

Project Spec and Plan

ROBERT STYNES
C00136717
SUPERVISOR
KEARA BARRETT

Table of Contents

Introduction	2
Project Overview.....	2
Who it's For.....	7
Inspiration.....	7
Deliverables	8
Non-Technical Deliverables.....	8
Primary Deliverables:	8
Secondary Deliverables:	8
Technical Deliverables.....	9
Primary Deliverables:	9
Secondary Deliverables:	9
Technologies	10
Languages	10
HTML.....	10
CSS.....	10
JavaScript	10
PHP.....	10
Python	10
Tools.....	11
XAMPP.....	11
Visual Studio Code	11
Bootstrap.....	11
Docker	11
Database	11
MySQL	11
Surveys.....	11
Microsoft Forms	11
Use Case Diagram	12
Use Cases.....	13
Metrics.....	15
FURPS.....	16
Functionality	16
Usability	16
Reliability	16
Performance	16
Security	16
Project Plan.....	17
References	18

Introduction

With the ever-growing threat of Cyber-attacks in the world, there is a need for people to be more aware with regards to their online presence and security, (Deloitte, 2016).

As the world moves and changes with most of life being lived online be that shopping, learning, working or even just social activity it heightens the need for more cyber awareness. Anyone can be a target at any point no matter if they are an executive of a big company or a parent trying to do the weekly shopping.

This projects aim is to be a learning tool to educate a vulnerable demographic, that being retirees and/or 55+ age group who would require the help needed to understand these threats and to be able to protect themselves. With this project it will give this demographic the chance to learn and feel safer while living in the modern online world with a focus on teaching them about phishing.

Project Overview

This project will be an online web application/website that will help to teach elderly people about the dangers of phishing and the various types that could be used against them, those being Email Phishing, Website (Search Engine) Phishing, Text message phishing (Smishing) and Vishing.

Although this project is similar to other learning/quiz websites out there for learning phishing those sites are all separate in what they are offering to learn, each is split to only be about one type of phishing i.e. only email phishing or only smishing. My project will put all aspects of phishing under the one umbrella, making it much easier for the user to learn in one location. This is especially important with my target user group being older and less tech savvy as they would not be able to or have the knowledge to go searching for all the various sites and information.

The platform will feature a two-part structure. The first aspect is the learning section, there will be a main page that will feature an overview on what phishing is in general and a breakdown of how it can be used in an attack along with a brief explanation that there are various types, the user will go through this page to help them learn about phishing and the various types before going to view the other pages which will be setup as sections within the website that the user can click on to navigate to each one at the top of the page and learn about each type of phishing separately, within these sections there will be a small quiz at the end of each with 3-5 questions to keep the user engaged as they go through them. The second part of the platform will be a quiz consisting of 8-12 questions covering all aspects learned and will be randomised from a pool of questions as to not allow the user to just repeat and pick the opposite answers.

Within the learning platform and the quiz, the aim is to cover as much about the different types of phishing without overloading the user with information. The learning side being where all the information is held and the quiz being used for the user to test their knowledge and see they are understanding the information. The quiz will be a mixture of a different styles that other sites have used together to try cover a full spectrum of ways to deliver the questions, for example the use of written scenarios with multiple choice answers or pictures that will show either a real email, text message etc and ones that show examples of phishing then the user has to say yes or no if they think it's a phishing email.

Below are some examples of these along with some brief explanations of each.

- **Email Phishing:** Email phishing is probably the most widely known and used form of phishing that an attacker uses (Webroot, n.d.). With email phishing there can be three types those being standard, Malware and Spear.

Standard: A standard email phish looks to steal sensitive or personal data from the victim through an email. This is done with the victim receiving an email that is pretending to be from a legitimate company, usually this is done with emails sent to multiple victims in bulk. An example of this being a bank stating the users account has some sort of issue and they need to verify their details.

Malware: Malware phishing is an attack that will try to get the victim to click on a malicious link or to download a malicious file that will then install malware onto the victim's device, for example an email from "Netflix" saying your account is locked with a link to a malicious site. This can lead to the attacker gaining access to files and information stored on the device or to the device being completely overtaken by the attacker to name just a few possibilities if this attack is successful.

Spear: Spear phishing is more commonly seen within an organisation as it is used to target specific sections of a company, it is a well-researched attack that will normally be used on executives or finance departments to try get sensitive information (Webroot, n.d.).

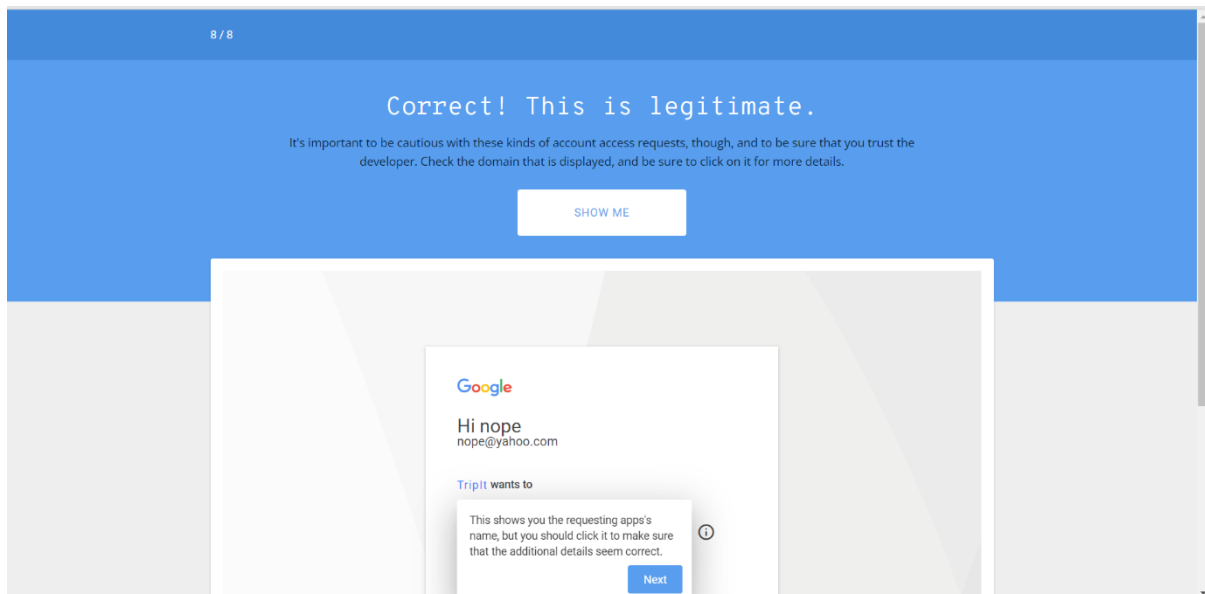


Figure 1 - Email Phishing (phishingquiz, n.d.)

- Website Phishing:** A phishing website is a website that has been created by a threat actor and made to be as close to a real website as possible, this is done with the intention to get a victim to think they are visiting the real site so they will try to login with their details allowing for the attacker to then steal those details which is called credential theft (BlueVoyant, n.d). As shown below the site looks like the user has visited eBay but it can be seen in the URL it isn't eBay. If successful this attack allows the attacker to use those details to commit credit card fraud or transfer money from the victims account along with many other options open to the attacker as they now have the victims' details.

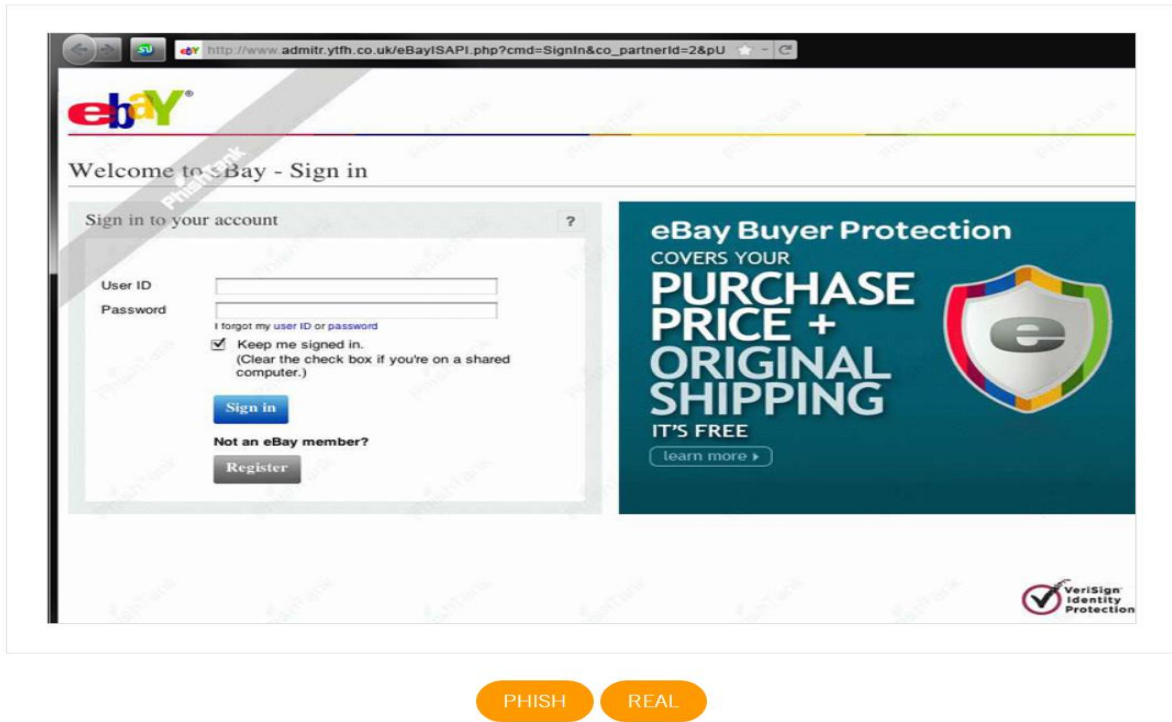


Figure 2 - Website Phishing

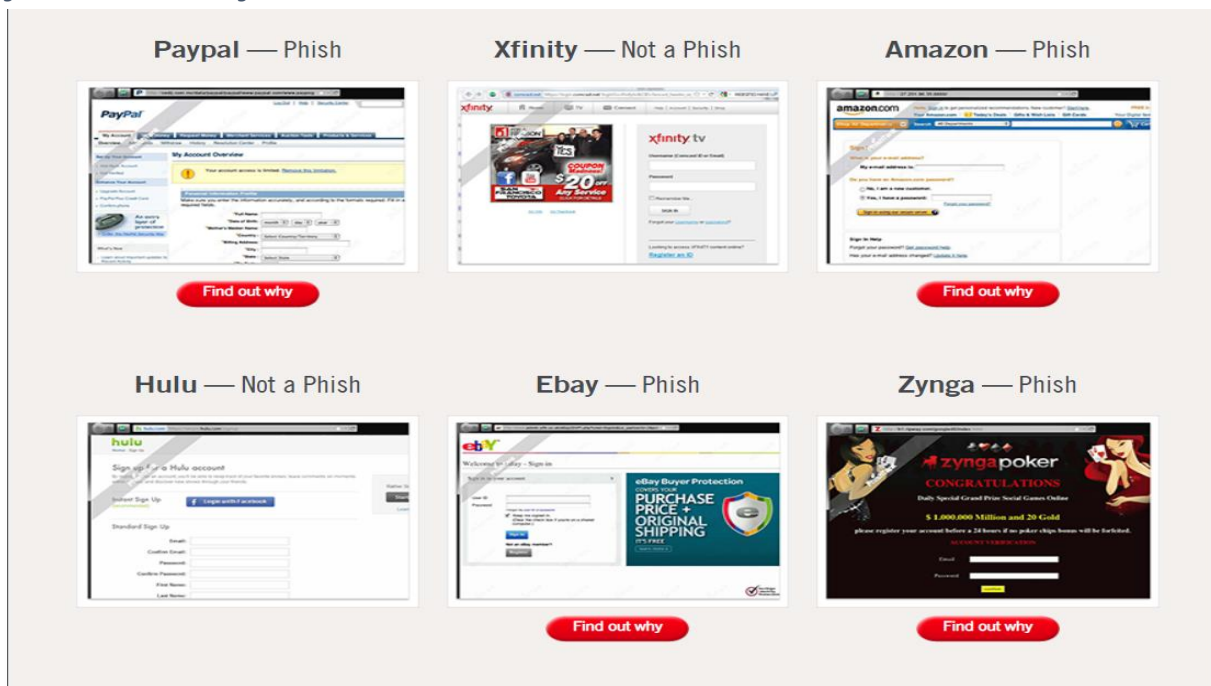


Figure 3 - Website Phishing (opendns, n.d.)

- Text Message Phishing (Smishing):** Smishing, the word being a combination of SMS and phishing, is an attack where an attacker will send a text message to a victim with the intention of getting them to send them personal or financial information, it can also include malicious links or files much like email phishing with the hope that the victim will click on them. These attacks although usually random and sent in bulk can be targeted with information stolen previously. This is usually done in the form of using a name of a family member or public known information like an address or their own name to try and trick the victim. There are many different types of smishing attacks some of which being Prize or Lottery scams, Bank Fraud Alerts or Account Verification Scams (Proofpoint, 2023).

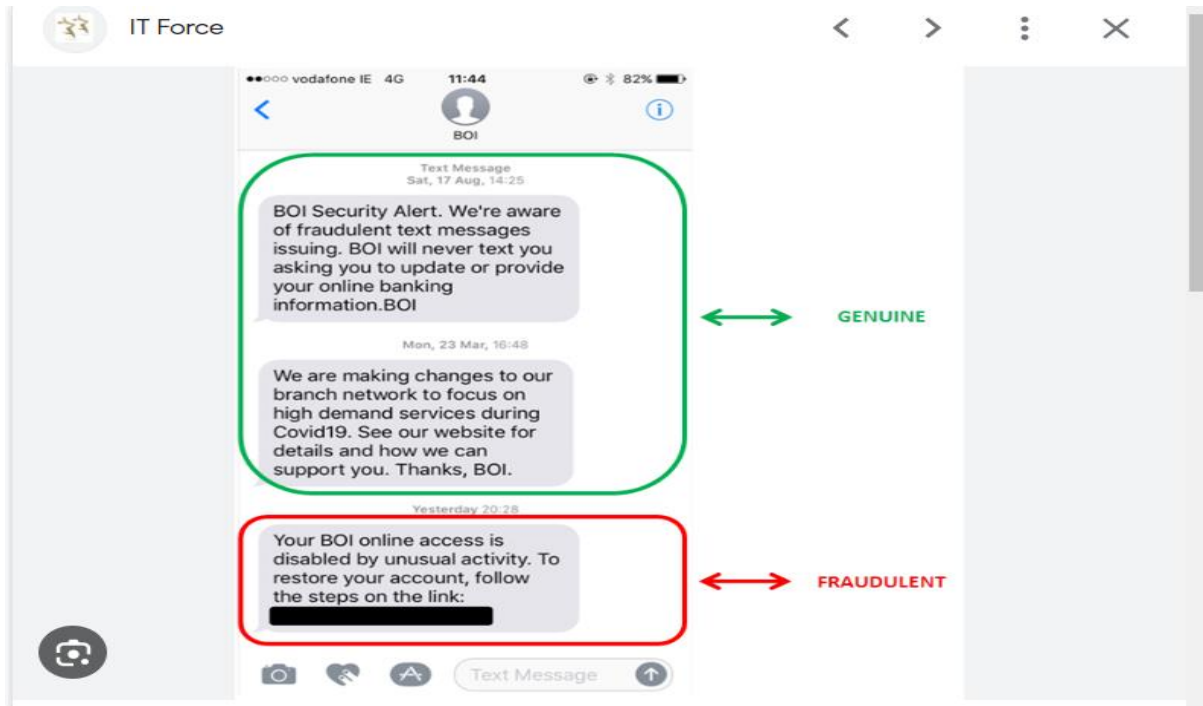


Figure 4 - Text Message Phishing (Smishing) (ITFORCE SQUARESPACE, 2021)

Quiz: Can You Spot Common Smishing Scams?

It's time to put your smishing knowledge to the test. Below are several multiple-choice questions, each featuring a potential smishing example. Think about whether each message is genuine or fraudulent, and consider how you would respond to these in real life.

- You receive a text message from an unknown number saying that your bank account has been temporarily frozen due to suspicious activity and you should click on a provided link to verify your account. Is this likely a smishing scam?
 A) Yes
 B) No
- A text message from a number claiming to be your service provider asks you to update your payment details through a provided link, citing problems with your current payment method. Do you suspect this is a smishing scam?
 A) Yes
 B) No
- You get an SMS from an unknown number, stating you've won a gift card from a major retailer, with a link to claim your prize. Could this be a smishing scam?
 A) Yes
 B) No

Figure 5 - Text Message Phishing (Smishing) (ITFORCE SQUARESPACE, 2021)

Vishing: Voice phishing (vishing) is when an attacker calls a victim and tries to trick them into giving out sensitive information be that financial or personal. A Scammer will call a victim and pretend to be a legitimate call from for example a bank and there is a problem with their account that requires immediate action and ask for the victim's details hoping the urgency will make them panic and they will give the information. These types of attacks are now becoming more targeted with attackers using information gained through online searches or through other means to convince the victim that they are the real bank or company they are pretending to be (TechTarget, 2023).

Scenario Question: Users will be given a specific phishing scenario that will be of a certain situation, this will follow with multiple choice answers that will be various options for them to choose which is the correct response for the given scenario, as shown below.

Cybersecurity Quizzes

Cybersecurity Basics Quiz

Phishing Quiz

Physical Security Quiz

Ransomware Quiz

Secure Remote Access Quiz

Tech Support Scams Quiz

Vendor Security Quiz

You get an email or text that seems to be from one of your company's vendors. It asks you to click on a link to update your business account. Should you click? Probably not. This could be a phishing attempt.

To find out how much you know about phishing, choose the best response for each question or statement.

1. Which one of these statements is correct?

A. If you get an email that looks like it's from someone you know, you can click on any links as long as you have a spam blocker and anti-virus protection.

B. You can trust an email really comes from a client if it uses the client's logo and contains at least one fact about the client that you know to be true.

C. If you get a message from a colleague who needs your network password, you should never give it out unless the colleague says it's an emergency.

D. If you get an email from Human Resources asking you to provide personal information right away, you should check it out first to make sure they are who they say are.

<https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/quiz/physical-security>

Figure 6 - Scenario Questions (ftc, 2021)

Who it's For

This application/website will be for people that might not necessarily have much of an understanding when it comes to phishing, and how they can be vulnerable to attacks.

As mentioned, my hope is to have this website help grow peoples understanding to help protect themselves better, people like the elderly or less tech savvy people. As this group of people have now become more tech enabled with the use of tablets, mobile phones etc especially since covid, they are now much more vulnerable and at risk of coming into contact with a phishing attack.

It will of course be beneficial to anyone at any level as it could be used to even just give a refresher to someone that might know a little bit about phishing.

The goal is to get this website to a state that anyone can use it, at any level to improve their knowledge of phishing to try and lower the possibility of people falling victim to an attack.

Inspiration

What led me to wanting to create this for my project was a few things, first having seen just how easily some of my family and friends were affected by or nearly and in some cases actually falling for phishing scams it led me to think about maybe it would be better if there was an easier all in one place to go to learn and understand phishing for these people that might not be tech savvy enough to do the research or multiple quiz's to learn about it.

Along with this there were two other reasons, first being seeing how our class found it awkward and difficult to research for the cyber awareness day that was held in the college. This added to wanting to streamline information and a quiz into one location for ease of access and use.

The final reason the led to this project was, while on my internship having worked within the security team, I seen on a daily basis just how many people were either falling for the organised training phishing emails from the company or in worse cases falling for real ones causing security concerns and incidents.

Combining all these reasons made the want and interest for me to decide on this website project as stated previously to try to help improve awareness in everyday lives.

Deliverables

Non-Technical Deliverables

Primary Deliverables:

1. Research Report:

This report is designed to help with the important decisions for this project like tools and platforms that will be used to create the project. It will be used to allow anyone that reads the report to understand the thought process behind each stage of the project, why the decisions were made to use specific technologies and why certain decisions were made for example why a certain look or design was implemented.

2. Project Report:

With this being the final report that will be delivered it will showcase any new skills that have been developed while working on this project, what you have learned i.e. any mistakes made and what was learned from them. It will show any issues both technical and non-technical and act as a way to show how the project got to its final implementation.

3. Project Spec and Plan:

This will be used to explain all the aspects of the project with those being what the project is, identifying the user group(s), how it will be deemed successful, along with information on the reason behind the project and how it is different from possible similar cases that exist already.

4. Research Poster:

The research poster will be used to summarise the research done and the information found by using a mixture of text, graphs, pictures etc.

5. Surveys Created: Three surveys will be created using the Microsoft Forms platform, they will have between 5-10 questions. One will be for the target users to gauge their level of knowledge of phishing, another also for users as a way of getting feedback on the website and its functionality to be able to make it more user friendly to the target user group. The final survey will be for non-target users to be used to test the website/quiz from different viewpoints for feedback on functionality and security.

6. Surveys Distributed: The surveys will be distributed at various stages of the project to get as much information as possible Firstly to non-users for feedback on the functionality of the website, then to the users before they use the platform and finally to the users after they have used the platform.

7. Surveys Analysed: Once all surveys have been distributed and a set amount have been completed, ideally as many as possible with a minimum of 15 users surveyed. Both for the user surveys to get percentages and data on knowledge levels to along with a feedback survey for possible website improvements for users and the non-user surveys to get feedback on the website and any issues.

Secondary Deliverables:

1. Changes Implemented: Once the Surveys have been analysed and notes have been made from both the users and non-users, I will first go through the non-user responses and try to implement as many as possible that benefit the functionality and security of the website, then the user responses will be implemented after.

Technical Deliverables

Primary Deliverables:

1. **Website Created:** The website will be setup at a basic level at first to make sure everything can run and is connected correctly, like the database linking correctly for user account creation and login. Once this has been done, the website will be then edited to be suited to the target user group, research will have been done to help decide what is the best layout and structure of the website that best suits the users, for example bigger text or brighter colours. While being coded security measures will be included in the various stages of the project, some of the measures that will be implemented will include data validation, page logout timer, along with all data being entered into the database being encrypted.
2. **Database Setup:** Database will be setup using MySQL, this will hold all the user's details entered when they are creating an account for the website and store them securely by encrypting the data in the database. It will also store all of the questions for the quiz that will be on the website.
3. **Created Questions:** Having looked at various ways that quiz's and learning tools were done for phishing I have a good idea of how I want to structure the questions for the quiz this knowledge will be used to create a pool of questions, these will be then used for the quiz with the quiz picking from the list at random to keep it different each time a user takes the quiz.
4. **Quiz Created:** The quiz will be created with the intention of being as robust as possible, it will cover as much information it can without overloading the user. The quiz will consist of 8 – 12 questions which will be mixed between scenario based and image-based questions which will give a broad view of different types of phishing to the user.
5. **User Tests:** Appropriate tests will have been conducted on the website to test its functionality and security, these will be done before the website is then put through some user tests of the specified user group.

Secondary Deliverables:

1. **Scoring System:** A scoring system will allow for users to gain points as they get correct answers, this will be used as a way to incentivise users to do the learning to get more points to be placed into a leader board.
2. **Email Users:** Potentially add functionality for users to be emailed their results, this will be from the email the user has used to sign up to the website and will be setup with the use of a crontab by adding any user's that sign up to the script that will trigger on completion of the quiz. This could also be used to send other functions like a badge or certificate if these are added at any point to the project.

Technologies

Languages

The languages being used within this project will be HTML which will be used to create the structure of the website, CSS to make the website have a look and style suitable to my target user group, JavaScript giving function to and allowing the website to be interacted with and PHP which will allow for linking of the database and for information to between the website and database. I was hoping to use Python for this project as I had wanted to learn it and feel it would have been beneficial along with helping to create my website. While this could still be done, I feel with the time restraints for this project that it is more reasonable to stick with the languages I have used previously as it will allow me to get started sooner on designing and creating the website.

HTML

HTML which stands for Hypertext Markup Language is used to give a structure to a website with the use of tags that will tell the browser what to do with the given text. It allows for options on a webpage like paragraphs and page breaks. I have chosen this to be used for my website as I have used it previously throughout various projects and it allows me to put the contents in to create a skeleton of a webpage to be built upon, (O'Grady, B, 2023).

CSS

Cascading Style Sheets otherwise known as CSS is what is used to add colour and style to a webpage which can be used in both an external style sheet or internally to the page you are editing/creating, it allows for the use of specific colours, layouts and fonts along with much more. This was chosen because of my knowledge of it along with the fact it functions well with HTML. It will be used to give my project a look that will be to benefit my target user group, (O'Grady, B, 2023).

JavaScript

JavaScript is what is used to make a website interactive and give life to a webpage controlling multimedia within the webpage, it allows for functions such as filling out forms or registering for an event, (O'Grady, B, 2023). As JavaScript allows me to make the website more engaging for my user group and gives it the functions I want on the website, along with my prior knowledge of the language is why I chose it to be used as a part of this project.

PHP

PHP is an open-source language that can be embedded into HTML and because of this it will be used within my project to build functionality and allow for various actions to be performed within the website. Having used PHP before and because it allows for me to take the data input by the user and send it to the database while storing and encrypting it were why I chose this to be used in the project, (O'Grady, B, 2023).

Python

Python is a high-level programming language with a reputation for being beginner friendly, it has replaced java as the most used introductory language as it handles a lot of the complexity, (Terradata, n.d.). With having an interest in learning Python, I want to as part of my research look into using it for the creation of websites to see if I will be able to possibly use this to create my website and learn a new language at the same time, from first glance online it seems to be quite popular to use Python along with Flask or Django to create websites, (Mieczkowski, O, 2023).

Tools

The tools that will be used in this project are a mixture of ones I have used before like XAMPP, Visual Studio Code and Docker along with a new tool Bootstrap that I feel will be of benefit to use for the project, provided the time restraints allow for me to learn and implement it.

XAMPP

XAMPP is an open-source web development environment that houses multiple tools into one location. The main reasoning for choosing this tool is that I have used it previously for projects and it houses an Apache Server allowing me to host and test the website and MySQL for storing my database in the one location for convenience, (cloudfoundation, 2023).

Visual Studio Code

VSC is a source code editor which is free but powerful, it runs on your desktop and has built-in support for JavaScript and Node.js along with extensions for most other languages like C++, Java, Python and PHP, (Heller, M, 2022). I chose to use this as my code editor as it is what I have the most experience in using for any form of coding and what I feel the most comfortable with.

Bootstrap

Bootstrap is a web development toolkit, it is a frontend development framework that allows you to quickly build responsive websites. With Bootstrap it can save time by removing the need for lots of CSS code and allow for more time to be spent on the design of the website with it having components like navigation bars and dropdowns amongst others, which I feel would make this a beneficial additional tool to the project for this reason, (Ouellette, A, 2023).

Docker

Docker is a software framework that allows for the building and managing of containers, it packages all code and dependencies in a standard format allowing it to be run quickly across environments, (Oracle, n.d.). The reason for looking into docker is because of a project last year, I had issues with databases and some got corrupted and upon switching to Docker I had no issues. My plan is to start with the built in XAMPP database application but back everything up and have Docker ready to go if needed.

Database

MySQL

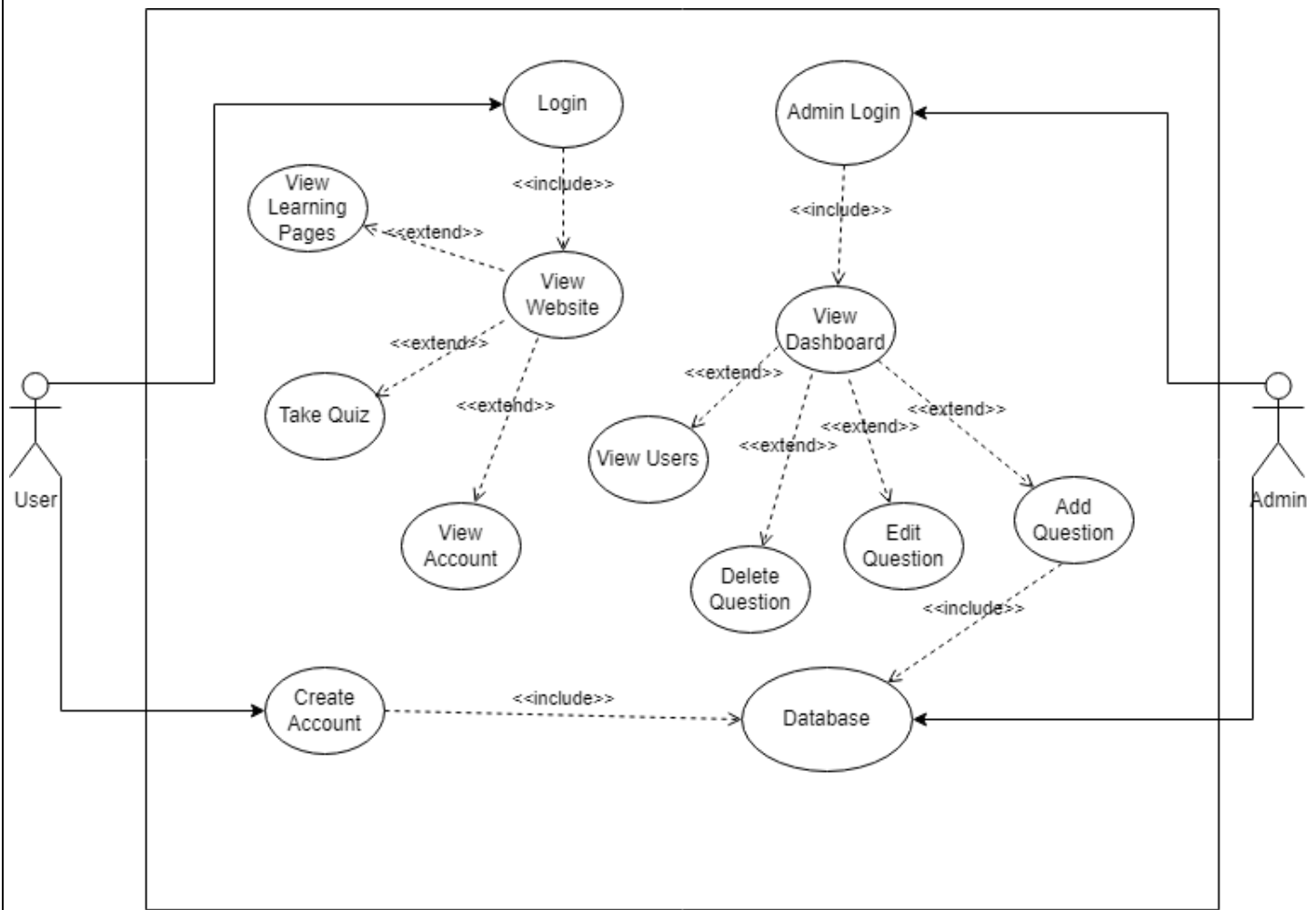
With MySQL being the world's most popular open-source database, it is used in most applications including Facebook (Meta) and Netflix among others it made it an easy choice to use this for my project to use for my database as it is widely compatible allowing me to make necessary changes if needed. Although MariaDB is becoming more popular, (cloudways, 2022) , I chose to stick with MySQL as it what I have knowledge of and have used before , (Oracle, n.d.).

Surveys

Microsoft Forms

Microsoft forms is a tool that allows a user to create surveys, quizzes and polls which has built in analytics to evaluate all responses. Once a survey is created it can be sent to be taken and be accessed on any browser or a mobile/tablet device, (Microsoft, n.d). Having looked into both Microsoft Forms and SurveyMonkey and seeing that a lot of the functions for SurveyMonkey were behind a paywall, along with the ease of use and built in analytics I chose Microsoft Forms as the platform to create and distribute my surveys.

Use Case Diagram



Use Cases

The below is a collection of uses case descriptions that will be of the various interactions with the website from two different actors, giving a better understanding of each functionality within the website. The actors being the User of the website and the admin account of the website.

Use Case 1	Create Account
Description	User creates account to access website
Actor	User
Trigger	User clicks signup button
Precondition(s)	User has email to create account
Main Success Scenario	User creates account successfully
Postcondition(s)	User can now use signup details to login

Use Case 2	Login to Account
Description	User logs into previously created account
Actor	User
Trigger	User Logs into website
Precondition(s)	User has an account on the website
Main Success Scenario	User can successfully login to their account
Postcondition(s)	User is now logged in and on main page

Use Case 3	Main Page
Description	User can go through the main page to access Learning
Actor	User
Trigger	User has successfully logged in
Precondition(s)	User is Logged in to account
Main Success Scenario	User can view Learning page
Postcondition(s)	Learning page is viewable by User

Use Case 4	Take Quiz
Description	User can navigate to and take Quiz
Actor	User
Trigger	User has successfully logged in
Precondition(s)	User is Logged in
Main Success Scenario	User finishes Quiz
Postcondition(s)	User can view and take Quiz

Use Case 5	View Users
Description	Admin can login and view User signed up
Actor	Admin
Trigger	Admin has successfully logged in
Precondition(s)	Admin is logged in
Main Success Scenario	Admin can view all users
Postcondition(s)	User's info is displayed to Admin

Use Case 6	Add Questions
Description	Admin can add new questions to quiz
Actor	Admin
Trigger	Admin is on the quiz edit screen
Precondition(s)	Admin is logged in
Main Success Scenario	Admin can add questions successfully
Postcondition(s)	New question is in the pool

Use Case 7	Edit Questions
Description	Admin can edit questions
Actor	Admin
Trigger	Admin is on the quiz edit screen
Precondition(s)	Admin is logged in
Main Success Scenario	Admin can edit any question
Postcondition(s)	Questions are successfully edited

Use Case 8	Delete Questions
Description	Admin can delete questions
Actor	Admin
Trigger	Admin is on the quiz edit screen
Precondition(s)	Admin is logged in
Main Success Scenario	Admin can delete a question
Postcondition(s)	Question is successfully deleted

Metrics

- 1. User Account Creation:** A user can visit and enter their details to create an account.
- 2. User Login:** A user can login successfully with their details used in the creation of the account.
- 3. User Navigation:** Once logged in the user will be able to navigate through the website to the different pages.
- 4. Quizzes populate correctly:** The quizzes in each section are populating correctly with the right amount of question in each, 3-5 for the sectional quizzes and 8-12 for the main quiz.
- 5. Users Stored Correctly and Securely in Database:** Database functions correctly and stores the information in the correct manor, while also storing it securely.
- 6. Questions are stored correctly in Database:** All questions being used for the quizzes are stored correctly within the database in their correct tables.
- 7. Admin Login:** Admin can login successfully to the admin dashboard.
- 8. Admin Navigation:** Admin can navigate successfully to the various sections of the dashboard.
- 9. Admin Question Functions:** Admins can perform all functionality on questions, those being add, edit and delete questions.
- 10. Admin Can View Users:** Admin can view users that have created an account in a table on the dashboards.
- 11. Surveyed Users Before:** A minimum of 15 users will be surveyed before visiting and using the site to get an idea of their knowledge before learning from the site.
- 12. Surveyed Users After:** Those Users will be surveyed after use of the site for their experience with it and for possible changes to make the user experience better.

FURPS

FURPS is a way to categorise functional and non-functional requirements, it is designed to help categorise requirements and verify the completeness of requirements, (Ziemek, M, n.d.).

Functionality

The main functional components of this project are as follows:

- User can create an account and login to the website.
- User's information is stored securely.
- User can navigate between pages.
- User can take quiz.
- Admin can login.
- Admin can view users.
- Admin can make changes to quiz.

Usability

With usability it sets the requirements to ensure the project is understandable and easy to use. The main concentration areas will be accessibility and consistency with making sure the website runs the same on most if not all browsers, along with keeping the layout consistent on each page and each section to make sure the user can follow through with as much ease of use as possible, (Ziemek, M, n.d.).

Reliability

Reliability defines the ability of a product to perform a function, this will be the website performing the correct functions as outlined in this document, (Ziemek, M, n.d.).

Performance

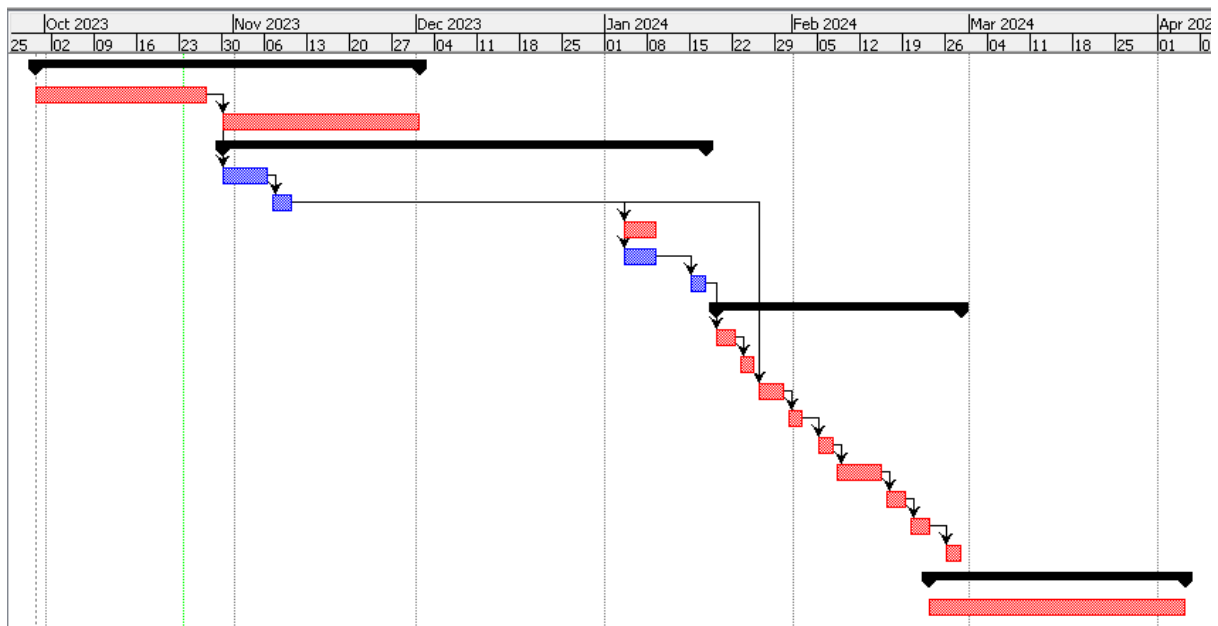
Performance is the degree in which a system or component performs its functions. This will be prevalent in this project with making sure the login time for a user does not take long and they can access the webpage in an adequate time, (Ziemek, M, n.d.).

Security

Security requirements refer to the grant of access control to an application and data protection during storage. Both parts of security will be a major aspect within this project as it will be made that only the person with the correct login details can access that account and all accounts created will have their data stored securely within the database, (Feronika, N, 2018).

Project Plan

	📌	Name	Duration	Start	Finish	Predecessors
1		📁 Starting Documentation	46 days	29/09/23 08:00	01/12/23 17:00	
2		Project Spec and Plan	21 days	29/09/23 08:00	27/10/23 17:00	
3	📄	Research Document	25 days	30/10/23 08:00	01/12/23 17:00	2
4		📁 Development	58 days	30/10/23 08:00	17/01/24 17:00	
5		Base Website Setup	6 days	30/10/23 08:00	06/11/23 17:00	2
6		Database Setup	4 days	07/11/23 08:00	10/11/23 17:00	5
7	📄	Learning Page Created	4 days	04/01/24 08:00	09/01/24 17:00	6
8	📄	Quiz Page Created	4 days	04/01/24 08:00	09/01/24 17:00	6
9	📄	Quiz Created	3 days	15/01/24 08:00	17/01/24 17:00	8
10		📁 Testing	29 days	19/01/24 08:00	28/02/24 17:00	
11	📄	Website Testing	2 days	19/01/24 08:00	22/01/24 17:00	9
12	📄	Implement Website Changes	3 days	23/01/24 08:00	25/01/24 17:00	11
13	📄	Database Testing	3 days	26/01/24 08:00	30/01/24 17:00	6
14	📄	Implement Database Changes	3 days	31/01/24 08:00	02/02/24 17:00	13
15	📄	Create Survey	3 days	05/02/24 08:00	07/02/24 17:00	14
16	📄	User Testing	6 days	08/02/24 08:00	15/02/24 17:00	15
17	📄	Survey Users	2 days	16/02/24 08:00	19/02/24 17:00	16
18	📄	Implement Final Changes	4 days	20/02/24 08:00	23/02/24 17:00	17
19	📄	Final Testing	3 days	26/02/24 08:00	28/02/24 17:00	18
20		📁 Final Documentation	31 days	23/02/24 08:00	05/04/24 17:00	
21	📄	Final Report	31 days	23/02/24 08:00	05/04/24 17:00	



References

1. Consumer Data under attack: The growing threat of cyber crime (2016) Deloitte Turkey. Available at: <https://www2.deloitte.com/tr/en/pages/risk/articles/consumer-data-under-attack.html> (Accessed: 18 October 2023).
2. Email phishing, Vishing & other types (no date) Webroot. Available at: <https://www.webroot.com/ie/en/resources/tips-articles/what-is-phishing> (Accessed: 21 October 2023).
3. Feronika, N. (2018) What do requirements stand for?, School of Information Systems. Available at: <https://sis.binus.ac.id/2018/02/12/what-do-requirements-stand-for/> (Accessed: 24 October 2023).
4. Heller, M. (2022) What is visual studio code? Microsoft's extensible code editor, InfoWorld. Available at: <https://www.infoworld.com/article/3666488/what-is-visual-studio-code-microsofts-extensible-code-editor.html> (Accessed: 22 October 2023).
5. How to identify a phishing website & 3 tips to prevent phishing (no date) BlueVoyant. Available at: <https://www.bluevoyant.com/knowledge-center/how-to-identify-a-phishing-website-3-tips-to-prevent-phishing> (Accessed: 21 October 2023).
6. Key differences – comparing mariadb with mysql (2022) The Official Cloudways Blog. Available at: <https://www.cloudways.com/blog/mariadb-vs-mysql/#:~:text=It%20comes%20with%20various%20inbuilt,applications%20and%20CMS%2C%20especially%20WordPress.> (Accessed: 23 October 2023).
7. Microsoft (no date) Microsoft Support. Available at: <https://support.microsoft.com/en-gb/office/what-is-microsoft-forms-6b391205-523c-45d2-b53a-fc10b22017c8> (Accessed: 22 October 2023).
8. Mieczkowski, O. (2023) Flask vs. Django in 2023 – which python framework to choose and when?, AI. Available at: <https://www.monterail.com/blog/flask-vs-django/#:~:text=Flask%20and%20Django%20are%20the,debate%20is%20not%20that%20simple.> (Accessed: 22 October 2023).
9. Nagendrag (2023) What is XAMPP? - cloudfoundation: Blog, CloudFoundation. Available at: <https://cloudfoundation.com/blog/what-is-xampp/> (Accessed: 22 October 2023).
10. O'Grady, B. (2023) What is HTML, and why should I learn it?, Code Institute Global. Available at: <https://codeinstitute.net/ie/blog/what-is-html-and-why-should-i-learn-it/> (Accessed: 22 October 2023).
11. Ouellette, A. (2023) What is bootstrap? an awesome 2023 beginner's guide, CareerFoundry. Available at: <https://careerfoundry.com/en/blog/web-development/what-is-bootstrap-a-beginners-guide/> (Accessed: 22 October 2023).
12. Phishing Quiz. (No date) Available at: <https://phishingquiz.withgoogle.com/> (Accessed: 18 October 2023).
13. Ritchie, J.N.& A. and Jayanti, S.F.-T. and A. (2021) Phishing quiz, Federal Trade Commission. Available at: <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/quiz/phishing> (Accessed: 18 October 2023).
14. Sheldon, R. (2023) What is vishing (voice or VoIP phishing)? – TechTarget definition, Unified Communications. Available at: [https://www.techtarget.com/searchunifiedcommunications/definition/vishing#:~:text=Vishing%20\(voice%20or%20VoIP%20phishing\)%20is%20a%20type%20of%20cyber,sensitive%20ata%20to%20unauthorized%20entities.](https://www.techtarget.com/searchunifiedcommunications/definition/vishing#:~:text=Vishing%20(voice%20or%20VoIP%20phishing)%20is%20a%20type%20of%20cyber,sensitive%20ata%20to%20unauthorized%20entities.) (Accessed: 21 October 2023).
15. Squarespace, Itf. (2021) How to identify a 'smishing' attempt on your smartphone, IT Force. Available at: <https://www.itforce.ie/blog-1/how-to-identify-a-smishing-attempt-on-your-smartphone> (Accessed: 18 October 2023).
16. What is Docker? (no date) What is Docker | Oracle Ireland. Available at: <https://www.oracle.com/ie/cloud/cloud-native/container-registry/what-is-docker/> (Accessed: 23 October 2023).

17. What is mysql? (no date) Oracle. Available at: <https://www.oracle.com/mysql/what-is-mysql/> (Accessed: 22 October 2023).
18. What is phishing? take the opendns phishing quiz (no date) OpenDNS. Available at: <https://www.opendns.com/phishing-quiz/> (Accessed: 18 October 2023).
19. What is python? (no date) Teradata. Available at: <https://www.teradata.com/Glossary/What-is-Python> (Accessed: 22 October 2023).
20. What is smishing? examples, protection & more: Proofpoint us (2023) Proofpoint. Available at: <https://www.proofpoint.com/us/threat-reference/smishing#:~:text=The%20term%20is%20a%20combination,downloading%20harmful%20software%20or%20applications.> (Accessed: 21 October 2023).
21. Ziemek, M. (no date) Marcin Ziemek, blog, article, documenting non-functional requirements using FURPS+. Available at: https://www.marcinziemek.com/blog/content/articles/8/article_en.html (Accessed: 23 October 2023).