Research Document

ROBERT STYNES
C00136717

SUPERVISOR
KEARA BARRETT

Abstract

The goal of this research document is to provide insight into various aspects that will be used to create the best possible learning platform for older adults. As older adults are adopting the use of tech year on year be that owning a smartphone or using the internet, this has increased the need for them to be more aware of the dangers of being online, be that browsing the internet, sending emails or as has seen an increase lately with scams sending a text message.

This report will discuss what phishing is and the various types, the target user group of this project is aimed at which is older adults and how they are affected with current tech and phishing, how surveys are done and best practices for creating a good one and finally the tools and technologies that could be used within this project and what has been chosen to be used.

Table of Contents

1. Introduction

In an increasingly changing cyber landscape, the online world has become an integral part of our daily lives, changing the way we communicate, work and operate, (Deloitte, 2016). With the internet constantly evolving so too are the many cyber threats and cyber criminals, increasingly exploiting weaknesses and vulnerabilities. Phishing has emerged as a major concern. The focus of this project is to understand and provide a tool that will help mitigate the impact of phishing on a specific vulnerable group, that being older adults. This research document's first section's goal is to provide information and analysis of what phishing is, how it impacts individuals and businesses, along with the various types of phishing that can be used. It is to help develop a deeper understanding of this topic and its effects on this project's user group.

The next section discusses the various platforms that currently exist online at the moment to teach people about phishing, it is split between websites that offer this and quizzes. This is done with the intention of giving examples of how both are done as this project aims to combine the two into a single location.

After this research is discussed on the target user group of this project (older adults) and how phishing is increasingly being targeted towards them. Following this although a separate section it is closely related to this, it is discussed about tech usage and its rise with an emphasis on covering statistics about the rise in older adults and tech.

Research is conducted on a multitude of various tools and technologies ranging from programming languages and IDEs to survey tools. Going through each individually with a conclusion of what will be used in this project and the decision behind using them.

With surveys being used within this project for research reasons, it was looked at what a survey is how it should be structured and how to make a good one. Along with qualitative research vs quantitative research to decide which is best for this project and how best to create surveys to get the most information.

Finally, there is a discussion on the security implications of this project and how they are addressed, what parts of cybersecurity are being addressed with the implementation of this project.

2. Phishing

2.1. What is Phishing?

Phishing is a social engineering cybercrime attack that is most often used to steal a victim's data which can include login information, private information or banking information. This is done with an attacker pretending to be a legitimate or trusted source to try and trick the victim into clicking on a malicious link or to send or enter their personal/bank details.

If successful, this attack can lead to an attacker gaining access to a person's personal information leading to the possibility of identity theft along with other devastating results like their money being stolen or purchases being made with their information.

The first lawsuit pertaining to phishing was filed in 2004, this was against a teenager in California. They had created a fake website and gained access to sensitive information from victims and use it to steal money from their accounts, (Kumar et al., 2021).

Phishing attacks can be done in many different ways to try and achieve the attacker's goals, those forms of phishing are email phishing, smishing, website phishing, vishing along with spear and whale phishing. These different types of phishing are covered in more detail below.

2.2. Phishing Types

2.2.1. Email Phishing

2.2.1.1 General Phishing

General or standard email phishing is probably the most widely known type of phishing attack, (Webroot, n.d). It is an attempt to steal sensitive or personal information from a victim by pretending to be sending an email from a legitimate organisation. This form of email phishing is not targeted and usually will consist of an attacker sending out hundreds or thousands of malicious emails with the hopes that someone will fall for the spoofed email which will allow them to steal data.

Most of the time when these emails are sent, they are created to showcase a sense of urgency trying to make the victim panic and fall for the attack, an example of this would be possibly pretending to be a bank with the email stating there is an issue with the account and the victim needs to click the link and enter their details or the attacker may have created a domain that includes a legitimate companies name like amazon or eBay to trick the victim, (Irwin, L, 2023).

2.2.1.2 Spear Phishing

Unlike a standard email phishing attack a spear phishing attack is used to target a specific person to steal financial information, access credentials or trick them into downloading malware. These attacks are usually well researched, with the attacker having some information on the victim and being able to then use this information against them to create an attack. (Giandomenico, N, 2023) Attackers using spear phishing will target victims who have put their personal information on the internet as it allows them to gather information relatively easy through social media accounts getting details like:

- The employees name.
- Job title.
- Email address.
- Role within company.
- Personal info like friends, hometown or places they visit often.

With the attacker now in possession of some or all of the above they can now manufacture an email to trick the victim, they can use their name and job title using these to make the email seem legitimate while using other information gained to disguise themselves as someone the victim knows or someone from a trusted company they may work with, (Irwin, L, 2023).

2.2.1.3 Whale Phishing

A whale phishing attack is where an attacker will target high profile employees such as a CEO or CFO to try and steal sensitive information from the company they work for or their own personal information. In some cases, an attacker may use a malicious website that has been created for the attack. Like spear phishing emails, whale phishing emails are highly personalised and will look to use the victim's information like name or job title.

These attacks will usually use social engineering techniques with attackers sending links to the malicious site as mentioned above, or possibly an attachment to infect their system with malware. They can fool victims as attackers are willing to spend more time and effort creating them as they can yield high return, (Shea, S, 2021).

With these attacks being highly targeted along with the possible use of names and information regarding the victim's company, it tends to mean they are usually more difficult to detect and prevent.

2.2.2. Text Message Phishing (Smishing)

Smishing is similar to email phishing in that it tries to deceive the victim with the use of deception, the difference is that this will target victims through SMS or text messages. Again, like email phishing the goal here of the attack is to trick a victim into parting with personal or financial information, downloading malware or clicking a link that leads to a malicious site they created.

The attacker will again use a tactic of trying to appear from a trusted source in the text message, for example a son or brother saying they are texting from a friend's phone, or they got a new phone and they need money. This will be combined with the use of social engineering techniques to create a sense of urgency of fear with the hope the victim will do what is being asked.

A lot of people know there are possible dangers when it comes to emails and receiving malicious ones, but with text messages less people are aware of dangers and risks when it comes to interacting with what is within a text message. Because of

this smishing is successful and profitable for attackers as people will be more trusting of a text message received, (Proofpoint, 2023).

2.2.3. Search Engine Phishing

Search engine phishing is when an attacker uses search engine optimisation the process of improving a websites visibility within search engines, this leads to an increase in people clicking on the link to the website as people are more likely to click higher up links in the search to make it so their malicious website that they created will appear at the top of the search results.

This will look like a legitimate website to the user so they will think it's safe to enter their details to login to their account, the website will be setup to steal their details as and when they are entered allowing the attacker to use them to access that account or possibly other accounts if the victim has used the same passwords, (Trevino, A, 2023).

2.2.4. Voice Phishing (Vishing)

Vishing, also known as VoIP phishing is an attack that will use voice and telephone technologies in the form of fraudulent calls to trick a victim into giving personal/sensitive information or giving money. This could be financial information like credit card information or if the victim is being targeted for who they work for, it could be for information based on the company.

Usually, an attacker might call a victim directly or leave a voicemail, once the victim has either answered or they have reached the voicemail they will play a recorded message or speak directly. Vishing will usually involve an attacker pretending to represent a trusted company, government agency like the social welfare or bank.

Just like with other forms of phishing an attacker will try to create a sense of urgency, this is to try and create fear which can lead to the victim acting without thinking and falling for the attack. These attacks are now becoming more targeted, with attackers using information they have gathered from online profiles or if the victim's information had been leaked online which will allow for them to convince the victim they are genuine, (Sheldon, R, 2023).

2.2.5. Summary

As seen above there are multiple forms of phishing out there, but given that the primary focus of this project is on helping older adults with their understanding of and how to protect themselves against phishing and other online dangers, and as there has been a rise in older people being targeted, (Greggwirth, 2023) it is sensible to streamline what types of phishing may not be as relevant to this specific user group.

Notably, spear phishing and whale phishing, which primarily target information within corporate settings, may be addressed briefly, or at the very least only discussed briefly. Since the elderly are typically not affiliated with companies that attackers might seek to exploit, these specific phishing methods may not be as pertinent to their cybersecurity education. Instead, the emphasis will be placed on more direct threats that older individuals face with the older generation using more technology especially after covid, (R.A., Mace et al., 2022).

2.3. Current Learning Platforms for Phishing

When it comes to learning platforms and resources there are plentiful to choose from on the internet, if you know where to look.

2.3.1 Websites

For phishing and learning about it there are a multitude of websites that cover various aspects of phishing. With a google search you can find next to anything online, and phishing is no different. Some of the sites that have stood out in the attempt to give people information on phishing and to help them learn are:

Imperva.com: On Imperva's website they give a brief and generic explanation of what a phishing attack is. The first paragraph does do a nice job of getting the point across about phishing, along with mentioning some of the key points like an attacker pretending to be someone trusted or that the attack could be through email or text message. This section is split between explaining phishing on a user and phishing in an organisational setting.

Following the section explaining phishing, the website shows an example of a phishing attempt. The example that they have provided is of an attempted email scam, it gives a brief explanation talking about the email being mass distributed along with the contents of the email. There is a small section at the end of this that explains what can happen if a user clicks on the link within the email, the first paragraph explains about the leading to possibly a fake webpage where the attacker can steal the information entered. The second paragraph discusses session hijacking, this is done at a high level which wouldn't been easily understood by a normal user not having some knowledge of cyber security.

They discuss phishing techniques but only go on to explain email phishing and spear phishing, while important there are more techniques that are just as important to know about, especially with the rise in the use of mobile phones, (Laricchia, 2023) it is important to show how phishing can be done through mobile phones.

In conclusion they discuss how to prevent phishing, talking about how users "vigilance is key" briefly explaining what to look for in spoofed messages. Following this, steps are given for companies to take like 2FA and password management policies, (Imperva, 2020).

TechTarget.com: This website begins with a brief explanation of what phishing is, included in here is a short video going over these points along with going over how to spot a phishing attack.

The next section explains how phishing works in general along with an attack possibly being an email, text message or even social media post used to gain sensitive information along with how they can use social media platforms to get information to be used to create a believable phishing email.

The site then goes on to discuss how an attack will take place, explaining that a message/email will appear to be from a known entity and that the attack takes place once the user clicks on a malicious link or file within the email or message, this is accompanied by an image of a spoofed email.

Following this a small section going over how to spot a phishing email which gives a few points to help indicate a message or email is attempting to phish, points like:

- Poor Grammer.
- Message tries to invoke fear or urgency.
- Includes a request for person information like passwords or financial information.
- Misspelled or suspicious URL's.
-

The webpage's second half, detailing phishing type, is informative, offering valuable high-level insights, it covers a wide range of types that are of value for a user to know which aren't seen in many other sites like calendar phishing, pharming and clone phishing. Also covered are the general phishing attacks like voice, SMS and spear.

One of the best sections on the website is he phishing techniques one as it has some valuable information in there explaining various techniques attackers can use like:

- **URL spoofing:** Where an attacker uses JavaScript to put a picture a legitimate URL over the address bar of the browser.
- **Link Manipulation:** Is where a malicious URL is shown to look like it points to a legitimate webpage but actually links to the attacker's malicious location.
- **Link Shortening:** Attackers will shorten a link to hide its destination with victims having no way to know if the link goes to a legitimate site or malicious one.

Along with others like Chatbots and AI voice generators making emails, messages and calls harder to detect if they are legitimate or not.

Finally covered are how to prevent phishing with recommendations like spam and phishing filters, antivirus, firewalls and antispyware. Following this they give some good examples of phishing, discussing scams such as digital payment, financed based and work-related phishing attacks, (Gillis, 2023).

Phishing.org: This website's main page when visited first starts with a brief explanation of what phishing is, following this it goes into detail on features of phishing emails:

- **Too good to be true:** Designed to grab attention with an offer or deal like winning an iPhone, as the saying goes if it looks too good to be true it usually is.
- **Sense of urgency:** A technique used by a lot of attackers, the message will be created to incite fear in the victim to react without thinking. Usually done to state details are needed urgently in the hope the victim will send details.
- **Hyperlinks:** Links may not always be what they appear to be, hovering over a link can show that it actually goes to a completely different page.
- **Attachments:** If an attachment in an email is not expected never open it, they usually will contain malware.
- **Unusual sender:** If anything seems off with the sender don't click on it.

These details are accompanied by an image that shows an example of a phishing email along with various red flag to look out for as shown below:

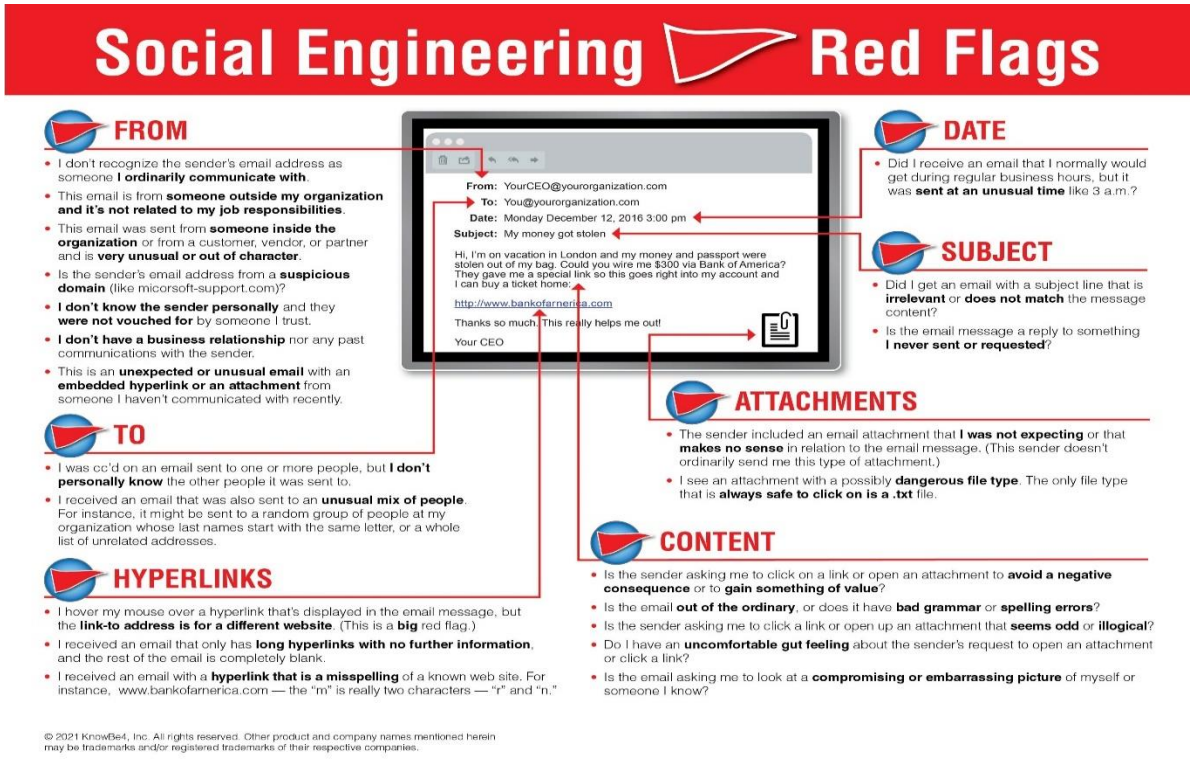

Figure 1 – Examples to look for in Phishing Email, (KnowBe4, n.d.).

Finally on the page how to prevent phishing attacks is discussed, some being the same as discussed on other sites like spam filters and checking URLs by hovering over link but also other that only appear here like changing browsing habits and changing browser settings.

The layout of this website is done with dropdown sections at the top of the page, each offering sections on various aspects of phishing. The sections split into sub-sections when clicked offering options to select to learn the phishing 101 section houses the main page as discussed above along with a section discussing phishing techniques, this section covers a lot f the same techniques as other pages like spear phishing, email/spam, web based and voice phishing.

Types of Phishing scams once selected has four sub sections:

- **Common phishing scams:** which discusses various scams like credit card, bank, website and email phishing scams.
- **Phishing examples:** This sub section goes through various images while explaining the phishing example.
- **Phishing and spoofing:** Goes into more detail explaining email and website spoofing.
- **Phishing and identity theft:** Discusses personal data and what attackers can do with it and how to avoid identity theft.

The final sections discuss ways to avoid phishing like being aware before clicking on links and attachments, using firewalls or using antivirus. The quiz at the end is very generic with the same questions every time, (KnowBe4, n.d.).

Cisco.com: Cisco have structured the presentation of phishing in sections on the webpage that you can scroll through or select from a bar that sits at the top of the page. Each section it presents is quite small, the first section which is What is Phishing? Although small is informative and gets right to the point of describing phishing, it doesn't pad with needless information but rather tells the user precise facts like stating phishing appears to be from a legitimate source, usually through a text message or email, and what the attacker's goal is with a phishing attack, that being to steal money, gain information or install malware.

The section that follows this has some information given more space on the page than maybe needed over others. They go into nearly double the detail on why an attacker sends a phishing scam over how phishing tricks users, following this they discuss how phishing works, adding to what was stated higher up with points like attackers using fear and urgency.

One section on this webpage that stands out is one that talks about AI, it discusses how phishing is evolving with AI and attackers are now using AI to "carry out sophisticated and targeted attacks by correcting spelling mistakes and personalizing messaging", (cisco, 2023).

The webpage goes on to discuss phishing prevention, this section while informative is more leaning into measures a company can take than people. Two recommendations from here are useful to users those being:

- Avoid posting personal or contact information online.
- Create a unique email address – i.e., don't use first name and last name.

While this site does explain some detection methods like checking examining links and checking for misspellings within the body text of an email, it has a nice brief but informative breakdown of "additional" steps the individuals can take.

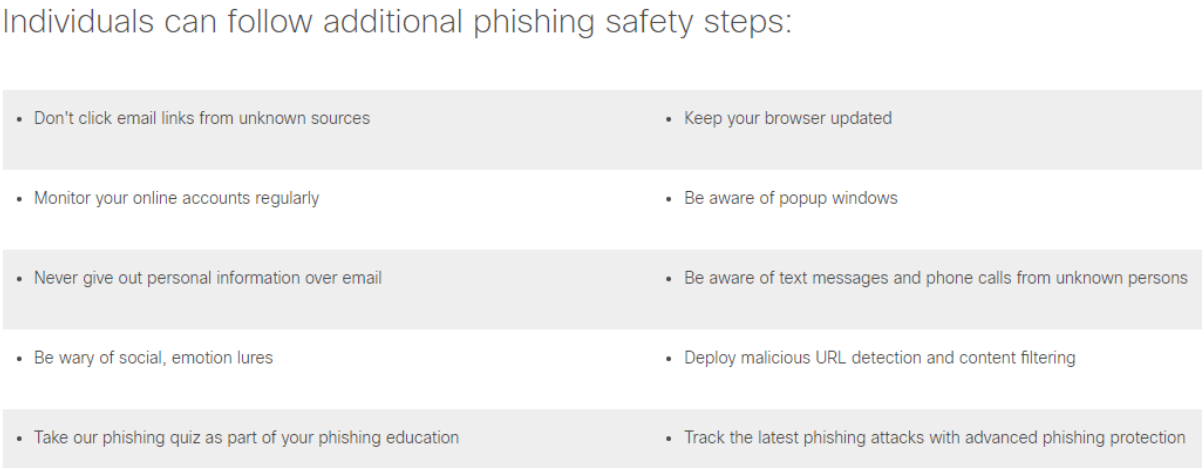

Figure 2 – Additional Phishing Safety Tips, (cisco, 2023).

The final two sections consist of first discussing the most common types of phishing attacks, within this section it is mainly focused on threats related to business email compromise with threats like employee impersonation and payroll diversion fraud. Following this is a small quiz at the very end with the questions covering various aspects discussed throughout the webpage, (cisco, 2023).

All these websites have a common theme of being a bit basic, they will have either information on the various types of phishing but with a minimal amount or they will just talk about phishing in general, leaving you to go in search of more websites to find out about the rest of phishing and how it can affect you or how to protect yourself. While this is by no means a major issue for most people, it still isn't ideal to have to go to various websites to find the answer you are looking for.

The exception in these sites would be TechTarget as they have a decent amount of information including soe that most other sites fail to discuss, but just like the others is in the same boat with the design and structure being at times too high-level. A lot of the information although good is not necessarily worded in a way that everyone could understand and may lead to a user not benefitting fully from learning off these sites.

The goal of this project is to take the good aspects these sites have and build upon them while making the finished webpage user friendly and easy to understand for the target user group with using designs and language that they would find easier

2.3.2 Quizzes

Online quizzes are a great way to test your knowledge on a given subject matter, they provide some validation to what you have been trying to learn. Below are some of these quizzes:

Opendns.com: The approach this quiz takes is to test the user's ability to identify whether a website is legitimate or phishing, this is done by presenting the user with various images of webpages for them to investigate with their knowledge and decied if the webpage is legitimate or not. By using a varied number of known webpages, it tests the user's perception to identify the subtle changes if it is indeed a phishing attempt, (opendns, n.d.).

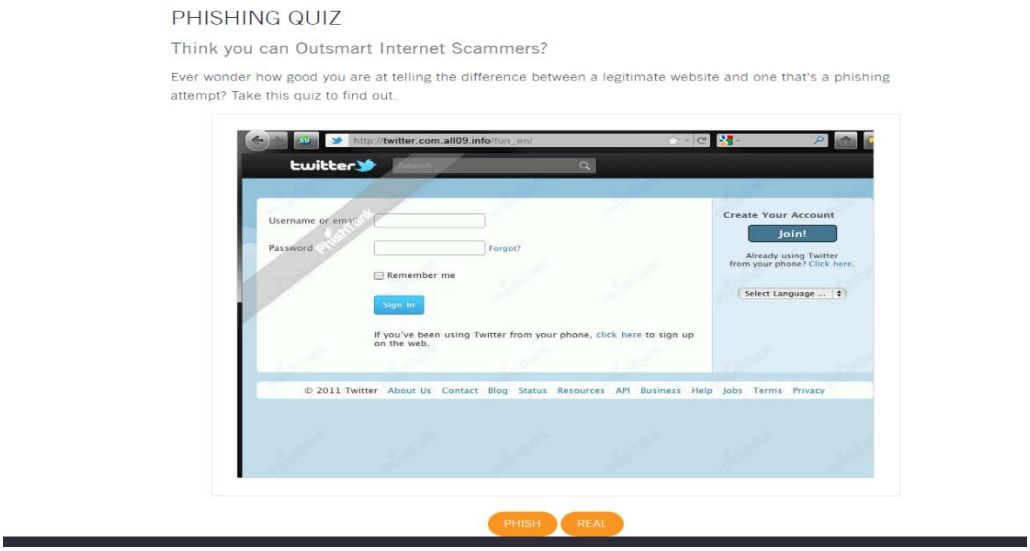

Figure 3 – Opendns quiz, (opendns, n.d.).

Phishingquiz (google): This quiz differs from the previous as it presents the user with specific scenarios that they have to investigate by hovering over links and sections of the scenarios to decide if they are phishing or legitimate. This quiz also improves upon the previous as it has interactive elements keeping the user engaged and puts into practice one of the steps to be phishing aware, hovering over links, (Google, n.d.).

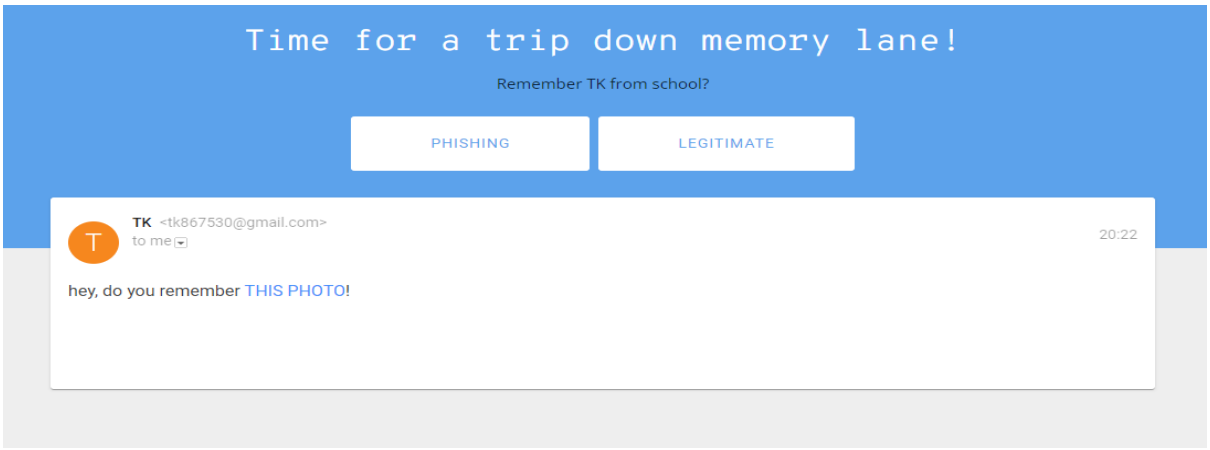

Figure 4 – Phishinquiz Example, (Google, n.d.).

Ftc.gov: This quiz is one of the more basic ones online, it has a structure similar to the previous quiz in that it gives the user scenarios to decipher but there are no images in this one. It is all text base with a scenario explained followed with a list of possible answers, giving the quiz a multiple answer structure, (Ritchie & Jones, 2021).

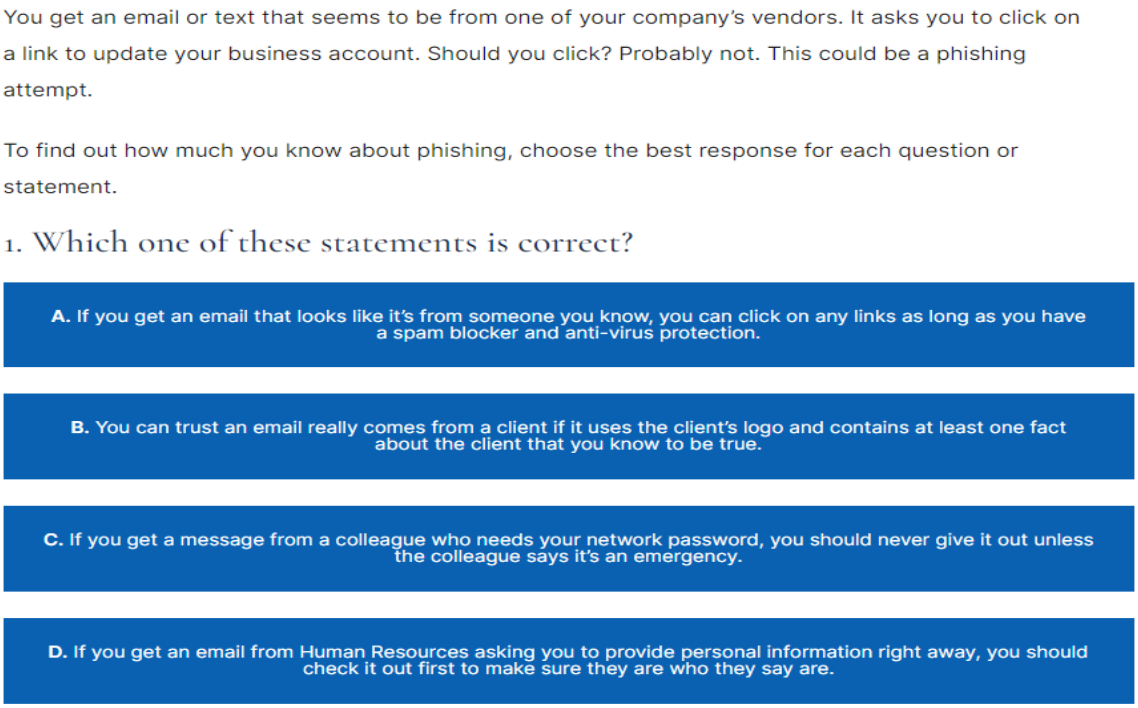

Figure 5 – FTC.gov quiz Example, (Ritchie & Jones, 2021).

Sonicwall.com: This website follows a similar pattern to the second quiz, it shows images that are interactable allowing the user to hover over various parts. Ten questions are given each a different image of an email and the user has to decide if it is legitimate or a phish, (sonicwall, n.d.).

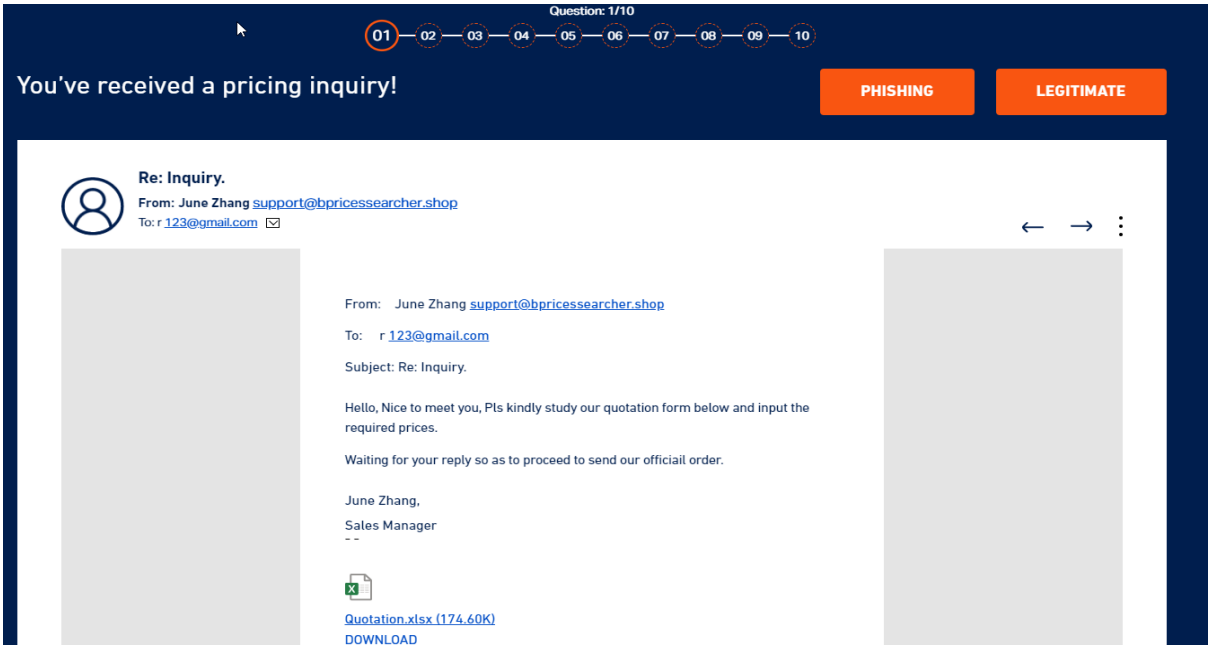

Figure 6 – Sonicwall quiz, (sonicwall, n.d.).

Phishingtackle.com: This quiz stood out as it is a mixture of the formats of the other quizzes above, its mixes scenario images of emails with general phishing questions testing the user on both the knowledge of spotting a phishing email and general phishing. While this site is probably one of the best in that it combines various methods of questions, it still has its flaws. One major one being some of the images used for the scenario questions are too small making it extremely difficult to actually figure out if it is legitimate or phishing, (phishingtackle, 2023).

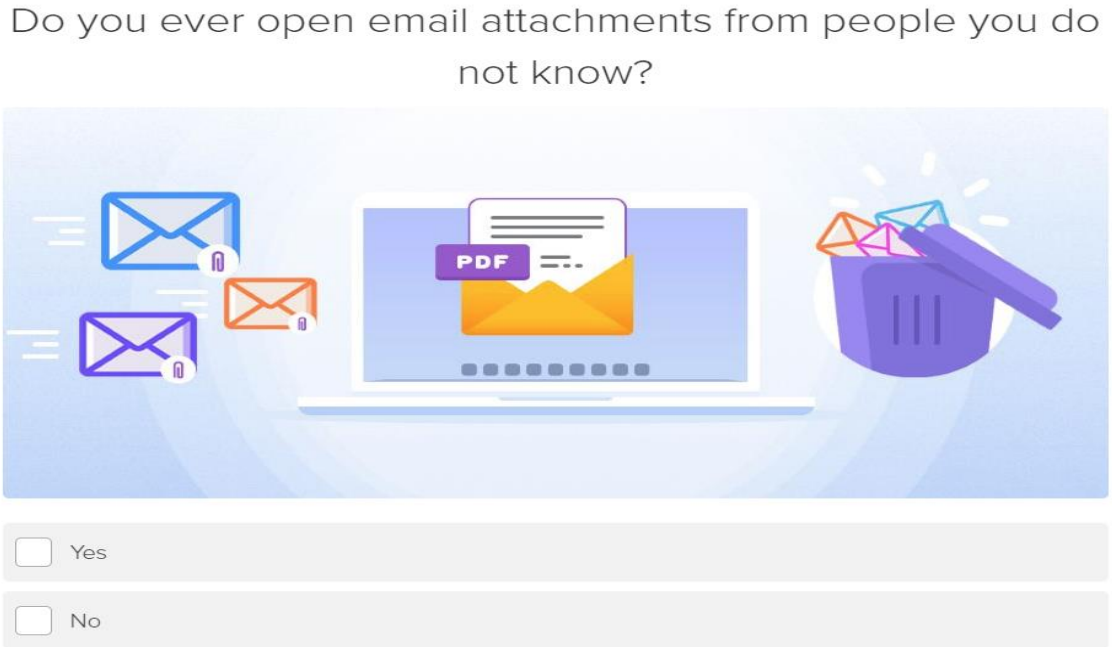

Figure 7 – phishingtackle quiz, (phishingtackle, 2023).

With the exception of the final quiz, all of the above quizzes along with others online follow very similar patterns sometimes slightly tweaking their structure like the ftc quiz being scenario based but not having images, with some even using the same images and scenarios.

These quizzes achieve the goal of asking questions based on phishing but feel very one dimensional, they all mostly concentrate on how to spot a phishing email. Very little is covered if anything at all of other aspects of phishing like smishing or vishing until finding the final quiz on phishingtackle.com, although it doesn't cover these topics it at least ventures away from only asking if something is legitimate or a phish.

2.3.3 Summary

The websites and quizzes all have their pros and cons. While some have unique parts to their structure like the TechTarget website having more in-depth information on various phishing techniques that the others don't, or the phishingtackle quiz being a mix of various phishing aspects. One thing that stands out, which this project will address is the lack of language or structure that is aimed at older adults, this project will also help to bring all the various aspects and parts that these websites and quizzes do well together, essentially pulling all the best parts to make a one stop shop that an older adult user can visit and learn everything they need to in one location.

3. User Group

3.1. Older Adults and Phishing

Senior citizens specifically 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).

These scams have increased drastically since Covid with many businesses having to go digital due to lock downs. Over the last two years since Covid with everyone having to socially distance themselves there was an emergence of newer and more sophisticated scams mainly involving contact tracing and signing up for vaccinations.

The scams weren't limited to the older generation but due to social distancing senior citizens would not have had the awareness to question these scams especially when these messages were health related. The scams themselves would ask for a person's information including but not limited to name, address and PPS (social security number) (Gardainfo, n.d.).

In China where there was an increase in covid related health issues more advanced scams would claim to have stock of the much-coveted Paxlovid (covid treatment drug created by Pfizer). People would sign up for a chance at getting their hands on the treatment and would pay these scammers up front, (Yang, 2023).

There are many ways in which we can help the older generation when it comes to protecting them and their assets from scammers. The main way to avoid these is creating awareness and ensuring they know the several ways (email, phone calls, text messages) that scammers use to target them, (Flynn, 2023). In Ireland at the moment three out of every ten adults are currently not using the internet in any capacity. Out of the rest of the adults who do use the internet they actually do not have the most basic skills required to use the internet in a safe manner. It has been found that at least 62% of adults over the age of 60 are digitally excluded. Charities such as Age Action Ireland have courses set up specifically for the older generation to teach them how to use computers and smart phones properly and in a safe manner. Over 45000 people have availed of these courses since their launch. Each learner is set up with a volunteer tutor over five weeks and they are shown the basics from online shopping to setting up their online banking, (ageaction, n.d.).

4. Tech Usage

4.1. Smartphones

Phishing awareness for all ages is more important than ever with the growth in the amount of smartphone users increasing year on year over the last 5 years by at least 5%, along with roughly 6.84 billion smartphones worldwide accounting for roughly 85% of the global population, which rises to around 10 billion if we include people owning more than one smartphone, (Howarth, 2023).

In 2016 there were around 3.67 smartphone users, this shows an increase by at least 300 million a year. From 2016 to 2021 the number has risen by 73.88%.

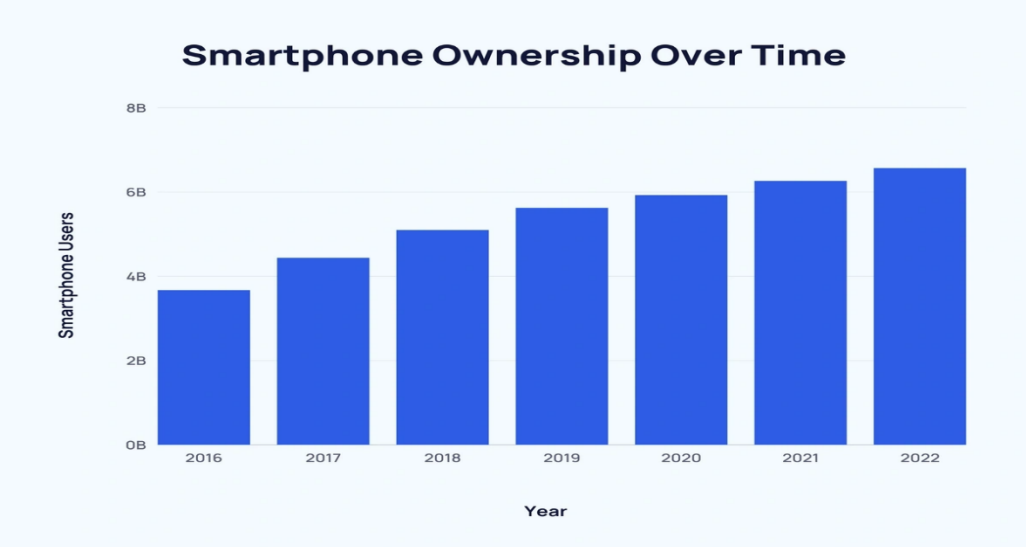

Figure 8 – smartphone owners by year, (Howarth, 2023).

It is predicted the growth of the number of smartphone owners will continue to grow over the next 5 years, with the expected amount to exceed 7 billion in the next 2 years.

Year	Number of Smartphones	Number of Mobile Devices	Proportion of Smartphones
2021	6.37 billion	14.91 billion	42.7%
2022	6.57 billion*	15.96 billion*	41.17%
2023	6.84 billion*	16.8 billion*	40.71%
2024	7.07 billion*	17.72 billion*	39.9%
2025	7.30 billion*	18.22 billion*	40.07%%
2026	7.51 billion*	-	-
2027	7.69 billion*	-	-

Figure 9 – Smartphone owners growth, (Howarth, 2023).

This is backed up with the number of smartphones that are worldwide in general and the predicted amount to also increase for this, (Laricchia, 2023).

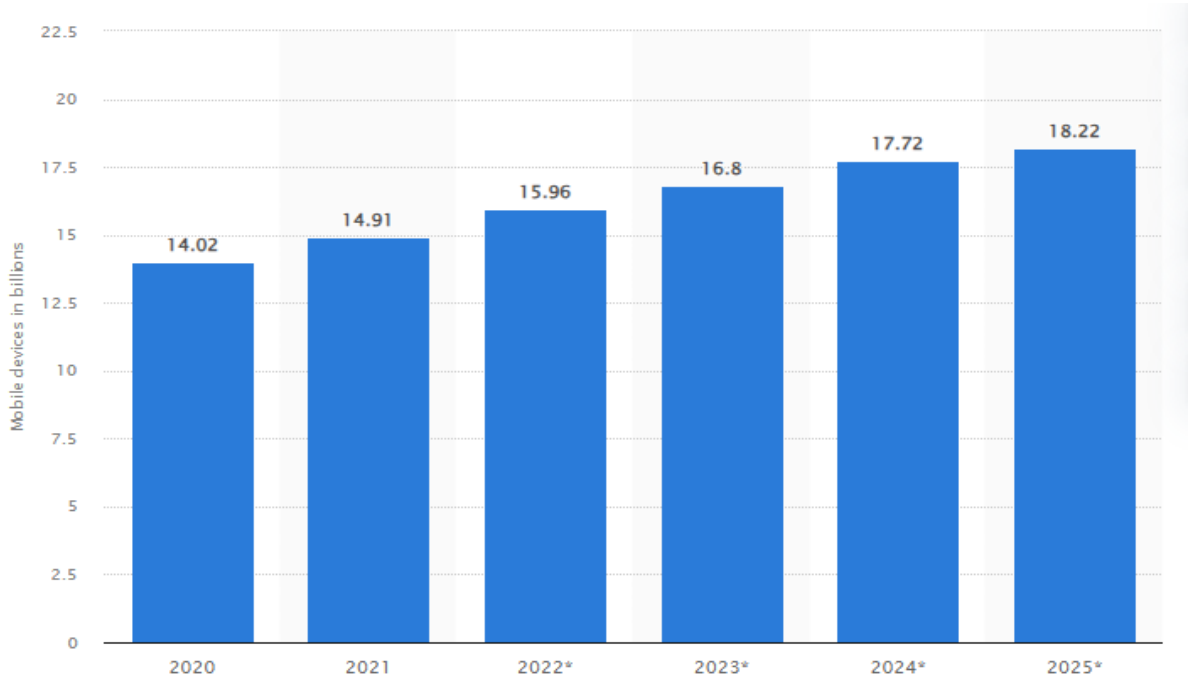

Figure 10 – Number of smartphones worldwide, (Laricchia, 2023).

Pew Research Center have done a study on smartphone, internet and social media use, in their study after conducting surveys across 18 countries they came to results that further back up the points made above in regards to steady increase in smartphone owners/user. The image below shows the results of the 18 countries combined in percentage.

Figure 11 – Median of smartphone owners, (Anderson, 2017).

Also, as part of this research Pew were able to show the increase in smartphone ownership amongst older adults, countries 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).

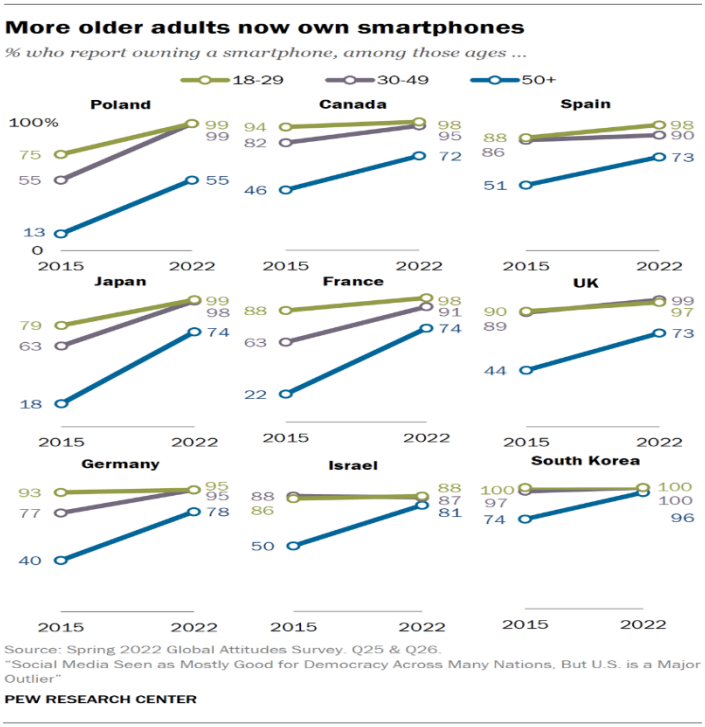

Figure 12 – Smartphone owners by country, (Anderson, 2017).

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).

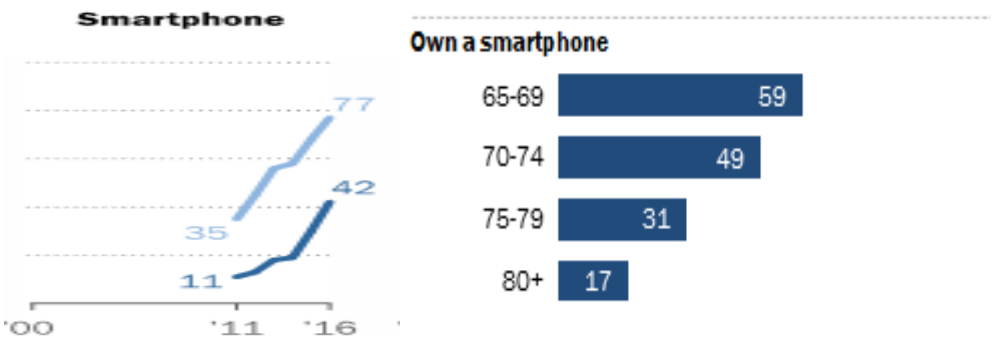

Figure 13 – Smartphone owners, (Anderson, 2017).

4.2. Other Tech

Just like with smartphones the use of other tech or online amenities has risen over the last decade, for example the use of internet. In early 2000 the Pew Research Center started tracking internet adoption, which at that point was only 14% of older adults but now it is up to 67% of older adults going online in some capacity, (Anderson, 2017).

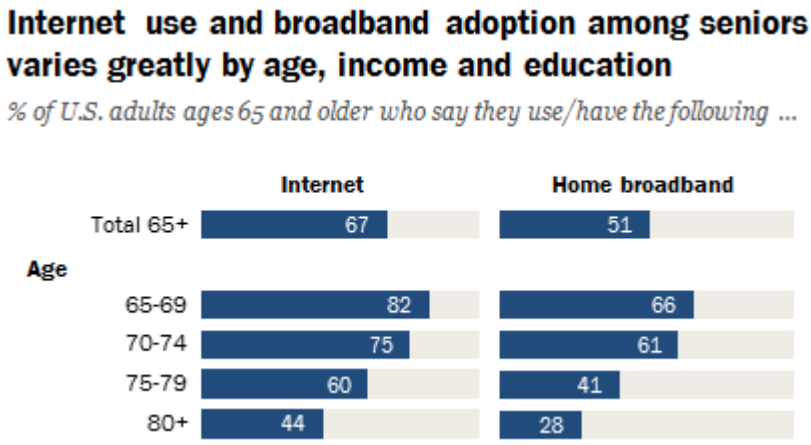

Figure 14 –

Along with this there has been an increase seen in the use of tablet devices among older adults, as part of the same study it was found that around 32% of older adults own a tablet device, (Anderson, 2017).

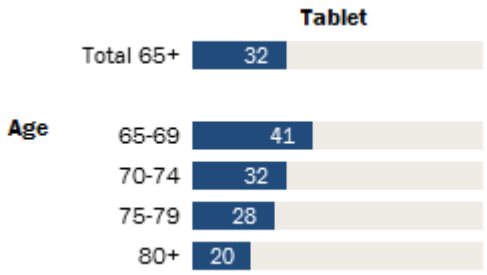

Figure 15 – Tablet use older adults, (Anderson & Perrin, 2017).

The Pew Research Center continued their research into older adults and tech by tackling social media and their use of it. With the rise in popularity of social media

especially for finding news and information along with connecting with family and friends, this rise within older adults can also be seen. A total of 34% aged 65 and over have stated they use social media in some capacity, this shows a 7% increase from when it was 27% back in 2013, (Anderson & Perrin, 2017).

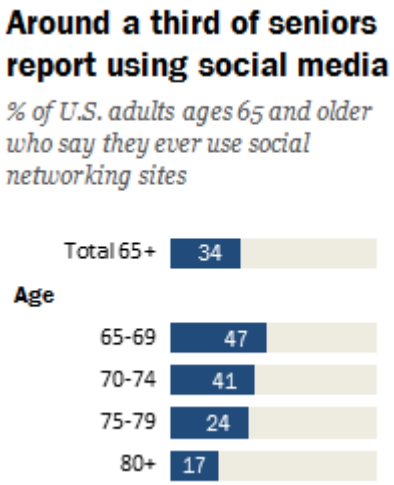

Figure 16 – Social Media use older adults, (Anderson & Perrin, 2017).

Once the older adults have gotten online this study shows that most of them have adopted internet use into their lives as part of their daily routine. Around three quarters of older adults are going online daily which was further broken down into showing that 17% will go online at least once a day, 51% going on several times a day and 8% stating they use it constantly.

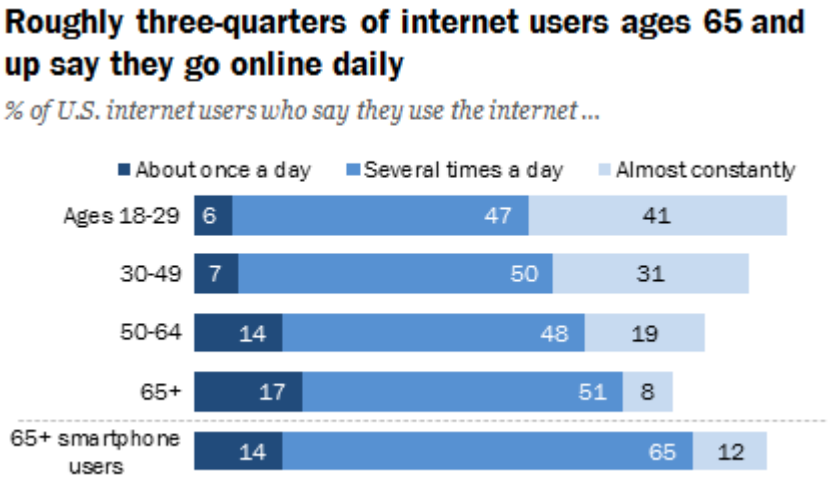

Figure 17 – Older adults percentage of internet use, (Anderson & Perrin, 2017).

4.3. Summary

With the above research along with the information provide earlier in this document about older adults being targeted with phishing, it shows that this project has a place to be valuable to the target user group. As shown the rise in usage of not just smartphones and tablets but the internet and online use as a whole showcases a need for this group to be helped with protecting themselves.

Yes, the above study showed that older adults are increasingly using tech and the internet but just because an older adult is using or adopting the use of these technologies, it does not necessarily mean they understand how to work it or what the dangers are.

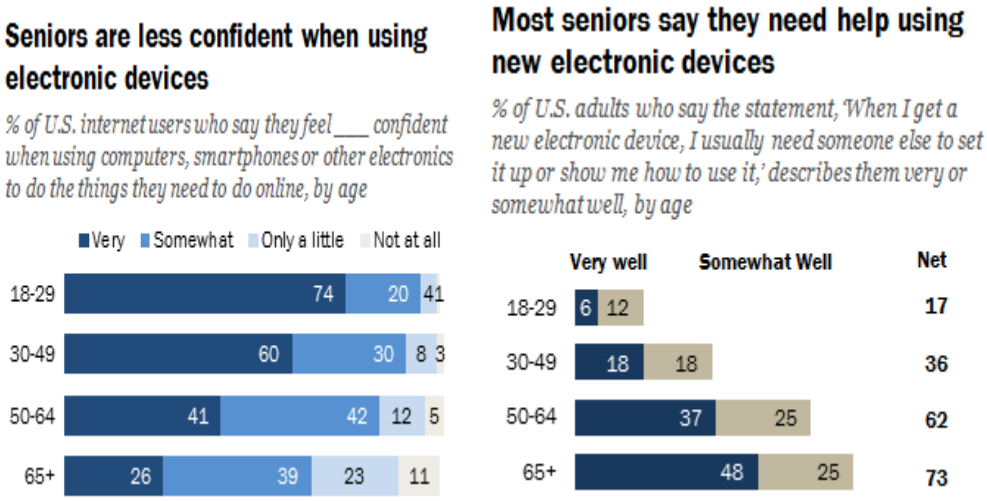

Figure 18 – Older Adults help with tech, (Anderson & Perrin, 2017).

This project will help them to at the very least protect themselves when it comes to some the dangers that comes with their adoption of these technologies like using their mobile phone, general online use or email use. This will be achieved with the learning of text message scams, website/web search scams and phishing emails.

5. Tools and Technologies

5.1. Languages

5.1.1. HTML

HTML is the language that is used to create most websites, it is what allows for webpage's to be created and function. It was first created in 1989 by Tim Berners-Lee, Robert Cailliau along with others, the meaning of HTML is Hyper Text Markup Language with hypertext meaning a document contains links allowing the reader to jump to other places within the document or even a completely different document. Markup Language allows computers to speak to each other to control the way in which text is processed and displayed, HTML achieves this by using tags and attributes, (Moraes, 2020).

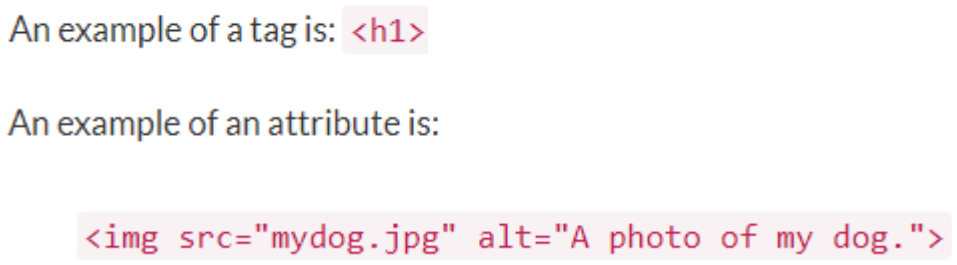

Figure 19 – Example of HTML Tags, (Moraes, 2020).

The basic structure of HTML code uses these along with a head section and a body section. The head section houses the information about the webpage like its title or any linked stylesheets, this does not appear on the webpage but is used for presentation. The body section is where the content goes that appears on the webpage like text, images, links etc, (ellow, 2023).

An Example of basic structure:

```
<!DOCTYPE html>
<html>
<head>
<title>My First Web Page</title>
</head>
<body>
<h1>Welcome to My Page</h1>
<p>This is a simple example of HTML. </p>
</body>
</html>
```

Figure 20 – HTML full example, (ellow, 2023).

5.1.2. JavaScript

JavaScript is a scripting language that is used to create websites and control the content within that website, basically anything that moves or changes on the website like animated graphics or forms. Websites like Facebook (Meta) use JavaScript to make it so the timeline on the main page when signed in updates automatically.A website will be created with the use of HTML and CSS with JavaScript then being implemented to make the website dynamic. It can be added directly to a webpages code with the use of the <script> tags in a similar way to how CSS is used, (Morris, 2023).

```
<!DOCTYPE html>
<html>
<body>

<h2>Demo JavaScript in Body</h2>

<p id="demo">A Paragraph.</p>

<button type="button" onclick="myFunction()">Try it</button>

<script>
function myFunction() {
  document.getElementById("demo").innerHTML = "Paragraph changed.";
}
</script>

</body>
</html>
```

Figure 21 – JavaScript Code, (Morris, 2023).

5.1.3. PHP

PHP is an open-source server-side programming language, it is used in website creation as it can be embedded into HTML. Its functionality with HTML helps to simplify HTML code. As PHP is a server-side language it does all its work on the server itself, with the only thing needed on the client side being a web browser. IT is used to connect to the database and have the information displayed back as a HTML page, (Simplilearn, 2023).

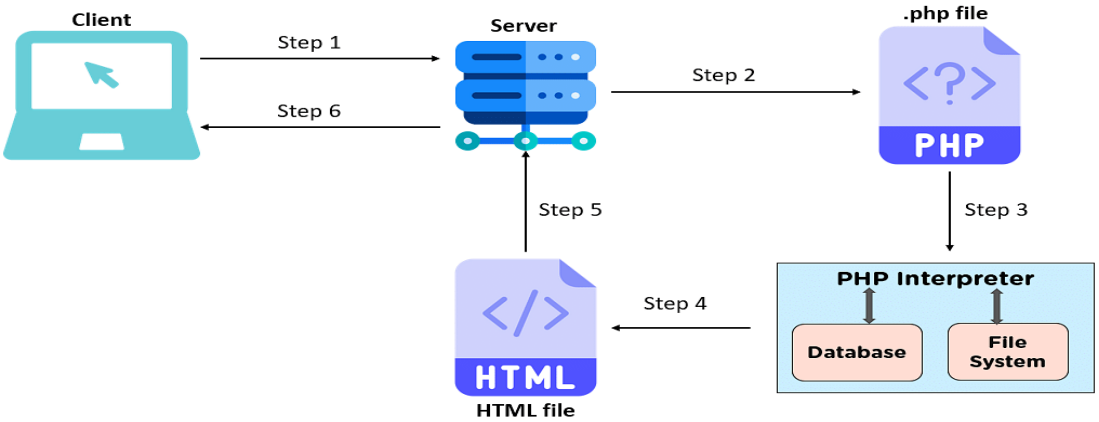

Figure 22 – PHP Data Flow, (Simplilearn, 2023).

5.1.4. CSS

Cascading Style Sheets (CSS) is what is used in the creation of websites to specify the style of the page, it controls the layout, colour and font within a webpage. CSS interacts with HTML using syntax, for example if the webpage contains an element that has a paragraph CSS can be used to make that paragraph appear in a specific colour and font style, or change the colour of the page or other elements, (Morris, 2023).

```
<style>
p {
  color: red;
  text-align: center;
}
</style>
</head>
<body>

<p>Hello World!</p>
<p>These paragraphs are styled with CSS.</p>
```

Hello World!

These paragraphs are styled with CSS.

Figure 23 – CSS Example, (Morris, 2023).

CSS can be used in two different ways, it can be done external where a separate stylesheet is created with all the CSS done within and then that sheet is linked to the HTML file by placing a header section with a link in it, (Morris, 2023).

```
<head>
<link rel=”stylesheet”  type=”text/css”  href=mysitestyle.css”>
</head>
```

Figure 24 – External CSS, (Morris, 2023).

The other way is don internally within the HTML file, this is done by placing the CSS code within the header of the file. If only a single page is needing a specific look internal CSS is useful, (Morris, 2023).

```
<head>
<style>
body {  background-color: thistle;  }
p {  font-size:20px;  color: mediumblue;  }
</style>
</head>
```

Figure 25 – Internal CSS, (Morris, 2023).

5.1.5. Python

Python is a programming language used for creating scripts to automate tasks, for data analysis and is used for creating websites. It is versatile as it is a general-purpose language, it can create a multitude of different programs. The versatility of it and it being beginner friendly have made it one of the most used programming languages today, (coursera, n.d.).

Automation/Scripting: Python is used to make scripts for automating tasks, it can be used for tasks such as error checking, simple math execution or removing duplicate within data. It is helpful to beginners also by being used to make scripts for simple tasks like renaming files or sending emails, (coursera, n.d.).

Web Development: Python is used in web development for creating the back end of the website which is the parts the user doesn’t see., such as communicating with servers and ensuring security. It offers frameworks for web development such as Flask and Django, (coursera, n.d.).

```python
# Python program to find the SHA-1 message digest of a file

# importing the hashlib module
import hashlib

def hash_file(filename):
   """This function returns the SHA-1 hash
   of the file passed into it"""

   # make a hash object
   h = hashlib.sha1()

   # open file for reading in binary mode
   with open(filename,'rb') as file:

       # loop till the end of the file
       chunk = 0
       while chunk != b'':
           # read only 1024 bytes at a time
           chunk = file.read(1024)
           h.update(chunk)

   # return the hex representation of digest
   return h.hexdigest()

message = hash_file("track1.mp3")
print(message)
```

Figure 26 – Python Code, (coursera, n.d.).

5.1.6. Swift

Swift is a programming language that was initially created for iOS development but now is being used to write code for Window and Linux. It is open source and was created by Apple with the intention to be a replacement for all C based languages. It is known for being safe, fast and easy to use but can be restrictive for some programmers.

It was only created in 2014 and released in 2015 but since has gone on to now be the 20th most used language in the world, while also being the 14th most popular among programmers, (Coursera, n.d.).

5.1.7. C#

C# is a programming language which was designed for windows, it is a general-purpose high-level programming language that can support multiple paradigms. This makes it able to be used to perform a wide range of tasks.

The main function of C# is to create applications for Windows, but it can also be used for web development more specifically sever-side, which is how users interact with the servers to get information. It is often used to create dynamic and professional looking websites, with it being an object-oriented language it can create sites that are efficient and easy to maintain, (blacklightsoftware, 2023).

```
C#

using System;

class Hello
{
    static void Main()
    {
        // This line prints "Hello, World"
        Console.WriteLine("Hello, World");
    }
}
```

Figure 27 – C# Code, (blacklightsoftware, 2023).

5.1.8. Perl

Perl is a high-level programming language used for developing websites and other applications. It was created in 1987 by Larry Page so is an older open-source language, with it being very close to C in terms of syntax used.

More that 101,449 websites use Perl with it being the 10th most popular language being used. It is easier to pick up and use than languages like C and C++. It was once a primary language being used but now not as widely used, it is still preferred by some because of things like it borrows from other languages and Unix and other systems can make use of the Perl interpreter as it can be integrated into databases and web servers, (Tuama, 2022).

5.1.9. Ruby

Ruby is an object-oriented programming language which focuses on productivity and simplicity, it can be used in various areas of computer science including web development and data analysis. Ruby is considered to be more user friendly that languages like Java or C as it has an English like syntax, because of this someone who has never written code could might be able to understand what a basic program wrote in Ruby does.

One of the reasons that makes Ruby such a popular programming language is due to the Ruby on Rails framework that is used for web development. The Rails frame work comes with everything a developer needs to build a scalable website, (builtin, n.d.).

5.2. Tools

5.2.1. XAMPP

XAMPP is an open-source web solutions kit that provides Apache delivery for a variety of servers along with MariaDB, PHP and Perl, its name is an acronym for all of these. With XAMPP you can validate a website on a computer through a local host or server.

Essentially it houses multiple tools in one location for web development with Apache server, MySQL database, PHP and Perl languages. It also comes equipped with the web-based utility phpMyAdmin for working on MySQL databases easily, (Nagendrag, 2023).

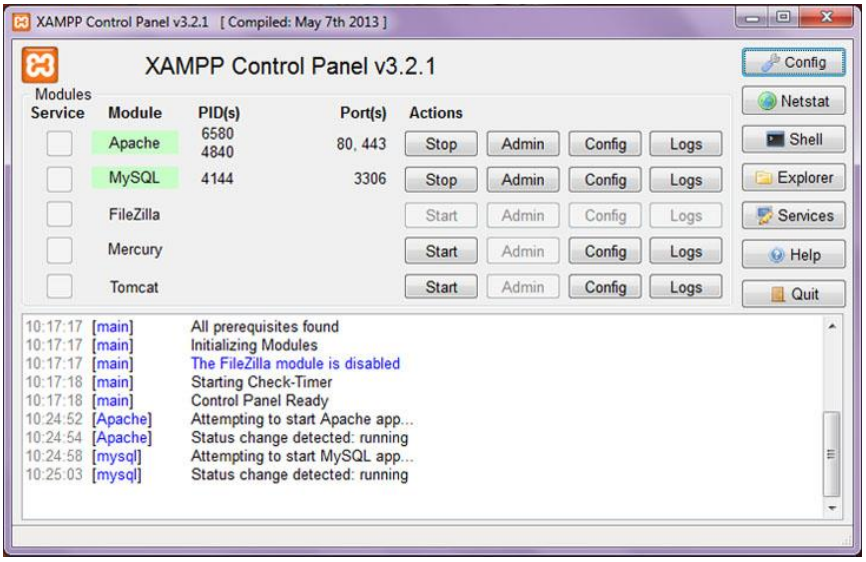

Figure 28 – XAMPP, (geeksforgeeks, 2022)

5.2.2. Ruby on Rails

Ruby on Rails which is also referred to as just Rails is a full-stack frame work that is written in Ruby and available on most operating systems like Mac, Windows and Linux. It contains a rich toolkit with features covering both frontend and backend concerns.

With Rails being built on a set of predefined libraries and frameworks it allows beginners, and professionals to implement various functionalities like sending mail or reading data from an SQL database quickly, (builtin, n.d.).

5.2.3. Bootstrap

Bootstrap is an open-source web development framework, it is designed that aims to simplify the process of creating responsive, mobile-first websites. It achieves this by offering a set of syntax for designing templates.

Essentially Bootstrap allows developers to build websites faster because they don't need to worry about any basic commands and functions, it is designed to ensure all interface elements of a website work on screens of all sizes. It contains scripts based in HTML, CSS and JavaScript for several web design functions and components, (A., 2023).

5.2.4. Eclipse

Eclipse is a powerful and widely used integrated development environment (IDE) and is a free java-based development platform, it supports multiple languages like C++ and Java along with Python. It is known for its plugins that allow developers to test and develop code written in other languages. Eclipse can be used as an IDE for any programming language for which a plug-in is available, (Hanna, 2021).

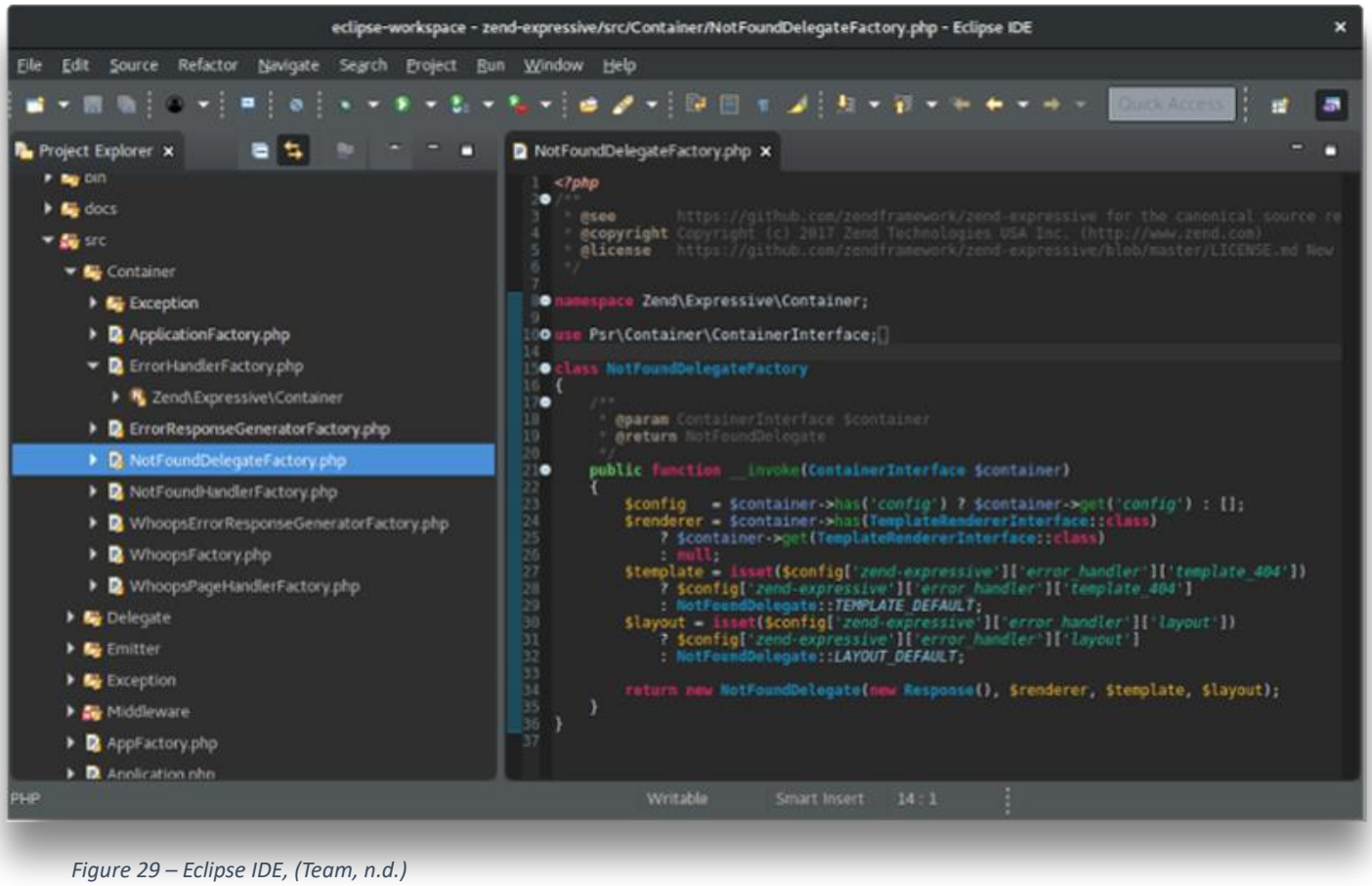

Figure 29 – Eclipse IDE, (Team, n.d.)

5.2.5. Visual Studio Code

Visual Studio Code is a lightweight but powerful source code editor that is free, it runs on your desktop or is available on the web. It has built in support for JavaScript, TypeScript and Node.js with a multitude of extensions for other programming languages like C#, Java, Python and PHP along with environments such as Docker and Kubernetes, (Heller, 2022).

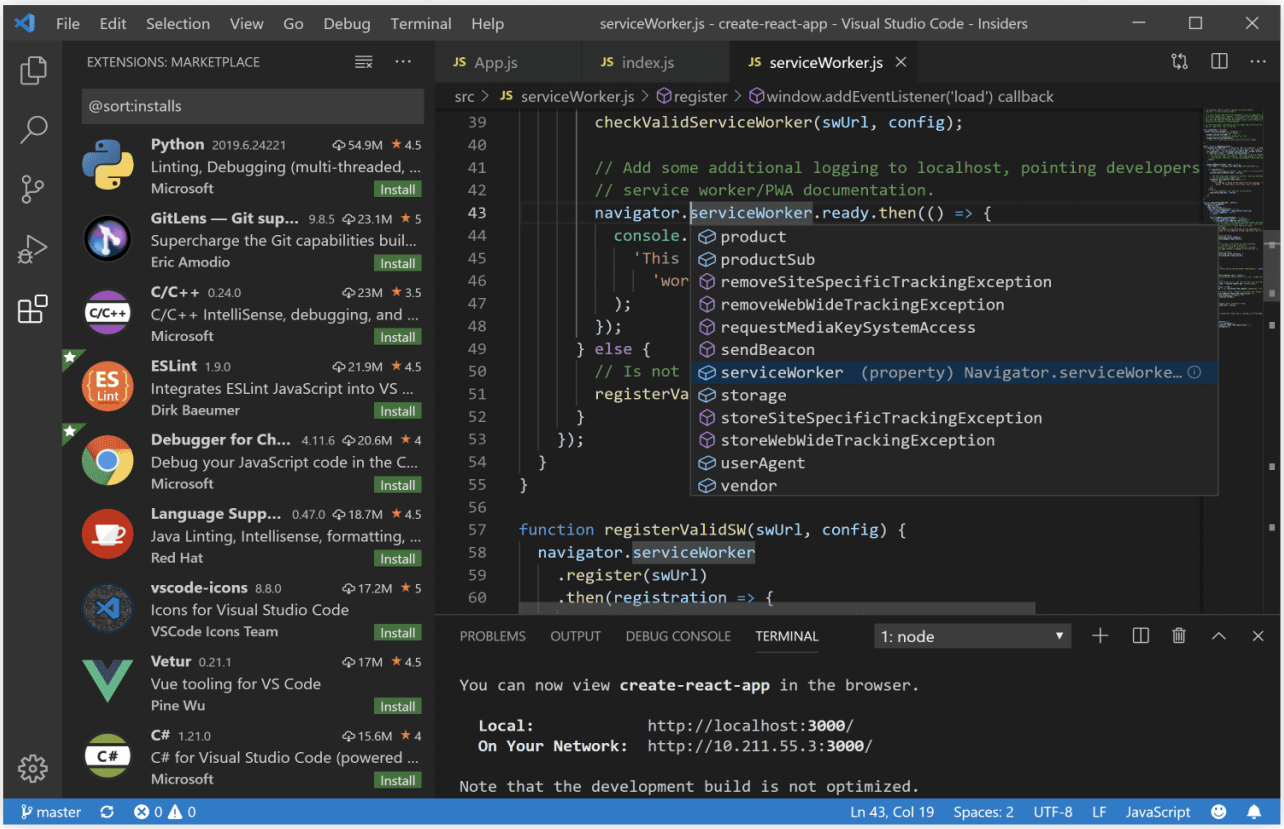

Figure 30 – Visual Studio Code, (academy, n.d.)

5.2.6. Kubernetes

Kubernetes which is also referred to as K8s is a portable, extensible, open-source platform for managing containerized workloads and services across a cluster of networked resources, it can be used with or without docker. Kubernetes was created by Google an they state that its “main design goal is to make it easy to deploy and manage complex distributed systems, while still benefiting from the improved utilization that containers enable”.

It bundles together a set of containers which are managed on the same machine, this helps to reduce network overhead and increase resource usage efficiency, with an example of a container set being an app server and SQL database, (Atlassian, n.d.).

5.2.7. Docker

Docker is an open platform for developing, shipping and running applications, it enables you to separate applications from infrastructure to deliver software quickly. It can significantly reduce the delay between writing code and running it in production. Docker helps developers build deploy and run containers, containers can be built without Docker but is made is made easier by the platform. If there is a ned to run or manage containers in a large-scale Docker alone will find it challenging but it can be combined with Kubernetes to solve this problem, (Atlassian, n.d.).

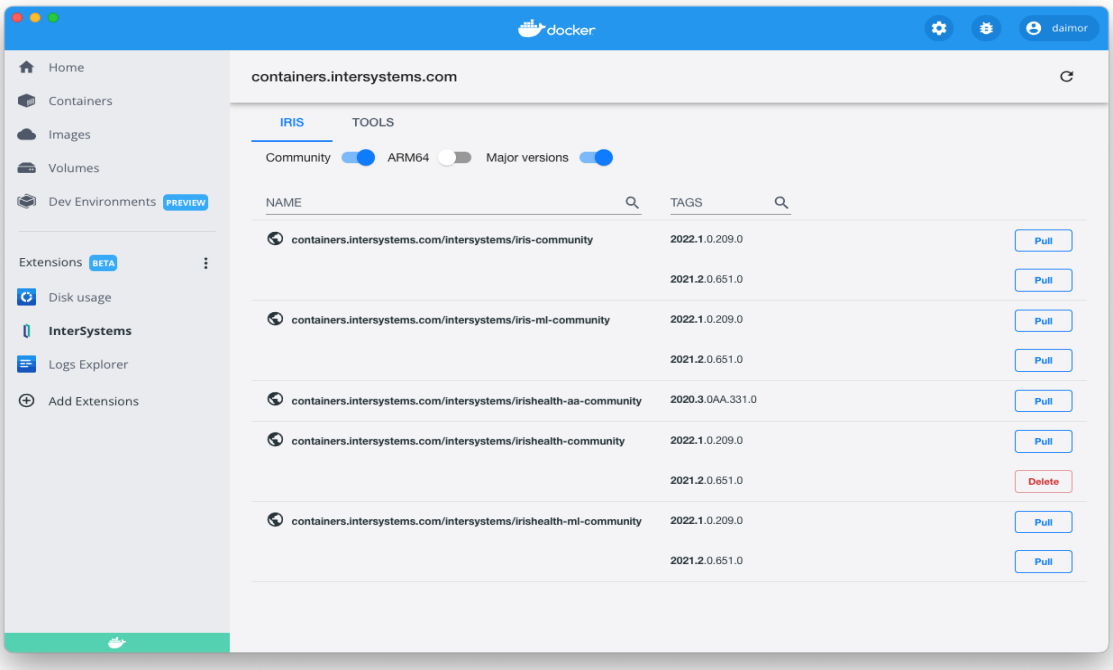

Figure 31 – Docker, (Maslennikov, n.d.)

5.2.8. SurveyMonkey

SurveyMonkey is a cloud-based tool that helps users to create, send and analyse surveys. Surveys can be emailed to intended survey users or post them on a website/social media page to increase the response rate. This tool allows users to send surveys and check their results from a mobile device. This tool helps to reduce data bias by implementing question, page, block and order randomisation, in addition it provides multiple question types like video, ranking or slider. One of the main drawbacks of this tool is a lot of the features are locked behind a paywall, with a pricing of $12.22 a month for the standard tool, (softwareadvice, n.d.).

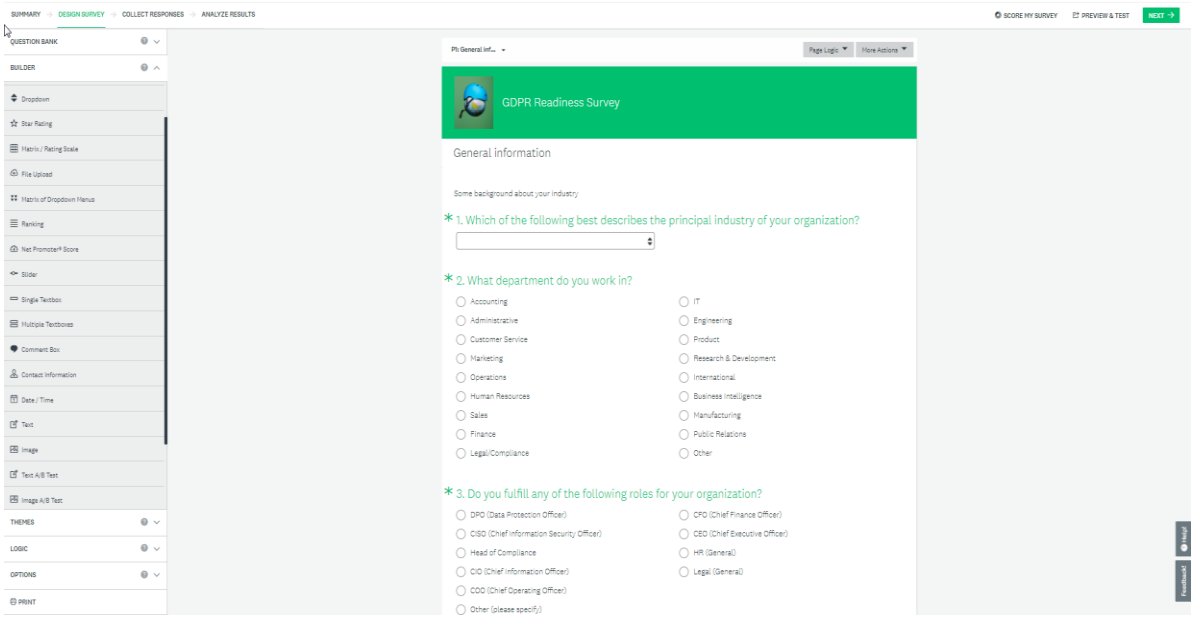

Figure 32 – SurveyMonkey, (softwareadvice, n.d.)

5.2.9. Microsoft Forms

Microsoft Forms is an online survey/questionnaire creator which was created by Microsoft in 2016. It is part of the Office 365 product line and accessible to anyone with a Microsoft account with extra features for owners of Office 365, it comes with user friendly tools allowing users to easily create quizzes, surveys, profile forms, feedback forms and more. Surveys and quizzes created can be shared with anyone and can be integrated with Excel and OneDrive, this allows for the results to appear in an Excel spreadsheet in real-time, (Dublin, n.d.).

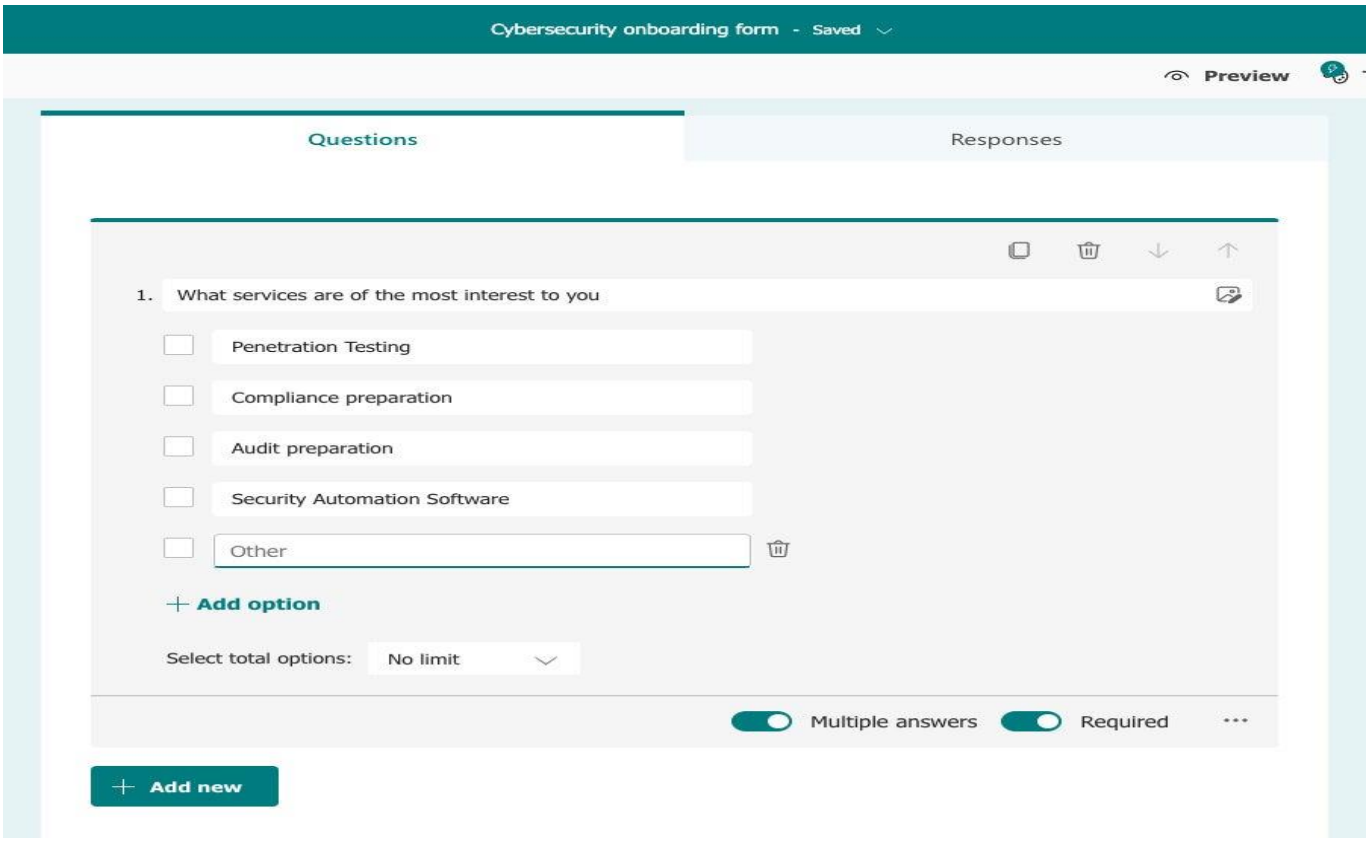

Figure 33 – Microsoft Forms, (Brathwaite, 2023)

5.2.10. phpMyAdmin

phpMyAdmin is an open source and free website software package, it is written in PHP and handles the administration of a database in a web browser. It allows users to manage databases, tables, permissions etc with a user interface that allows any SQL statement to be executed directly, (dreamhost, n.d.).

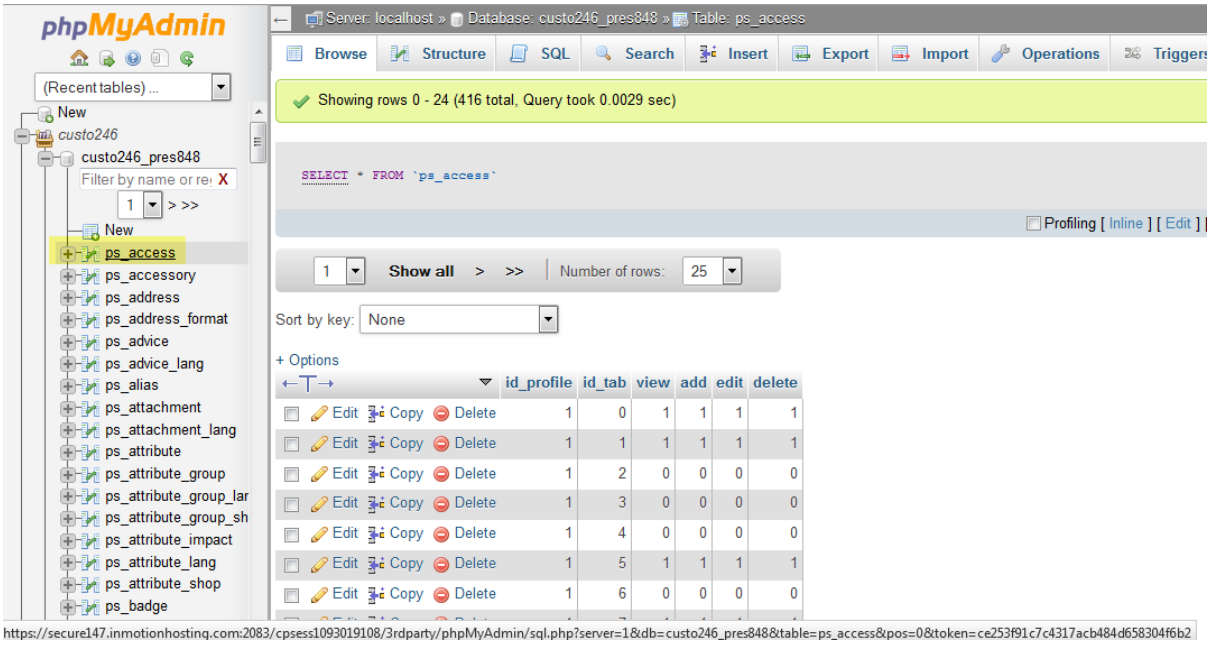

Figure 33 – Microsoft Forms, (Custodio, 2021)

5.2.11. dbForge Studio

dbForge Studio is a multi-functional General User Interface (GUI) for MySQL, it was developed to handle and perform most tasks on database development and management. It has more functionality that phpMyAdmin but unlike phpMyAdmin is not web based, adding to the differences between the 2 phpMyAdmin is free to use where dbForge requires payment.

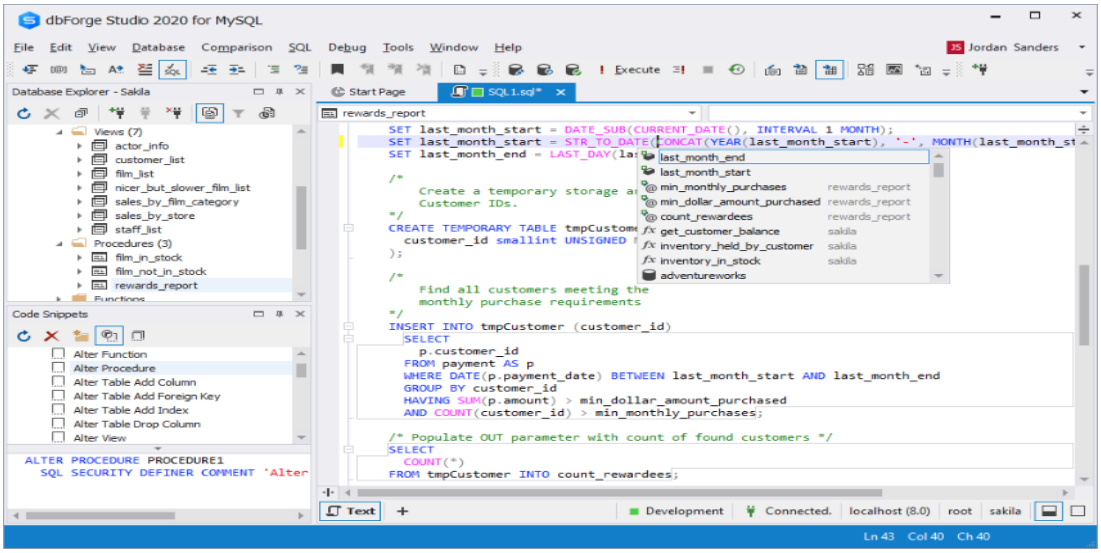

Figure 33 – dbForge, (Team, 2023)

5.3. Summary

With having researched various possible programming languages and tools to help with developing a website or application, there are an abundance of choices when it comes to programming languages and each have their pros and cons.

As part of this project my intention is to distribute various surveys to older adults before any interaction with the website in this project to test their phishing knowledge and get some baseline data. Another survey I plan to distribute is after the website has been used/tested for feedback on any possible improvements or changes. These surveys will be created in Microsoft Forms, the decision to go with Microsoft Forms over SurveyMonkey was a simple one for me as Microsoft Forms offers more options for free than SurveyMonkey, SurveyMonkey requires a monthly fee to access more features.

For the coding aspect of this project my initial intentions were to learn Python and use that for the coding within this project, but with time being tight already so far this year I have decided to stick to what I have used before and learned in college. So, for this project I will be coding with HTML, PHP and JavaScript, I have created small sites throughout the first few years of this course so will look to use that knowledge and expand on it to make the website for the project the best I can. I intend to still learn Python when I can and see if it may be usable or there is enough time to implement it in this project.

Having used and gone over two IDEs above in Eclipse and Visual Studio Code, both are adequate for the task of coding my website and offer various plugins to help the project. For this project I will be using Eclipse as I have more experience with the plugins for web development and have linked it to other applications before so will only require a bit of a refresher to achieve it rather than learn fresh.

Other tools intended to be used for this project from the research conducted above are XAMPP which will be used to host and test the website along with the database as it has the Apache server and phpMyAdmin connection built in, it was also used for a previous project so having some experience with using it again means just a quick refresher will be needed. Docker is another tool that may be used as part of this project, for a previous project I had to use Docker as issues arose with my database but I intend to begin without it with my database being done through phpMyAdmin, although forgeDB has better functionality I have experience with phpMyAdmin and it is free to use.

6. Surveys

6.1. What is a survey?

A survey can come in many different types with the most common being written, online or as a questionnaire. It is at its core a way to gather information with the use of questions from groups or individuals, they help to provide data and valuable insights allowing for informed decisions or to draw conclusions. One of the key aspects of a successful survey is to ask question that are unbiased, clear and concise, avoiding questions that could lead or influence the answers given, (qualtrics, 2022).

"Surveys are a powerful tool for data collection, enabling us to collect valuable data quickly and efficiently. By understanding the purpose and process of surveys, we can gather accurate and meaningful data that can inform our decisions and lead to successful outcomes.", (Bhat, 2023).

With it now being more common to do an online survey as they can be sent via social media, emails or URLs, it has become the more natural way to conduct a survey. The functionality online surveys bring make it less time consuming than doing one to one interaction.

6.2. What makes a good survey

If a survey is done well, it provides good and accurate responses, which is what you are looking for to make sure your data from them is useful and more importantly reliable. With avoiding some common mistakes and making sure your survey follows certain step will help to achieve this.

Give Purpose: People that you are asking to take your survey will be more likely to do so if there is value to be seen in them. You want to explain the purpose or reason for the survey straight away at the beginning, when you explain the value and make it specific to the user group taking it you will get a better response rate, (qualtrics, 2022).

Speak Their Language: When writing the questions for your survey a good rule to follow is make them written in a way that is easy to understand, use clear and concise language making it easy to understand what is being asked. Make sure to avoid technical jargon as this can create survey bias as not everyone taking the survey will understand it, which in turn will skew the data you end up with, (qualtrics, 2022).

Keep it Simple: A good approach when creating questions for your survey is to keep the questions short, simple and direct. With increasing the length of questions and increasing how many questions are in the survey, you run the risk of people getting bored or frustrated while taking it, this can then lead to not receiving a completed survey, (qualtrics, 2022).

Use Funnel Technique: The funnel technique refers to the way in which the questions in a survey are setup or arranged, it is putting them in the best sequence order to engage people. The structure of this technique is to start with broad and easy to answer questions, then place the harder questions that may take time to think about what answer to give in the middle, finally finish with easier to answer questions to end the survey, (qualtrics, 2022).

6.3. Online Survey advantages

Online survey tools help to make this the most popular way of conducting surveys, with online surveys there comes benefits with choosing to do your survey online, such as:

Faster Responses: With traditional surveys you are using paper and sending out the surveys which means you then have to wait for those to come back, with online surveys answers can be received instantly as the survey is completed and stored in a database to be analysed. It is more likely a person being surveyed online will respond faster as it will be just a few clicks to complete it, (qualtrics, 2022).

Cheaper: Online surveys are cheaper in both money and time, it saves money as you do not have to print and post with it being hosted online. Time is saved as you do not have to manually enter responses that were filled in on paper or don't have to go around handing out surveys, (qualtrics, 2022).

Accuracy: With online surveys the margin of error is lower, this is from users taking the survey only having to click buttons or select answers with a click. According to a study conducted, as traditional methods of survey taking require human interference, this increases the margin of error by 10%, (Bhat, 2023).

Quick to Analyse: With online surveys the responses are registered online, this makes analysing them straightforward and speed up the process, (Bhat, 2023).

Easier for Participants: As discussed previously in this report, with the increase in use of technology and access to the internet survey user prefer receiving it over email. This is because it increases the ease at which they can access and take the survey, it allows them to choose a time and place that suits them to take the survey, (Bhat, 2023).

6.4. Qualitative vs Quantitative

Qualitative and quantitative research methods is what is used to gain a complete understanding of the target user groups needs, wants etc. But it will depend on the needs and goals of your research if you use either or both of these methods.

Quantitative research is all about gathering information which can be expressed numerically, it is often used for data in regards to specific demographics while being conducted through the use of surveys or web analytics. Usually, it will include a large amount of people to ensure statistical representation, but it can still be targeted for a specific group which is usually determined by age, gender or location.

Qualitative research focuses more on behaviours and habits or motivations behind people's decisions. The information in this research is gotten through inquiries or interviews, this is to learn about feelings, habits and attitudes which are harder to quantify but still offer valuable context to support the statistical data.

Combining both of these methods of research leads to gaining a complete set of data about a target groups demographics, behaviours, needs and more, (Ally, 2020).

7. Security Implications

With regards to Cybersecurity, this project will address a few areas and implications for cybersecurity, those being:

Phishing prevention: This project will directly address the prevention of phishing attacks which is a prevalent cyber threat. As discussed above in this report, older adults are being targeted due to their vulnerability so educating them on phishing and how to prevent/avoid it will be a small step in trying to mitigate this type of cyber risk.

Social Engineering: As phishing often can involve social engineering tactics to trick individuals into giving out their personal or financial information, this will be addressed as part of this project which will help to build a defence against social engineering.

Other: With this project being an online training website, it opens the door to cybersecurity risks that come with having an active website online, especially with taking user information and storing it. This will be addressed with various security implementations like encrypting the user's information as it is sent to the database, so if there was a breach to the database the data is not in plain text for the attacker to see.

8. Conclusion

Having finished this research document it has helped to give a structure to this project, beginning with the different types of phishing and how they are implemented it gives insight into what from these attacks can affect older adults, allowing me to put a greater emphasis on providing a streamlined and beneficial learning structure for this user group, taking out certain aspects of phishing that do not factor into my user group like Whale Phishing.

Researching various learning platforms that this type of content is being delivered was extremely beneficial, it allowed me to see what was done well and what I felt was not done well in the form of websites and quizzes. The goal now is to take the aspects from these websites and quizzes that deliver information well and have a good structure and use them as a building block to create a learning platform that is for older adults.

The research for my user group gave valuable insist and provided reasoning for my decision to pursue this project. It showed just how vulnerable older adults are. Along with statistics backing up the rise in the use of all forms of technologies, which pushes the need for an accessible platform for older adults to learn about the various dangers and how to protect themselves, this project will provide that for them.

The final aspects of this project that have been decided upon after the conclusion of this research document are, how surveys will be created with the structure of a good survey having been researched along with methods of research and what is best for this project like quantitative. Finally, as discussed in the summary of the research, the tools and technologies that will be used to create this project were also decide after researching multiple possible choices. Ranging from what IDE to use like Eclipse to what survey tool to use like Microsoft Forms or languages to use like HTML, PHP, JavaScript all of which will be used in this project.

9. Bibliography

1. (No date a) Sonicwall.com. Available at: https://www.sonicwall.com/phishing-iq-test/ (Accessed: 29 November 2023).

2. (No date) Google. Available at: https://phishingquiz.withgoogle.com/ (Accessed: 29 November 2023).

3. (No date) PhpMyAdmin overview – dreamhost knowledge base. Available at: https://help.dreamhost.com/hc/en-us/articles/214395638-phpMyAdmin-overview (Accessed: 11 December 2023).

4. A., J. (2023) What is bootstrap?, Hostinger Tutorials. Available at: https://www.hostinger.com/tutorials/what-is-bootstrap/ (Accessed: 10 December 2023).

5. Ally (2020) Qualitative vs Quantitative Survey Questions: Pollfish, Pollfish Resources. Available at: https://resources.pollfish.com/market-research/the-difference-between-quantitative-and-qualitative-research/ (Accessed: 12 December 2023).

6. 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).

7. Anderson, M. (2017a) 1. technology use among seniors, Pew Research Center: Internet, Science & Tech. Available at: https://www.pewresearch.org/internet/2017/05/17/technology-use-among-seniors/ (Accessed: 10 December 2023).

8. Anderson, M. and Perrin, A. (2017) Technology use among seniors, Pew Research Center: Internet, Science & Tech. Available at: https://www.pewresearch.org/internet/2017/05/17/technology-use-among-seniors/ (Accessed: 10 December 2023).

9. Atlassian (no date) Kubernetes vs. Docker, Atlassian. Available at: https://www.atlassian.com/microservices/microservices-architecture/kubernetes-vs-docker#:~:text=While%20Docker%20is%20a%20container,CRI%20(Container%20Runtime%20Interface). (Accessed: 10 December 2023).

10. Bhat, A. (2023) Surveys: What they are, characteristics & examples, QuestionPro. Available at: https://www.questionpro.com/blog/surveys/ (Accessed: 12 December 2023).

11. Brathwaite, S. (2023) Microsoft forms cheat sheet: How to get started, Computerworld. Available at: https://www.computerworld.com/article/3687048/microsoft-forms-cheat-sheet-create-online-surveys-quizzes-forms.html (Accessed: 11 December 2023).

12. 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).

13. Custodio, A. (2021) How to export a table in phpmyadmin: Inmotion hosting, InMotion Hosting Support Center. Available at:

https://www.inmotionhosting.com/support/website/phpmyadmin-export-table/ (Accessed: 11 December 2023).

14. Dublin, T. (no date) Technology services, TU Dublin. Available at: https://www.tudublin.ie/connect/technology-services/guides/microsoft-forms/ (Accessed: 11 December 2023).

15. Email phishing, Vishing & other types of (no date) Webroot. Available at: https://www.webroot.com/ie/en/resources/tips-articles/what-is-phishing (Accessed: 12 November 2023).
16. Exploring the ins and outs of C# web development (2023) Blacklight Software. Available at: https://www.blacklightsoftware.com/blog/posts/2023/march/exploring-the-ins-and-outs-of-c-web-development/#:~:text=As%20an%20object%2Doriented%20language,easy%2Dto%2Duse%20nature. (Accessed: 10 December 2023).

17. Flynn, S. (2023) How to help protect seniors from scammers, MUO. Available at: https://www.makeuseof.com/how-to-help-protect-seniors-from-scammers/ (Accessed: 30 November 2023).

18. Frank and Frank Moraes is an editor and writer at HTML.com and other nerdy websites. (2020) Home, ". Available at: https://html.com/ (Accessed: 30 November 2023).

19. Gardainfo (no date) Public advice - covid scams warning - Monday 25th January 2021, Garda. Available at: https://www.garda.ie/en/about-us/our-departments/office-of-corporate-communications/press-releases/2021/january/public-advice-covid-scams-warning-monday-25th-january-2021.html (Accessed: 30 November 2023).

20. Getting started computer training (no date) Age Action. Available at: https://www.ageaction.ie/how-we-can-help/getting-started-computer-training#:~:text=Age%20Action's%20Getting%20Started%20is,for%20older%20people%20in%20Ireland. (Accessed: 30 November 2023).

21. Giandomenico, N. (February 28, 2023) What is spear-phishing? defining and differentiating spear-phishing from phishing, Digital Guardian. Available at: https://www.digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing#:~:text=A%20definition%20of%20spear%2Dphishing,victim%2C%20often%20for%20malicious%20reasons. (Accessed: 15 November 2023).
22. Gillis, A.S. (2023) What is phishing and how does it work?: Definition from TechTarget, Security. Available at: https://www.techtarget.com/searchsecurity/definition/phishing (Accessed: 29 November 2023).

23. 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).

24. Hanna, K.T. (2021) What is Eclipse and the foundation behind it?, App Architecture. Available at: https://www.techtarget.com/searchapparchitecture/definition/Eclipse-Eclipse-Foundation (Accessed: 10 December 2023).

25. 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: 10 December 2023).

26. How to install xampp on windows ? (2022) GeeksforGeeks. Available at: https://www.geeksforgeeks.org/how-to-install-xampp-on-windows/ (Accessed: 10 December 2023).

27. How to write good survey questions (2022) Qualtrics. Available at: https://www.qualtrics.com/uk/experience-management/research/survey-questions/ (Accessed: 12 December 2023).

28. Howarth, J. (2023) How many people own smartphones (2023-2028), Exploding Topics. Available at: https://explodingtopics.com/blog/smartphone-stats (Accessed: 06 December 2023).

29. Irwin, L. (2023) The 5 most common types of phishing attack, IT Governance Blog En. Available at: https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack (Accessed: 13 November 2023).

30. KnowBe4 (no date) What is phishing?, Phishing. Available at: https://www.phishing.org/what-is-phishing (Accessed: 29 November 2023).

31. Kumar, H., Prasad, A., Rane, N., Tamane, N. & Yeole, A., 2021. Dr. Phish: Phishing Website Detector. In: ICCSRE 2021. E3S Web of Conferences, 297, 01032. Available at: https://doi.org/10.1051/e3sconf/202129701032.

32. Laricchia, F. (2023) Number of mobile devices worldwide 2020-2025, Statista. Available at: https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/#:~:text=In%202021%2C%20the%20number%20of,devices%20compared%20to%202020%20levels. (Accessed: 29 November 2023).

33. Laricchia, F. (2023) Number of mobile devices worldwide 2020-2025, Statista. Available at: https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/#:~:text=In%202021%2C%20the%20number%20of,devices%20compared%20to%202020%20levels. (Accessed: 06 December 2023).

34. Mace, R.A., Mattos, M.K. and Vranceanu, A.-M. (2022) Older adults can use technology: Why Healthcare Professionals Must Overcome Ageism in Digital Health, Translational behavioral medicine. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9494377/#:~:text=Consumer%20technology%20is%20ubiquitous%20in,%2B)%20in%202021%20%5B1%5D. (Accessed: 22 November 2023).

35. Maslennikov, D. (no date) InterSystems extension for Docker Desktop, InterSystems Developer Community. Available at: https://community.intersystems.com/post/intersystems-extension-docker-desktop (Accessed: 10 December 2023).

36. Morris, S. (2023) What is JavaScript? A guide for total beginners, Skillcrush. Available at: https://skillcrush.com/blog/javascript/#add (Accessed: 10 December 2023).

37. Morris, S. (2023a) What is CSS, how does it work and what is it used for?, Skillcrush. Available at: https://skillcrush.com/blog/css/ (Accessed: 10 December 2023).

38. Nagendrag (2023) What is XAMPP? - cloudfoundation: Blog, CloudFoundation. Available at: https://cloudfoundation.com/blog/what-is-xampp/ (Accessed: 10 December 2023).

39. 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).

40. Phishing quiz (2023) Phishing Tackle. Available at: https://phishingtackle.com/phishing-quiz/ (Accessed: 29 November 2023).

41. Programming in swift: Benefits of this popular coding language (no date) Coursera. Available at: https://www.coursera.org/articles/programming-in-swift (Accessed: 10 December 2023).

42. Ritchie, J.N.& A. and Jones, N. (2021) Phishing quiz, Federal Trade Commission. Available at: https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/quiz/phishing (Accessed: 29 November 2023).

43. Shea, S. (2021) What is a whaling attack (whaling phishing)?, Security. Available at: https://www.techtarget.com/searchsecurity/definition/whaling (Accessed: 22 November 2023).

44. 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%20data%20to%20unauthorized%20entities. (Accessed: 22 November 2023).

45. Simplilearn (2023) What is PHP: The best guide to understand its concepts, Simplilearn.com. Available at: https://www.simplilearn.com/tutorials/php-tutorial/what-is-php (Accessed: 10 December 2023).

46. SurveyMonkey (no date) SurveyMonkey Software Reviews, Demo & Pricing - 2023. Available at: https://www.softwareadvice.com/customer-experience/surveymonkey-profile/ (Accessed: 11 December 2023).

47. Team, dbForge (2023) Best phpmyadmin alternative (overview with comparison), Devart Blog. Available at: https://blog.devart.com/phpmyadmin-alternative.html (Accessed: 11 December 2023).

48. Team, P. (no date) Eclipse PHP Development tools, The Eclipse Foundation. Available at: https://eclipse.dev/pdt/ (Accessed: 10 December 2023).

49. Trevino, A. (2023) What is search engine phishing?, Keeper Security Blog - Cybersecurity News & Product Updates. Available at: https://www.keepersecurity.com/blog/2023/04/12/what-is-search-engine-phishing/ (Accessed: 22 November 2023).

50. Tuama, D.Ó. (2022) What is perl? an introduction, Code Institute Global. Available at: https://codeinstitute.net/ie/blog/perl-an-introductory-guide/ (Accessed: 10 December 2023).

51. Visual studio code nedir? Lesson (no date) Patika Dev. Available at: https://academy.patika.dev/courses/visual-studio-code-kullanimi/visual-studio-code-nedir (Accessed: 10 December 2023).

52. What is a survey (or questionnaire)? (2022) Qualtrics. Available at: https://www.qualtrics.com/uk/experience-management/research/surveys/ (Accessed: 12 December 2023).

53. What is phishing: Attack Techniques & Scam examples: Imperva (2020) Learning Center. Available at: https://www.imperva.com/learn/application-security/phishing-attack-scam/ (Accessed: 29 November 2023).

54. What is phishing? examples and phishing quiz (2023) Cisco. Available at: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#~how-phishing-works (Accessed: 30 November 2023).

55. What is phishing? take the opendns phishing quiz (no date) OpenDNS. Available at: https://www.opendns.com/phishing-quiz/ (Accessed: 29 November 2023).

56. What is python used for? A beginner's guide (no date) Coursera. Available at: https://www.coursera.org/articles/what-is-python-used-for-a-beginners-guide-to-using-python (Accessed: 10 December 2023).

57. What is ruby on rails? (no date) Built In. Available at: https://builtin.com/software-engineering-perspectives/ruby-on-rails (Accessed: 10 December 2023).

58. 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 November 2023).

59. What is the Ruby programming language? (no date) Built In. Available at: https://builtin.com/software-engineering-perspectives/ruby-programming-language (Accessed: 10 December 2023).

60. Yang, Z. (2023) China's Paxlovid Cyber Scams are everywhere, MIT Technology Review. Available at: https://www.technologyreview.com/2023/01/11/1066605/chinas-paxlovid-cyber-scams/ (Accessed: 30 November 2023).