

**SE
TU**

Ollscoil
Teicneolaíochta
an Oirdheiscirt

South East
Technological
University

PhishGuardian – An Online Phishing Awareness Tool for Older Adults

Robert Stynes
C00136717

Contents

1	Project Overview	3
1.1.1	Key Objectives.....	3
1.1.2	Key Achievements.....	3
2	What Was Achieved?.....	4
2.1	Research	4
2.1.1	Part 1	4
2.1.2	Part 2	5
2.2	Surveys.....	6
2.2.1	Survey One	6
2.2.2	Survey Two	11
2.3	Web Application.....	14
2.3.1	Application Design.....	14
2.3.2	Application Function.....	14
2.3.3	Quiz	15
3	Technologies	17
3.1	HTML	17
3.2	PHP	17
3.3	JavaScript	18
3.4	XAMPP.....	18
3.5	Docker	19
3.6	HeidiSQL.....	19
3.7	Ngrok	20
3.8	Microsoft Forms	20
4	What Wasn't Achieved?	21
4.1	Forgot Password	21
5	Application Development Evolution	22
5.1	Design Changes.....	22
5.2	Static to Dynamic HTML	23
5.3	Leaderboard Changes	24
5.4	Quiz Changes	25
6	Testing	26
6.1	Usability Testing.....	26
6.1.1	Methodology.....	26
6.1.2	Key Findings	26
6.2	Functionality Testing.....	27
6.2.1	Methodology.....	27

6.2.2	Key Findings	27
6.3	Working With Other Students	28
7	Technical Issues	29
7.1	Problems Encountered.....	29
7.1.1	Docker/MyPHPAdmin	29
7.1.2	Moving quiz to database.....	29
7.1.3	Final Survey/Hosting Site Online	30
7.1.4	Edit Content.....	31
8	General Issues.....	33
8.1	Problems Encountered.....	33
8.1.1	Surveys	33
8.1.2	Learning	33
9	What I learned.....	34
9.1	PHP Knowledge	34
10	What I Would Do Differently Starting Again.....	35
10.1	Use/Learn Python	35
10.2	Implement Security Earlier	35
11	Cyber Security Relevance	36
11.1	Projects General Relevance	36
11.2	Security Features to Enhance Cybersecurity	37
12	Conclusion	38
13	Acknowledgements.....	38
14	References.....	39
15	Appendix	40
15.1	User Interface.....	40
15.2	Admin Interface.....	45

1 Project Overview

This project is a web-based platform designed to deliver information and interactive learning modules on phishing prevention for older adults. It features clear language, and engaging multimedia elements to enhance user experience and comprehension. The content will cover various aspects of phishing, including common tactics used by cybercriminals, warning signs of phishing attempts, and best practices for safely navigating online environments.

1.1.1 Key Objectives

Accessibility: Ensure that the tool is accessible to older adults with varying levels of digital literacy by using simple language, clear visuals, and intuitive design.

Engagement: Promote user engagement through interactive elements such as quizzes, and real-life examples to reinforce learning and retention.

Relevance: Tailor the content to address the specific concerns and challenges faced by older adults in the context of online security, including tactics commonly employed to target this demographic.

Empowerment: Empower older adults to take proactive measures to protect themselves against phishing attacks by equipping them with practical knowledge and skills.

Feedback: Implement a feedback mechanism to gather user input and insights for continuous improvement and optimization of the tool.

1.1.2 Key Achievements

Surveys: Two surveys were conducted, the first was to get information on older adult's knowledge of phishing to help structure the content for the application. The second to get feedback on the look and design of the site regarding older adult's usability.

Website: Developed a website using HTML, CSS, PHP, and JavaScript. The website features a clean interface with simplified navigation, clear visuals, and readable text, ensuring accessibility and ease of use for older users with varying levels of digital literacy.

Quiz: Created a quiz within the website to reinforce learning of the various phishing content, it is comprised of 10 questions with each question having multiple choice answers,

Website (Admin Portal): An admin portal was created to allow an admin to have various abilities like add, edit and delete a user along with editing and adding questions and editing the site content.

2 What Was Achieved?

2.1 Research

With the research phase of the project, my aim was to address to main questions, the vulnerabilities of older adults to online scams and the design requirements for an accessible and user-friendly interface for older adults. This section explores the research questions posed, the findings obtained, and their implications on the development of the project.

2.1.1 Part 1

First, I researched how older adults were being targeted showing specifically that those aged 60+ are more at risk of becoming victims of scams due to their lack of knowledge surrounding all things tech related. Scammers aware of this lack of knowledge find these older people as the perfect targets for the ever increasingly sophisticated scams they create, (Greggwirth, 2023).

It is now more important than ever to bring awareness to the older generation about these scams and provide them with the basic knowledge to protect themselves and their assets. In the USA in 2021 alone scammers cost the government more than \$120 million by targeting senior citizens pretending to be representatives from various government offices from the likes of the IRS (internal Revenue service), Social Security Administration and Medicare. The scammers would pose as officers from the mentioned offices by text, phone and/or email asking for the victim to send on personal details to correct an issue that had occurred with the victim's account. These scammers would often tell them that they needed to settle a debt to avoid further fines and/or face jail time. Obviously, a threat like that to anybody would make them more susceptible to these scams and they would end up sending on the information to ensure there would be no action taken against them, (Greggwirth, 2023).

Along with this I found that there was a rise in tech usage of older adults, be that device usage like tablets and smartphones or general online browsing and found as part of their research, Pew were able to show the increase in smartphone ownership amongst older adults. Poland and Japan having massive increases over a 7-year period with the U.S. from 2012 to 2021 having an increase of 48% from 13% to 61%, (Pew Research Center, 2022).

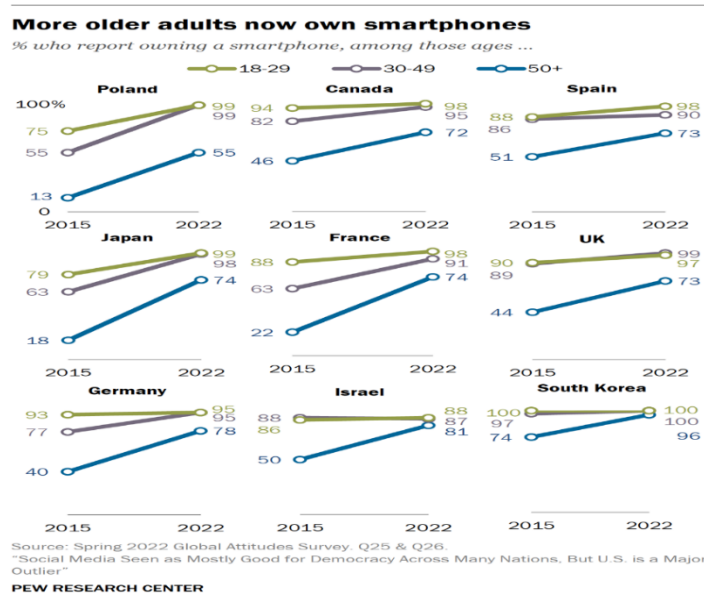


Figure 1 – Smartphone owners by country, (Anderson, 2017).

In another study by Pew Research Center, they concentrated on adults aged 65 and older. Within this study they showed that in the last 5 years smartphone usage/adoption has nearly quadrupled, stating that around 4 out of 10 adults over 65 own a smartphone which is about 42% which is up from 18%. The below images show the rise in both all adults (light blue) and adults over 65 (darker blue) and percent of adults by age who stated they own a smartphone, (Anderson, 2017).

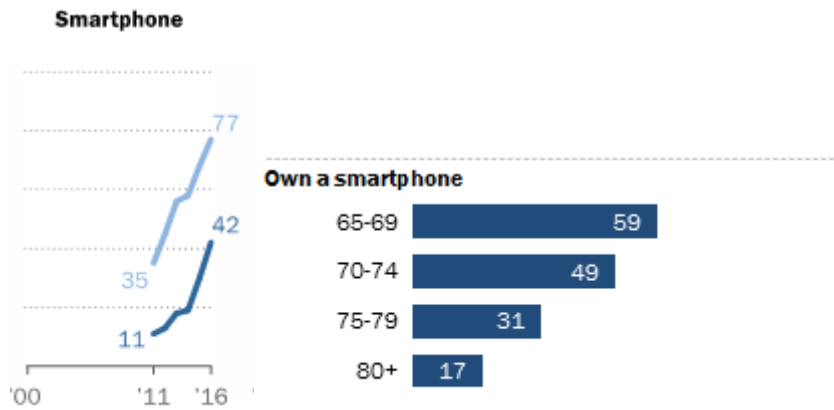


Figure 2 – Smartphone owners, (Anderson, 2017).

This is all covered more in depth in my research document ([Research Report](#)).

2.1.2 Part 2

In the second part of my research, I shifted my focus to how to design the application specifically for older adults. With the objective being to identify specific design aspects that would enhance the usability and accessibility for older adults.

Clear Formatting and Font Sizes:

Clear central formatting with larger font sizes and high contrast colour schemes are crucial for ensuring text readability, particularly for users with age-related vision changes. With initial findings stating as long as the font sizes were above 12 would be fine, (Moth, 2022). Once implementation started, I chose to increase the font to 20 for body text, with headings and important labels set higher. Regarding colour schemes, dark text on a light background or vice versa is optimal for readability. For example, black text on a white background or a dark grey background with white text.

Navigation and Interaction:

Straightforward navigation with clear labels is essential for facilitating ease of use. Easily clickable buttons and links improve user interaction, accommodating older adults who may have reduced motor skills or dexterity. Providing descriptive tooltips or icons alongside navigation elements can also reduce confusion while not fully being used in the application at the moment, it is something to be considered once feedback is received, (Making Your Website Senior Friendly 2019).

Feedback and User Input:

Implementing feedback mechanisms such as user surveys or suggestion forms allows older adults to provide input and share their experiences. This not only fosters a sense of involvement but also helps identify areas for improvement and optimization based on user feedback. This is being done with a section asking for feedback about the website and a button to link to a survey for users to give feedback on the design and general user experience of the application, (Adchitects blog, N.A.).

By incorporating these specific design aspects, the web-based application is tailored to meet the needs and preferences of older adults. With a focus on accessibility, readability, and ease of use, the application aims to empower older adults to navigate online environments confidently and securely. Ongoing testing and refinement, guided by user feedback, will ensure that the application continues to evolve and effectively support older adults in their digital experiences.

2.2 Surveys

As part of the project, I created and conducted two different surveys. The first survey was created to help get an understanding of older adult's knowledge of scams and phishing in general, the second survey was to get feedback from older adult users that have interacted with the application getting their input on the design and structure of the site to make sure it was easy to use for them and they could understand everything.

2.2.1 Survey One

It was initially going to be for a set age, but I then decided to change to a small age range of between 50 and 60+ as this gave a greater range of adults to survey. The hope was to still get mostly over the age of 60 which thankfully was the case.

1. What age bracket do you fall under?

[More Details](#)

[Insights](#)

● 50-55	7
● 56-60	9
● 60+	34



I wanted to get an idea of how much the older adults are using or accessing the internet, as seen below the use was quite frequent with most survey users stating that they used it daily. Along with this I asked which devices are used with a high use between both mobile phones and laptops, with mobile phones being the slightly preferred choice. This information helped to showcase what I had found while doing research that older adults had higher activity online and were using devices more, especially since Covid.

2. How often do you use the internet?

[More Details](#)

[Insights](#)

Daily	34
Weekly	10
Monthly	4
Never	2



6. What device(s) do you use to access the internet?

[More Details](#)

Laptop	35
Tablet	11
Mobile Phone	37



A critical piece of information that was found with the survey was 68% of the older adults taking the survey had never even heard of phishing, let alone knew what it was or its danger to them.

3. Have you ever heard of the term "phishing"?

[More Details](#)

[Insights](#)

Yes	16
No	34



Continuing from the data above, 64% said they felt they wouldn't be able to spot potential scam that they could be targeted by. These two statistics alone begin to highlight the need for older adults to be helped to gain a better knowledge of these dangers and how to protect themselves, especially against phishing with most of them using mobile phones and laptops for their online activities.

5. Do you feel you would be able to identify potential online scams?

[More Details](#)

[Insights](#)

● Yes	18
● No	32



This is further proven when you look at this with what they are using their devices for, with most of the activity being to send/receive emails or do online banking. This is a massive vulnerability to these older adults with most not knowing what a phishing email or text message may look like and accessing their bank account for example and falling victim to a phishing email that gains access to their accounts.

7. What activities do you do on the Internet?

[More Details](#)

● Email	41
● Shopping	24
● Social Media	21
● Online Chatting	8
● Banking	36



Interestingly, even though most had said they felt they would not be able to identify online scams, majority did say they received what they believe to have been suspicious looking emails or text messages. This could be from taking the online scam question to mean a more specific scam like on websites or it could be from the lack of knowledge of phishing combined with the fear of online scams as shown below. In saying that, they also mostly said they would not know what to do with a suspicious email or text message, which is still dangerous as they could accidentally click a malicious link or fall victim to other tactics.

8. How safe do you feel while using your devices online?

[More Details](#)

[Insights](#)

● Very safe	8
● Somewhat safe	18
● Somewhat unsafe	17
● Very unsafe	7

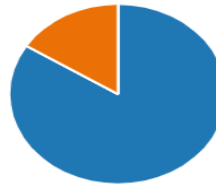


9. Have you ever received a suspicious looking email or text message?

[More Details](#)

[Insights](#)

● Yes	42
● No	8



10. Do you know what to do if you did receive a suspicious email or text message?

[More Details](#)

[Insights](#)

● Yes	18
● No	32



There were a small number of older adults who said they had been a victim of a phishing or online scam before. But concerningly some of those then stated that they wouldn't know what to do when/if they were a victim.

11. Have you ever been the victim of a phishing/online scam?

[More Details](#)

[Insights](#)

● Yes	9
● No	41



12. Would you know how to report it if you were?

[More Details](#)

[Insights](#)

● Yes	5
● No	45



Finally, the data shows that it was an even split down the middle with the survey users and their knowledge of what to do with their data online, this is a worrying statistic as it could lead to a lot of the older adults possibly sharing their information with the wrong person online which could lead to them falling victim to an attacker.

13. Do you know what information should never be shared online?

[More Details](#)

[Insights](#)

● Yes 25
● No 25



The findings from the survey conducted among older adults regarding their knowledge of scams and phishing reveal significant gaps in awareness. Despite the increasing use of the internet and digital devices among this demographic, a worrying number of respondents reported limited familiarity with phishing, with 68% indicating they had never even heard of it. This lack of awareness is compounded by the fact that 64% felt ill-equipped to identify potential scams targeting them online.

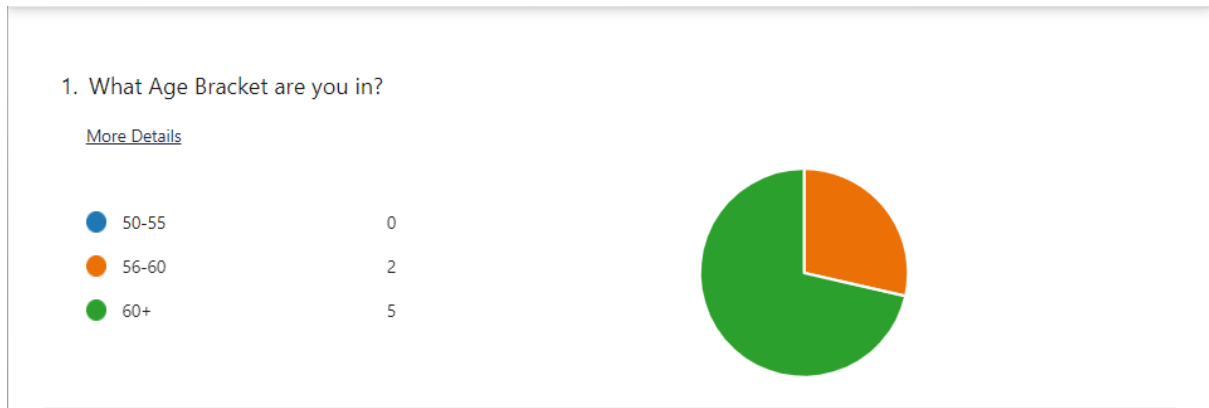
The data underlines the critical need for targeted education and support for older adults to improve their online safety. With most respondents using mobile phones and laptops for activities such as email communication and online banking, they are particularly vulnerable to phishing attacks. While many reported receiving suspicious emails or text messages, the majority expressed uncertainty about how to handle such situations effectively.

The survey also revealed a worrying inconsistency in knowledge regarding online data protection, with half of respondents unsure about safeguarding their personal information online. This knowledge gap increases the risk of inadvertently sharing sensitive data with malicious actors, potentially leading to devastating consequences.

In conclusion, addressing the knowledge gaps revealed by the survey through targeted educational initiatives is critical in safeguarding older adults against online scams and phishing attacks. By leveraging the insights collected from this research, I can develop proactive strategies to enhance resilience among this vulnerable demographic, ultimately fostering a safer and more secure online experience for all.

2.2.2 Survey Two

For the second survey I didn't get as much user feedback as I would of liked, but the data from the few I got back still proved to be extremely valuable as it showed me the website was achieving what it was suppose to with its design and structure



I stuck to the same age bracket for this as I had hoped to get feedback from all of the original users but was unable to in time.

2. Did you find the text on PhishGuardian easy to read?

[More Details](#)

Yes	7
No	0



All user that tested the website found that the test was easy to read, this validated my choice of increasing the font from the initial size to a accommodate more users.

4. Did you feel comfortable using PhishGuardian's interface?

[More Details](#)

Yes	7
No	0



Thankfully all users felt comfortable using the site and interacting with the various functions of the website.

6. Did you encounter any difficulties navigating through the website?

[More Details](#)

● Yes	0
● No	7



The next question asked the users if they had any difficulties navigating the website, with none having any issues and finding it easy to navigate and find where they wanted to go.

8. Did you find the instructions provided on PhishGuardian clear and easy to follow?

[More Details](#)

● Yes	7
● No	0



All users found the instructions throughout the site provided them with clear instructions helping them use the application fully.

9. Were you able to understand the wording used throughout the website?

[More Details](#)

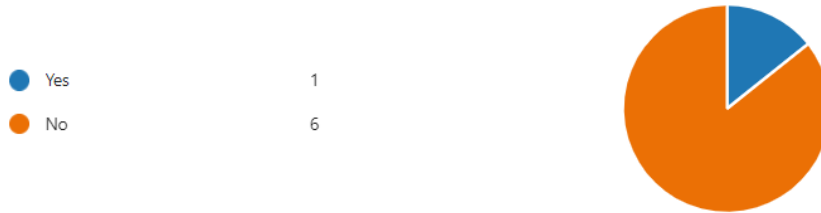
● Yes	7
● No	0



Next, users were asked about the content of the website and if they could understand the wording that was being used in the sections, I tried to make sure the language used was as simple as possible so users of all levels could understand and benefit. Thankfully all users said they were able to understand.

11. Were there any features or elements of the website that confused you?

[More Details](#)



I asked users if any parts of the website had confused them, most had found nothing did, but one user selected that something had confused them. Unfortunately, they did not put an answer for what it was in the box below this question, so I was unable to make any changes to improve this.

13. Do you have any additional comments or suggestions for improving the usability and design of PhishGuardian?

7 Responses

ID ↑	Name	Responses
1	anonymous	None that I can think of
2	anonymous	no
3	anonymous	no
4	anonymous	Website very easy to navigate
5	anonymous	grand job. enjoyed the quiz.
6	anonymous	no
7	anonymous	Found it very easy to use

Finally, I asked users for any suggestions or additional comments with most stating they had none and a few stating they found the site easy to use.

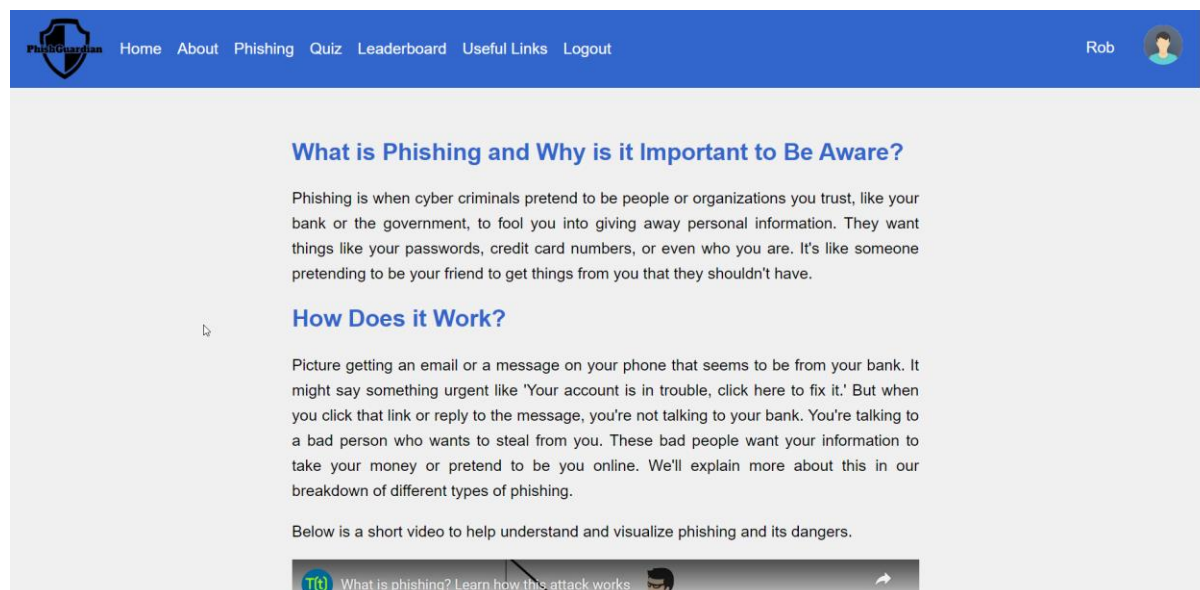
While the response rate for the second survey may have been lower than anticipated, the feedback received proved invaluable in validating the effectiveness of the website's design and structure. Despite the limited number of responses, the unanimous consensus among users regarding the ease of readability, navigation, and understanding of instructions confirmed the success of the design choices. The positive feedback regarding the clarity of language used in the content further emphasises the platform's accessibility to users of varying levels of digital literacy. While the identification of a potential point of confusion highlights the importance of getting thorough feedback, the survey results underline the website's ability to fulfil its intended purpose of providing a user-friendly and intuitive experience for older adults navigating the digital landscape.

2.3 Web Application

2.3.1 Application Design

I kept the design of the website as basic as I could with a grey background, this made it not as sharp on the eyes allow for the user to read the content easier. The font is clear and big for the older adult's ease of understanding and reading, I also centred all the text to keep it structured and easy to follow.

As part of the design process of this project I also created a logo for PhishGuardian, which can be seen in the top left corner of each of the web pages.



2.3.2 Application Function

The website has various functions with the main site being for users and then an area for admins to login and interact with various elements of the website.

2.3.2.1 Users

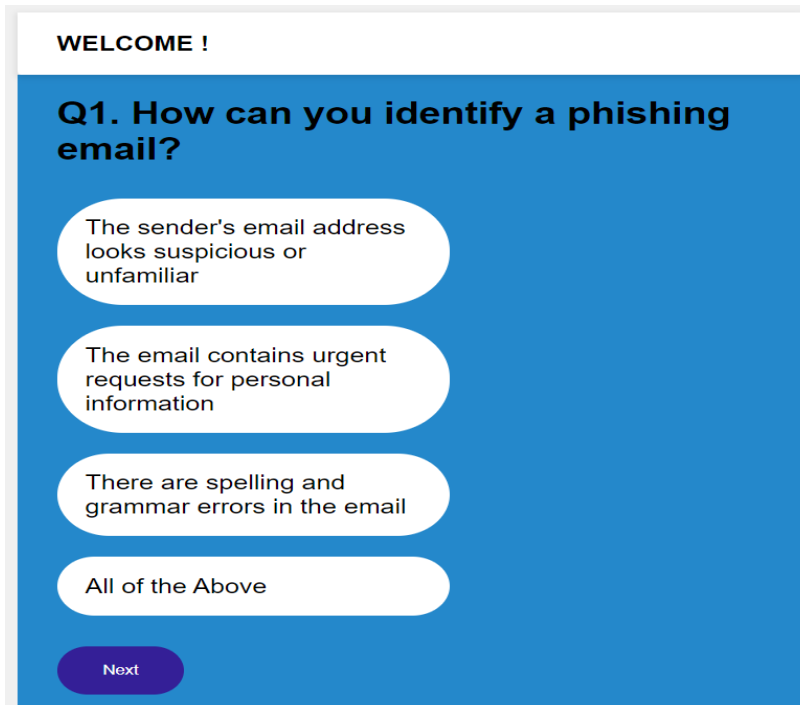
On the user side they can register, login, navigate through the various pages and sections, take the quiz, view, and edit their profile and view the leaderboard for all users who have taken the quiz.

2.3.2.2 Admins

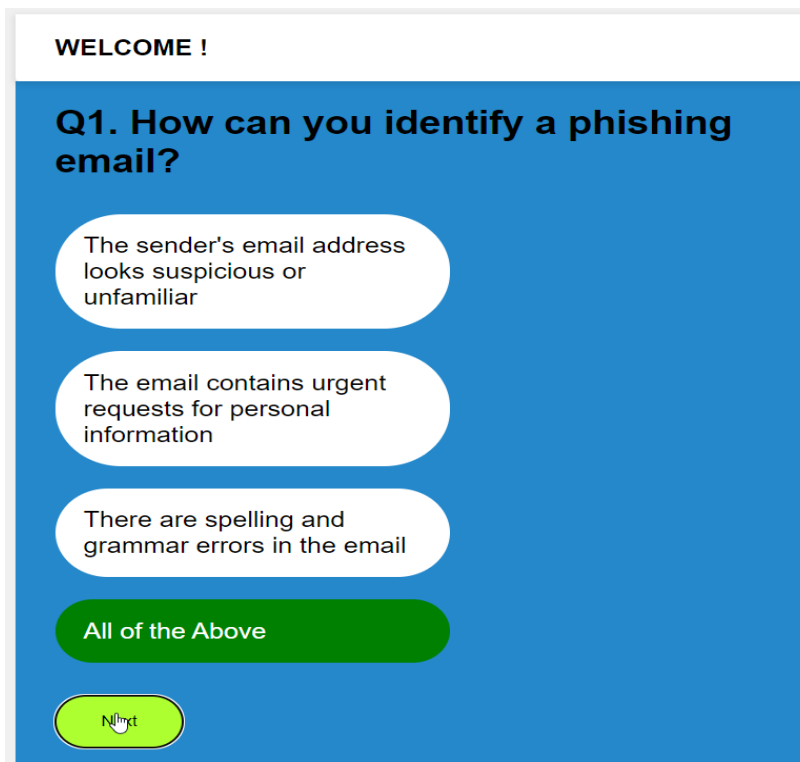
With the admins I created a portal for them to be able to do various functions like manage users (add/edit/delete), edit the content of the webpages, add questions to the quiz, edit the questions in the quiz and to add other admins.

2.3.3 Quiz

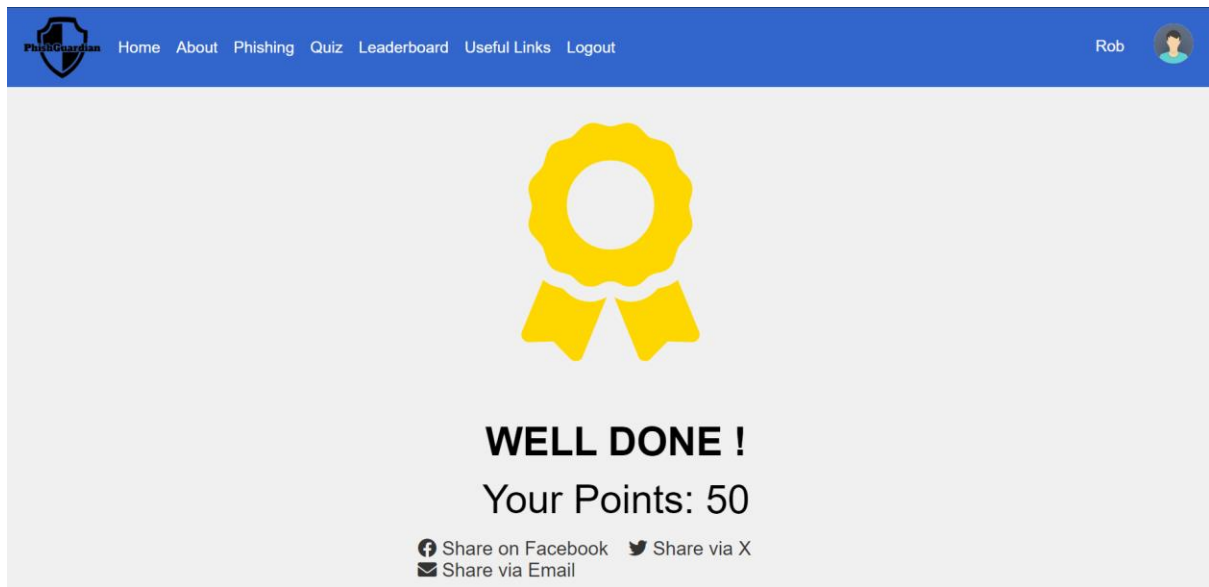
The quiz was fully completed, all of the questions are stored within the database which is what allows the admin to be able to interact with it from the admin portal. It is displayed to the user in a box in the middle of the screen with the question at the top and four possible answers.




The user then selects their answer and clicks the next button which will then change the selected answer to green or red indicating to the user if the answer was right or wrong. With the next question then being displayed to the user.



Once the user finishes the quiz, they are presented with a screen that displays their points from the quiz along with options to share to various places.



PhishGuardian Home About Phishing Quiz Leaderboard Useful Links Logout Rob



WELL DONE !
Your Points: 50

[Share on Facebook](#) [Share via X](#)
[Share via Email](#)

3 Technologies

For the development of this project, I used a number of different technologies, below is a brief run through of what was used and how they were used within the project.

3.1 HTML

I used HTML as the coding language for this project, it was used to create the structure and define the layout of each webpage.

```
1 <!DOCTYPE html>
2 <html>
3 <head>
4   <link rel="stylesheet" type="text/css" href="login.css">
5   <title>PhishGuardian</title>
6 </head>
7 <body>
8   <header>
9     <h1>PhishGuardian</h1>
10  </header>
11
12  <div class="container">
13    <form method="post" action="login.php">
14      <label for="Username">Username:</label>
15      <input type="text" id="Username" name="Username"><br><br>
16
17      <label for="Password">Password:</label>
18      <input type="password" id="Password" name="Password"><br><br>
19
20      <input type="submit" value="Login">
21    </form>
22  <div class="register-link"></div>
23  <p>Don't have an account? <a href="RegisterPage.php">Register Here</a>.</p>
24  <p>Admin? <a href="adminLoginPage.php">Login Here</a>.</p>
25 </div>
26
27 </body>
28 </html>
```

3.2 PHP

Most of the project is coded in and within PHP files, this was done because it was the main way I knew of building a web application. While I was able to get it done there are better options out there to keep the file count lower.

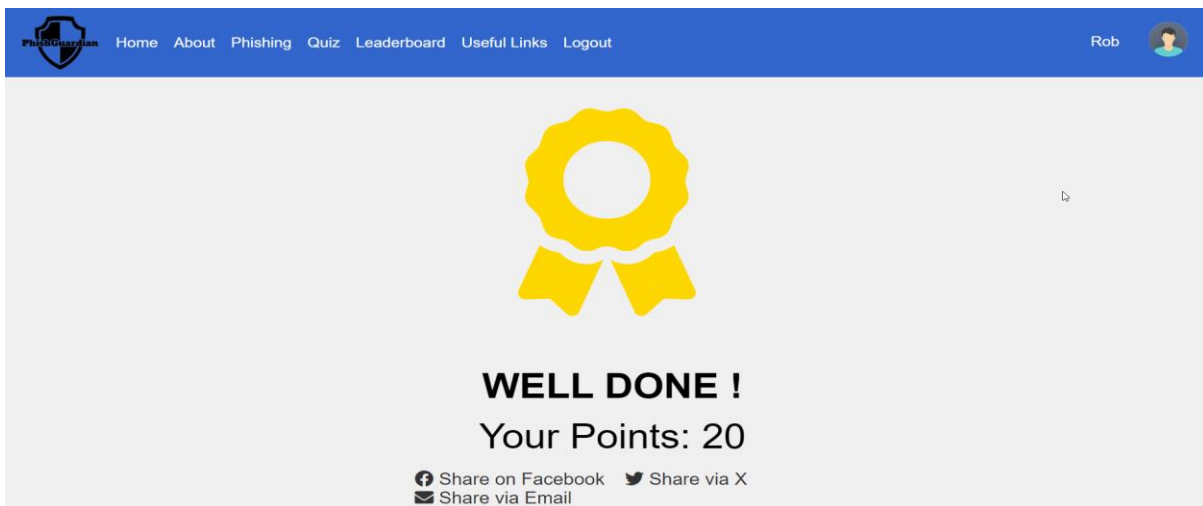
```
<?php
include_once 'dbh.inc.php';
include_once "decrypt.php";
include_once 'dbhKey.inc.php';
session_start();

// Retrieve user's key data from KeyStore
$FK_USER_ID = $_SESSION['User_ID'];
$stmt = $conn2->prepare("SELECT keyData FROM KeyStore WHERE User_ID = ?");
$stmt->bind_param("s", $FK_USER_ID);
$stmt->execute();
$result = $stmt->get_result();
```

3.3 JavaScript

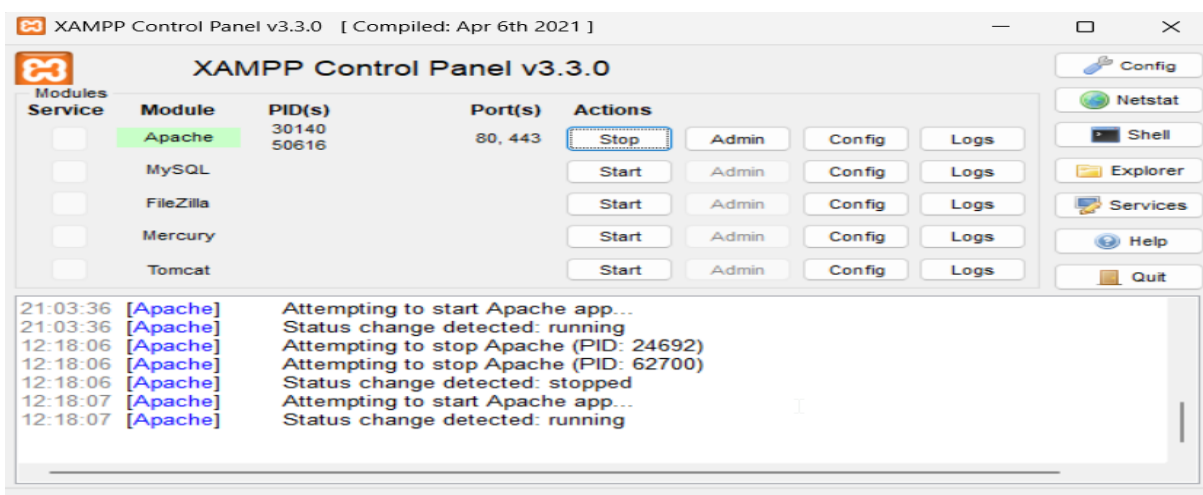
There is also a small amount of JavaScript being used in the project, this is used to be able to display the users score from the quiz at the end on a final page to show them how they did. I had tried to incorporate it to show how many answers were correct but could not get it to function correctly.

```
FYP > JS userinfo.js > ...
1 let user_name = sessionStorage.getItem("name");
2 let user_points = sessionStorage.getItem("points");
3 let user_correct_answers = sessionStorage.getItem("correctAnswers");
4
5 document.querySelector("span.name").innerHTML = user_name;
6 document.querySelector("span.points").innerHTML = user_points;
7 document.querySelector("span.correct").innerHTML = user_correct_answers;
8
```



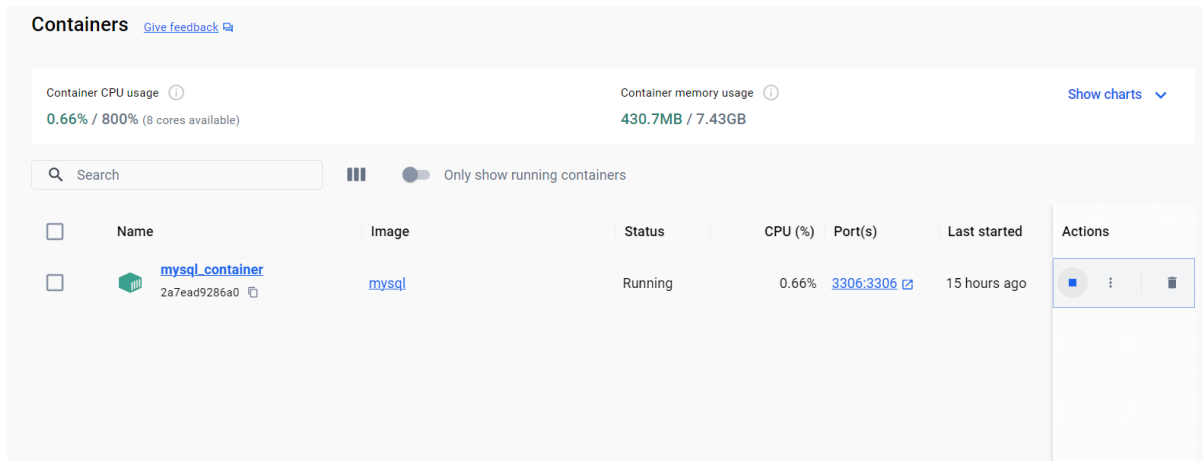
3.4 XAMPP

To be able to test and view the application when any edits and changes were made along with making it functional, I used XAMPP for the backend of the project. XAMPP allowed me to create a local environment on my machine with its Apache server letting me access it through a web browser to see and use it in that environment.



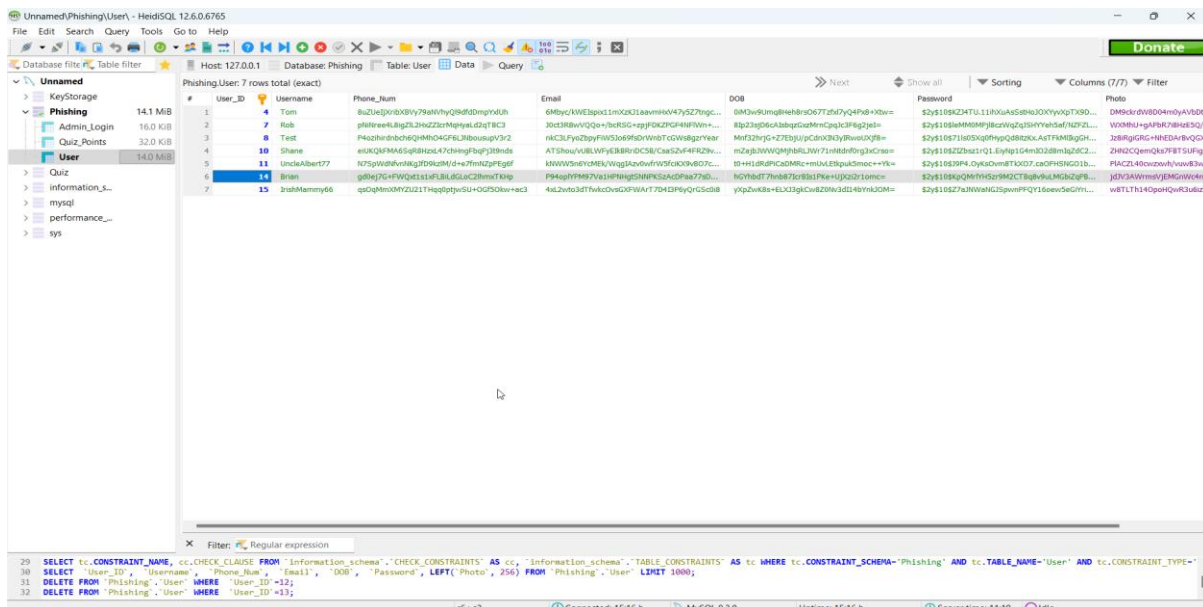
3.5 Docker

At the beginning of the project, I was using the in-built function within XAMPP for my database, but after coming into issues which I will speak about in more detail later in the document I swapped to docker. By containerising the database using Docker I could start up my database instance quickly and test the database without any issues.



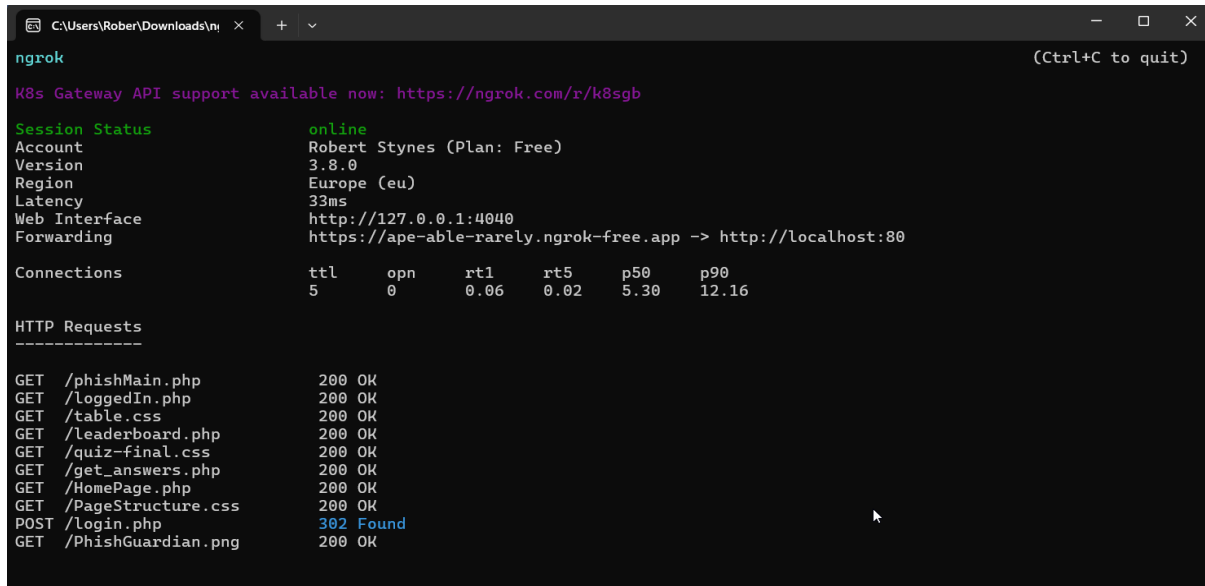
3.6 HeidiSQL

With the swap to docker I needed a new database management tool, having used it before I decided to go with HeidiSQL as I found its user interface to be very easy to use and understand. This let me interact with my database seamlessly making all the tasks I needed to perform nowhere near as trivial.



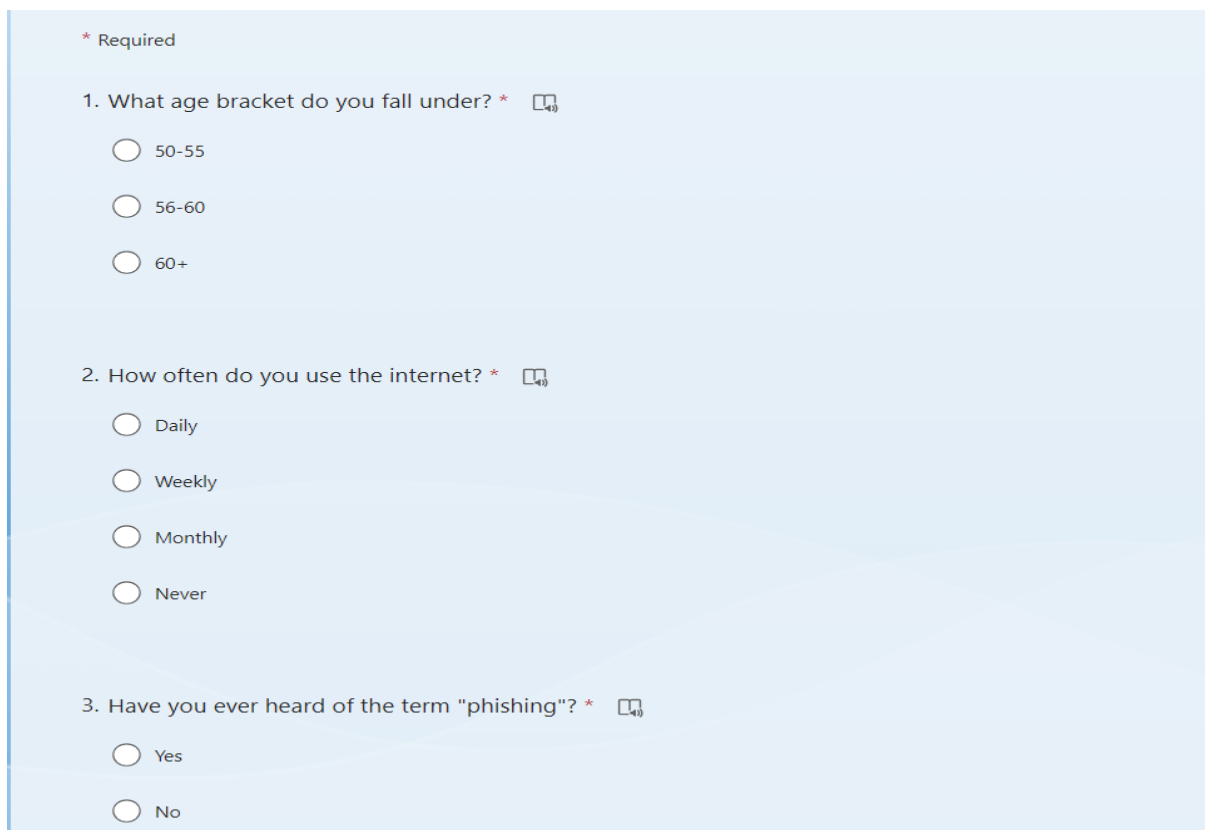
3.7 Ngrok

One of the final tools I used was ngrok, this allowed me to create a secure tunnel to my localhost web application. This tunnel then was what allowed me to send a link to users for them to be able to access my application on their own machines for testing.



3.8 Microsoft Forms

For my two surveys that I conducted, I chose to go with Microsoft Forms for both. This allowed me to create questions structured in a way I wanted to be able to get the best feedback.



4 What Wasn't Achieved?

4.1 Forgot Password

A feature I wanted to implement for this website was the ability to allow the user to reset their password if they had forgotten it, this would have been done through a link on the login page that would bring them to a page to enter their email address to receive a link to reset their password for the application.

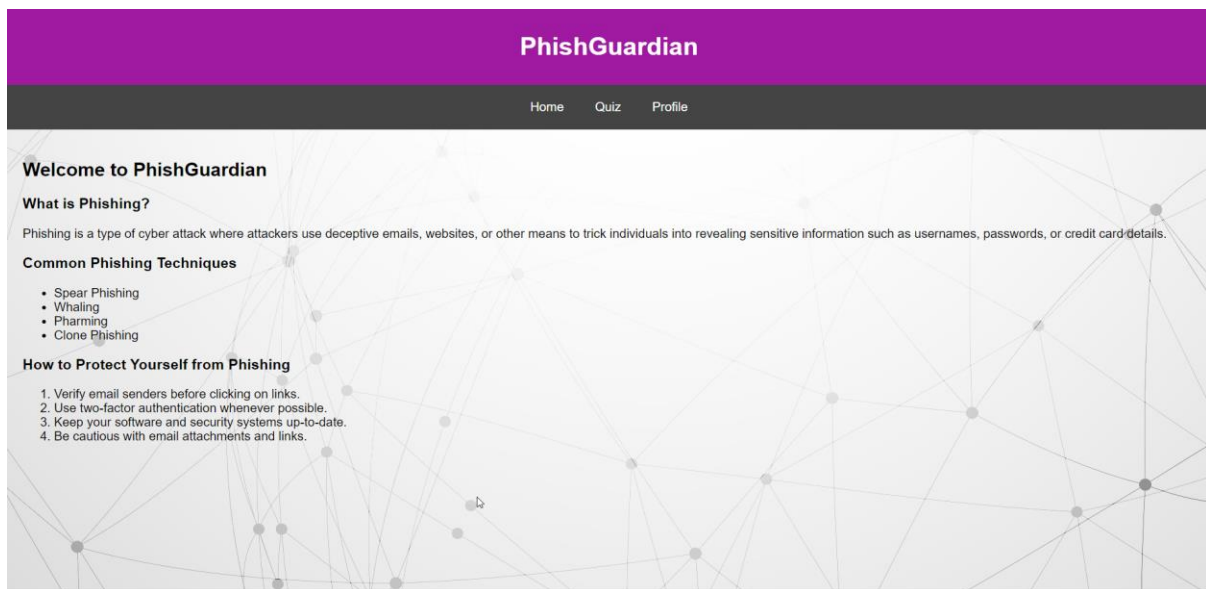
Despite thorough testing and debugging efforts, the password reset link failed to function as intended. Various troubleshooting methods were employed, including checking server configurations, and reviewing code syntax. However, the root cause of the issue could not be found.

With the deadline for project completion coming up and despite dedicating considerable time to troubleshooting, the challenge persisted, ultimately leading to the decision to abandon the feature due to time constraints.

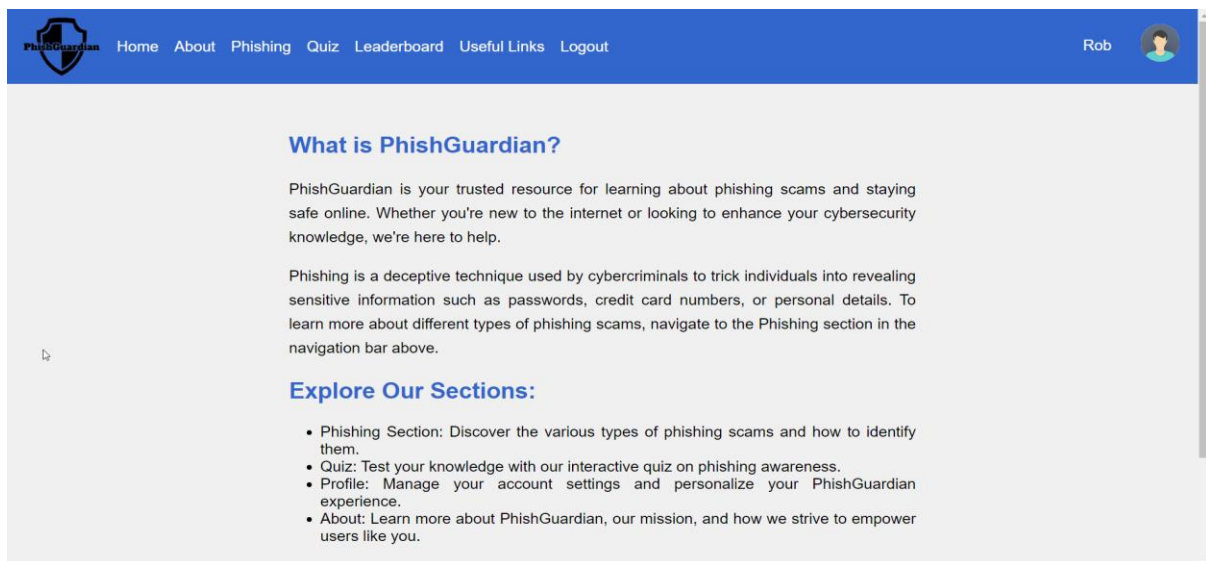
5 Application Development Evolution

5.1 Design Changes

With the varying level of knowledge that the user group for this application would have I wanted to keep the design of the application at a somewhat basic level, easy to read and understand. The initial design I felt was too basic and didn't look either enticing or as easy to use as I would have liked.



The colours didn't fit right for use with the vision of older adults, I also wasn't happy with the top bar and nav bar being separate. The font also felt not fully right, while all black while works against the background, I originally wanted a background image like above but realised it just made it harder for the text to be read. This all lead to the changes that I made which were to remove the background image, increase the font size and centre it along with changing the colour and style of the headings, combine the nav bar and top coloured bar into one while also adding a logo I created for PhishGuardian and making it so the users avatar displays when they are logged in. This can all be seen below:



5.2 Static to Dynamic HTML

When creating the webpages initially all the html content was static and hardcoded into each of the pages as shown below.

```
24 <main>
25 <section id="about-section">
26 <h2>Welcome to PhishGuardian!</h2>
27 <p>PhishGuardian is your trusted resource for learning about phishing scams and staying safe online. Whether you're new to the internet
28 <p>Phishing is a deceptive technique used by cybercriminals to trick individuals into revealing sensitive information such as passwords,
29 <h2>Explore Our Sections:</h2>
30 <ul>
31 <li><strong>Phishing Section:</strong> Discover the various types of phishing scams and how to identify them.</li>
32 <li><strong>Quiz:</strong> Test your knowledge with our interactive quiz on phishing awareness.</li>
33 <li><strong>Profile:</strong> Manage your account settings and personalize your PhishGuardian experience.</li>
34 <li><strong>About:</strong> Learn more about PhishGuardian, our mission, and how we strive to empower users like you.</li>
35 </ul>
36 <h2>Start Learning Today!</h2>
37 <p>Begin your journey towards a safer online experience by exploring the sections above. If you have any questions or concerns, feel free
38
39 </section>
```

This was done at the time as it was the only way I knew how, after a few attempts at different ways of changing to a more dynamic form so the content wasn't hardcoded in along with discussions with my supervisor and other students I settled on the below.

```
C:\xampp\htdocs\FYP > content.php
1 <?php
2 //Homepage
3 $homepageContentH2 = <<<HTML
4 what is PhishGuardian?
5 HTML;
6 $homepageContentP1 = <<<HTML
7 PhishGuardian is your trusted resource for learning about phishing scams and staying safe online. Whether you're new to the internet or looking to e
8 HTML;
9 $homepageContentP2 = <<<HTML
10 Phishing is a deceptive technique used by cybercriminals to trick individuals into revealing sensitive information such as passwords, credit card nu
11 HTML;
12 $homepageContentHead = <<<HTML
13 Explore Our Sections:
14 HTML;
15 $homepageContentList = <<<HTML
16 Phishing Section: Discover the various types of phishing scams and how to identify them.
17 Quiz: Test your knowledge with our interactive quiz on phishing awareness.
18 Profile: Manage your account settings and personalize your PhishGuardian experience.
19 About: Learn more about PhishGuardian, our mission, and how we strive to empower users like you.
20 HTML;
21 $homepageContentHead2 = <<<HTML
22 Start Your Learning Today!
23 HTML;
24 $homepageContentP3 = <<<HTML
25 Begin your journey towards a safer online experience by exploring the sections above. If you have any questions or concerns, feel free to reach out
26 HTML;
```

The content for each page is housed in a single PHP file with each part of the specific page i.e. heading or paragraph are held in their own variables using a heredoc syntax, this is done to define a large block of text so when an admin is editing the content they won't hit a small limit.


```

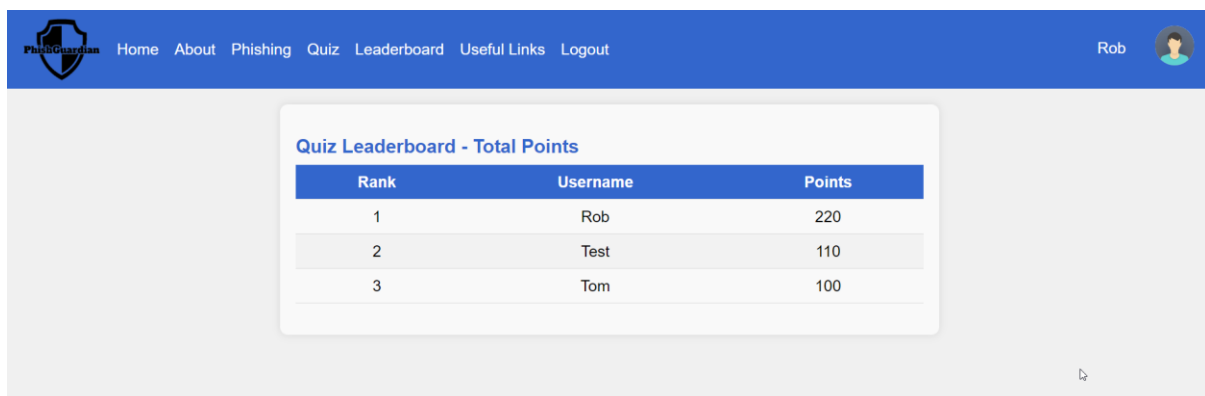
<main>
  <section class="content-block">
    <?php
      include_once 'content.php';
    ?>
    <h2><?php echo $homepageContentH2; ?></h2>
    <p><?php echo $homepageContentP1; ?></p>
    <p><?php echo $homepageContentP2; ?></p>
    <h2><?php echo $homepageContentHead; ?></h2>
    <ul>
      <?php
        // Explode the heredoc string by newline
        $listItems = explode("\n", $homepageContentList);
        foreach ($listItems as $item) {
          // Trim any leading/trailing whitespace
          $item = trim($item);
          // Output each item as a list item
          echo "<li>$item</li>";
        }
      ?>
    </ul>
    <h2><?php echo $homepageContentHead2; ?></h2>
    <p><?php echo $homepageContentP3; ?></p>
  </section>
</main>

```

The content is pulled from the PHP page it is stored in and echoed out here within the html tags allowing the structure to be set here to keep each page having the same design and look, so when the content is being edited it is only the test getting edited and the page itself is not being affected.

5.3 Leaderboard Changes

Initially with the leaderboard I had it that each attempt a user makes would be displayed within the leaderboard showing a “Top 10” but then realised that after a while that would be pointless as when enough users got max points it would just be a leaderboard of all max point attempts.



After that I decided to include the above version of the leaderboard which is an accumulation of the user’s points from every attempt they have on the quiz, alongside the original but in the end I decided it was best to just have this leaderboard.

5.4 Quiz Changes

When creating the quiz, I made it with everything being hard coded into a JSON file as shown below which worked fine but wasn't good for what I wanted to do with my quiz.

```
1
2 let questions = [
3   {
4     id: 1,
5     question: "What is phishing?",
6     answer:"A social engineering attack aimed at stealing sensitive information",
7     options: [
8       "A type of fishing technique",
9       "A social engineering attack aimed at stealing sensitive information",
10      "A computer virus that spreads through emails",
11      "A secure method of online communication"
12    ]
13  },
14  {
15    id: 2,
16    question: "Which of these is a type of Phishing?",
17    answer:"All of these",
18    options: [
19      "Smishing",
20      "Vishing",
21      "Email",
22      "All of these"
23    ]
24  }
25 ]
```

So, after discussing with my supervisor, I decided to move away from this and transfer my quiz and store it in my database, this allowed for more functionality and control over the quiz along with the adding the ability for admins to edit the quiz and add questions from the admin portal.

Quiz:Quiz: 13 rows total (exact) >> Next Show all Sorting Columns (7/7) Filter

#	QuizID	QuestionText	Ans1	Ans2	Ans3	Ans4
1	3	Which of these is a type of Phishing	Smishing	Vishing	Email	All of these
2	6	Which of the following is a common phishing ...	Brute force attack	Denial-of-service attack	Spoofed emails or webstes	Firewall intrusion
3	7	What is the purpose of a phishing website?	To provide helpful information	To collect sensitive information from users	To promote online safety	To buy Fishing equipment
4	8	What is Smishing	A phishing attack through text messages	A phishing attack through smart devices	A phishing attack through emails	None of the Above
5	9	What is phishing?	A social engineering attack aimed at stealing s...	A type of fishing technique	A computer virus that spreads through emails	A secure method of online communication
6	10	How can you identify a phishing email?	The sender's email address looks suspicious or...	The email contains urgent requests for person...	There are spelling and grammar errors in the ...	All of the Above
7	11	What should you do if you receive a suspicious...	Reply with the requested information	Click on any links provided to verify your identity	Ignore the email and delete it	Forward the email to all your contacts for awa...
8	12	How can you verify the authenticity of a text m...	Call the sender using a known, trusted phone ...	Reply directly to the text message with your pe...	Click on any links provided to see where they L...	Share the message with all your contacts to w...
9	13	What type of information might a smishing atta...	PPS Number	Bank account details	Passwords or PINs	All of the Above
10	14	What is a common tactic used by attackers in ...	Requesting urgent action or threatening conse...	Offering free gifts or rewards	Asking for permission to access your computer...	Asking for permission to access your computer...
11	15	What is a common tactic used by attackers to ...	Speaking in a foreign accent to sound authentic	Providing personal information about the victim...	Offering large sums of money upfront	Threatening legal action if immediate complian...
12	16	How do vishing attackers typically manipulate t...	By impersonating authority figures or trusted e...	By offering genuine assistance without any ulte...	By asking vague questions with no clear purpose	By making jokes and building rapport with the ...
13	17	Vishing typically involves?	Sending malicious links through text messages	Phishing through voice calls	Sending phishing emails with attachments	None of the above

6 Testing

6.1 Usability Testing

Once the site was fully functional and I felt it was at an appropriate design level for users to interact with it I began the testing. To get started the testing involved setting up a tunnel with Ngrok, allowing the web application to be accessed by users on their own computers. This approach enabled users to interact with the site in their natural environments and allowed me to avoid having to setup a location to get user to come to or to go to the users with my own device to get testing done.

6.1.1 Methodology

Ngrok Tunnel Setup: To conduct the usability testing, a tunnel was established using Ngrok, a tool that creates secure tunnels to localhost. This allowed the web application to be accessed by users on their own computers.

Users: Various older adult users were asked to participate in the usability testing process. I tried to select a diverse range of demographics and digital literacy levels, this was in the hopes of getting comprehensive feedback and insights.

User Interaction: Users were instructed to perform specific tasks within the web application, such as creating an account, navigating the site, accessing phishing content, taking the quiz, and providing feedback through the survey in the about page.

Feedback Survey: After using the site for a few minutes, users were directed to complete a feedback survey. The survey solicited input on various aspects of the site, including design, layout, navigation, content clarity, and ease of use.

6.1.2 Key Findings

Navigation and Layout: Users generally found the navigation and layout of the site to be intuitive and easy to understand. However, some users expressed difficulty locating specific features or content, highlighting the importance of clear labelling.

Content Readability: The readability of the content was identified as a crucial factor by users. Larger font sizes and high contrast colour schemes were positively received.

Interactive Elements: Interactive elements such as the quiz along with the images, videos and real-life examples were well-received by users, fostering engagement, and reinforcing learning.

The information gathered with the user testing helped to make sure the design of the website is up to the correct standards for the target user group, and it allows them to engage with the application fully.

6.2 Functionality Testing

Functionality testing played a pivotal role in assessing the performance of the application, making sure that all features and functionalities operated as intended. This testing aimed to identify any bugs, errors, or malfunctions within the web application, it involved performing my own testing along with collaboration with fellow students and non-older adults to provide feedback on the site's functionality and usability.

6.2.1 Methodology

Test Setup: I set specific tests for the testers to do, this was to try and cover the full range of functionalities within the website. These included:

On the user side user registration, login, site navigation, accessing content, taking the quiz, viewing leaderboard and profile page after quiz is taken and the logout function.

On the admin side login, access of all pages, functionality on each page i.e. can edit users, edit content, edit quiz etc.

Testers: Fellow students and non-older adults were asked to participate in the functionality testing process. When asking people to be a part of the testing I tried to include different levels of knowledge and familiarity with web applications.

Bug Reporting: Testers were asked to report any bugs, errors, or other issues they came across at any point while using the application. These were then used to help make any necessary fixes and changes.

6.2.2 Key Findings

Registration and Login: Testers were able to register for the site along with login with no major issues being reported. Some mentioned about a forgot password option, which as I talked about earlier in the report I tried to get working but was unable to.

Site Navigation: Overall testers found the navigation through the application straightforward and functioning correctly. Also reported was the correct functionality of the logout.

Content: The content was found to be easily accessible and found, with only a few small issues mentioned. Those being minor issues like spelling or placement which was fixed straight away.

Quiz: The quiz was positively received by testers, who found it engaging and informative. Some testers did report minor issues in quiz scoring, which were due to some small calculation errors and fixed straight away.

Admin Functions: Some classmates were also asked to test the functionality of the admin portal. After testing all functionality was reported to be functional, they could edit, add, and delete a user, add, and edit questions to the quiz and edit the web page content. The only issue reported was some of the pages were calling the error page which was due to an issue with the login check code, this was fixed after being reported.

The information gathered with the user testing helped to make sure the design of the website is up to the correct standards for the target user group, and it allows them to engage with the application fully.

6.3 Working With Other Students

At different points during the development of this project I worked with some fellow students on various parts.

Design: As I was creating the webpages and working on the structure and design, I met with a student from the IDAD course, she worked with me on what good design practices to implement and various options on how to structure the webpages.

I showed her what I had done so far and got feedback on what worked and what didn't, I implemented some of her suggestions like placing the text on each of the pages in the centre, changing the colour of the header from purple to blue and placement of certain aspects like the logo for the application and the user avatar picture. Using these suggestions added to the look of the website while still keeping the simplicity of it for the older user.

Security: With creating a web application comes the need for security implementation, during the development stage I began to implement various security features into the application like session management and cross site scripting protection as discussed earlier in the report.

Having gotten to a point where I had what I thought was most if not all security implementations in place, a fellow cyber student offered to test my application by running it through his own final year project. His project being a vulnerability scanner, after he ran it through his application, he was able to give me a list of the vulnerabilities that still existed within the application. This allowed me to then implement mitigations for them increasing the security of my application. It also helped in finding a small bug with his project, so it was beneficial to both of us.

Working alongside other students at different stages of the project had a significant positive impact on both the design and security aspects of the project. Working with a design-focused student I was able to implement visual improvements while maintaining simplicity for older users. Collaborating with a cybersecurity student for application security testing proved extremely beneficial in identifying and addressing previously undetected vulnerabilities. This teamwork not only elevated the project's overall quality but also provided an shared learning and mutual benefits among fellow students.

7 Technical Issues

7.1 Problems Encountered

7.1.1 Docker/MyPHPAdmin

When I began my project, I was using the in-built database within xampp MyPHPAdmin but after about a week I began having issues with MyPHPAdmin, it stopped working and wouldn't allow me to access my database or load up at. Once this happened, I decided to move away from using this for my database as I had a similar issue with a project in a previous year. With having this issue before I chose to use Docker to host a container for my database as I had both used it before and it freed up some space on my machine housing it in a container, this along with HeidiSQL are how I am now running my database. HeidiSQL I find to be much more useful as a tool and find the UI all better to use

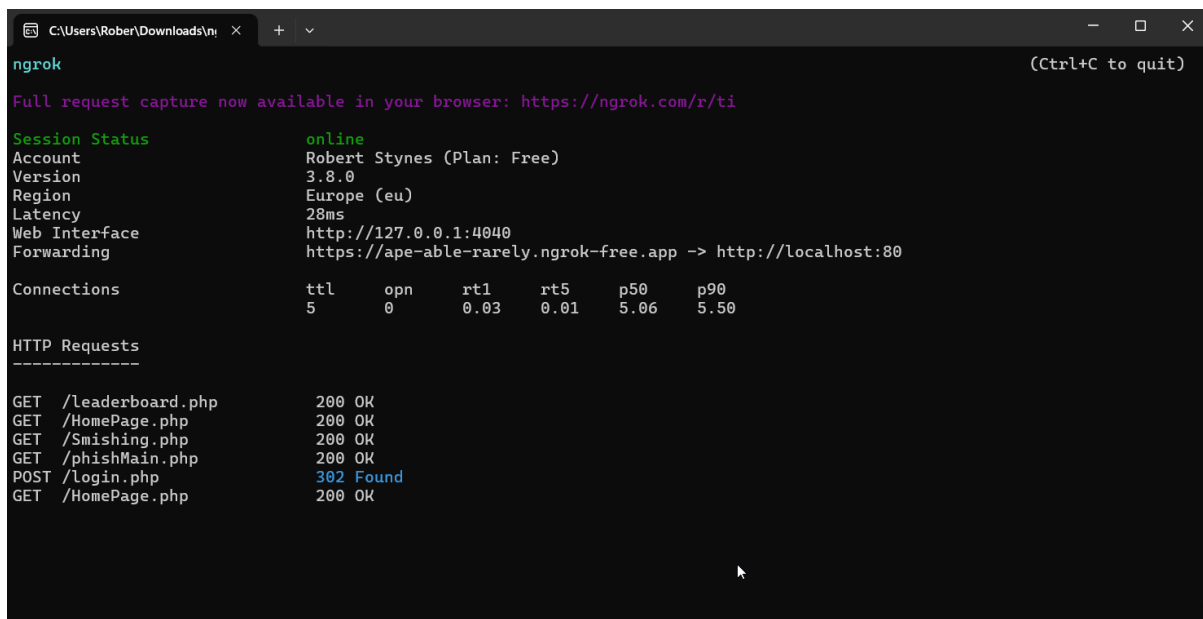
7.1.2 Moving quiz to database

As discussed above I moved the quiz from being hard coded in a file to being in the database and made it so an admin can edit the quiz and add questions. This proved to be more difficult than I first thought as I had not done something of this scale before with regards to content in a database and editing it. The main issue was getting it into a format to be able to edit the quiz content and add questions, ultimately the decision was made to make a PHP file for the quiz that would also act as the webpage. This allowed for the quiz content to be retrieved from the database and used then to create the quiz for the user on the page.

7.1.3 Final Survey/Hosting Site Online

For my final survey I asked users that had been interacting with the site to take a feedback survey to get their opinions on how the site functions and its design. To be able to do this I needed to have my website be functioning online otherwise I would have had to go to users to get them to test the site locally, which wasn't an option. After having done some research on different ways to host a site online I was getting frustrated as I found that most options required a premium account or subscription to host, eventually I found ngrok which is a reverse proxy that secures and protects applications and network services. It allowed me to use a domain from them for free to host my application online that allows me to send the link to users to access my application from their own devices.

It took a lot of trial and error to get ngrok to work with my application as I had never done this before, but once I managed to get it working it has proven to be extremely valuable for getting users to test the site.



```
C:\Users\Robert\Downloads\ngrok> ngrok
ngrok (Ctrl+C to quit)
Full request capture now available in your browser: https://ngrok.com/r/ti

Session Status      online
Account             Robert Stynes (Plan: Free)
Version             3.8.0
Region              Europe (eu)
Latency              28ms
Web Interface        http://127.0.0.1:4040
Forwarding           https://ape-able-rarely.ngrok-free.app -> http://localhost:80

Connections
  ttl   opn   rt1   rt5   p50   p90
   5     0    0.03  0.01  5.06  5.50

HTTP Requests
-----
GET /leaderboard.php      200 OK
GET /HomePage.php        200 OK
GET /Smishing.php        200 OK
GET /phishMain.php       200 OK
POST /login.php           302 Found
GET /HomePage.php        200 OK
```

7.1.4 Edit Content

With the decision to move all of the HTML content to a more dynamic style and change it from being hardcoded in each webpage came the challenge of what way to achieve this. Initially I moved each page's HTML content into a singular PHP file placing each in their own variable by using which allows you to define a block of text without needing to manually escape special characters and assign it to a variable.

```
$webPhishing = <<<HTML
<h2>Website Phishing</h2>
<p>
  Website phishing is a form of cyber attack where attackers create fake websites that mimic legitimate ones in order to steal sensitive informati
</p>
<p>
  Here are some common characteristics of website phishing attacks:
</p>
<ul>
<li><strong>URL manipulation:</strong> Attackers may use URLs that closely resemble those of legitimate websites, but with slight variations or
<li><strong>Deceptive content:</strong> Phishing websites often contain forms or login pages that prompt users to enter sensitive information su
<li><strong>Impersonation of trusted brands:</strong> Attackers may impersonate well-known brands, financial institutions, or government agencie
<li><strong>Urgency or fear tactics:</strong> Phishing websites may use urgent language or fear tactics to pressure users into taking immediate
</ul>
<p>
  Below is an example of a phishing website that impersonates popular shopping website Amazon:
</p>
<div class="image-examples">

</div>
<p>
  To protect yourself from website phishing scams, consider the following precautions:
</p>
<ul>
<li><strong>Check the URL:</strong> Always check the URL of a website before entering any sensitive information. Look for HTTPS encryption and v
<li><strong>Use bookmarks:</strong> Instead of clicking on links in emails or messages, use bookmarks or type the URL directly into your browser
<li><strong>Enable browser security features:</strong> Many web browsers offer built-in security features, such as phishing filters and website
<li><strong>Stay informed:</strong> Stay up-to-date on the latest phishing techniques and scams, and educate yourself on how to recognize and av
</ul>
<p>
  By remaining vigilant and cautious when browsing the web, you can help protect yourself from falling victim to website phishing attacks.
</p>
```

Although this was sufficient and worked the main issue came when I was creating the admin page for editing the website content, with this implementation it made it so the full content including all of the HTML tags were being displayed to the admin when they selected the page to edit.

PhishGuardian Logout Add Question Edit Questions Manage User

Edit Content

```
<h2>What is Phishing and Why is it Important to Be Aware?</h2>
<p>Phishing is when cyber criminals pretend to be people or organizations you trust, like your bank or the government, to fool you into giving away personal information. They want things like your passwords, credit card numbers, or even who you are. It's like someone pretending to be your friend to get things from you that they shouldn't have.</p>
<h2>How Does it Work?</h2>
<p>Picture getting an email or a message on your phone that seems to be from your bank. It might say something urgent like "Your account is in trouble, click here to fix it." But when you click that link or reply to the message, you're not talking to your bank. You're talking to a bad person who wants to steal from you. These bad people want your information to take your money or pretend to be you online.</p>
<p>We'll explain more about this in our breakdown of different types of phishing.</p>
<p>Below is a short video to help understand and visualize phishing and its dangers.</p>
<div class="video-container">
  <iframe width="560" height="315" src="https://www.youtube.com/embed/Y7zN1E9DmI4" frameborder="0" allowfullscreen></iframe>
</div>
<h2>Explore More</h2>
<p>Ready to learn more about phishing and how to protect yourself online? Click the buttons below to explore different types of phishing attacks:</p>
<a href="websitePhishing.php" class="next-button">Website Phishing</a>
<a href="Vishing.php" class="next-button">Vishing</a>
<a href="Smishing.php" class="next-button">Smishing</a>
```

Save Homepage Content Phishing Content About Content Email Phishing Content Vishing Content Smishing Content Web Phishing Content Resources Content

Having reviewed it and discussed it with my supervisor, I ultimately decide to go with a different approach for this as I wanted the content to be editable but not the HTML tags. This is because I wanted to keep the design and style of each page a set way as it was designed for the older adults using it.

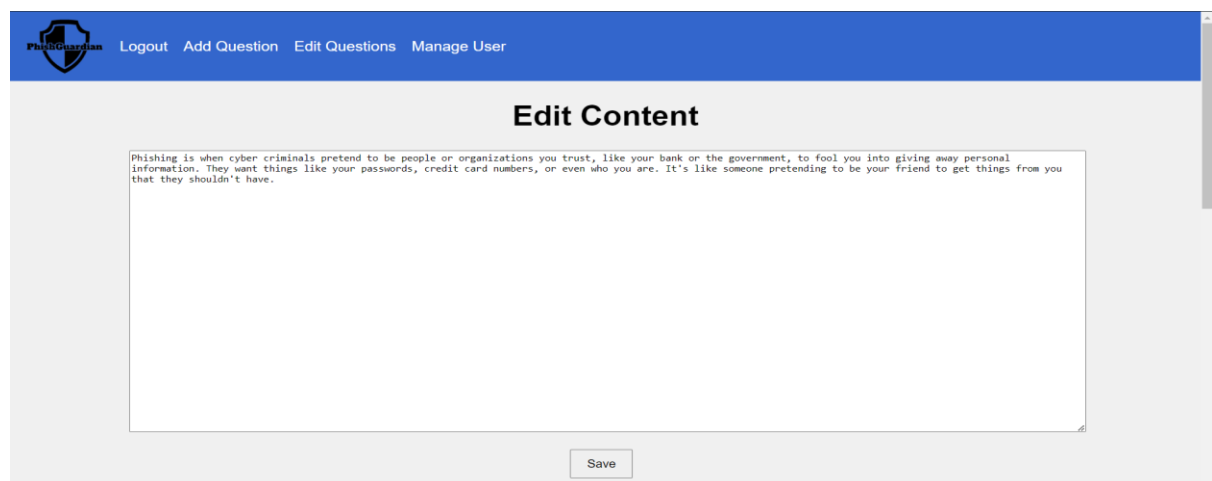
What I ended up going with that worked was the below, I moved each section of the pages into individual variables. Each with a set label to be able to know what I was calling like \$smishingContentH1 for the first heading on the webpage or \$smishingContentP3 for the 3rd piece of text on the webpage.

```
//Smishing
$smishingContentH1 = <<<HTML
Smishing (SMS Phishing)
HTML;
$smishingContentP1 = <<<HTML
Smishing, also known as SMS phishing, is a type of cyber attack where scammers use text messages to deceive individuals into providing personal info
HTML;
$smishingContentP2 = <<<HTML
Here are some signs of smishing to watch out for:
HTML;
$smishingContentList1 = <<<HTML
Urgent or Suspicious Messages: Be cautious of text messages that use urgent language or request immediate action, especially if they ask for persona
Unknown Sender: If you receive a text message from an unknown sender or an unfamiliar number, be wary of clicking on any links or responding to the
Grammatical Errors: Smishing messages often contain grammatical errors or spelling mistakes, as they are typically sent hastily by scammers.
Requests for Personal Information: Legitimate organizations typically do not request sensitive information via text message. Be cautious if a messag
HTML;
$smishingContentP3 = <<<HTML
Below is an image showing some of these signs and how they might be displayed in a text message:
HTML;
$smishingContentImg = <<<HTML
<div class="image-examples">
| 
|</div>
HTML;
$smishingContentP4 = <<<HTML
To protect yourself from smishing scams, follow these tips:
HTML;
$smishingContentList2 = <<<HTML
Verify Sender Identity: Before responding to a text message, verify the sender's identity by checking the phone number or contacting the organizatio
Avoid Clicking on Links: Do not click on links in text messages from unknown senders, especially if they seem suspicious or lead to unfamiliar websi
Report Suspicious Messages: If you receive a suspected smishing message, report it to your mobile carrier and delete it immediately. You can also fo
Trust Your Instincts: If a message seems too good to be true or raises suspicions, trust your instincts and refrain from interacting with it.
HTML;
$smishingContentH2 = <<<HTML
Frequently Asked Questions
HTML;
```

This allowed me to then call each of the parts separately and place them within HTML tags, keeping the structure of the page coded a set way.

```
<main>
<section class="content-block">
<?php
include_once 'content.php';
?>
<h2><?php echo $emailContentH1; ?></h2>
<p><?php echo $emailContentP1; ?></p>
```

This was one of the more difficult and time-consuming challenges I faced, but once I got the change implemented it turned out close to how I wanted it.



8 General Issues

8.1 Problems Encountered

8.1.1 Surveys

During the stage of the project, when the surveys were being conducted there were a few issues that arose. One of the main issues was the delay in getting the responses back from the people asked to take the survey, despite some follow up reminders there were a few that took a long time getting their responses completed.

Another problem during this was analysing the data as it was time consuming, this was due to the fact that it was my first time doing this and wanted to make sure I was getting the correct information needed from the analysis. With the first survey it was critical to get the analysis fully correct as it was the bases for building the content for the website, for the second survey I needed to be correct with it as it would help make any necessary changes to the application for the benefit of the older adult users.

8.1.2 Learning

Although I had used PHP before, we had only ever been shown the absolute basics. So this helped but at a lot of different points throughout the development of this project I found myself having to find out how to do certain things like creating the quiz, making the page content dynamic and creating the admin pages for editing the various aspects of the project.

My basic level of PHP led to an increased number of files being created and used, I was not happy with having so many files but with time restraints did not have the capacity to go and change anything to condense it down.

Designing the application led to a small number of issues with trying to balance keeping the look basic and easy to view for the older users with performance and security. This was mostly heightened with only being able to implement my security mitigations late in the development as we were still learning about them in my other module.

9 What I learned

During this project, I gained valuable knowledge and skills. Firstly, I enhanced my technical skills in web development, particularly in PHP and database management. Learning code in PHP that was new to me.

Overall, this project provided a valuable learning experience that improved my skill set, expanded my knowledge base, and equipped me with the skills needed to tackle future challenges.

9.1 PHP Knowledge

When I began this project my level of knowledge of PHP was pretty basic, but once I got further along with the development of this project my knowledge grew thanks to the hands-on experience coding this project along with the large number of guides and videos online it helped me overcome various challenges and trouble shoot throughout.

Tasks such as session management, handling the page content among others gave me the opportunity to learn. Through my own trial and error along with getting help from other and online I was able to get valuable information on ways to fix or achieve what I was trying to do.

Working on this project gave me the opportunity to learn new and increase my own PHP skills, with the various challenges throughout.

10 What I Would Do Differently Starting Again

Looking back on the development process, I have identified two areas where I could have taken a different approach to enhance the efficiency, security, and user experience of the PhishGuardian platform. Two key aspects that stand out are the utilization of Python and implementing robust security measures at earlier stages.

10.1 Use/Learn Python

One major change I would make, given the chance, is using Python as the primary programming language for the platform instead of PHP. While PHP served its purpose and in the end, got the job done, Python would have been a more versatile and developer-friendly language, offering extensive libraries and frameworks that could have streamlined the development process.

The syntax and readability of Python are greater than those of PHP, making it easier to write, understand, and maintain code. Additionally, Python's compatibility with popular frameworks like Django and Flask would have provided a more structured and efficient approach to developing and scaling the platform.

The main frustration I had with PHP was the difficulty in managing large codebases and maintaining consistent coding standards. Debugging and troubleshooting were often time-consuming, especially when dealing with complex errors. In hindsight, adopting Python would have likely saved time and effort during development and maintenance, ultimately resulting in a better platform.

10.2 Implement Security Earlier

During the development of PhishGuardian, I focused heavily on creating educational content and user-friendly features but overlooked the importance of including security measures from the outset. Although security was eventually addressed, integrating it earlier in the development process would have resulted in a lot less issues than trying to integrate it into code later.

One notable difficulty with implementing security measures later was the need to change code and restructure the platform to accommodate these features. This not only prolonged development time but also presented challenges in ensuring that security measures were effectively integrated throughout the platform.

In retrospect, prioritising security from the beginning would have led to better code organisation, reduced vulnerability to potential attacks, and improved user confidence in the platform's ability to protect sensitive information. This valuable lesson will inform my approach to future projects, ensuring that security remains at the forefront of the development process.

11 Cyber Security Relevance

11.1 Projects General Relevance

The development of this web-based platform holds significant relevance to the wider field of cybersecurity, especially when it comes to protecting older adults from phishing attacks and online scams. This project addresses critical gaps in awareness and knowledge among older adults regarding cybersecurity threats, as shown by research and survey data.

The results from the project's research exposed a severe lack of awareness about phishing and online scams among older adults. Most participants were unfamiliar with phishing and doubted their ability to spot online scams, putting them at high risk, considering their growing dependence on digital devices and online activities like emails and online banking.

PhishGuardian tackles this issue by providing an engaging learning section that cover different aspects of phishing, such as common tactics, warning signs, and safety measures. The platform uses real-life examples and interactive elements like quizzes to enhance learning and empower older adults with the skills and knowledge necessary to spot and deal with online threats effectively. By making resources accessible and easy to use, PhishGuardian hopes to bridge the knowledge gap and give older adults the confidence to navigate the online world safely.

PhishGuardian can play a significant role in cybersecurity by tackling the unique challenges faced by older adults in today's digital world. Being a platform that empowers seniors with the necessary knowledge and skills to stay safe from phishing attacks and online scams.

PhishGuardian's continuous educational approach, and user feedback contribute to a more secure online experience for older adults and the entire community. Ultimately, this final year project has the potential to greatly impact the safety of older adults online.

11.2 Security Features to Enhance Cybersecurity

As part of the development process, several security features were implemented to enhance the platform's resilience against common cyber threats. These features bolster the website's security while also contribute to its overall relevance in the field of cybersecurity.

Session Management:

Session management practices were implemented to ensure secure user sessions throughout the browsing experience. This includes generating unique session identifiers, employing session expiration policies, and implementing regenerating the session id to prevent session fixation.

CSRF (Cross-Site Request Forgery) Protection:

To mitigate CSRF attacks, token-based authentication was integrated into the web application. This involves generating and validating unique tokens for each user session to verify the authenticity of requests, preventing unauthorised actions from attackers.

SQL Injection (SQLi) Prevention:

To protect against SQL injection, prepared statements were used in database interactions. By properly sanitising user inputs and validating SQL queries, the risk of SQL injection attacks, which exploit database query vulnerabilities to manipulate or extract sensitive data, is significantly reduced.

XSS (Cross-Site Scripting) Mitigation:

Input validation was employed to mitigate XSS vulnerabilities. This involves validating user inputs to detect and reject potentially malicious scripts, this was done by implementing my own function to clean the input, thereby mitigating the risk of XSS attacks.

Cookie Handling:

Strict cookie security policies were enforced including setting secure flags and HttpOnly flags on cookies to prevent unauthorised access or tampering by malicious entities, thereby reducing the risk of session hijacking.

Caching:

Careful consideration was given to caching, secure caching practices such as implementing cache control headers making it so the pages never cache was employed to prevent information leakage and unauthorised access to cached content.

By incorporating these security features into the website, the platform not only provides valuable insights into cybersecurity best practices. This approach enhances the platform's relevance in addressing the evolving challenges of online security and contributes to a safer and more secure online environment for users.

12 Conclusion

In conclusion, this project has provided invaluable insights and learning opportunities, this project has not only enabled the creation of a potentially impactful solution for users but has also served as a platform for personal growth and skill development. Concentrating on equipping older adults with the necessary knowledge and resources to navigate the online world securely, I've seen how technology can effectively close gaps in awareness and bolster cybersecurity measures.

This project has grown my skills in various aspects, from web development and user interface design to cybersecurity best practices.

13 Acknowledgements

I would like to thank my supervisor Keara Barrett, she was there to guide me through every step of this project. Always made sure to check in with progress and gave extremely valuable feedback at all stages, be it on documents or various aspects for the project itself giving me multiple solutions to issues I was having.

Another thank you goes out to all my other lecturers that helped me throughout the year either with types and advice or just answer a quick question.

Finally, I would like to thank my fellow cyber students, we all climbed a mountain this year and helped each other get to the top so thank you for all the help and advice throughout the year and project.

14 References

A guide to interface design for older adults: Adchitects blog (no date) Award-Winning Web Design Agency. Available at: <https://adchitects.co/blog/guide-to-interface-design-for-older-adults> (Accessed: 07 December 2023).

Anderson, M. (2017) Tech adoption climbs among older adults, Pew Research Center: Internet, Science & Tech. Available at: <https://www.pewresearch.org/internet/2017/05/17/tech-adoption-climbs-among-older-adults/> (Accessed: 10 December 2023).

Greggwirth (2023) Fraudsters targeting senior citizens with multiple financial scams, Thomson Reuters Institute. Available at: <https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/senior-citizens-financial-scams/> (Accessed: 30 November 2023).

'Making Your Website Senior Friendly' (2019). NATIONAL INSTITUTE ON AGING.

Moth, D. (2022) Six design tips for making your website senior friendly, Econsultancy. Available at: <https://econsultancy.com/six-design-tips-for-making-your-website-senior-friendly/> (Accessed: 09 December 2023).

Pew Research Center (2022) 3. internet, smartphone and social media use, Pew Research Center's Global Attitudes Project. Available at: <https://www.pewresearch.org/global/2022/12/06/internet-smartphone-and-social-media-use-in-advanced-economies-2022/> (Accessed: 06 December 2023).

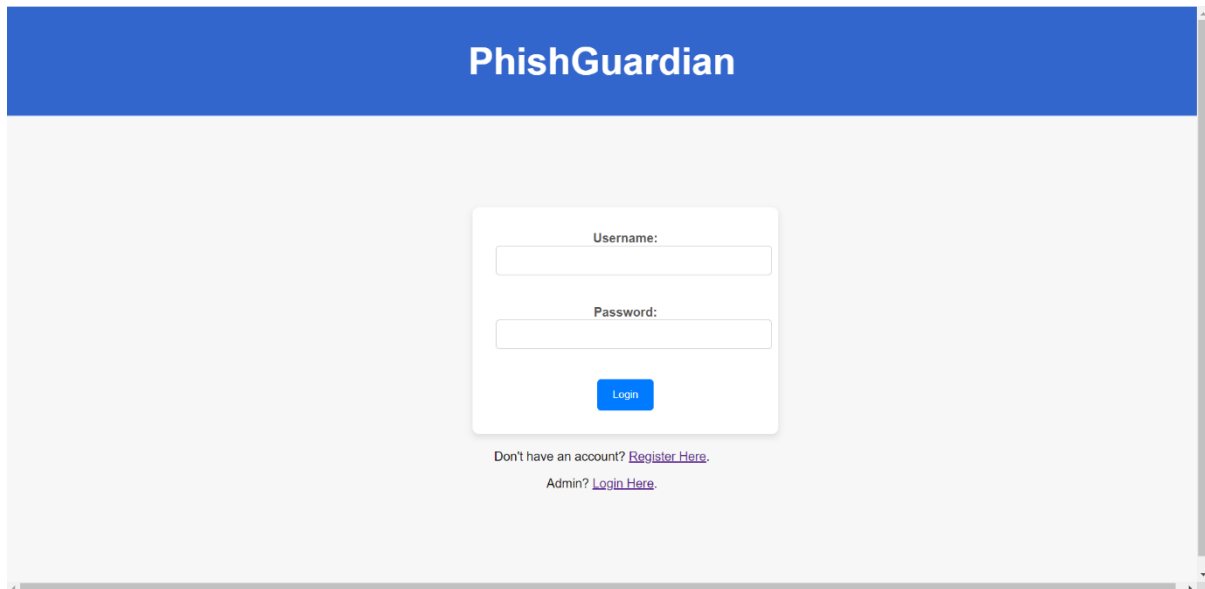
15 Appendix

15.1 User Interface

The application is split across multiple pages to create an easy-to-follow interface for users to access various options.

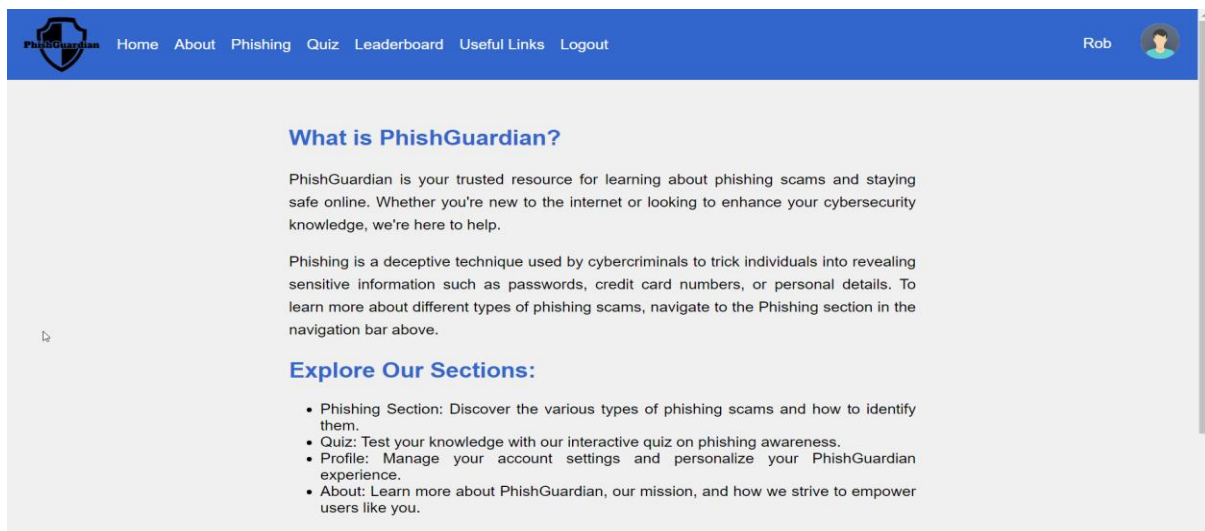
Login Page

The login page serves as the entry point for users to access PhishGuardian. Users can log in with their existing credentials or create a new account if they don't have one. Additionally, an option is provided for administrators to access admin features through a separate login link.



Homepage

The homepage provides users with an overview of the application and its key features. It introduces PhishGuardian as a resource for learning about phishing and staying safe online. Users are encouraged to explore various sections of the application, including the phishing pages, about page, quiz section, leaderboard, and profile page.



Phishing Pages

The phishing pages section educates users about different types of phishing attacks, including email phishing, smishing, vishing, and website phishing. Each subsection provides detailed information and visual aids to help users recognise and understand the various tactics used by cybercriminals.



What is Phishing and Why is it Important to Be Aware?

Phishing is when cyber criminals pretend to be people or organizations you trust, like your bank or the government, to fool you into giving away personal information. They want things like your passwords, credit card numbers, or even who you are. It's like someone pretending to be your friend to get things from you that they shouldn't have.

How Does it Work?

Picture getting an email or a message on your phone that seems to be from your bank. It might say something urgent like 'Your account is in trouble, click here to fix it.' But when you click that link or reply to the message, you're not talking to your bank. You're talking to a bad person who wants to steal from you. These bad people want your information to take your money or pretend to be you online. We'll explain more about this in our breakdown of different types of phishing.

Below is a short video to help understand and visualize phishing and its dangers.



Explore More

Ready to learn more about phishing and how to protect yourself online? Click the buttons below to explore different types of phishing attacks:

- Email Phishing
- Website Phishing
- Vishing
- Smishing

About Page

The about page offers users a more in-depth explanation of PhishGuardian's goal and objectives. It also asks the user for feedback and asks users to provide input on the site's design, layout, and functionality through a survey. This feedback link allows continuous improvement of the application.



About PhishGuardian

At PhishGuardian, we understand the importance of staying safe online, especially for older adults who may be new to the digital world or who want to enhance their cybersecurity knowledge. That's why we've created a specialised online learning platform tailored just for you.

What is PhishGuardian?

PhishGuardian is your dedicated resource for learning about phishing and improving your online safety skills. Phishing is a common cyber threat where scammers try to trick you into giving away personal information, like passwords or credit card numbers. This is done by pretending to be someone trustworthy, such as a bank or government agency. Our platform provides comprehensive education and practical tools to help you recognize and avoid these scams.

Designed specifically for older adults, PhishGuardian offers user-friendly and accessible resources that cater to your learning needs. Whether you're new to the internet or looking to sharpen your cybersecurity skills, our platform provides clear and easy-to-follow

Information, tips, and a quiz to help you get ready to be online with confidence.

What You'll Learn

- Understanding Phishing: Learn what phishing is, how it works, and why it's important to stay vigilant online.
- Spotting Phishing Attempts: Discover common tactics used by scammers and develop skills to recognize phishing emails, messages, websites and more.
- Protecting Yourself: Discover simple and effective ways to keep your personal information and money safe from phishing scams.
- Reporting Phishing: Learn how to report phishing attempts and contribute to making the internet safer for everyone.

Help us make it better

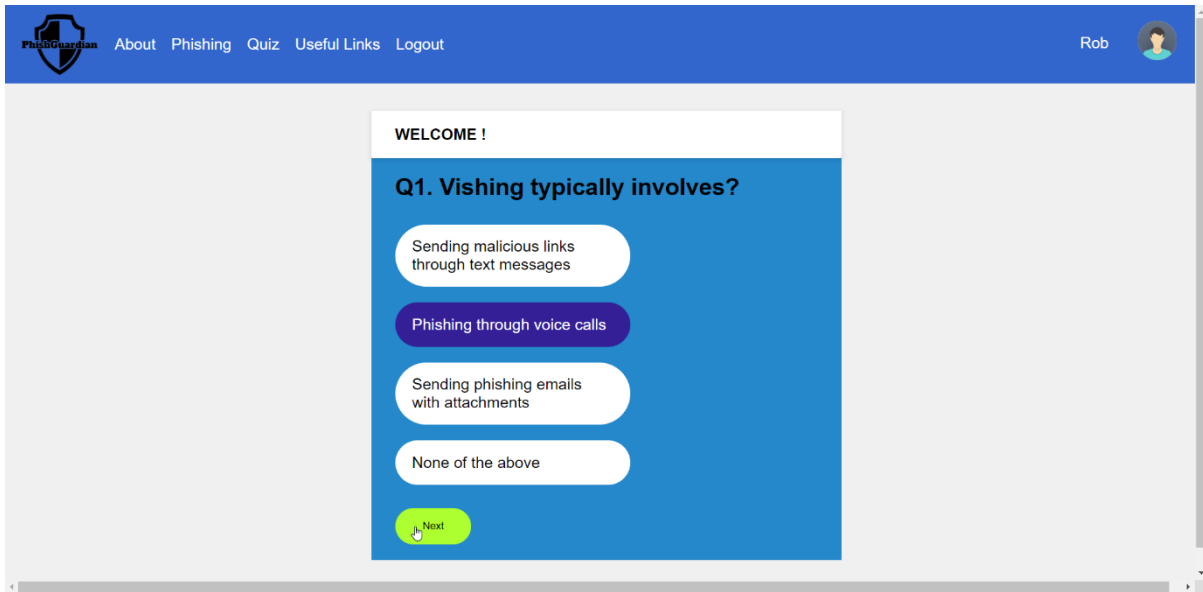
Once you have gone through the various features and locations within this site, please take a few minutes to give us some feedback in the below survey to help make improvements to make it easier and more valuable for everyone. Thank you!

[Survey](#)

Quiz

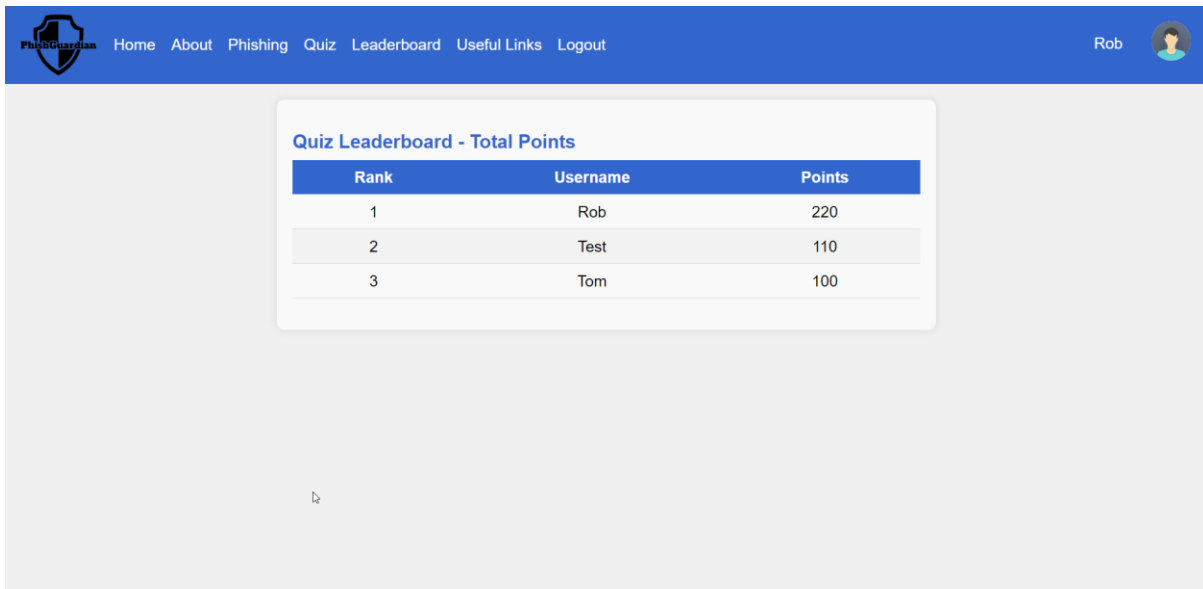
The quiz section allows users to test their knowledge of phishing awareness. Questions are based on the content provided in the phishing pages section. Users receive immediate feedback on their answers, with correct responses indicated in green and incorrect responses in red.

Upon completion, users are presented with their score and given the option to share their results with others.



Leaderboard

The leaderboard showcases user rankings based on their quiz scores. This gamification element encourages users to engage with the application and strive for higher scores. It gives a sense of competition while also promoting learning and retention of phishing awareness knowledge.



Profile Page

The profile page allows users to manage their account and personal information. They can update their email, username, date of birth, and phone number as needed. This section provides users with control over their account settings and ensures their information remains up to date.

The screenshot shows a user profile page for 'Rob' on the PhishGuardian platform. The page has a blue header with the PhishGuardian logo and navigation links: Home, About, Phishing, Quiz, Leaderboard, Useful Links, and Logout. The user's name 'Rob' and a profile icon are in the top right corner.

User Details

Username	Phone Number	Email	DOB	
Rob	087-2598710	rob@gmail.com	1982-06-05	Edit

Avatar

Points Earned

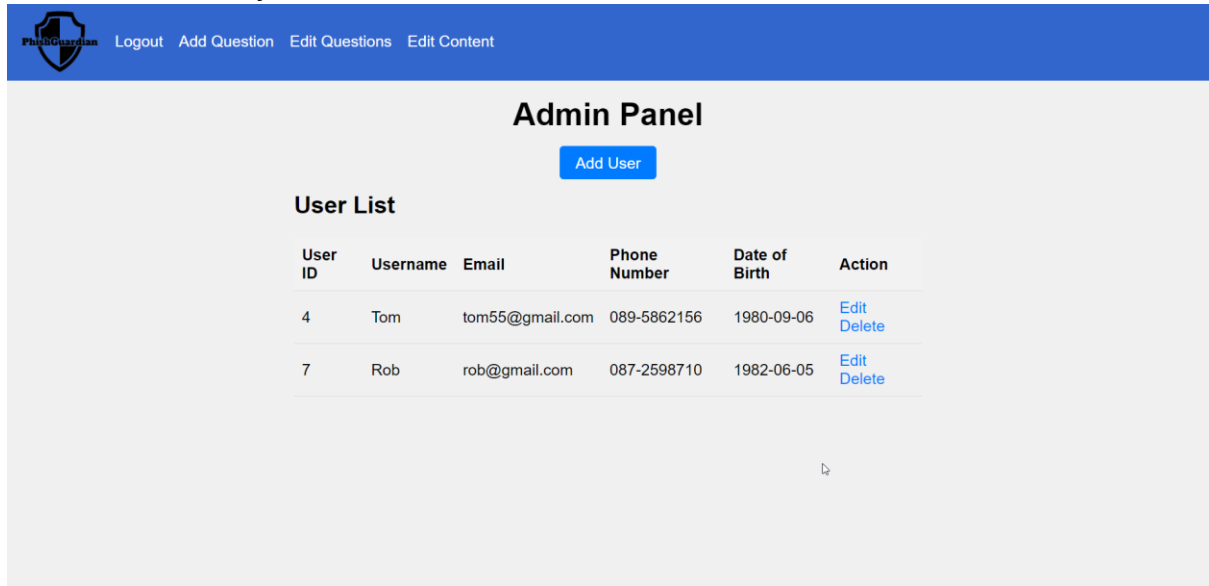
Attempt Number	Points
1	10
2	20
3	20

15.2 Admin Interface

In addition to providing a user-friendly experience for older adults, PhishGuardian includes an admin interface designed to facilitate administrative tasks and manage the platform effectively.

Add/Remove User

The Add/Remove User feature allows admins to manage user accounts within PhishGuardian. Admins can add new users to the system by providing necessary information such as username, email, date of birth, and phone number. Additionally, they have the capability to remove user accounts if necessary.

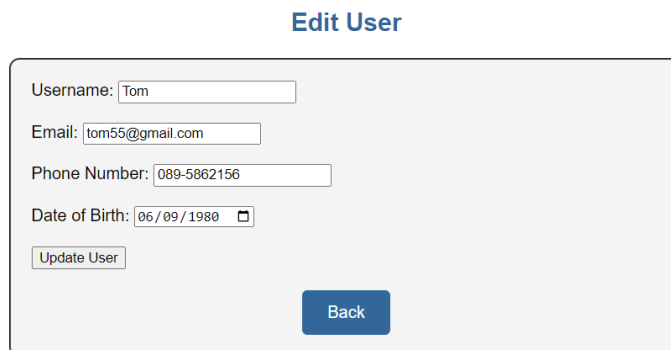


The screenshot shows the PhishGuardian Admin Panel. At the top, there is a blue navigation bar with the PhishGuardian logo and links for Logout, Add Question, Edit Questions, and Edit Content. Below the navigation bar, the main content area is titled "Admin Panel" and features a blue "Add User" button. Underneath, there is a "User List" section containing a table with the following data:

User ID	Username	Email	Phone Number	Date of Birth	Action
4	Tom	tom55@gmail.com	089-5862156	1980-09-06	Edit Delete
7	Rob	rob@gmail.com	087-2598710	1982-06-05	Edit Delete

Edit User

The Edit User feature enables admins to modify user account details as needed. This includes updating user information such as email addresses, usernames, dates of birth, and phone numbers.



The screenshot shows the "Edit User" form. It contains the following fields and buttons:

- Username:
- Email:
- Phone Number:
- Date of Birth:
-
-

Add Questions

Admins can add new questions to the questions that are stored in the database. The Add Questions feature allows administrators to create multiple-choice questions related to phishing

awareness and online security.

Edit Questions

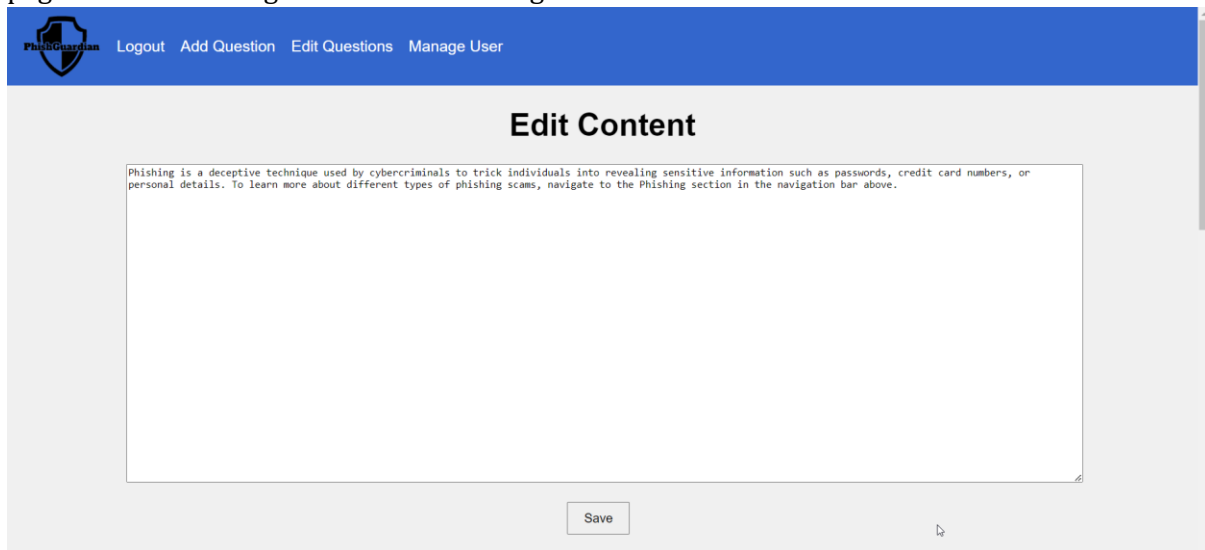
The Edit Questions feature allows admins to make changes to the existing questions that are stored in the database. Admins can edit question content, adjust answer choices, and update question categories or tags as necessary. This ensures that quiz questions remain relevant and up to date.

ID	Question	Answer 1	Answer 2	Answer 3	Answer 4	Correct Answer	Action
3	Which of these is a type of Phishing?	Smishing	Vishing	Email	All of these	All of these	Edit
6	Which of the following is a common phishing method?	Brute force attack	Denial-of-service attack	Spoofed emails or websites	Firewall intrusion	Spoofed emails or websites	Edit
7	What is the purpose of a phishing website?	To provide helpful information	To collect sensitive information from users	To promote online safety	To buy Fishing equipment	To collect sensitive information from users	Edit
8	What is Smishing	A phishing attack through text messages	A phishing attack through smart devices	A phishing attack through emails	None of the Above	A phishing attack through text messages	Edit
9	What is phishing?	A social engineering attack aimed at stealing sensitive information	A type of fishing technique	A computer virus that spreads through emails	A secure method of online communication	A social engineering attack aimed at stealing sensitive information	Edit
10	How can you identify a phishing email?	The sender's email address looks suspicious or unfamiliar	The email contains urgent requests for personal information	There are spelling and grammar errors in the email	All of the Above	All of the Above	Edit
11	What should you do if you receive a suspicious email asking for personal	Reply with the requested information	Click on any links provided to verify your identity	Ignore the email and delete it	Forward the email to all your contacts for	Ignore the email and delete it	Edit

Edit Site Content

Admins can edit site content to keep information current and accurate. The Edit Site Content allows administrators to modify text, images, and other elements displayed on various pages of

PhishGuardian. This includes updating content on the homepage, about page, and phishing pages to reflect changes in content or design.



16 Plagiarism Declaration



Work submitted for assessment which does not include this declaration will NOT be assessed

DECLARATION

1. I declare that all material in this submission e.g., thesis/essay/project/assignment is entirely my own work except where fully acknowledged.
2. I have cited the sources of all quotations, paraphrases, summaries of information, Tables, diagrams, or other material; including software and other electronic media in which intellectual property rights may reside.
3. I have provided a complete bibliography of all works and sources used in the preparation of this submission.
4. I understand that failure to comply with SETU's regulations governing Plagiarism constitutes a serious offence.

Student Name (Printed): _____ Robert Stynes _____

Student Number(s): _____ C00136717 _____

Student Signature(s): _____ Robert Stynes _____

Date: _____ 19/04/2024 _____