  
Junk

**Contacts**  
• Kelly Reid  
• Andrew Graham  
• Claire Pickett  
• Robert Walker  
• Amy Palmer

**Focused**   **Other**

- EPHish**  
Hi Emma! Welcome to the ephish Quiz  
Welcome to the EPhish anti-phishing learning tool...
- Microsoft**  
**URGENT: restore your account**  
Dear user, we have noticed some...
- Amy Palmer**  
**Sales Annual Meeting Invitation**  
Hi Emma, Hope you are well...
- Kelly Reid**  
**(No Subject)**   **new**
- Claire Pickett**  
**Message from HR**   **new**  
Hello, An information document has been...
- Life of Giving Foundation**  
**Your donation could help save a life**   **new**  
For 30 years we have been helping...
- Estlips**  
**Payslip Error**   **new**  
Dear employee, There was a problem..
- Robert Walker**  
**IMPORTANT: Transfer Needed TODAY**   **new**  
Hi Emma, I need you to do me a favour...
- Andrew Graham**  
**Annual IT Newsletter Available!**   **new**  
Hi all, A quick reminder that the annual...

No further emails

**Help**   **Phishing**   **Not Phishing**   **Previous**   **Next**

**AP** <amy.palmer@OXbanking.com>  
16:22

**Subject:** FW: Sales Annual Meeting Invitation (9:00am)

**To:** Emma

Hi Emma,

Hope you are well.

I'm just forwarding you a Teams invitation for the meeting that is being held on Monday at 9:00am. Having looked over the meeting agenda i thought your input would be useful.

Please can you let me know if you can make it by accepting the invite ASAP.

All the best,

Amy Palmer

 Amy Palmer  
Sales | OXbanking  
+48 67875523001 | EXT: 00123  
amy.palmer@OXbanking.com

B. Email 3 - Employee IS THIS YOU scam email (phishing)

The screenshot displays an Outlook mailbox interface. On the left, there is a navigation pane with 'Mailbox' at the top, followed by 'Compose +', and folders for 'Inbox', 'Sent', 'Drafts', and 'Junk'. Below these are 'Contacts' with a list of names: Kelly Reid, Andrew Graham, Claire Pickett, Robert Walker, and Amy Palmer. The main area is divided into 'Focused' and 'Other' tabs. The 'Focused' tab is active, showing a list of emails. The top email is selected and checked, with a subject line 'EPHish' and a preview 'Hi Emma! Welcome to the ephish Quiz. Welcome to the EPhish anti-phishing learning tool...'. Below it are several other emails, each with a 'new' badge in a red circle. The bottom of the list shows 'No further emails'. On the right, the selected email is displayed in detail. It is from 'KR <kelly.reid@OXbanking.com>' at 15:45. The subject is 'No subject' and the recipient is 'Emma'. The body of the email contains the text 'IS THIS YOU!' followed by a circular logo with a bird and contact information for Kelly Reid, Customer Services | OXbanking, including a phone number and email address.

C. Email 4 - Message from HR (phishing)

The screenshot displays an email client interface with a dark sidebar on the left and a main content area on the right. The sidebar includes a 'Mailbox' section with a 'Compose +' button, and folders for 'Inbox', 'Sent', 'Drafts', and 'Junk'. Below these are 'Contacts' for Kelly Reid, Andrew Graham, Claire Pickett, Robert Walker, and Amy Palmer. The main area shows a list of emails under 'Focused' and 'Other' tabs. The selected email is from 'HR' (claire.pickett@OXbanking.com) with the subject 'Message from HR'. The email body contains a greeting, a message about an information document, a link to login, and a signature. A 'CONFIDENTIALITY NOTICE' is visible at the bottom of the email content.

**Mailbox**  
Compose +

**Inbox**  
Sent  
Drafts  
Junk

**Contacts**  
• Kelly Reid  
• Andrew Graham  
• Claire Pickett  
• Robert Walker  
• Amy Palmer

Search [ ] [ ] [ ] [ ]

**Focused**   **Other**

- EPfish**  
Hi, Emma! Welcome to the ephish Quiz  
Welcome to the EPfish anti-phishing learning tool...
- Microsoft**  
**URGENT: restore your account**  
Dear user, we have noticed some...
- Amy Palmer**  
**Sales Annual Meeting Invitation**  
Hi Emma, Hope you are well...
- Kelly Reid**  
(No Subject)
- Claire Pickett**  
Message from HR  
Hello, An information document has been...
- Life of Giving Foundation**  
**Your donation could help save a life**  
For 30 years we have been helping... **new**
- Eslips**  
**Payslip Error**  
Dear employee, There was a problem.. **new**
- Robert Walker**  
**IMPORTANT: Transfer Needed TODAY**  
Hi Emma, I need you to do me a favour... **new**
- Andrew Graham**  
**Annual IT Newsletter Available!**  
Hi all, A quick reminder that the annual... **new**

No further emails

**Help**   **Phishing**   **Not Phishing**   **Previous**   **Next**

**HR** <claire.pickett@OXbanking.com>  
12:31

**Subject:** Message from HR

**To:** Emma

Hello,

An information document has been sent to you by the HR department.

[click here](#) to login to view the document. Thanks!

Regards

Claire Pickett

Human Resources

CONFIDENTIALITY NOTICE: This email and any attachments may contain confidential information that is protected by law and is for the sole use of the individuals or entities to which it is addressed. If you are not the intended recipient, please destroying all copies of the communication and attachments. Further use, disclosure, copying, distribution of, or reliance upon the contents of this email and attachments is strictly prohibited. Please consider the environment before printing this e-mail

D. Email 5 - Fake Charity (phishing)

The screenshot displays an email client interface. On the left is a sidebar with 'Mailbox' and a 'Compose +' button. Below are folders for 'Inbox', 'Sent', 'Drafts', and 'Junk', and a 'Contacts' list including Kelly Reid, Andrew Graham, Claire Pickett, Robert Walker, and Amy Palmer. The main area shows a list of emails under 'Focused' and 'Other' tabs. The selected email is from 'Life of Giving Foundation' with the subject 'Your donation could help save a life!'. The email body contains a blue box with text: 'For 30 years we have been helping to save lives through your donations but we still have a way to go! Your support and kindness will help people give vulnerable children the support and care they desperately need during these unforgivable times. To help save a life today follow the link below to donate. We thank you greatly for your kindness.' Below this is a 'Save a life today!' section with a 'Donate' button. At the bottom, it says 'If you wish to not receive further emails please [unsubscribe](#) by clicking unsubscribe.'

E. Email 6 - Payslip Error (phishing)

The screenshot shows an email client interface with a dark sidebar on the left containing 'Mailbox', 'Compose +', 'Inbox', 'Sent', 'Drafts', 'Junk', and 'Contacts'. The main area is split into a list of emails and a detailed view of the selected email. The selected email is from 'Eslips <eslips@gmail.com>' with the subject 'Payslip Error'. The body of the email contains a phishing message: 'Dear employee, There was a problem generating your payslip. Please provide your details in the following link in order for you to be paid correctly. Failure to do so will result in not being paid. click here yours faithfully, Eslips Administrative Team'. The interface also shows a 'Phishing' warning icon and a 'Not Phishing' status.

**Mailbox**  
Compose +

Inbox  
Sent  
Drafts  
Junk

Contacts  
Kelly Reid  
Andrew Graham  
Claire Pickett  
Robert Walker  
Amy Palmer

Search

Focused Other

- EPhish  
Hi Emma! Welcome to the ephish Quiz  
Welcome to the EPhish anti-phishing learning tool...
- Microsoft  
URGENT: restore your account  
Dear user, we have noticed some...
- Amy Palmer  
Sales Annual Meeting Invitation  
Hi Emma. Hope you are well...
- Kelly Reid  
(No Subject)
- Claire Pickett  
Message from HR  
Hello, An information document has been...
- Life of Giving Foundation  
Your donation could help save a life.  
For 30 years we have been helping...
- Eslips  
Payslip Error  
Dear employee, There was a problem...
- Robert Walker  
**IMPORTANT: Transfer Needed TODAY**  
Hi Emma. I need you to do me a favour... **new**
- Andrew Graham  
**Annual IT Newsletter Available!**  
Hi all, A quick reminder that the annual... **new**

No further emails

Help Phishing Not Phishing Previous Next

Eslips <eslips@gmail.com>  
01:00

Subject: Payslip Error

To: Emma

Dear employee,  
There was a problem generating your payslip. Please provide your details in the following link in order for you to be paid correctly. Failure to do so will result in not being paid.  
[click here](#)  
yours faithfully,  
Eslips Administrative Team  
All Right Reserved | Acceptable use Policy | Privacy Notice

F. Email 7 - CEO fraud (phishing)

The screenshot shows an Outlook mailbox interface. On the left is a navigation pane with 'Mailbox' (Compose +), 'Inbox', 'Sent', 'Drafts', 'Junk', and 'Contacts' (listing Kelly Reid, Andrew Graham, Claire Pickett, Robert Walker, and Amy Palmer). The main area is split into 'Focused' and 'Other' tabs. The 'Other' tab shows a list of emails, with the most recent one from Robert Walker selected. This email is marked as 'Phishing' and has a subject line 'IMPORTANT: Transfer Needed TODAY'. The email body contains a request for a transfer, stating that the sender is on holiday and cannot access their accounts, and asks the recipient to transfer money to a provider. The email is signed 'Robert Walker'.

Search [ ] [ ] [ ] [ ]

Help Phishing Not Phishing << Previous Next >>

**Focused** Other

- EPhish  
Hi Emma! Welcome to the ephish Quiz. Welcome to the EPhish anti-phishing learning tool...
- Microsoft  
URGENT: restore your account  
Dear user, we have noticed some...
- Amy Palmer  
Sales Annual Meeting Invitation  
Hi Emma. Hope you are well...
- Kelly Reid  
(No Subject)
- Claire Pickett  
Message from HR  
Hello, An information document has been...
- Life of Giving Foundation  
Your donation could help save a life  
For 30 years we have been helping...
- Eslips  
Payslip Error  
Dear employee, There was a problem...
- Robert Walker  
IMPORTANT: Transfer Needed TODAY  
Hi Emma, I need you to do me a favour...
- Andrew Graham  
Annual IT Newsletter Available!  
Hi all, A quick reminder that the annual... **new**

No further emails

**RW** <robert.walker@OXbanking.com>  
9:00

**Subject:** IMPORTANT: Transfer Needed TODAY

**To:** Emma

Hi Emma,

I need you to do me a favour. There is a pending invoice to one of our providers and as i am on holiday i cannot access the accounts from here. I have told them to send through their email to you with their account link and the amount of money they require (check spam folder in case accidentally blocked!). Just click on link in their email and transfer the amount they have requested.

This needs to be done TODAY as a high priority.

Any questions, please reply to this email. I cannot take calls right now so reply to the email instead.

Thanks,

Robert Walker

G. Email 8 - IT Newsletter (Not Phishing)

The screenshot shows an email client interface. On the left is a sidebar with 'Mailbox' and a 'Compose +' button. Below are folders: 'Inbox', 'Sent', 'Drafts', 'Junk', and 'Contacts'. The 'Contacts' list includes Kelly Reid, Andrew Graham, Claire Pickett, Robert Walker, and Amy Palmer. The main area shows a list of emails under 'Focused' and 'Other' tabs. The selected email is from Andrew Graham (AG) with the subject 'Annual IT Newsletter Available!'. The email content includes a greeting, a reminder about the newsletter, and a signature 'Andy'.

**Mailbox**  
Compose +

**Inbox**  
Sent  
Drafts  
Junk

**Contacts**  
• Kelly Reid  
• Andrew Graham  
• Claire Pickett  
• Robert Walker  
• Amy Palmer

Search

**Focused**   **Other**

- EPhish  
Hi Emma! Welcome to the ephish Quiz  
Welcome to the EPhish anti-phishing learning tool...
- Microsoft  
URGENT: restore your account  
Dear user, we have noticed some...
- Amy Palmer  
Sales Annual Meeting Invitation  
Hi Emma. Hope you are well...
- Kelly Reid  
(No Subject)
- Claire Pickett  
Message from HR  
Hello, An information document has been...
- Life of Giving Foundation  
Your donation could help save a life  
For 30 years we have been helping...
- Eslips  
Payslip Error  
Dear employee, There was a problem...
- Robert Walker  
IMPORTANT: Transfer Needed TODAY  
Hi Emma, I need you to do me a favour...
- Andrew Graham  
Annual IT Newsletter Available!  
Hi all, A quick reminder that the annual...

No further emails

Help   Phishing   Not Phishing   << Previous   Next >>

AG <andrew.graham@OXbanking.com >  
10:00

Subject: Annual IT Newsletter Available!

To: Emma; Amy Palmer; Robert Walker; Kelly Reid; Claire Pickett

Hi all,

A quick reminder that the annual IT newsletter is now available. I think its really important everyone reads it to find out the latest IT news. You can either access the newsletter [here](#) or pick a copy up at the front desk.

Happy reading!

Kind Regards,

Andy

## H. Canvas.Js charting library (Pie Charts)

```
// Make pie chart for Correct/Incorrect

function make_chart() {

  var co = window.sessionStorage.getItem('Correct');
  var ico = window.sessionStorage.getItem('Incorrect');

  var chart = new CanvasJS.Chart("chartContainer", {
    animationEnabled: true,
    title: {
      text: "Overall chart of Incorrect to Correct answers"
    },
    data: [{
      type: "doughnut",
      startAngle: 240,
      yValueFormatString: "##0",
      indexLabel: "{label} {y}",
      dataPoints: [
        {y: co, label: "Correct:", color: "#ccff66"},
        {y: ico, label: "Incorrect:", color: "#ff6666"},
      ]
    }]
  });
  chart.render();
}
```

## 9. References

- [1] Rosenthal.Maddie.(2021).Must-Know Phishing Statistics Updated 2021. Available at: [https://www.tessian.com/blog/phishing-statistics-2020/#:~:text=Google%20has%20registered%20%2C145%2C013%20phishing,same%20period%20\(up%2032%25\)](https://www.tessian.com/blog/phishing-statistics-2020/#:~:text=Google%20has%20registered%20%2C145%2C013%20phishing,same%20period%20(up%2032%25).). (Accessed 10/02/2021).
- [2] IBM.(2020). Cost of a Data Breach Report Highlights Available at: <https://www.ibm.com/security/data-breach> (Accessed at 03/02/2021).
- [3] Laliberte.Marc.(2019).Why phishing education has nexver been more critical to your business Available at:<https://www.helpnetsecurity.com/2019/06/18/phishing-education/>.(Accessed 03/02/2021).
- [4] H.Jason.(2007).Does Anti-Phishing Training work? Available at: <http://www.cs.cmu.edu/~jasonh/publications/apwg-ecrime2007-johnny.pdf>. (Accessed 03/02/2021).
- [5]Petock.Mike.(2020).Anti-Phishing Training: Is It working? Is It Worth It?.Available at: <https://insights.sei.cmu.edu/blog/anti-phishing-training-is-it-working-is-it-worth-it/> (Accessed 04/02/2021).
- [6] Sheng.Steve, Holbrook.Mandy, Kumaraguru.Ponnurangam, Cranor.Lorrie, Downs.Julie.(2010).Who Falls for Phish? A Demographic Analysis of Phishihng Susceptibility and Effectiveness of Interventions.Available at:<https://lorrie.cranor.org/pubs/pap1162-sheng.pdf> (Accessed 04/02/2021).
- [7] Rutten.Nico, R.van Joolingen.Wouter, T.van der veen.Jan.(2011).The learning effects of computer simulations in science education.Available at:<https://www.sciencedirect.com/science/article/abs/pii/S0360131511001758>.(Accessed 05/02/2021).
- [8] Alraddady.Sara, Luong.Danny, Young.G.(2014).A study of Kinesthetic Learning Activities Effectiveness in Teaching Computer Algorithms.Available at:<https://search.proquest.com/openview/e8fd77095fc686dd061f373c134decf9/1?pq-origsite=gscholar&cbl=1976352>.(Accessed 05/02/2021).
- [9] Reinheimer.Benjamin, Aldag.Lukas, Mayer.Peter, Mossano.Mattia, Duezguen.Reyhan, SECUSO-Security, Usability, Society, Karlsruhe Institute of Technoogy; Lofthouse.Bettina, Landesamt fur Geoinformation und Landesvermessung Niedersachsen; von Landesberger.Tatina, Volkamer.Melanie, SECUSO-security, usability,society, Karlsruhe Institute of Technology.(2020).An investigation of phishing awareness and education over time:when and how to best remind users.Available at:[https://www.usenix.org/system/files/soups2020-reinheimer\\_0.pdf](https://www.usenix.org/system/files/soups2020-reinheimer_0.pdf).(Accessed 10/02/2021).
- [10] Zambito.Victoria.(2018).11 principles of eLearning: Demystified And Applied. Available atL<https://elearningindustry.com/principles-of-elearning-demystified-applied>.(Accessed 10/02/2021).
- [11] Nielsen.Jakob.(2020).10 Usability Heuristics for User Interface Design.Available at:<https://www.nngroup.com/articles/ten-usability-heuristics/>.(Accessed 10/02/2021).
- [12] Forcepoint.(2021).What is spoofing? Available at:[https://www.forcepoint.com/cyber-edu/spoofing#:~:text=Spoofing%20is%20the%20act%20of,Name%20System%20\(DNS\)%20server.](https://www.forcepoint.com/cyber-edu/spoofing#:~:text=Spoofing%20is%20the%20act%20of,Name%20System%20(DNS)%20server.)(Accessed 12/02/2021).
- [13] Greany.Kirstie.(2019).ELearning best practices. Available at:<https://www.elucidat.com/elearning-best-practice/>.(Accessed 11/02/2021).

- [14] UC Berkley Information Security Office.(2017).Phishing Example:Message from human resources.Available at:<https://security.berkeley.edu/news/phishing-example-message-human-resources>. (Accessed 20/02/2021).
- [15] Alsultanny.Yas, Mohamed.Nouby.Ahmed, Al-Enazi Tala.(2014).Effects of using simulation in e-learning programs on misconceptions and motivations towards learning.Available at:[https://www.researchgate.net/publication/280904596\\_Effects\\_of\\_using\\_simulation\\_in\\_e-learning\\_programs\\_on\\_misconceptions\\_and\\_motivations\\_towards\\_learning](https://www.researchgate.net/publication/280904596_Effects_of_using_simulation_in_e-learning_programs_on_misconceptions_and_motivations_towards_learning).(Accessed 20/02/2021).
- [16] Ellis.David.(2021).7 ways to Recognise a Phishing Email: Email Phishing Examples. Available at:<https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email>.(Accessed 20/02/2021).
- [17] Cofense.(2021). How to Spot Phishing Emails - 7 Helpful Tips for Employees.Available at:<https://cofense.com/knowledge-center/how-to-spot-phishing/>.(Accessed 20/02/2021).
- [18] Benishti.Eyal.(2017).The Limitations of Phishing Education.Available at:<https://www.darkreading.com/threat-intelligence/the-limitations-of-phishing-education/a/d-id/1327786>.(Accessed 20/02/2021).
- [19] Kaspersky daily.(2021).The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within.Available at:<https://www.kaspersky.com/blog/the-human-factor-in-it-security/>.(Accessed 20/02/2021).
- [20] Damian.(2017).The Power of Immediate learner Feedback in E-Learning.Available at:<https://www.capytech.com/index.php/2017/05/23/power-immediate-learner-feedback-e-learning/>.(Accessed 21/02/2021).
- [21] Rosenthal.Maddie.(2021).Phishing Awareness Training: How Effective is Security Training? Available at:<https://www.tessian.com/blog/pros-and-cons-phishing-awareness-training/#not-targeted>.(Accessed 21/02/2021).
- [22] Dzuba.Elaine.(2020).Phishing Education & Awareness Training. Available at:<https://www.area1security.com/blog/phishing-education-awareness/>.(Accessed 28/02/2021).
- [23] Lord.Nate.(2020).Phishing Attack Prevention: How to Identify & Avoid Phishing Scams in 2019.Available at:<https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams>.(Accessed 28/02/2021).
- [24] Lee.James, Li.Wanru, L.Greitzer.Frank, Yousefi.Bahram, B.Laskey.Kathryn, Purl.Justin.(2020).Experimental Investigation of Demographic Factors Related to Phishing Susceptibility.Available at:<https://scholarspace.manoa.hawaii.edu/bitstream/10125/64015/1/0221.pdf>.(Accessed 28/02/2021).
- [25] P.Yonelinas.Andrew.(2002).The Nature of Recollection and Familiarity: A review of 30 Years of Research.Available at:<https://www.sciencedirect.com/science/article/abs/pii/S0749596X02928640>.(Accessed 01/03/2021).
- [26] Kirschner.Josh.(2019).Facebook "IS THIS YOU?" Video Scam Steals Your Login Info.Available at:<https://www.techlicious.com/blog/facebook-is-this-you-video-scam/>.(Accessed 27/02/2021).
- [27] GCFGGlobal.(2021).Email Basics: Common Email Features.Available at:<https://edu.gcfglobal.org/en/email101/common-email-features/1/>.(Accessed 02/03/2021).
- [28] Chaudhry.Aliya.(2020).How to change your inbox layout in Gmail.Available at:<https://www.theverge.com/21310155/gmail-inbox-layout-email-customize-tabs-priority-messages-google>.(Accessed 02/03/2021).

- [29] Protonmail.(2021).Available at:<https://protonmail.com/support/wp-content/uploads/2016/01/Screen-Shot-2016-01-20-at-9.46.04-AM.png>.(Accessed 03/03/2021).
- [30] Outlook Team.(2015).New Features coming to Outlook on the web.Available at:<https://www.microsoft.com/en-us/microsoft-365/blog/2015/08/04/new-features-coming-to-outlook-on-the-web/>.(Accessed 03/03/2021).
- [31] Tian.Chuan, L.Jensen.Matthew.(2019).Effects of Emotional Appeals on Phishing Susceptibility.Available at:[https://www.albany.edu/wisp/includes/WISP2019\\_proceedings/WISP2019\\_paper\\_6.pdf](https://www.albany.edu/wisp/includes/WISP2019_proceedings/WISP2019_paper_6.pdf).(Accessed 03/03/2021).
- [32] Express Computer.(2020).The impact of COVID-19 on the data breach landscape.Available at: <https://www.expresscomputer.in/guest-blogs/the-impact-of-covid-19-on-the-data-breach-landscape/61884/>.(Accessed 10/03/2021).
- [33] Brewster.Thomas.(2020).Coronavirus Scam Alert: Watch Out For These Risky COVID-19 Websites And Emails.Available at:<https://www.forbes.com/sites/thomasbrewster/2020/03/12/coronavirus-scam-alert-watch-out-for-these-risky-covid-19-websites-and-emails/>.(Accessed 10/03/2021).
- [34] RedJelli Technology LTD.(2021).Microsoft Phishing Email.Available at:<https://www.redjelli.com/microsoft-phishing-email/>.(Accessed 10/03/2021).
- [35] Northwestern Bank.(2020).Watch out for these coronavirus related scams.Available at:<https://www.nwbonline.bank/about/blog/watch-out-for-these-coronavirus-related-scams>.(Accessed 10/03/2021).
- [36] Calvert.Deb.(2021).Six preferred learning styles for adults-Adapt your message for better response.Available at:<http://www.managingamericans.com/Workplace-Communication-Skills/Success/Six-preferred-learning-styles-for-adults-424.htm>.(Accessed 20/04/2021).
- [37] Meharchandani.Dhwani.(2020).Staggering Phishing Statistics in 2020.Available at:<https://securityboulevard.com/2020/12/staggering-phishing-statistics-in-2020/#:~:text=The%20Shocking%20Phishing%20Statistics%20of%202020&text=Only%203%25%20of%20t>.(Accessed 20/04/2021).
- [38]
- [39] Liang.Hai, J.H.Zhu.Jonathan.(2017).Big Data, Collection of (Social Media, Harvesting).Available at:[https://www.researchgate.net/profile/Hai-Liang/publication/320929016\\_Big\\_Data\\_Collection\\_of\\_Social\\_Media\\_Harvesting/links/5a25fef80f7e9b71dd09db5d/Big-Data-Collection-of-Social-Media-Harvesting.pdf](https://www.researchgate.net/profile/Hai-Liang/publication/320929016_Big_Data_Collection_of_Social_Media_Harvesting/links/5a25fef80f7e9b71dd09db5d/Big-Data-Collection-of-Social-Media-Harvesting.pdf).(Accessed 21/04/2021)
- [40] Liyange.Eranga.(2016).10 Usability heuristics explained.Available at:<https://medium.com/@erangatl/10-usability-heuristics-explained-caa5903faba2> .(Accessed 21/04/2021).
- [41] Langmajer.Michal.(2019).10 Usability Heuristics Every Designer Should Know.Available at:<https://uxdesign.cc/10-usability-heuristics-every-designer-should-know-129b9779ac53>.(Accessed 01/05/2021).
- [42] UC Berkley Information Security Office.(2021).PHISHING EXAMPLE:UPDATE EMAIL:Don't lose access to your account!!.Available at:<https://security.berkeley.edu/news/phishing-example-update-email-dont-lose-access-your-account>.(Accessed 01/03/2021).

[43] Sherwin.Katie.(2018).Natural Mappings and Stimulus-Response Compatibility in User Interface Design.Available at:<https://www.nngroup.com/articles/natural-mappings/>.(Accessed 01/03/2021).

[44] Center for Internet Security.(2021).A short guide for spotting Phishing Attempts.Available at:<https://www.cisecurity.org/blog/a-short-guide-for-spotting-phishing-attempts/>.(Accessed 01/03/2021).

[45] Quostar.(2020).4 examples of scam emails targeting businesses.Available at:<https://www.quostar.com/blog/business-scam-email-examples/>.(Accessed 03/03/2021).

[46] UC Berkley Information Security Office.(2021).<https://security.berkeley.edu/resources/phish-tank>.(Accessed 01/03/2021).

[47] UC Berkley Information Security Office.(2016).Phishing Example: Important Announcement from Chancellor Dirks.Available at: <https://security.berkeley.edu/news/phishing-example-important-announcement-chancellor-dirks>.(Accessed 03/03/2021).

[48] CanjvasJS.(2021).Available at:<https://canvasjs.com/>.(Accessed 04/03/2021)

[49] Your Dictionary.(2021).Examples of Heuristics in Everyday Life.Available at:<https://examples.yourdictionary.com/examples-of-heuristics.html>.(Accessed 05/03/2021).

[50] Konstanrinovsky.Michelle.(2020).You already User Heuristics Every Day.Here's What They Are.Available at:<https://science.howstuffworks.com/life/inside-the-mind/human-brain/heuristics.htm>.(Accessed 05/03/2021).

[51] Steinberg.Joseph.(2019).Why Scammers make Spelling and Grammar "mistakes".Available a:<https://josephsteinberg.com/why-scammers-make-spelling-and-grammar-mistakes/>.(Accessed 10/03/2021).

[52]Pyorre.Josh.(2020).Grammar and Spelling Errors in Phishing and Malware.Available at: <https://umbrella.cisco.com/blog/grammar-and-spelling-errors-in-phishing-and-malware>.(Accessed 10/03/2021).

[53] Shashidhar.Narasimha, Hossain,Nabil, Verma.Rakesh.(2012).Detecting Phishing Emails the Natural Language Way.Available at:[https://www.researchgate.net/publication/278689575\\_Detecting\\_Phishing\\_Emails\\_the\\_Natural\\_Language\\_Way](https://www.researchgate.net/publication/278689575_Detecting_Phishing_Emails_the_Natural_Language_Way).(Accessed 10/03/2021).

[54] Turunen.Helina.(2021).Attachments in Phishing 101 Available at:<https://www.hoxhunt.com/blog/attachments-in-phishing-101/>.(Accessed 12/03/2021).

[55] Ducklin.Paul.(2020).Serious Security:Phishing without links when phishers bring along their own web pages.Available at:<https://nakedsecurity.sophos.com/2020/10/02/serious-security-phishing-without-links-when-phishers-bring-along-their-own-web-pages/>.(Accessed 12/03/2021).

[56] Porter.Kim.(2020).What is Phishing? How to recognize and avoid phishing scams.Available at: <https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html>.(Accessed 12/03/2021).

[57] Usecure.(2021).Free resources & content to help you drive security awareness.Available at:<https://www.usecure.io/resource-centre>.(Accessed 12/03/2021).

[58]IT Governance.(2021).Free Phishing Resources.Available at: <https://www.itgovernance.co.uk/phishing/free-phishing-resources>.(Accessed 12/03/2021).

[59] Cisco.(2021).The modern cybersecurity landscape scalding for threats in motion.Available at: [https://umbrella.cisco.com/info/technical-paper-modern-security-landscape-scaling-threats-motion?utm\\_medium=search-paid&utm\\_source=google&utm\\_campaign=UMB\\_21Q4\\_UK\\_EN\\_GS\\_Nonbrand\\_Threats&utm\\_term](https://umbrella.cisco.com/info/technical-paper-modern-security-landscape-scaling-threats-motion?utm_medium=search-paid&utm_source=google&utm_campaign=UMB_21Q4_UK_EN_GS_Nonbrand_Threats&utm_term)

=pgm&utm\_content=UMB-FY21-Q2-Content-Technical-Papers-The-Modern-Cybersecurity-Landscape&\_bt=517637600316&\_bk=%2Banti%20%2Bphishing&\_bm=b&\_bn=g&\_bg=122332508795&gclid=CjwKCAjwnPOEBhA0EiwA609ReZyfiaBu\_yGTPgS47KSOy8Nt3DwFEYrtbLhE1fYU5VFFhSs0\_hDIYRoCLRMQAvD\_BwE.(Accessed 12/03/2021).

[60] Sophos Phish Threat.(2021).Sophos Phish Threats.Available at:[https://www.sophos.com/en-us/products/phish-threat.aspx?gclid=aw.ds&&cmp=75925&utm\\_campaign=GPD-2020-UKI-PaidSearch-Google-EN-RLSA-NB-Education-DG-75925&utm\\_medium=cpc&utm\\_content=NB\\_Education&utm\\_term=%2Bphishing+%2Beducation&utm\\_source=google-search&gclid=CjwKCAjwnPOEBhA0EiwA609ReS\\_kzf8KGHZazCGRNLHDYfs6\\_Cs16YPenY-NmYgYWr43q3pVXtwshoCsvoQAvD\\_BwE](https://www.sophos.com/en-us/products/phish-threat.aspx?gclid=aw.ds&&cmp=75925&utm_campaign=GPD-2020-UKI-PaidSearch-Google-EN-RLSA-NB-Education-DG-75925&utm_medium=cpc&utm_content=NB_Education&utm_term=%2Bphishing+%2Beducation&utm_source=google-search&gclid=CjwKCAjwnPOEBhA0EiwA609ReS_kzf8KGHZazCGRNLHDYfs6_Cs16YPenY-NmYgYWr43q3pVXtwshoCsvoQAvD_BwE).(Accessed 12/03/2021).

[61] Cofense.(2021).Available at:<https://cofense.com/awareness-resources/>.(Accessed 13/03/2021).

[62] APWG.(2021).Unifying the Global Response to cybercrime.Available at:<http://phish-education.apwg.org/r/en/index.htm>.(Accessed 13/03/2021).

[63] Jampen.Daniel, Gur.Gurkan, Sutter.Thomas, Tellenback.Bernhard.(2020).Don't Click:towards an effective anti-phishing training. A comparative literature review.Available at:<https://hcis-journal.springeropen.com/articles/10.1186/s13673-020-00237-7>.(Accessed 04/05/2021).

[64] Paci.Federica, De Bona Marco.(2020).A real world study on employees' susceptibility to phishing attacks.Available at:<https://dl.acm.org/doi/abs/10.1145/3407023.3409179>.(Accessed 13/04/2021).

[65]hashedout.(2021).The Dirty Dozen The 12 most expensive phishing attacks in history.Available at: <https://www.thesslstore.com/blog/the-dirty-dozen-the-12-most-costly-phishing-attack-examples/#:~:text=Phishers%2C%20pretending%20to%20be%20the,phone%20number%20was%20registered%20using>.(Accessed 14/03/2021).