

Abstract

Is cyber hygiene a factor that affects the ability of people in their 60s to detect a phishing email?

This paper explores the prevalence and impact of phishing attacks, especially on individuals aged 60 and above. It discusses the evolution of phishing emails, their creation stages, and the role of cyber hygiene in protecting against such attacks. The main objective of the paper is to find out if cyber hygiene has an impact on older people's ability to distinguish a genuine or phishing email. A Microsoft Survey, consisting of two parts, assesses participants' cyber hygiene and phishing detection abilities which is then analyzed using Chi-square. No significant relationship has been found but the paper found key areas that need to be improved to improve cyber hygiene levels in older people.

1 INTRODUCTION

The evolution of computer software has provided enormous benefits to humanity. From business transactions to health care and even online teaching was made online during a time when humanity was at its lowest, technology is a constant in these turbulent times. However, with such a prominent role to play, there are those out there who seek to take advantage for malicious purposes. One of the most alarming crimes done by these people is identity theft which is when they pretend to be someone else to steal their personal information or belongings or to do malicious acts while impersonating them [1].

There are many methods an attacker can use to steal information and commit identity theft, with one of the most common methods being social engineering, specifically Phishing Attacks. This attack is a very popular social engineering attack and has become one of the leading causes of security breaches and unauthorized access to sensitive information according to GOV.UK [4]. To perform this attack, the attacker needs to impersonate a well-known or trustworthy organization to build trust with the victim and deceive them into sharing personal information. Phishing attacks have already led to damaging losses and could affect the victim financially but also reputation-wise or have catastrophic consequences in terms of national security [2]. Cybercrime, in general, costs more than 1+ billion pounds worldwide every year according to Cybersecurity Ventures [3] and according to a recent study done in the 2020 Proofpoint annual report [5], it is statistically proven that phishing attacks are on the rise and that they constitute a major "tool" used for this cybercrime attacks. This report found that 90% of organizations were targeted by phishing attacks and from these organizations, 88% experienced spear-phishing attacks, 83% faced voice phishing, 86% dealt with social media attacks, 84% reported SMS phishing and 81% reported malicious USB drops. By comparing these statistical numbers to the ones found in the 2019 Proofpoint annual report [5] and the ones found in the 2021 APWG report [6], it shows that each year there is an exponential increase in phishing attacks specifically phishing email attacks. Phishing attacks using emails as a medium are a major problem in cyber security and unfortunately, there have been many successful attacks for example one of the most known cases is the FACC attack [12], in this attack, the company fell victim to a \$61 million Business Email Compromise scam in 2016. A phisher impersonated the president of the company and manipulated the CEO to send 61 million dollars to the attacker's account. The company fired the CEO after that and took legal action, but it was already too late because the money had already been transferred to the attacker. If better training had been given, then this could have been prevented.

Using emails as a medium to perform phishing attacks allows the attackers to exploit human curiosity, greediness, trust, inattention to details, and overreliance on technology. In a survey done by Age UK on people in their 60s, it was revealed that 53% of participants believed that they had been targeted online by online fraudsters, with 70% of people losing money and 33% losing more than £1000+ [7]. The Age UK survey concluded that up to 500,000 older adults (in the UK) may have been victims of cybercrime. If we consider that this study was made 3 years ago, that the statistics found are just an estimate, and that during the survey there might have been biases/limitations, then we can assume that this number could be currently bigger than what has been estimated.

Unfortunately, older people in their 60s or above are preferred targets by attackers for various reasons. The reason why older adults are preferred targets is because they are more susceptible to falling victim to phishing email attacks and countless studies support this claim. For example, a study made in 2021[9] concluded that the ability to accurately distinguish between genuine and phishing emails declines with age and that older adults showed a significantly reduced decision-making ability to distinguish between phishing and genuine emails compared to younger adults, so they have the tendency to judge genuine emails as potentially unsafe and view phishing emails as overly trustworthy. Another study made in 2017 [10] found out that older adults admitted to needing help/training because they found technology overwhelming and complex and another study made in 2021 [11] concluded that cyber awareness training for older adults is crucial. All these studies concluded that technology, lack of training, and cyber awareness are major factors for why older people fall victim to phishing attacks but none of them analysed if Cyber Hygiene is also a major factor required for older people to successfully distinguish between phishing emails and genuine emails. For these reasons, the research question is: "Is cyber hygiene a factor that affects the ability of people in their 60s to detect a phishing email?". This research will specialize in finding if there is a correlation between Cyber Hygiene levels and the phishing email detection ability of people in their 60s. This is important because if there is a correlation, then that would signify that not only Cyber awareness training would be crucial for older people as suggested in previous studies [11] but also Cyber Hygiene training would be crucial as well to reduce the number of older

people falling victims to phishing email attacks. In this research, questions will be posed to participants through a Microsoft Form to assess their cyber hygiene level. Each section of the form will analyse the participant's behaviour in 4 security areas: Device securement, password generation, updating, and proactive awareness. These results from the research could give more insight into what areas need to be prioritized in older people's security training. By addressing these areas, the findings will significantly improve online security for older individuals, making them less susceptible to phishing email attacks.

1.1 Hypothesis

The hypothesis for this research is that individuals who show higher levels of Cyber Hygiene will demonstrate a greater ability to detect phishing emails compared to individuals that show a lower level of Cyber Hygiene.

In the next section, we will discuss Phishing emails in more detail, and Cyber hygiene definition.

2 BACKGROUND

2.1 History of phishing

Phishing is a form of illegal activity, in which a cybercriminal tries to steal personal/sensitive information such as username, password, and online banking details from their victims [13]. There are many types of mediums used for phishing attacks, but the most common medium is emails because they provide anonymity and allow the attacker to deceive his victims from a safe distance. The earliest recorded incident occurred in 1996 when attackers targeted AOL users. The attacker sent out crafted emails and used the same colours, fonts, and text used in AOL emails. In the phishing emails, the attackers pretended to be AOL employees and since this was a new type of attack at the time, the attackers were successfully able to collect their sensitive information. Between 2000-2010 is when phishing attacks started becoming a common occurrence and fully started taking shape of the devastating attack we know today [15]. During this period there was a rise of eCommerce and online payment systems such as eBay and PayPal. Cybercriminals exploited the trend by sending deceptive emails to PayPal users and tricking them into providing private information. Phishers also registered numerous domains which resembled legitimate payment system websites. In 2008 the launch of bitcoin and cryptocurrencies facilitated anonymous financial transactions, causing a rise in phishing attacks. From 2010 onwards, phishing continued to evolve and adapt quickly to new technologies to the point where for example in 2013 an attacker spread cryptographic malware (ransomware) using phishing to infect 250,000 personal computers and ever since that attack more and more phishing emails containing malware has been sent worldwide. Even HTTPs which instilled a sense of security in people, were being used by cybercriminals to make a fake website seem legitimate.[15]

Ever since the term Phishing Emails has been globally used, anyone can be affected for example individuals, businesses, and due to lack of training, there are countless people falling victim every day especially as shown in Age UK, people above the age of 60. Countless existing technologies are used to counter phishing emails but due to technological evolution, attackers are coming up with new strategies to bypass existing countermeasures. Older people are the main target, for this reason, it is important to create more effective cyber training for older adults.

2.2 Stages of phishing

To perform a phishing email attack, an attacker usually follows stages: The first stage is the "Planning stage" in which the attacker conducts research (e.g. by using OSINT which is the process of collecting information using publicly available information) to identify potential targets that possess sensitive and valuable information. The second stage is the creation of the email, and in this stage, the attacker crafts a deceptive email to make it seem legitimate. The commonly crafted emails targeted to older people are financial scams, pension schemes scams, and healthcare scams. These phishing emails usually exploit human vulnerabilities, and in the case of older people in their 60s those vulnerabilities would be curiosity, greediness, trust, inattention to details, and overreliance on technology, by using these vulnerabilities the attacker can encourage the victim to click links, download infected attachments, and provide sensitive information. The third stage is the delivery of the email, and this stage could be a mass email sending or specifically targeted to individuals. The final stage is the collection/covering tracks stage in which the attacker collects the information from the victim and covers its tracks to erase any evidence of a phishing campaign.[14]

2.3 Cyber hygiene

Cyber awareness is about understanding cyber-attacks and how to protect yourself from them. Countless studies concluded that lack of cyber awareness in individuals is a major factor of susceptibility. For example, in A Portsmouth case study [7] older participants confessed to falling victim to phishing attacks and some of them confessed to falling victim to the same scam multiple times. In this case study, many people confessed to falling victim to phishing attacks due to their lack of cyber awareness. Most past papers mention the importance of cyber awareness but none of the papers discuss if cyber hygiene influences vulnerability to detect phishing scams and that's why my research will aim to find out if there is a statistical relationship between cyber hygiene and phishing detection accuracy.

Cyber hygiene refers to all the practices online users adopt to maintain the safety and security of their devices (e.g. mobile phones, laptops, and computers).[34]

Key components of cyber hygiene are:

- Password management: Using strong, unique passwords for different accounts and regularly changing them.
- Antivirus and firewall protection: Installing and keeping antivirus and firewall software up to date with the latest updates.
- Proactive awareness: Avoid clicking on suspicious links and verify legitimacy of the link.
- Using biometrics like multifactor authentication, passcodes, fingerprint etc...
- Email security: Being careful with information shared online and verifying the legitimacy of an email or unexpected request for personal data or avoiding opening it.[34]

Many online users have poor cyber hygiene because they do not follow the key components needed to have a good one. For example, they freely share passwords and are quick to share private information on online platforms like social media or email. In America alone, the total money lost in 1 year was more than 1 billion dollars with people in their 60s being the prime victims [29]. No matter how secure a system might be, the end user often serves as the backdoor an attacker uses to infiltrate a system due to their poor cyber hygiene which causes them to not follow the best security practices, leading them to reveal personal information [29], a known example of this could be the U.S. presidential election in 2016. In this attack, performed to influence presidential votes, John Podesta which was Hilary Clinton's manager received a scam email with the catchy subject line "Someone has your password" and the content of the email greeted him with his name "Hi John, Someone just used your password to try to sign into your Google Account john.podesta@gmail.com". Unfortunately, John Podesta clicked the email and disclosed his information. It was later found out that the filtering system allowed the email to pass because the attacker utilized Bitly (a web server shortening service) to bypass the filtering system.[16]. John Podesta, born in 1949, was in his 60s at the time of the attack. This incident clearly demonstrates how important cyber hygiene is because If Podesta had followed security practices to have a better cyber online hygiene, he would have not fallen victim to this phishing scam. This event could have been more devastating, for this reason, we can conclude that Podesta's experience should be used as a lesson to teach people more about how to maintain a good cyber hygiene. Podesta was a member of the government so he probably got a lot of training in cybersecurity good practices, but despite all that he still fell victim to the phishing scam, so imagine how someone who never got trained before would react to the phishing email situation. For this reason, we must provide proper training to prevent this from happening again.

Unfortunately, a lack of Cyber hygiene is a major factor in why older people fall victim to phishing attacks [22]. A 2021 study [25], has proven that people's cyber hygiene practices are correlated to having better online security because, in the survey, it was proved that people who had reported having healthy online security habits were less susceptible to deception and less likely to click on phishing links compared to individuals who admitted to occasionally click on links in email messages without verifying their legitimacy. Another study conducted by Dawn M. Sarno (2022) [32], discovered that there was a significant relationship between Cyber hygiene and the classification of phishing emails. In this research they found out that individuals with a higher number of correct phishing email detection were more likely to have reported being more "cyber hygienic", so they concluded that a higher level of cyber hygiene is directly correlated to phishing detection ability. Their paper was not done on individuals above the age of 60, which is why my research will aim to fill this gap by investigating if there is a correlation between cyber hygiene and phishing detection ability in older adults in their 60s.

3 METHOD

As mentioned earlier, this research aims to find out if cyber hygiene is a factor that influences older adults' ability to distinguish between phishing emails and genuine emails. To carry out this research, qualitative data collection was the best approach because the aim of the research is not to test hypotheses and determine the opinions, and attitudes of people dealing with phishing emails, but the research aim is to deal with categories and frequencies (in this case cyber hygiene level and the number of correct and incorrect detections). Using quantitative data collection offers a better statistical view of the data which makes it easier to analyse the relationship between cyber hygiene and phishing detection ability. Wilcoxon test or t-test could be used if dealing with means or other continuous variable types, but in this case, chi-squared is the best approach because we are dealing with categorical variables to test if there is a statistically significant association between cyber hygiene and phishing detection. The sample size is going to be around a minimum of 20 people in their 60s or above. The decision to use a minimum of 20 people in the study rather than using a smaller sample size is to enhance the accuracy and reliability of the data collected. A smaller sample size may compromise the statistical significance of the finding. To facilitate data collection, a Microsoft Survey has been created to collect the participant's data which will later be used for chi-square analysis.

3.1 Materials

The Microsoft form is divided into two parts. The first part consists of questions aimed at assessing the participant's cyber hygiene level and classifying them as low or high cyber hygiene categories. The second part will be 4 questions designed to evaluate an individual's ability to detect phishing from genuine emails.

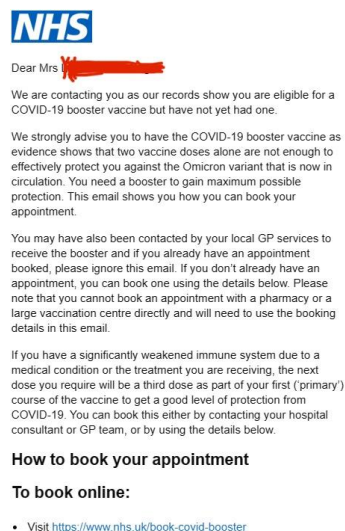
The first part of the survey will contain 16 questions from a 2015 paper by Serge Elgelman [26] [questions are shown in figure 1]. The reason why self-made questions were not used in my research was to avoid bias because those self-made questions would have lacked expert review and approval.

In Serge Elgelman's [26] paper each of the 16 questions had 5 possible responses: Never, Rarely, Sometimes, Often, and Always. However, in the current research, the response "Sometimes" has been removed from the possible available responses because many papers proved that "Sometimes" provides unnecessary biases in data collection due to the fact that it does not indicate favouritism of a participant towards specific response categories [27]. For these reasons, this research will only use Never, Rarely, Often, and Always in the list of allowed responses. Each response is scored from 1 to 4 with "never" being the lowest possible score (1) and "always" being the highest score (4). Some of the questions that end with a special character 'r' are reverse scored, which means that the scoring scale is reversed during calculation, ranging from 1 to 4, with "never" now assigned the highest score (4) and "always" the lowest (1). Furthermore, this research paper will number the questions as question 1, question 2 etc instead of using f4, f6 etc. After data collection, the scores from each participant are added up and recorded on a Microsoft Excel sheet. To determine the minimum, score an individual needs to score to be classified in the high cyber hygiene category, the total points of each participant will be arranged in ascending order to determine the median of the data and that will be used as a reference point. So, participants that scored below the median will be classified as low cyber hygiene level and participants that score more or equal will be classified as high cyber hygiene.

#	Device Securement (28.47% of variance explained; $\lambda = 4.555$)	μ	σ
F4	I set my computer screen to automatically lock if I don't use it for a prolonged period of time.	3.20	1.559
F6	I use a password/passcode to unlock my laptop or tablet.	3.78	1.525
F3	I manually lock my computer screen when I step away from it.	2.63	1.343
F5	I use a PIN or passcode to unlock my mobile phone.	3.21	1.733
#	Password Generation (12.95% of variance explained; $\lambda = 2.071$)	μ	σ
F12	I do not change my passwords, unless I have to. ^r	2.65	1.091
F13	I use different passwords for different accounts that I have.	3.75	1.037
F15	When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.	3.31	1.096
F14	I do not include special characters in my password if it's not required. ^r	3.30	1.292
#	Proactive Awareness (8.36% of variance explained; $\lambda = 1.337$)	μ	σ
F8	When someone sends me a link, I open it without first verifying where it goes. ^r	4.01	1.014
F11	I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar. ^r	3.17	1.077
F16	I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon). ^r	3.69	1.102
F10	When browsing websites, I mouseover links to see where they go, before clicking them.	3.69	1.027
F7	If I discover a security problem, I continue what I was doing because I assume someone else will fix it. ^r	4.08	0.976
#	Updating (6.77% of variance explained; $\lambda = 1.082$)	μ	σ
F1	When I'm prompted about a software update, I install it right away.	3.07	1.035
F2	I try to make sure that the programs I use are up-to-date.	3.78	0.890
F9	I verify that my anti-virus software has been regularly updating itself.	3.55	1.228

Security behaviour

Figure 1 [26]



NHS

Dear Mrs [REDACTED]

We are contacting you as our records show you are eligible for a COVID-19 booster vaccine but have not yet had one.

We strongly advise you to have the COVID-19 booster vaccine as evidence shows that two vaccine doses alone are not enough to effectively protect you against the Omicron variant that is now in circulation. You need a booster to gain maximum possible protection. This email shows you how you can book your appointment.

You may have also been contacted by your local GP services to receive the booster and if you already have an appointment booked, please ignore this email. If you don't already have an appointment, you can book one using the details below. Please note that you cannot book an appointment with a pharmacy or a large vaccination centre directly and will need to use the booking details in this email.

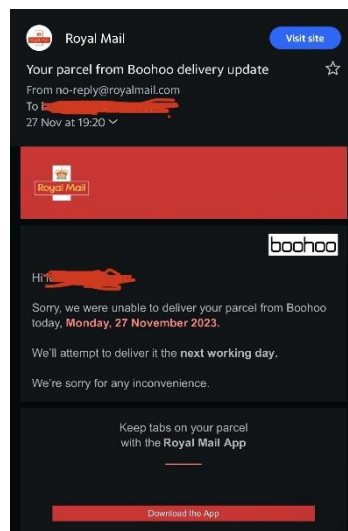
If you have a significantly weakened immune system due to a medical condition or the treatment you are receiving, the next dose you require will be a third dose as part of your first ('primary') course of the vaccine to get a good level of protection from COVID-19. You can book this either by contacting your hospital consultant or GP team, or by using the details below.

How to book your appointment

To book online:

- Visit <https://www.nhs.uk/book-covid-booster>

Figure 2



Royal Mail

Your parcel from Boohoo delivery update

From no-reply@royalmail.com
To [REDACTED]
27 Nov at 19:20

boohoo

Hi [REDACTED]

Sorry, we were unable to deliver your parcel from Boohoo today, **Monday, 27 November 2023**.

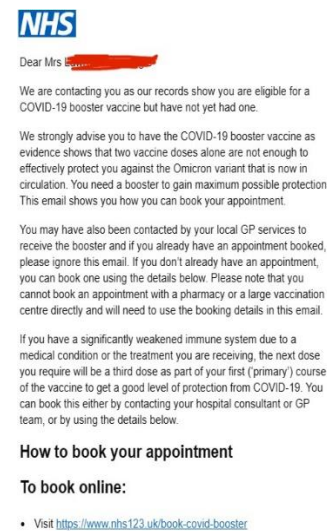
We'll attempt to deliver it the **next working day**.

We're sorry for any inconvenience.

Keep tabs on your parcel with the Royal Mail App

Download the App

figure 3



NHS

Dear Mrs [REDACTED]

We are contacting you as our records show you are eligible for a COVID-19 booster vaccine but have not yet had one.

We strongly advise you to have the COVID-19 booster vaccine as evidence shows that two vaccine doses alone are not enough to effectively protect you against the Omicron variant that is now in circulation. You need a booster to gain maximum possible protection. This email shows you how you can book your appointment.

You may have also been contacted by your local GP services to receive the booster and if you already have an appointment booked, please ignore this email. If you don't already have an appointment, you can book one using the details below. Please note that you cannot book an appointment with a pharmacy or a large vaccination centre directly and will need to use the booking details in this email.

If you have a significantly weakened immune system due to a medical condition or the treatment you are receiving, the next dose you require will be a third dose as part of your first ('primary') course of the vaccine to get a good level of protection from COVID-19. You can book this either by contacting your hospital consultant or GP team, or by using the details below.

How to book your appointment

To book online:

- Visit <https://www.nhs.uk/book-covid-booster>

figure 4

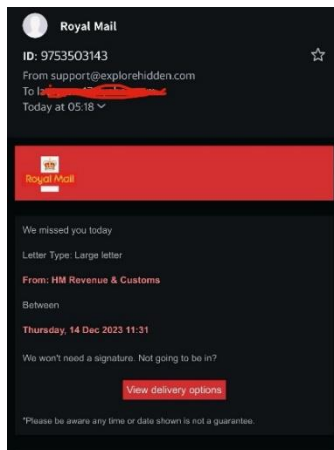


figure 5

In the second part of the Microsoft form, participants will be presented with four different emails and tasked with identifying genuine and phishing emails. 4 emails were chosen to ensure the validity and reliability of the data to prevent it from being unreliable. To have a balance in the collected data, 2 emails were phishing emails [figure 4, 5] and the other 2 were genuine emails [figure 2, 3]. The 2 phishing emails are respectively identical in type and content in relation to the 2 genuine emails, with the addition of specific characteristics that made them a phishing email.

The “genuine” emails used in the research are from real emails sent to me by Royal Mail [figure 3] and NHS [figure 2]. The genuine emails, received from Royal Mail and NHS, remain unaltered to preserve their authenticity. The Royal Mail and NHS email respectively are used as a template to craft the 2 phishing emails used in the survey. The NHS phishing email [figure 4] that was created is the same copy of the genuine NHS email [figure 2], the only difference is that the real URL contained in the real email was modified to a fake one in the phishing email. However, what makes the phishing email by Royal Mail [figure 5] different from the original Royal Mail email [figure 3] is the time the message was sent, the subject, and the email address of the sender. The reason why the phishing emails were self-crafted was to analyze the participant's ability to read URLs in emails, the subject, and the sender's email before determining if an email was genuine or not.

The Chi-Square Testing Table is shown in Figure 6.

	Correct detections	Incorrect detections
Low security hygiene		
High security hygiene		

Figure 6 [28]

In this study, a statistical calculator was used to find Chi-square [28]. The total number of correct detections and incorrect detections of people with low cyber hygiene and the number of correct detections and incorrect detections of people with high cyber hygiene were added to the table [figure 6]. In this research the Null Hypothesis (H0) is that there is no significant relationship between the Cyber hygiene of an individual and their ability to detect phishing emails and the Alternative Hypothesis (H1) is that there is a significant relationship between the high-security hygiene of an individual and their ability to detect phishing emails.

The significance level should be set to 0.05. If the p-value is less than 0.05 then H0 should be rejected and H1 should be approved, in this case this would mean that there is a significant relationship between the cyber hygiene level of an individual and their ability to detect phishing emails, but if the p-value is greater than 0.05 then approve H0 and reject H1 which would mean that there is no significant relationship between the Cyber hygiene of an individual and their ability to detect phishing emails.

3.2 Ethics

To ensure confidentiality and protect participants' privacy in the collected data, the anonymous feature on Microsoft Forms has been enabled, and this allows the gathered data to remain anonymous.

To allow participants to withdraw their data if they decide not to participate in the survey, a unique number will be provided to them at the start of the survey. The unique numbers will be assigned sequentially so the first participant will get number 1, the second participant will get number 2, etc... Participants will need to input this number as the response to the initial survey question: "What number was provided to you?". This is important because if the participant wants to delete their data from the research, it will be quicker and easier since they only need to provide the unique number associated with their form to the person responsible for the data collection, who will then be responsible to look for the form associated with that unique number and then delete it.

Finally, get consent from participants by explaining the research objective and addressing any questions or concerns they may have, after explanations, the participants must fill out the consent form.

3.3 Inclusion criteria

The first criterion for participants to meet is the minimum age requirement of 60 years old because the study specifically focuses on people who are 60 or above. The second criterion is that the participant should have an email and know how to use it because a lack of this skill might put them at a disadvantage when answering the second section of the Microsoft Form because this section is about phishing email detection, so not knowing not having an email or knowing how to use it (e.g. sending, receiving etc) would impact the way they answer this section and this could make the collected data inaccurate. The final criterion is that participants should have enough cognitive capacity to provide informed consent and that they do not have a significant decline in cognitive ability e.g. memory, decision-making, and attention, because it was found by other researchers that individuals that have a decline in cognitive ability have a higher susceptibility to phishing emails [17]. So, using people who have a significant decline in cognitive ability would make this research biased and inaccurate.

3.4 procedure

Raw data from the 2017 Eurobarometer Survey suggests that among the people born before 1964, only 40% use the internet every day and 48% confessed never using the internet at all [7]. To ensure participants feel at ease and to avoid biases in my research, face-to-face data collection was preferred over an online survey. For these purposes, two tablets were supplied for participants to utilize in completing the survey. By allowing them to fill out the form on my tablet I can be able to give them support. To make research unbiased when a participant asks for assistance, any assistance provided will be focused solely on explaining how to submit questions or clarifying unfamiliar terms such as "Scam" or "HTTP" etc... Since the data collection was going to be face-to-face, a church setting was chosen due to its higher population of older adults. I do voluntary work in a church so at the end of the church service I stood at the entrance of the church and asked people who were entering or exiting the building if they wanted to participate in my school survey. If the person refused, then I apologized for consuming their time and wished them a good day otherwise if they agreed to participate, I would explain to them the criteria for participating in the survey.

All participants meeting the inclusion criteria were told to sign the consent form (which was on my phone). After completion of the consent form, they were assigned a unique number and asked to complete the survey on a tablet.

The participants, had to answer question one with the unique number assigned to them at the start of the survey and then answer 16 questions regarding their online security behaviour across four categories: Device securement, password generation, updating, and proactive awareness. Upon completion of the 16 questions, the participant will be required to complete the final four questions to assess their ability to differentiate real from phishing emails. Completion of the survey should take around 5 to 10 minutes.

4 RESULT

Data was collected from a total of 21 participants, unfortunately, while examining the results it was discovered that 2 participants wrote the same unique number. Consequently, both results were voided because having 2 results with the same unique number would make it harder to withdraw data if requested. So, in the end, the total number of participants data collected was 19 results which is below the minimum expected target of 20 people.

The maximum total mark that an individual could have scored in the 16 questions was 64 points and I found out that the highest score in my research was 48 and the lowest was 25. After arranging the total points of every participant in descending order it was determined that the median score was 35. So, every participant who scored less than 35 was categorized as having low-security hygiene, while those who scored more or equal to 35 were classified as high-security hygiene. As a result, 9 participants were classified as low-security hygiene and 10 were classified as high-security hygiene.

A statistical calculator [28] was used to perform the chi-squared test and the p-value found was 0.423808. Given that this value exceeds 0.05, the H1 was rejected and H0 was accepted this means that there is no significant relationship between cyber hygiene and phishing email detection. This suggests that practicing good cyber hygiene habits may not necessarily correlate with an individual's ability to detect phishing emails. This result is different from the initial predictions which was that cyber hygiene had a significant relationship with phishing detection but despite this deviation, the collected data provided valuable insights.

Analysis of participants' security hygiene practices revealed that older people followed good security hygiene practices in regard to Device Securement (Q2 to Q5) because this is the section that had the highest "always" and "Often" responses. Specifically, 26.25% of the participants selected "Often", and 42.25% voted "always". In contrast, the Updating section (Q14 to Q16) displayed lower security hygiene scores, with 37% responding "never" and 43.7% choosing "rarely". In the second part of the Microsoft form, combining all participants' detections showed a total of 54 correct detections out of 76 and 22 incorrect detections. Among these, individuals with low-security hygiene had 24 correct detections and 12 incorrect detections, while participants with high-security hygiene had 30 correct detections and 10 incorrect detections. [figure 7]

While no significant correlation was found between overall cyber hygiene and phishing detection accuracy in older people because the p-value of 0.423808 was higher than 0.05, participants with high-security hygiene demonstrated a higher total correct detection rate compared to people with low-security hygiene. Six participants were able to score 4 out of 4 in the phishing detection section, 4 of these participants were in the high category and 2 were in the low. The category that had the most number of participants achieving only one correct detection out of 4, was the low-security hygiene category.

Participants who replied “Often” to question 13(**figure**) were more likely to score 3 or more correct detections out of 4, compared to those who replied with “Never” or “Rarely”. These results suggest that people who mouse-hover URLs will have a higher chance of detecting phishing emails that contain invalid/malicious URL links compared to people who do not mouse-hover links. Question 21 was a phishing email question that contained a fake link with unusual characters, and participants who admitted to not hovering over links were more likely to give incorrect detection in this question. This could be because participants who hover over links might spend more time inspecting the legitimacy of the email containing the suspicious link, this is important because it provides an opportunity to examine the URL for signs of spoofing, such as misspelled domain names, or unusual characters. These results allowed me to conclude that hovering over a link is important in phishing detection. Similar results were also found in another paper [30], in which the researcher also concluded that when a user hovers over a link, their chance of detecting a genuine or phishing email increases because they spend more time inspecting the legitimacy of the email containing the suspicious link.

Question 1 was a phishing email that had a suspicious email subject and sender details, and 78% of the participants in my research were able to detect that it was a phishing email, this means that most older adults know how to examine an email and recognize suspicious subjects and sender details.

	Correct detections	Incorrect detections
Low security hygiene	24	12
High security hygiene	30	10

Figure 7 [28]

5 DISCUSSION

The statistical results found in the first part of the Microsoft form also share a similarity with the statistics presented in the “An exploratory study of cyber hygiene behaviours and knowledge” paper [29]. This previous paper reported that out of 329 people surveyed, 67% of the participants did not update their antivirus, this result similarly aligns with the results found in this current paper because the Updating section revealed that 80.7% of the participants voted either “Never” or “Rarely”, and 53% admitted of not updating their antivirus software. Having an antivirus is very important because, in modern times, antiviruses can perform email filtering of suspicious emails, furthermore, they use signature-based detection so they can detect if an email contains a malicious attachment. So, not having an updated antivirus is a major security concern nowadays [31], because it increases the probability of the victim falling for the scam. I also found out that 42% of participants (in my paper) replied “Never” to question 7, this result aligns with the statistic presented in the cyber hygiene study[29] because it stated that 31% of users use the same password. This is another security concern because it means that if an individual falls victim to a phishing email, and his password gets stolen then most of his accounts would be compromised.

Participants who replied “Often” to question 13(**figure**) were more likely to score 3 or more correct detections out of 4, compared to those who replied with “Never” or “Rarely”. These results suggest that people who mouse-hover URLs will have a higher chance of detecting phishing emails that contain invalid/malicious URL links compared to people who do not mouse-hover links. Question 21 was a phishing email question that contained a fake link with unusual characters, and participants who admitted to not hovering over links were more likely to give incorrect detection in this question. This could be because participants who hover over links might spend more time inspecting the legitimacy of the email containing the suspicious link, this is important because it provides an opportunity to examine the URL for signs of spoofing, such as misspelled domain names, or unusual characters. These results allowed me to conclude that hovering over a link is important in phishing detection. Similar results were also found in another paper [30], in which the researcher also concluded that when a user hovers over a link, their chance of detecting a genuine or phishing email increases because they spend more time inspecting the legitimacy of the email containing the suspicious link.

I also found out that 63% of the participants who replied with “Always” and “Often” to the question “When someone sends me a link, I open it without first verifying where it goes”, had the worst performance in detecting if an email is a phishing email or genuine compared to people that replied with “Never” or “rarely”. The fact that some participants would open a link without first verifying where it goes, means that they have trust in the sender, and as I stated in my background section of this paper, trust is one of the reasons why older people are susceptible to falling victim to scams because they put a lot of

trust in emails...causing them to be less cautious and have a harder time in having a good phishing detection accuracy performance compared to people that have less trust and are more cautious.

In the paper by Dawn M. Sarno (2022) [32], the researchers discovered that there was a relationship between Cyber hygiene and the classification of phishing emails. In this research they noticed that the more correct phishing email detections an individual had then the more likely they were to have reported more “cyber hygienic”, so they concluded that a higher level of cyber hygiene is directly correlated to phishing detection. The results found by Dawn M.sano(2022) [32] are opposite to the results I found from my research because in my research I found out that there is no significant relationship between cyber hygiene and phishing detection but in his research, he found out that there is a significant relationship.

Despite the research results deviating from initial expectations, the study contributes valuable insights into the realm of cyber training. The data collected highlights specific areas that require focus in educating individuals aged 60 and above. Key focus areas that mainly need to be taught to older people in their 60s are Password hygiene, specifically, the importance of using different passwords for different accounts that go beyond the site minimum requirement. Additionally, there is a crucial need to educate individuals on keeping software, such as antivirus tools, regularly updated to effectively counter evolving phishing tactics in the digital landscape.

5.1 Limitations

There are many reasons why my results are different from initial expectations and Dawn M.Sarno(2022) [32] paper, firstly my research participant's sample was different from Dawn M.sarno's paper because my participants were individuals above the age of 60 whereas in his paper he focused on undergraduate students. also, he used a different scale from the one I used in my research to measure the cyber hygiene level of an individual so it might be that individuals who were classified in the high category using the scale that I used in my research, might be classified in the low category if they completed the scale that Dawn M.Sarno(2022) [32] used in his research. Furthermore, the emails I used to test an individual phishing detection ability were self-crafted by me but the ones used in their research were reviewed and approved questions moreover I only used only 4 emails to test participant accuracy whereas they [32] used 100+ emails which means that the results he found are more accurate than mine due to the larger sample size.

Further limitations in my research that might have caused my research to have different results from my expected results might be caused by many factors such as:

- Classifications method: The 2 categories used in this research are “high-security hygiene” and “low-security hygiene” which might be too general or unreliable to classify individual cyber hygiene. Furthermore, individuals were classified based on the median split, which was 35, which is very likely to not be a good representation of what the minimum threshold should be for an individual to be classified as high cyber hygiene.
- Sample size: The sample size used might be too small which makes the data inaccurate because 19 participants isn't enough to represent the entire population of older people above the age of 60 living in the UK. Furthermore, having such a small sample size makes results more susceptible to random variations which means that the probability of obtaining extreme values that do not reflect the true central distribution of the population will be higher.
- Phishing questions: Unlike the first section of the form, the phishing emails were self-crafted, so it might be that those crafted questions were not a good representation of what an actual phishing email would look like in a real-world scenario. In the creation of the phishing email I might have unintentionally included characteristics that would make my questions more straightforward and less sophisticated compared to a real phishing email, and this would make it easier for participants to distinguish the genuine and phishing emails.
- Response bias in the first part of Microsoft Forms: Participants' behaviour might be different in real-case scenarios. For example, the answers a participant gave in the first part of my Microsoft form might be different from how they would regularly behave in a real scenario. These inaccurate responses by the participants would cause my data results to be inaccurate.
- Response bias in the second part of the Microsoft Forms: Participants probably assumed that in the 4 questions to test their phishing detection ability at least one question would be a phishing email. The fact that they knew this information, probably made them more cautious before giving their responses to these 4 questions causing my data to be an inaccurate representation of a real-world case scenario because, in reality, no one knows when they will get a phishing or genuine email. So, there is a probability that participants who correctly answered the questions in the form might fall victim to the phishing email if they do it during their day-to-day activities.
- Psychological factors: cognitive ability, mental health, or depression were not tested unlike other research [26] might cause a bias in participant responses because participants might have different levels of cognitive abilities.
- Time: Participants might have felt pressured to complete the Microsoft form as fast as they could. Causing data to be inaccurate
- Training: Some of the participants might have done cyber awareness training in the past so they might have been taught how to recognize a phishing email. This knowledge gives some participants a better advantage in detection compared to participants who had no training.

5.2 Future Work

To improve this research in the future and reduce the possible limitations, make sure you use a bigger sample size to make the data collected more accurate, and let phishing questions be validated by experts to ensure that the questions accurately reflect the complexity of a real-world phishing email, use psychological scales to assess individual psychological factors such as cognitive ability and mental health instead of using self-reported data by participants. Finally, ask participants if they had any prior training and note down their responses while keeping them anonymous, to reduce time pressure bias, and ensure that participants understand that they are not being timed and they can take as long as they want to complete the form.

6 REFLECTION

In this paper, I learned more about cyber hygiene and how it affects phishing detection in older adults. I learned how to do sample collection while following correct ethics such as consent and I also learned how to keep the data I collected anonymous while still being able to withdraw specific data if the user doesn't want to participate in the research anymore.

I learned how to not use self-crafted papers and to use pre-crafted research questions instead because those questions have been approved and reviewed by experts.

I learned how to interpret data even if my results are different from my expected results. I also realized that using a church as a location to perform data collection was a good strategy that allowed me to find the right participants for my research, but after my paper, I realized that using only one specific location(church) for the data collection might have limited the participant pool and introduced bias. To prevent this from happening in my final year project, I should use a larger sample size to make my results more accurate compared to the results found in this paper and use multiple locations for example senior centres and online communities for my data collection to increase the sample pool.

Furthermore, I learned that quantitative data collection might have not been the best approach so in my final year project I might decide to use focus groups and discussions, rather than focusing on more stats and numbers. This would enable a deeper understanding of the factors influencing cyber hygiene and phishing detection. If I still decide to use quantitative data collection, I learned that chi-squared might have not been the best analysis I could have used in my current research, so, for example, I could use a t-test to compare the mean cyber hygiene scores of participants who correctly identified the phishing emails with those who did not.

Lastly, I learned how to reduce the possible limitations in my study for a better final year project by following what I wrote in the "Future Work" section of this report which was: I will use a bigger sample size to make data collected more accurate, let phishing questions to be validated by experts to ensure that the questions accurately reflect the complexity of a real-world phishing email, I will use psychological scales to assess individual psychological factors such as cognitive ability and mental health instead of using self-reported data by participants. Finally, I will ask participants if they had any prior training and note down their responses while keeping them anonymous, to reduce time pressure bias, and ensure that participants understand that they are not being timed and they can take as long as they want to complete the form.

7 References

- [1]<https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=ad580f4be151ef7b57cdbe29b838e23b44335674>
- [2] Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf, and Imtiaz Khan. 2021a. Phishing attacks: A recent comprehensive study and a new anatomy. (January 2021). Retrieved December 15, 2024 from <https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full>
- [3] steve morgan. 2019 official annual Cybercrime Report - Herjavec Group. Retrieved December 15, 2023 from <https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf>
- [4] Anon. Cyber security breaches survey 2020. Retrieved January 15, 2024a from <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020>
- [5] Retrieved January 10, 2024 from <https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-state-of-the-phish-2020.pdf>
- [6] Phishing activity trends reports. Retrieved January 15, 2024b from <https://apwg.org/trendsreports/>
- [7] Dr. Vasileios Karagiannopoulos et al. 2021. Cybercrime awareness and victimization in individuals over 60 years: A Portsmouth case study. (October 2021). Retrieved January 10, 2024 from https://www.sciencedirect.com/science/article/pii/S0267364921000881?fr=RR-2&ref=pdf_download&rr=82363b2b9c8d7199
- [8] Katherine Denham. 2023. What is the UK state pension age and will it go up? (August 2023). Retrieved January 10, 2024 from <https://www.thetimes.co.uk/money-mentor/pensions-retirement/state-pension/state-pension-age>
- [9] Matthew Grilli. Is This Phishing? Older Age Is Associated With Greater Difficulty Discriminating Between Safe and Malicious Emails . Retrieved January 10, 2024 from <https://academic.oup.com/psychogerontology/article/76/9/1711/6055602>
- [10] Eleftheria Vaportzis, Maria Giatsi Clausen, and Alan J. Gow. 2017. Older adults perceptions of technology and barriers to interacting with tablet computers: A FOCUS Group Study. (September 2017). Retrieved January 10, 2024 from <https://www.frontiersin.org/articles/10.3389/fpsyg.2017.01687/full>

- [11] Author links open overlay panelDr. Vasileios Karagiannopoulos a et al. 2021. Cybercrime awareness and victimisation in individuals over 60 years: A portsmouth case study. (October 2021). Retrieved January 10, 2024 from https://www.sciencedirect.com/science/article/pii/S0267364921000881?fr=RR-2&ref=pdf_download&rr=82363b2b9c8d7199
- [12] Chkadmin. 2022. The top 5 phishing scams of All time. (May 2022). Retrieved January 10, 2024 from <https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/the-top-5-phishing-scams-of-all-times/>
- [13] Tatyana Stojnic, 2020. Phishing email strategies: Understanding cybercriminals' strategies of crafting phishing emails. Retrieved January 10, 2024, from https://onlinelibrary.wiley.com/doi/epdf/10.1002/spy2.165?saml_referrer
- [14] JAMES MACKAY, HOW TO EXECUTE A SUCCESSFUL PHISHING SIMULATION CAMPAIGN: ESSENTIAL STEPS, Retrieved January 15 from <https://www.metacompliance.com/blog/phishing-and-ransomware/run-phishing-simulation-campaign>
- [15] Amy McNeal. 2023. History of phishing: Origins and evolution. (September 2023). Retrieved January 10, 2024 from <https://www.graphus.ai/blog/history-of-phishing/>
- [16] Tatyana Stojnic, 2020. Phishing email strategies: Understanding cybercriminals' strategies of crafting phishing emails. Retrieved January 10, 2024 from https://onlinelibrary.wiley.com/doi/epdf/10.1002/spy2.165?saml_referrer
- [17] Shang Y, 2022. The psychology of the internet fraud victimization of older adults: A systematic review. Retrieved January 15 from <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9484557/>
- [18] Patricia A. Boyle, Lei Yu, Robert S. Wilson, Keith Gamble, Aron S. Buchman, and David A. Bennett. Poor decision making is a consequence of cognitive decline among older persons without alzheimer's disease or mild cognitive impairment. Retrieved January 10, 2024 from <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0043647>
- [19] Anon. Retrieved January 15, 2024a from <https://www.tandfonline.com/doi/abs/10.1080/08946566.2013.821809>
- [20] Lichtenberg P. A., Stickney L., Paulson D. (2013). Is psychological vulnerability related to the experience of fraud in older adults?. Clin. Gerontol. 36, 132–146.
- [21] Gizem Ögütçü et al. 2015. Analysis of Personal Information Security Behavior and awareness. (November 2015). Retrieved January 10, 2024, from <https://www.sciencedirect.com/science/article/pii/S0167404815001406>
- [22] Michael Ovelgönne UMIACS et al. 2017. Understanding the relationship between human behavior and susceptibility to cyber attacks: A data-driven approach: ACM Transactions on Intelligent Systems and Technology: Vol 8, no 4. (July 2017). Retrieved January 10, 2024 from <https://dl.acm.org/doi/10.1145/2890509>
- [23] Retrieved 10 January, 2024 from [OP-CYBE190016 1..17 \(silverchair.com\)](https://www.silverchair.com/OP-CYBE1900161.17)
- [24] Eleftheria Vaportzis, Maria Giatsi Clausen, and Alan J. Gow. 2017. Older adult's perceptions of technology and barriers to interacting with tablet computers: A FOCUS Group Study. (September 2017). Retrieved January 10, 2024, from <https://www.frontiersin.org/articles/10.3389/fpsyg.2017.01687/full>
- [25] Frank L. Greitzer PsyberAnalytix et al. 2021. Experimental investigation of technical and human factors related to phishing susceptibility. (June 2021). Retrieved January 10, 2024 from <https://dl.acm.org/doi/pdf/10.1145/3461672>
- [26] Serge Egelman International Computer Science Institute & University of California et al. 2015. Scaling the security wall: Proceedings of the 33rd annual ACM conference on human factors in computing systems. (April 2015). Retrieved January 10, 2024 from <https://dl.acm.org/doi/abs/10.1145/2702123.2702249>
- [27] Retrieved January 15, 2024a from https://kar.kent.ac.uk/49093/1/Response_biases_Final_accepted_version.pdf
- [28] Chi-square calculator. Retrieved January 10, 2024 from <https://www.socscistatistics.com/tests/chisquare/default2.aspx>
- [29] Author links open overlay panelAshley A. Cain et al. 2018. An exploratory study of cyber hygiene behaviors and knowledge. (August 2018). Retrieved January 10, 2024 from <https://par.nsf.gov/servlets/purl/10083310>
- [30] Author links open overlay panelMarcus Butavicius a et al. 2022. Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails. (September 2022). Retrieved January 10, 2024 from <https://www.sciencedirect.com/science/article/pii/S0167404822003297>
- [31] Author links open overlay panelBilal Naqvi a, a, b, c, d, and AbstractPhishing attacks are among the most prevalent attack mechanisms employed by attackers. The consequences of successful phishing include (and are not limited to) financial losses. 2023. Mitigation strategies against the phishing attacks: A systematic literature review. (July 2023). Retrieved January 10, 2024 from <https://www.sciencedirect.com/science/article/pii/S0167404823002973>
- [32] Dawn M. Sarno. Retrieved January 10, 2024 from <https://journals.sagepub.com/doi/epub/10.1177/0018720821999174>
- [33] Timothy A. Salthouse. 2009. When does age-related cognitive decline begin? (April 2009). Retrieved January 10, 2024 from <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2683339/>
- [34] 2023. Cyber Hygiene explained: Common mistakes + best practices. (May 2023). Retrieved January 10, 2024 from <https://www.crowdstrike.com/cybersecurity-101/security-operations/cyber-hygiene/>

