Est. 1841 | YORK ST JOHN UNIVERSITY

What is the Level of Cyber Security Awareness Amongst Young Adults Aged 16 to 18 in the UK?

Miss Melissa Ann Forfitt

Submitted in accordance with the requirements for the degree of Master of Science by Research

York St John University

School of Science, Technology and Health

May 2022

The candidate confirms that the work submitted is her own and that appropriate credit has been given where reference has been made to the work of others.

Acknowledgements

I would like to thank Dr Aminu Usman for his continued support of my studies throughout my Master's by Research and for the feedback on my work that he has contributed. Moreover, I would like to thank Dr Beth Bell and Dr Daniel Madigan for their support and for supervising my research. The York St John University Research Office has offered tremendous support throughout my time as a Master's by Research student, supporting not only this research but the development of my personal skills and projects.

In personal acknowledgements, I would like to thank my Mum and Dad: Susan and Laurence Forfitt. My parents inspire me with the constant hard-work and ambition that they put into everything, including myself. My Nan, Ann Forfitt, has always been a firm supporter of my research, even if she still doesn't quite understand it. The final acknowledgement goes to my fiancé, Harrison Hoggarth. I will never be able to put into words the thanks I have for him, apart from saying a big thank you for his continued support, patience, and hot chocolates.

Abstract

Technology is becoming more integrated into our lives by the day. With the COVID-19 global pandemic, this has become even more prominent with society having a heavier reliance on technology. This research aimed to understand the level of cyber security awareness amongst young adults between the ages of 16 and 18 in the UK, to determine whether this age demographic understand the security risks of emerging technologies and how to react to cyber threats. The methodology for this research involved using the Human Aspects of Information Security Questionnaire (HAIS-Q) to survey young adults who live in the UK. This questionnaire covers the spectrum of cyber security by defining cyber security into seven key categories: Password Management, Email Use, Internet Use, Social Media, Mobile Devices, Information Handling, and Incident Reporting. The results of the questionnaire allowed us to assess a participant's level of cyber security awareness. In addition to the HAIS-Q questions, demographic questions related to age and gender were asked in addition to parents' education and free school meals, to determine the socioeconomic status of participants. These questions were asked as an aim of this research was to test whether a person's level of cyber security awareness is affected by their age, gender, or socioeconomic status. Participants were recruited online via forums, social media, and academic research participant recruitment boards. In total, 811 participants took part in the research, with 691 valid responses. The results of the research showed that young adults have an average level of cyber security awareness, with potential action that needs to be taken to improve the overall level of cyber security awareness. An intervention strategy is recommended to improve this level, such as providing general cyber security awareness training in schools and colleges.

Table of Contents

Chapter One: Introduction

1.1 Introduction

There is an estimated 67.1 million people in the UK (ONS, 2020). Narrowing that down, there are 2.18 million 16- to 18-year-olds in the UK. Young adults are amongst the most active of internet users, with 99% of young adults aged 16 to 24 in the UK regularly using the internet in 2022 (Ofcom, 2022). This has been especially prevalent in the recent COVID-19 pandemic (ONS, 2021). During the UK's multiple lockdowns, young adults were forced to rely increasingly on technology for tasks such as communication, entertainment, and remote learning. Furthermore, education moved from in-person learning in schools to remote learning via tools such as Microsoft Teams and Zoom (ONS, 2021). To make technology more available for those who did not have access to computers or the internet, the UK Government provided grants for families with children for computers and 4G routers to enable them to have access to the internet (UK Government, 2020).

With the rise of technology usage comes the increase of people taking the opportunity to exploit technology (Utica University, 2022). A cyber-attack is a malicious attempt of accessing computer systems, networks, or devices, including attempts to damage, disrupt or gain unauthorised access (NCSC, 2022). These attacks are carried out through a cyber means, which is the use of computers, the internet, and information technology (Merriam-Webster, 2022). Cyber-attacks can target anyone, including individuals, businesses, and charities. Some of the most common cyber-attacks involve the distribution of malware (malicious files that can implant software onto a computer), phishing (fraudulent emails that are typically

distributed in mass, which convince unsuspecting users that they are coming from a reliable source), and password attacks (in which attackers gain access to people's passwords and use them to log into the victim's accounts) (Fichtner, 2022). These are just a few of the diverse range of cyber-attacks that are being carried out every day to unsuspecting victims. The breakdown of the most common cyber-attacks that were experienced by businesses and charities can be seen in Figure 1 below.

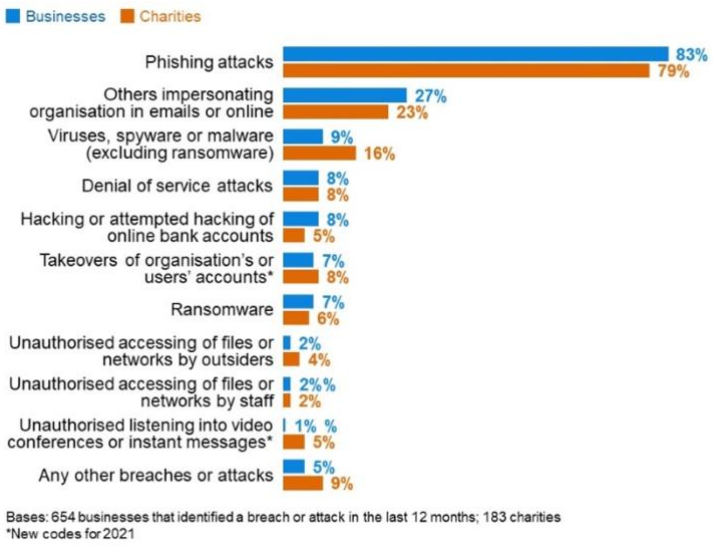

Figure 1 - Cyber-attacks experienced by businesses and charities in 2021 (GOV.UK, 2021).

Cyber security awareness is the level of which a person understands cyber security in terms of awareness of cyber threats and best cyber hygiene practices. As we become more reliant on technology, technology is becoming more available and therefore it is inevitable that there are growing numbers of technology users. With cyber-attacks becoming more sophisticated, cyber security awareness is a vital skill that is important for everyone who is engaging with technology. If a person is aware of cyber-attacks, they will be able to spot the signs of a cyber-attack and apply best practices to minimise their risk of becoming a victim. Being a victim of a cyber-attack is potentially detrimental, with the repercussions ranging from personal

financial loss to global data loss (for example, a data leak at a company). In the year 2020 to 2021, 86% of organisations in the UK fell victim to a cyber-attack (O'Driscoll, 2023). Furthermore, 71% of organisations in the UK fell victim to a ransomware attack, with 13% of organisations paying the ransom. The average cost of these ransomware attacks was $1.96 million. Despite this, just 11.2% of IT budgets of organisations in the UK is spent on security (O'Driscoll, 2023).

Whilst cyber security awareness is a vital skill for all members of society who are engaging with technology to have, this research specifically focuses on those who are aged 16 to 18 years old who currently live in the UK. The school leaving age in the UK is 16 and at this age young adults can stay in full-time education, start an apprenticeship, or work 20 hours per week whilst in part-time education (UK Government, 2022). So, at this age, young adults have finished (or are coming up to the completion of) compulsory school education and have more freedom to decide on their next steps. However, they must stay in some form of education. Therefore, it is vital to understand the level of cyber security awareness amongst young adults so that we can ensure they are being prepared for their future, whether this be university, work, or in their personal lives. With the results of this study, we can understand the extent to which young adults have a good level of cyber security awareness. A good level of cyber security awareness would indicate that they understand the risks of technology in different contexts and what the best cyber hygiene practices are for those situations. If young adults have a good level of cyber security awareness when they have finished compulsory education, these skills can be employed diversely and will help to minimise the young person's risk of becoming a victim of a cyber-attack. If young adults do not have a good level of cyber security awareness, the results of this study will highlight the areas of weakness in young adults' cyber

security awareness knowledge so that further work can be done to educate and therefore improve young adults' level of cyber security awareness. This could have a significant impact on the number of cyber-attacks that young adults fall victim to.

Currently, cyber security education is not mandatory in the national curriculum of education. However, in a survey carried out by the National Cyber Security Alliance and Microsoft in the USA, it was found that 91% of teachers wanted cyber security to be taught in schools (StaySafeOnline, 2021). With the increase in usage of technology, especially in recent times with the COVID-19 pandemic, cyber security education is vital for two key reasons. Firstly, there is a global shortage of cyber security professionals (Burrell, 2020) and therefore cyber security education would provide young adults with the foundational understanding of cyber security, and this may encourage them to pursue a career in this industry. Secondly, cyber security education would provide young adults with the awareness of cyber-attacks and the best practices for cyber hygiene.

The research done in this study will analyse the current level of cyber security awareness amongst young adults aged 16 to 18 in the UK. After statistical analysis, the results will inform us of the extent to which young adults understand how to be secure on the internet and how to handle situations that they may be faced with. The results will also show us whether there are any gaps in the knowledge and therefore if there are any focus areas that an intervention strategy is required to improve.

1.2 Research Questions

Research Questions

This research has a main research question (RQ) that we are seeking to answer. However, as cyber security awareness is a broad research area that encompasses many different technical areas and elements, the research question has been broken down into four specific questions, which are the sub-questions (SQs).

RQ: What is the level of cyber security amongst young adults aged 16 to 18 in the UK?

SQ1: How do age, gender, and socioeconomic status affect a young adult's level of cyber security awareness?

SQ2: What cyber security awareness education are young adults currently being provided and how effective is it in contributing to their level of cyber security knowledge?

SQ3: Is an intervention strategy to improve young adults' level of cyber security awareness required and, if so, how could this be done?

SQ4: What is the importance of cyber security education for young adults in protecting themselves from cyber-attacks?

1.3 Hypotheses

Hypothesis (H_1): A young adult's level of cyber security awareness is affected by their age.

Null Hypothesis (H_{1_0}): A young adult's level of cyber security awareness is not affected by their age.

Hypothesis (H_2): A young adult's level of cyber security awareness is affected by their gender.

Null Hypothesis (H_{2_0}): A young adult's level of cyber security awareness is not affected by their gender.

Hypothesis (H_3): A young adult's level of cyber security awareness is affected by their socio-economic status.

Null Hypothesis (H_{3_0}): A young adult's level of cyber security awareness is not affected by their socio-economic status.

1.4 Research Question Summary

The research question that this thesis is aiming to answer is 'What is the level of cyber security awareness of young adults aged 16 to 18 who currently live in the UK?'. In this thesis, we will be answering this question by breaking down the research into four sub questions. Firstly, we will use a questionnaire to determine how age, gender and socioeconomic status affect a young adult's level of cyber security awareness. We will use the questionnaire results and the existing literature to determine what cyber security awareness education young adults are

currently being provided and what the effectiveness of this is. We will also determine whether an intervention strategy is required to improve young adults' level of cyber security awareness and if it is, we will explore different methods of intervention. Finally, we will use the existing literature to explore the extent to which cyber security education is important for young adults. By focusing the research into these four sub questions, if we can get a sample group that is representative of the population, we should be able to determine the level of cyber security awareness of young adults aged 16 to 18 in the UK.

1.5 Thesis Outline

In Chapter One, we firstly described the background of the study in addition to the research questions. In Chapter Two, we carried out a literature review of the existing literature to determine what technology was being used by young adults at the time of the study and the extent to which this had been affected by the COVID-19 pandemic. We then explored the existing literature on cyber security awareness and then focused specifically on cyber security awareness in young adults. Then we researched different methods that exist and have been tested for validity, to test a person's level of cyber security awareness and we decided the appropriateness of the methods for determining a young adult's level of cyber security awareness. We also looked at existing cyber security awareness education that was being provided at the time of the study. At the end of Chapter Two, we looked at different intervention strategies for improving cyber security awareness, should the results have determined that the level of cyber security awareness needed to be improved. In Chapter Three, the methodology was described and carried out. This involved surveying 16- to 18-year-olds who currently live in the UK to understand their level of cyber security awareness. We captured demographic information to test the hypotheses of the research, which tested

cyber security awareness levels against age, gender, and socioeconomic status to determine whether these factors affect a young adult's level of cyber security awareness. In Chapter Four, we reported on the results of the questionnaire, reporting on the demographic statistics of the participants in addition to the results of each section from the HAIS-Q. Moreover, in Chapter Five, we discussed the results and analysed what the results mean in the wider context of cyber security and the extent to which the results are reliable and valid. In Chapter Six, we summarise the findings from the study and answer the research questions.

1.6 Ethics

This research received full ethical approval from the ethics committee on 9th June 2021 and the approval letter can be seen in Appendix A.

1.7 Chapter Summary

Chapter One introduces the thesis. The first section of the chapter introduces the background of the research, providing general information and statistics around technology use and outlines why this is an important research area. In the next section, we define the research questions that this thesis aims to answer and the specific sub questions that contribute to answering this. Following this, the hypotheses are introduced which inform what is being tested in this research. A more detailed analysis of the research question is discussed in the next section, which is followed by an outline of the thesis.

Chapter Two: Literature Review

2.1 Introduction

Cyber security is defined as the measures that individuals and organisations take to reduce the risk of cyber attacks (NCSC, 2023). Technology is a fundamental part of the modern world, with much of the world depending on it. In the year 2021 to 2022, cybercrime losses in the UK totalled to £3.1 billion (O'Driscoll, 2023).

More young people (those aged 18 and under) than ever are using the internet; about 50% of ten-year-olds in the UK have their own smartphone, with almost all children having their own smartphone by the age of 15 (Ofcom, 2020). There are unfortunately a significant number of cybercrimes that involve young people that take advantage of, for example, anonymous sharing (sending messages and images that only show for a set amount of time), emails (phishing), and video games (building relationships with strangers online) (StaySafeOnline, 2018). As young people in the UK are among the most active of internet users during their leisure-time, with 24.1% spending more than six hours on the internet on weekdays and with 37.3% spending more than six hours on the internet on weekends (Education Policy Institute, 2017), it is important that they are made aware of the cyber security threats that they may be faced with when using the internet.

The UK Government defines cybercrimes within two categories: cyber-dependent crimes (crimes that rely solely on the use of ICT) and cyber-enabled crimes (traditional crimes that are enhanced by ICT) (HM Government, 2022). An example of a cyber-dependent crime is one that utilises platforms that are only available using ICT, such as YouTube. YouTube is the video

platform of choice for those aged 15 to 25 in the UK (Statista, 2022), with 82% of those in this age demographic using the platform. Furthermore, YouTube is also the platform of choice for 5- to 15-year-olds (Ofcom, 2020). Cyber criminals take advantage of this; one YouTube-based cyber-dependent crime occurred in 2017, when seemingly innocent videos of cartoon characters which contained violence or abusive messages were being watched by children across the world. If children were not aware that the internet cannot always be trusted, then they may have been hurt by what they saw (Bernard, 2017). This highlights the importance of cyber awareness amongst young people. An example of a cyber-enabled crime amongst young adults is cyberbullying. In the academic year 2017/2018, about 7% of young people experienced cyberbullying (Department for Education, 2018). In the academic year 2019/2020, this increased to 19%, which equates to 764,000 children (ONS, 2020). As the internet is becoming more available, young people are becoming more exposed to cyberbullying (hence why this is a cyber-enabled crime: bullying is a traditional form of harassment and is being enhanced and reaching a wider range of victims by utilising technology). In a study carried out by the ONS, it was found that 52% of those who had experienced online bullying behaviours would not describe it as bullying, and 26% would not report their bullying experiences to anyone (ONS, 2020). This is a high percentage and highlights that it is important for young people to know what the signs of online bullying are and how to report these experiences.

2.2 Pandemic Technology Utilisation

During the COVID-19 pandemic, technology has been more vital and utilised than ever before (Statista, 2020). A dependency was developed on technology for work, study, and socialising (De' et al., 2020). A study (Chandra et al., 2020) published in the year of the first COVID-19

lockdown carried out a risk assessment using the fuzzy failure mode and effects analysis (FMEA) method with a sample of work-from-home activities. The activities that returned with the highest risk values (medium to high risk) were video conference activities, social media communication, application downloads, and website access (Chandra et al., 2020). These are all activities that require an internet-connected device and an internet connection. Each of these activities has associated cyber-attacks that exploit the task. For example, video conferencing typically uses webcams and microphones to allow for communication. If software does not use end-to-end encryption, there is opportunity for an attacker to intercept the connection and eavesdrop on the call (Kapersky, 2022). Over the lockdowns when dependency of video conferencing software was at a peak, there was an increase in 'Zoom bombings' where attackers joined calls shouting abusive language (Forbes, 2020). Social media can be exploited by attackers from several perspectives: from accessing accounts due to insecure passwords to sending harassment from anonymous accounts. Due to the social nature of platforms such as Twitter and Instagram, social engineering can be used to obtain personal information such as identifying information about a person's workplace, home address, or even what the name of their pet is. All this information can be valuable for attacker when making a 'profile' of a victim. For example, the name of their pet could be the answer to a security question for one of their online accounts (Woods, 2020). It can be risky to download applications from the internet as there are typically many sources and locations where you can download the file you want from. It is important to download applications from the most trusted sources (for example, downloading Microsoft Teams from the Microsoft website). This is to ensure that downloads are legitimate and do not contain malicious software, such as malware. There are also cyber-attacks known as 'drive by downloads' which install malicious software to a computer without a user having to do

anything; the software silently installs in the background (Kapersky, 2022). With the national lockdowns imposed in the UK, all these activities were being carried out more due to the higher dependency on technology.

Education is compulsory for everyone in the UK up to and including the age of 18 (UK Government, 2022). Therefore, when the COVID-19 pandemic lockdowns were enforced, this meant that education had to move from in-person teaching to online teaching. Young people were therefore required to access their education through video conferencing software (for example, Microsoft Teams and Zoom). Social media was more heavily relied on for keeping connected with friends and family. One study carried out surveyed 260 parents to determine the extent to which them and their child(ren)'s technology and social media usage had changed because of the pandemic. The results showed that most parents and their children had increased their use of technology since the start of the pandemic (Drouin et al., 2020).

In the UK, the Department for Education have provided more than 1.3 million devices to help disadvantaged pupils and students access remote education throughout the pandemic (GOV.UK, 2021). Due to this, more young people than ever before had access to technology and the internet; technology was more available and was more relied upon. Whilst technology becoming more available has great benefits in terms of accessing remote education, socialising and entertainment, there are also associated risks with this. Those who have not had access to technology before may not therefore have been exposed to cyber security risks before. This highlights the importance of analysing the level of cyber security awareness amongst young adults as this will provide us with the information of whether there are any gaps in young adult's cyber security knowledge. If gaps in young adults' cyber security

awareness knowledge does exist, then we can identify what these gaps are and develop intervention strategies to reduce them.

2.3 Cyber Security Awareness

Cyber security awareness is the level at which people understand cyber security threats and their associated risks. In a world that is growing in its technology dependence, cyber threats are becoming more prominent. With the COVID-19 pandemic and more people than ever before using technology from home, cyber criminals are taking advantage of this and so more than ever it is important for the end users of technology to be aware of cyber security and how to stay safe online. In fact, most internet users experience cyber-attacks on their privacy and identity on a daily frequency, likely without the user's awareness. Some of the activities that cyber criminals are becoming more advanced at concealing include (but are not limited to): mining and misusing data, bullying, victimisation, terrorist radicalisation, and sexually motivated grooming (Springer, 2018).

In the context of the working environment, it is important for employees of an organisation to have a good level of cyber security awareness as they play a key role in their organisation's security. In the Global State of Information Security survey carried out in 2018, 9500 businesses were interviewed from 122 countries, with 560 of these from the UK (PwC, 2018). It was discovered that in the UK, 28% of businesses do not know how many cyber-attacks they have had, and 33.3% do not know how the cyber-attacks happened. Cyber-attacks are costly for businesses, with an average financial incident cost of £857,000 in the UK. Furthermore, 17% of respondents said that their organisation does not prepare or drill for cyber-attacks (PwC, 2018). Organisations that do not provide adequate cyber security training for their

employees are prone to many risks, including transmission of malware from personal devices to the organisation's infrastructure, poor incident reporting culture and external attacks. One key strategy to manage these risks is to maintain user awareness of cyber security risks and regularly assess employee security skills (NCSC, 2019).

Cyber security awareness is important not only from a business perspective, but also an individual perspective. Research carried out in Malaysia determined that the level of cyber security awareness of Malaysians was low and that 99% of successful cyberattacks in Malaysia were due to human error (Ariffin et al., 2020). Another study carried out on the cyber security awareness of people in Bangladesh surveyed 400 computer-literature adults of various backgrounds. The results of this study showed a low level of awareness, with the population being unaware of cybersecurity policies and practices (Ahmed et al., 2019). Moreover, a quantative cyber security awareness study carried out in Saudi Arabia had similar results, finding that participants have a very limited awareness of cybercrime threats, best cyber security practices, and how their information is secured across the internet (Alotaibi et al., 2017). From these studies, it is evident that there is a low level of cyber security awareness across the globe.

2.4 Cyber Security Awareness in Young adults

Very little research has been carried out so far in the realms of cyber security awareness in young adults in the UK. The research that has been carried out thus far suggests that cyber security material that is being taught in schools is poor and limited. This is demonstrated through a study (Brittan et al., 2018) carried out in 2018 which aimed to examine 'the effect of early education on cyber security awareness', by surveying teachers across the UK. The

results showed that just 30% of ICT teachers hold a relevant ICT degree or higher, with 49.6% of ICT teachers holding no relevant ICT qualification post A-Level (Brittan et al., 2018). This suggests that ICT is neglected and those teachers who teach ICT are not specialists in that subject area. It was found that very little cyber security awareness is being taught in schools, with the focus on teaching coding. Cyber security awareness is usually taught to those students who are going to study GCSE (or equivalent) Computer Science, with only 12% of students choosing to study Computer Science at this level, as opposed to cyber security awareness education for all (Brittan et al., 2018). This research surveyed teachers, not the young adults themselves, and so cannot accurately suggest the cyber security awareness level of young adults in the UK.

There have been several pilot studies across the world that aim to understand the level of cyber security awareness amongst the young people in different countries. One pilot study carried out in Australia involved conducting interviews with preschool children aged 4 to 5 years old, to understand what young children think the internet is. The interview was constructed in two parts: the first testing the child's technology and internet recognition, with the second part testing the child's cyber-safety awareness. Interview techniques including showing the children visual pictures to help them understand the question and traffic light systems were used to record the child's response. The results from the pilot suggested that the questions designed did not provide a sufficient opportunity for children to explain their understandings of the internet and cyber-security, and questions should have been more direct, putting the child into the scenario, not a character (Dodge et al., 2011). This shows that when researching cyber security awareness, the questions need to be designed so that they are understandable but still provide an opportunity for participants to explain their

understanding. As the participants in this research (aged 16- to 18-years-old) are significantly older than those in the pilot study (aged 4- to 5-years-old), this balance will be of less importance as participants should be able to read the questions themselves without visual aid, however, it is still an important consideration for ensuring the research is accessible to those with disability (for example, learning difficulties) and inclusivity (for example, those who cannot read or write).

Much research carried out on the topic of cyber security awareness of young people has focussed more on the people that young people are surrounded by (for example, their teachers and parents) rather than the young people themselves. A study in Malaysia (Ahmad et al., 2018) surveyed 872 parents of children aged 17 and under to understand their level of cyber security awareness. The results from this study were that 80.5% of parents were found to have awareness and knowledge of potential threats that their children could experience online (Ahmad et al., 2018). This is a positive result and shows that parents know what their child may experience when on the internet. The limitations of this research are that despite parents being aware of online threats, they may not know how to deal with them if their child was to experience them online. Furthermore, we cannot conclude the online safety of children from this as we do not know whether parents monitor their children's internet activities and we do not know how aware children are of the threats themselves.

One study that was carried out in Nepal tested to find the cyber security awareness level of teenagers aged 13 to 19 years old in the country (Adhikari, 2018). This study surveyed students across five different secondary schools in Nepal. Participants were provided a structured questionnaire to complete that contained cyber security-related questions.

Statistical analysis was carried out to determine the results. The results of the research showed that most teenagers use strong passwords, however they do not change them often. Furthermore, the results showed that most teenagers use social media and they use long passwords to protect these accounts (Adhikari, 2018). Whilst it is good that teenagers use strong passwords, a limitation of this research is that a strong password has not been defined here. Different organisations have different views on what makes a strong password, for example the NCSC recommends that strong passwords should be made up from 'three random words' (NCSC, 2021). Furthermore, there is a broad developmental age gap between 13 and 19 years old. In this research, we will be focusing on 16 to 18 years old so that we can understand the level of cyber security awareness in-depth for this narrower age demographic.

2.4.1 Cyberbullying

One area that is encapsulated within cyber security awareness amongst young adults is cyberbullying. According to research carried out by ONS, 19% of children aged 10 to 15 in the UK experienced at least one type of online bullying behaviour in the academic year 2019/2020 (ONS, 2020). It was found that the most common type of online bullying was name-calling, swearing or sending insults, with 10.5% of 10- to 15-year-olds experiencing this, shortly followed by nasty messages with 10.1% of the demographic experiencing this (ONS, 2020). Between 2018 and 2020, it was reported that 19.2% of all bullying globally happens through social media, with a further 11% through text messages and a further 7.9% of cyberbullying happens via video games (Comparitech, 2020).

Cyberbullying is especially prevalent with the rise in usage of social media. YouTube is the most popular social media platform, with 82% of 15- to 25-year-olds using it. This is followed

by Facebook at 80%, WhatsApp at 79% and Instagram at 76% (Statista, 2020). The full graph of social networking sites used by 15- to 25-year-olds can be seen in Figure 1. In one study in the USA, it was found that 60% of parents with children aged 14 to 18 reported that their child had been bullied in 2019. In the same study, it was found that 20% of all bullying happens through social media (Comparitech, 2022). In 2018, it was reported that 59% of teenagers living in the USA had been bullied or harassed online, meaning that the majority of teenagers have experienced cyberbullying (Pew Research Center, 2018). Research carried out during the COVID-19 pandemic determined that the pandemic had a direct effect on the rise of cyberbullying on Twitter. In total, 456,046 tweets were analysed which showed a direct link between cyberbullying incidents and the pandemic (Karmakar et al., 2021). This shows that a key area that this research needs to include is social media as it is so prevalent in young adults' online lives.

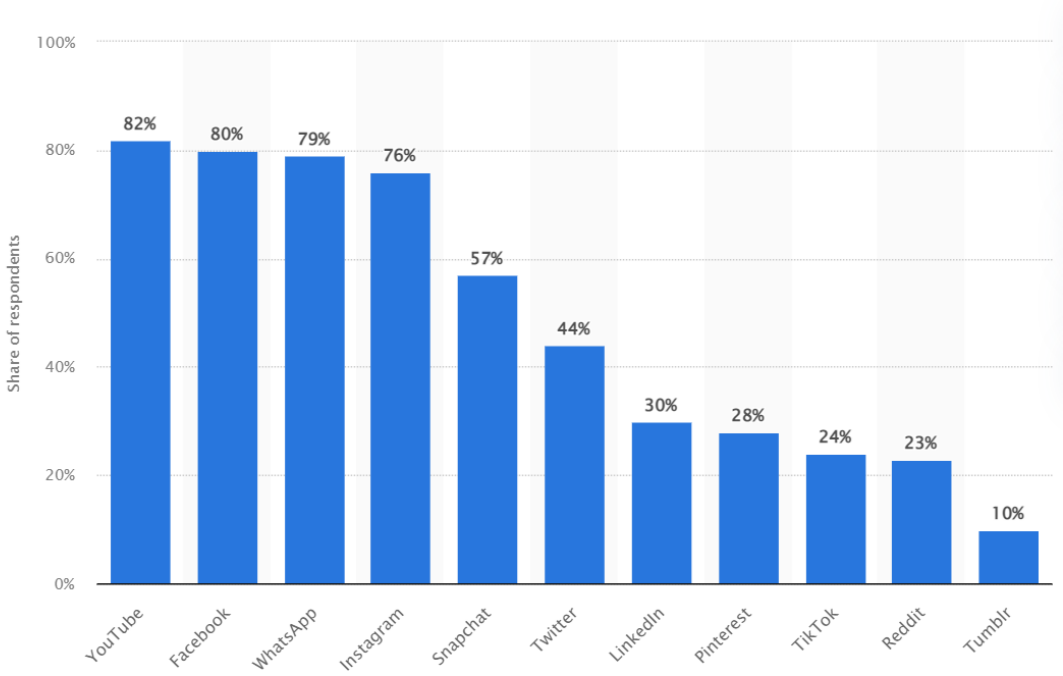

Figure 2 - Social networking websites used by 15- to 25-year-olds in the UK (Statista, 2020)

One study carried out in Turkey aimed to determine the level at which teachers are aware of cyberbullying. During the 2012-2013 academic year, 184 teachers were surveyed, with the results showing that teachers have an 'average' level of awareness of cyberbullying, with different awareness levels depending on gender and how often the teacher uses the internet. Recommendations were made from such research that students need to be made more aware of these issues to ensure that they know how to identify cyberbullying and how to handle the situations, should they arise (Sezer et al., 2014). A more recent study carried out in Australia in 2020 tested 105 teachers and parents in the primary school community on their perceptions of bullying and cyberbullying. The results found that almost one fifth of adults were unable to identify when scenarios were incidents of bullying, and 60% - 80% of participants called a scenario bullying when it was not (Campbell, 2018). The results from both studies suggest that teachers are not as knowledgeable on cyberbullying as they perhaps should be, especially as cyberbullying affects so many young adults. If teachers are not aware of cyberbullying, then they are likely to miss the signs of it. Being able to detect early signs of cyberbullying would allow the situation to be dealt with before it escalates and feels uncontrollable for the victim. Safeguarding is a key element of protecting children and young adults in schools and colleges. The 'Keeping Children Safe in Education' document published by the Government provides a list for teachers of websites that teachers and parents can visit to obtain information on how to keep young people safe online. This list includes websites such as Childnet (www.childnet.com), NSPCC (www.nspcc.org.uk), and the NCSC (www.ncsc.gov.uk) (Department for Education, 2021). It is vital that teachers understand the best practices of online safety so that teachers know what support to provide in those situations.

2.5 Measuring the Level of Cyber Security Awareness

Cyber security is a broad subset topic of technology that applies to every aspect of it. Due to this, there are many different areas of cyber security that can be focussed on in research. For this research, we want to gain an understanding of the level of general cyber security awareness; covering a broad spectrum of topics to gain an overall understanding of the level. Therefore, we need to ensure that the method that we use encapsulates all the different domains of cyber security. The domains of cyber security include password management, email use, internet use, social media, mobile devices, information handling, and incident reporting. To have a good overall level of cyber security awareness, a person should have a good knowledge of cyber hygiene measures for each of these domains. As cyber security awareness is a broad topic, a mixed-methods approach (collecting both quantitative and qualitative data) could be beneficial here, to provide a holistic view of the current level of cyber security awareness. Studies that use a mixed-method approach provide us with more context and a deeper understanding (Hanif et al., 2021). Therefore, this should be considered when determining the method which is going to be used to measure the level of cyber security awareness.

2.5.1 Human Aspects of Information Security Questionnaire (HAIS-Q)

Upon carrying out the literature review, it was evident that a method that can be used to measure the level of cyber security awareness is the utilisation of the Human Aspects of Information Security Questionnaire (HAIS-Q). The HAIS-Q was designed to be a valid and reliable method of testing and quantifying a person's level of information security awareness. The questionnaire covers seven topic areas that are encompassed within the cyber security

domain. These areas were derived from studying information security policies, interviews, and surveys and were designed to be relevant to computer users and those who are prone to non-compliance (Parsons et al., 2014). The areas are: password management, email use, internet use, social networking site use, mobile computing, information handling, and incident reporting. The HAIS-Q covers each of these topics from the three dimensions of knowledge: knowledge, attitude, and behaviour, to gain a full understanding of a person's thoughts and feelings towards policy and procedures (Parsons et al., 2013).

The questionnaire has been tested on several groups of people, including employee participants in a work context. One study (Zulfia et al., 2019) used the HAIS-Q to test their employees' levels of cyber security awareness. The results of this study showed that their employees have a sound understanding of information security, however the HAIS-Q highlighted some key areas that the organisation needs to improve their employee's practices on, including clicking on links and downloading files. This indicates that a benefit of using the HAIS-Q is that it can show exactly what areas people have a strong knowledge in and what areas people have a weaker knowledge in, as the HAIS-Q is broken down into the seven areas. This could be very valuable for organisations as cyber security awareness training can then be more tailored to the employees' needs (Zulfia et al., 2019). A similar study (Cindana et al., 2018) used the HAIS-Q to understand their employees' level of cyber security awareness; the results show that their employees have a good understanding of knowledge (with a score of 87.59). However, the results of the HAIS-Q indicated that the weaker area of knowledge in these particular employees is internet usage (Cindana et al., 2018). Again, this shows that a strength of the HAIS-Q is that it can locate exactly what areas of knowledge an organisation's

employees are weaker in, in addition to showing the areas that employees have a strong level of knowledge of.

An important part of any methodology is the validity of it. This means to what extent does the study's results represent the actual results of the population; how accurately does it measure the variables. In the case of the HAIS-Q, for it to be a successful method of testing a person's level of cyber security awareness, it must accurately represent that person's level of cyber security awareness. One study (Parsons et al., 2017) tested the validity of the HAIS-Q by comparing the participant results of the HAIS-Q to participant results of a phishing experiment. The study proved that the HAIS-Q has convergent validity as those participants who scored higher on the HAIS-Q also scored higher on the phishing experiment. Another study (Parsons et al., 2017) carried out by the same researchers tested the construct validity of the HAIS-Q by providing the questionnaire to 505 working Australians and carrying out statistical analysis of the results. The results of this second study showed that the HAIS-Q is a reliable measure for testing a person's level of information security awareness (Parsons et al., 2017). Another study carried out aimed to test the reliability of the HAIS-Q for employees in a working context (McCormac et al., 2017). The study applied a test-retest approach to understand the reliability of the HAIS-Q. With a sample size of 197, this is a limitation to this research as it is close to the lower limit of recommended precision (200 to 400 participants). Despite this, the results of the study showed that the HAIS-Q is externally reliable and internally consistent, in a workplace context. As a result of these validity tests on the HAIS-Q, we can establish that the HAIS-Q is an appropriate option to measure a person's level of cyber security awareness and is one that could be considered for the purpose of this research.

A potential limitation of the HAIS-Q for the purpose of this research is that the questionnaire consists of 63 questions. This is likely to be a significant time commitment for potential participants, and so could dissuade young adults from wanting to participate in this research. Furthermore, the attention span of a teenager is less than that of an adult's (Brain Balance, 2022) and so this needs to be considered when developing a method that is appropriate for the age demographic of the research. Another limitation of the HAIS-Q is that it is been tested and used primarily in the workplace. Whilst carrying out the literature review, no research was found on the HAIS-Q being used to test a young adult's level of cyber security awareness. This could affect the validity and therefore reliability of the results, so extra statistical tests (such as Cronbach's Alpha which compares variance to assess reliability) would have to be run to ensure the reliability of the results.

2.5.2 Alternative Questionnaires

There are many different questionnaire approaches that can be taken to analyse a person's level of cyber security awareness. Research carried out in Saudi Arabia aimed to measure the level of cyber security awareness for cybercrime in the country, as the country had recently had a reported increase in cyber-attacks (Alzubaidi, 2021). The research involved developing a questionnaire to test the population's level of cyber security awareness, by breaking down what 'cyber awareness level' means into three main sections: how the participants behave when accessing the internet; how participants feel about best security practices and cybercrime; and how participants react when they are faced with a cybercrime situation. The questionnaire was tested for validity and reliability using the Content Validity Index ad Cronbach's alpha. Ultimately, the results of the research showed that there are significant improvements required to increase the population's level of cyber security awareness. As a

result of the research, further work can now be carried out to develop an effective program to increase the cyber security awareness level of the population (Alzubaidi, 2021).

2.6 Cyber Security Awareness Education

To provide young adults with the skills and knowledge that they need to handle issues that may arise whilst they are using technology and the internet, it is essential that young adults receive cyber security awareness education. One study carried out in the USA researched the need for this education at different levels, within it highlighting the importance of students being exposed to cyber security from a young age, with a focus on data privacy and general cyber security (Ahmad et al., 2021). The aspects of cyber security that are taught within this education will shape what a young adult knows about cybercrime and the best cyber hygiene practices to follow to reduce their risk of becoming a victim of a cyber-attack. Cyber security awareness education is important not only for aiding the prevention of falling victim to cyber-attacks, but also for the reaction in case they do fall victim. If a young adult is aware of the appropriate action and steps to take should they face being a victim of a cybercrime, they will be better equipped to handling and regaining control of the situation with confidence.

It is clear from the literature review of the significant investment that the National Cyber Security Centre (NCSC) is putting into schools in the UK. This investment is in terms of cyber security education. The NCSC has introduced many schemes into schools, for example the CyberFirst scheme, which has introduced cyber security to over 56,000 11- to 17-year-olds (NCSC, 2023). The NCSC has also done work to aim to reduce the gender divide in cyber security, with the CyberFirst Girls Competition, exclusively for girls. These programmes are designed to get young people into cyber security and introduce them to the potential future

careers that they could have in cyber security, teaching them skills such as forensics, ethical hacking, and cryptography (NCSC, 2021). Furthermore, it was reported in 2017 that the Department for Digital, Culture, Media, and Sport (DCMS) was starting a cyber security training programme for schoolchildren aged 14 to 18 years old, with the government investing £20 million into the programme (Flinders, 2017). The focus of these programmes is to reduce the skills gap in the cyber security workforce by introducing young people to cyber security as a career, as opposed to general cyber security training for all (without the career-focussed aim). This research focuses on more general cyber security awareness, with the aim of understanding the overall understanding of cyber security awareness of young adults aged 16 to 18 years old, regardless of whether they wish to pursue a career in cyber security.

Research has been carried out in several countries across the world to determine the level of importance that cyber security education holds, with further research being carried out to determine what cyber security awareness education children are currently being provided. A study called 'Cyber security education is as essential as "the three R's"' (Ventera et al., 2019) shows the results of the results of the research through the title alone. The research was carried out in South Africa and discovered that there is no formal educational curriculum that addresses cyber security in South African schools. As you can see in Figure 2, it was found that 80% of children in secondary school own smartphones, however children are completing secondary school with no formal cyber security education. Only those who go onto studying Computer Science at university level receive cyber security education as part of their course, which shows that not everyone is receiving the level of cyber security education that is required to be secure in today's technological world (Ventera et al., 2019).

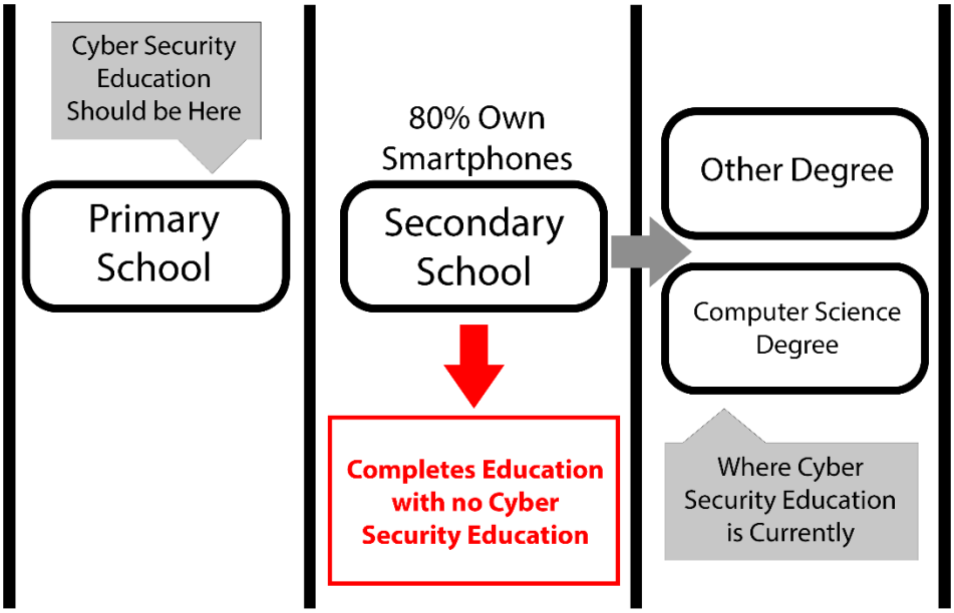

Figure 3 - The reconsideration of the security education approach in South Africa (Ventera et al., 2019)

2.6.1 Gamification of Cyber Security Education

One study carried out in Norway (Quayyum, 2020) analysed how cyber security education could be provided through gamification; targeting 13 to 16 year olds (as these are the more likely age category to have access to multiple internet-connected devices and engaging in risky behaviours online), the study outlined that games are currently being used to teach children cyber security awareness, for example 'Cybersecurity Lab' and 'The Internet Safety', which teach children cyber security skills and internet safety skills respectively through games. Whilst the study is a work-in-progress, it was concluded that, as games are currently used in some cyber security awareness education, this provides many more innovative and creative opportunities to improve how this education is provided to children. The researchers are currently designing a tool to make cyber security awareness education through gamification efficient, motivating, and sustainable (Quayyum, 2020). Moreover, the NCSC have developed a game called 'CyberSprinters', which is aimed at 7- to 11-year-olds. This

game teaches children key cyber security terms and presents them with scenarios in which they must select the most appropriate response for (NCSC, 2022). This is designed to teach cyber security in a fun and interactive way. Whilst these games are an engaging way to teach cyber security education to young people, no data was found when carrying out the literature review to determine how many young people had played the game and how many schools had incorporated the game into their ICT or computing lessons. It could be interesting to also determine how effective the game is, for example by surveying children before and after playing the game to see what children have learned from the game. This could be done over several sessions, too, to determine the longevity of the learning and knowledge.

2.6.2 Cyber Security Awareness Resources

Carrying out a quick search on the internet can result in many different cyber security awareness resources, each targeted at different social groups and demographics. For example, the NCSC have dedicated cyber security information for different groups of people. These include individuals and families; self-employed; small and medium organisations; large organisations; public sector; and cyber security professionals (NCSC, 2022). The most relevant section for this research is 'individuals and families'. Here, the NCSC has produced a special website called 'Cyber Aware', which shares clear actions that individuals should take to improve their cyber hygiene (NCSC, 2022). These include actions such as using three random words to create a strong password and turning on 2-step verification to improve the security of email accounts (NCSC, 2022). The information on this website is clearly presented, however individuals would have to be actively seeking cyber awareness information to find this information. It is likely that those who are seeking this information already have at least a sound understanding of what cyber security and cyber hygiene is.

For children and young people, there are several video resources on YouTube that aim to provide cyber security training. On the whole, these videos are short, have a main character and cover the fundamentals of staying safe on the internet. On the Malwarebytes YouTube channel, there is a 3-minute video for children that talks about the dangers of the internet (Malwarebytes, 2020). It starts with a character called 'Dr Evil' who can take control of children's computers, hack passwords, and steal your computer. The video ends with a good character who tells children how to prevent 'Dr Evil' from achieving his aims. The video uses scare tactics to show children the dangers of the internet (Malwarebytes, 2020). Another 5-minute video of a similar nature is based in India and follows the life of a schoolgirl, 'Alia'. It has a friendly approach and covers a wide range of topics (including viruses, firewalls, passwords, and bullying) (WNS Global Services, 2019). These videos show that there are several different approaches to educating young people about cyber security awareness, mainly from either a scare tactic approach or a friendly approach. Further research could be done in this area to determine to what extent is each approach effective.

The UK Safer Internet Centre have published cyber security resources specific for 11- to 19-year-olds, which provides top tips on how to stay safe on the internet (UK Safer Internet Centre, 2022). Furthermore, it provides signposting links to other trusted websites (for example, CEOP) that young people can access to obtain more information on cyber security (UK Safer Internet Centre, 2022). CEOP (Children Exploitation and Online Protection Command) is part of the National Crime Agency and works to protect young people from online child sexual abuse. The CEOP website is part of the programme to provide education and training for those aged 4 to 18 years old. The website provides a diverse range of

information from outlining the qualities of a healthy relationship to educating about what sexual consent is (CEOP, 2022). This information is easy to access through the website, however similar to the NCSC, the information is online so young people would have to actively seek this information to find it. Furthermore, they would require access to an internet-enabled device and internet connection.

2.7 Improving Cyber Security Awareness

Several studies have been carried out to test how we can improve a user's decisions when it comes to making decisions around safety and security on the internet. One group of researchers carried out two experiments to determine how the visual design of network data could support an internet user in making decisions around their privacy and security (Carroll et al., 2020). The first experiment surveyed participants to understand how they feel about their own online privacy and security and how it might be improved. The second experiment used a visual design of a Network Denial of Service (DoS) attack to determine the uncertainty level of participants. This tested different ways of visually representing the DoS attack, for example manipulating hue, saturation, blue, and jaggedness to see if varying the visual displays of network data effects student perception of cyberattacks. The participants involved in the research were 17 postgraduate Computer Science students (six female and ten male participants) between the ages of 18 to 45. The results of the research showed that, overall, people are becoming more concerned about their privacy and security online and that focus-based techniques and geometry-based techniques were easier to understand on a visual representation of a DoS than colour-based techniques. A limitation of this research is that all the participants were from a Computer Science background and so the results from this

research are not representative of the general population, as those involved have a strong technical background (Carroll et al., 2020).

2.7.1 Improving Cyber Security Awareness Through Games

One approach to improving cyber security awareness is through gamification and serious games. Several games have been developed to utilise gamification to teach cyber security, including Elevation of Privilege (Microsoft), Protection Poker (Williams et al., 2010), and Hacker ThinkFun. These games are designed to make cyber security education engaging in a different context to conventional learning. They are designed to promote best cyber security practices, for example Protection Poker instils the best practice of 'building in' cyber security instead of adding security in post-development (Louis et al., 2019). Several serious games have been developed to improve cyber security awareness. These include CyberCIEGE (developed by the US Naval Postgraduate School) and PERSUADED (Aladawy et al., 2018). One paper (Hart et al., 2020) reviewed these games and identified that these games do not convey the breadth of cyber-attacks and defences to players, do not allow players to practice offensive and defensive skills, and they are not easily adaptable. So, they developed a new game called 'Riskio' (Hart et al., 2020). This is a tabletop card game that aims to increase the level of a player's cyber security awareness and has a target audience of people who work in industry and do not have a technical background. The game was tested with two groups of people: employees with no technical background and university students who needed to learn cyber security as part of their course. Results of the study showed that employees were more confident than students that this game can increase their level of cyber security awareness, possibly because the students could not find the game relatable (as it was set in an industry office context). In future studies, the game could be adapted to have a context

which matches the background of the players (for example, a university environment for university students) to make it more relatable and therefore potentially a more useful educational tool (Hart et al., 2020). Research has also been carried out to test the most effective platforms to run cyber security awareness games on. One study determined that mobile gaming applications are an effective method of creating cyber security awareness (Alotaibi et al., 2016). As this is a developing area, future research could be done to compare the effectiveness of these different platforms, for example comparing tabletop card games to mobile devices.

2.7.2 Intervention Strategies

If it is determined that the level of cyber security awareness needs to be improved, then an intervention strategy would be required. This is a strategy designed to intervene and provide the required education in an effective way to provide an improved, successful outcome. One research paper that was published in 2018 (Amo et al., 2018) tested cyber security intervention strategies for teenagers. In this research, two studies were carried out to determine the most effective teaching method that can be used as an effective intervention strategy. The first study involved 79 students taking part in a cyber security workshop, completing a questionnaire both before and after the workshop. The workshop focused on computer networking; however, participants did not actually use any technology in the workshop. In the second study, 34 participants took part in week-long lessons where they used technology to complete tasks such as building their own websites and defending themselves from cyber-attacks. Questionnaires were completed at three points throughout the week. The results of the research showed that the second study had more positive cyber security self-efficacy for females relative to males (Amo et al., 2018). Therefore, longer and

more involved workshops that utilise technology could have more successful outcomes than short, one-off workshops. Whilst this study had a focus on cyber security careers (reducing the skills gap in the cyber workforce), the same principles could apply to cyber security awareness training. If the results of this research show that an intervention strategy is required to improve the level of cyber security awareness, an effective method could be to have regular workshops that involve the use of technology.

2.8 Summary

From the literature review, it is evident that cyber security awareness is an emerging topic that has an increasing number of studies being carried out in the area. We can understand from the literature that cyber security awareness is the level of which people understand the threats associated with technology and preventative measures that can be taken to protect against cyberattacks. A low level of awareness would indicate a high susceptibility to cyberattacks, meaning that a high level of awareness indicates a sound knowledge of preventative measures thus reducing the susceptibility of falling victim to a cyberattack. Currently, little research has been carried out on the level of cyber security awareness of groups within society, with even less research being carried out specifically on the level of cyber security awareness of the UK population. It is therefore important that research to determine the level of cyber security awareness of the general population and groups within that population is carried out, so that we can understand whether any gaps exist within that knowledge and, if required, an appropriate intervention strategy can be developed to reduce these gaps. Furthermore, if any gaps do exist within the knowledge, further research can be carried out to determine how these can be reduced (if not eliminated) from earlier stages within the development of a person's cyber security knowledge. For example, if cyber security

education can be provided at a younger age (in schools), this may result in a greater level of cyber security awareness by the time that children are of school leaving age. From carrying out this literature review, it was clear that there exists a gap in research for cyber security awareness amongst young adults. There was minimal existing literature on the cyber security awareness of children and young adults. Whilst this research is focussing on the level of cyber security awareness amongst young adults, more research needs to be done in the future to also test the level of cyber security awareness amongst children, to fully develop this research area and have a thorough understanding of the education that children and being provided and the effectiveness of this education. The research in this study is short-term, with participants only being required to participate for the duration it takes them to complete the questionnaire. In future research, longer studies could be carried out that follow children from youth to young adulthood, to obtain exact results on cyber security education and its effectiveness. This could also test the longevity of knowledge gained over years.

2.9 Chapter Summary

Chapter Two provides a review of the existing literature that exists within this research area. The first section is an introduction to the literature review, outlining what a cybercrime is and the different types of cybercrimes that young adults are susceptible to. Next, the utilisation of technology is discussed in the context of the pandemic. This discusses how technology usage has changed due to the COVID-19 pandemic. The topic of cyber security awareness is then discussed in a general context, with a review of the literature and studies that have contributed to cyber security awareness research. This is then reviewed from a narrower perspective, specifically looking at cyber security awareness amongst young adults, the topic of this thesis. Within this, we review the literature that exists on the topic of cyberbullying.

Next, we review the methods that have been used to measure a person's level of cyber security awareness. It is here that the Human Aspects of Information Security Questionnaire (HAIS-Q) is introduced. Cyber security awareness education is discussed in the next section, looking at the different approaches to education and the resources that have been used to educate people on the topic of cyber security awareness. Next, we review the literature on improving cyber security awareness, where we also review research that has been done through gamification of cyber security awareness education and viable intervention strategies.

Chapter Three: Materials and Methods

3.1 Materials

The aim of this research is on the human aspect of cyber security, with the focus of the research around humans and their knowledge and understanding of cyber security. As a result of this, the research required very few materials. The full list of materials required for this research is outlined below.

Hardware:

- **Computer (Laptop: Macbook Pro M1, macOS Big Sur)** – The computer was used to create an online questionnaire that can be provided to participants. The questionnaire was online to enable it to be as accessible as possible, maximising the outreach for this research. Furthermore, a computer was required to access the data that had been collected from the questionnaire, carrying out statistical analysis of the data, and for reporting the results.
- **Internet-Connected Device** – As the questionnaire was online for this research, to participate, participants required a device that could connect to the internet. This could be in the form of a mobile phone, tablet, or computer. Participants were provided with a URL (in the form of a link/QR code) that they could use to access the questionnaire via their device. We also used various mobile phones, tablets, and computers to test that the survey worked as expected before it was sent to participants.

Software:

- **Qualtrics Software** – This is the software that we used to create the questionnaire that was provided to participants (that tested their level of cyber security awareness). Using this software, we could create an online questionnaire by inputting the questions that the participants were required to answer. This could be in the form of a quantitative or qualitative response. All of the required information that the participant needed was built into the questionnaire. This included the participant information sheet, consent form, and the debrief. The participant had to consent to taking part in the research by selecting a checkbox to confirms their consent. If a participant did not consent, they were taken to the end of the questionnaire, to the debrief page. The output of this software was a website link that was distributed to participants that, when accessed, provided them with the participant information sheet and the inputted form of the questionnaire that they could then complete.
- **QR Code Generator** – This is an online website that was used to generate a QR (Quick Response) code that could then be used to distribute the questionnaire. The questionnaire (that was created on Qualtrics) was online and was accessed via a website link, however this software could turn the website link into a QR code that could be used in various formats to promote the research, such as on a poster.
- **Canva** – This is graphic design software that was used to design and create graphics to promote the research to potential participants. The posters created on this software were bright and colourful so that they were eye-catching to the age demographic of the research. The QR code that was generated using the QR Code Generator software was present on the posters that were designed using Canva. The created posters were

distributed on social media platforms to promote the research to potential participants.

- **Outlook** – This is communication software that was used for sending emails to get into contact with potential schools, sixth forms, and colleges to ask if they could promote the research through displaying the posters around the institution. This software was also used to get into contact with any online platforms that were able to help recruit participants, such as 'Call for Participants'.
- **Social Media** – Several social media platforms were used for promoting the questionnaire to aid in the participant recruitment process. Platforms that could be used to find and target specific age demographics ('subreddit' forums on Reddit and 'hashtags' on Twitter) were used for this research.
- **SPSS** – This is statistical software by IBM that was used to carry out the statistical analysis of the data that accumulated from the questionnaire responses.

3.2 Methodology

For this research, a questionnaire was developed which was used to analyse the participant's level of cyber security awareness. To understand what the level of cyber security awareness of 16- to 18-year-olds is in the UK, the following methodology was used.

The steps of the method are as follows:

1. The first step was to research what current questionnaires exist for determining a person's level of cyber security awareness. Upon carrying out this research, we discovered the Human Aspects of Information Security Questionnaire (HAIS-Q)

(Parsons et al., 2013) which had been tested for reliability and validity in previous studies. Therefore, we decided it was appropriate to use the questions from this questionnaire for this research.

2. Next, we had to determine whether the HAIS-Q needed to be adapted to be appropriate for the target age demographic (16- to 18-year-olds). As the HAIS-Q consists of 63 questions and is primarily aimed at employees, we decided it was appropriate to take a subset of the HAIS-Q questions to reduce the amount of time it takes for a participant to complete the questionnaire and to reduce the length of attention required to dedicate to completing the questionnaire.
3. Then, the questionnaire had to be put onto a platform where it could be accessible for participants to complete (for example, on an online questionnaire website). In this research, we used the Qualtrics Software. The participant information sheet, consent form, and debrief were all built into the questionnaire, for the participant's ease and convenience.
4. Once the questionnaire had been developed, the next step was to design and develop promotional material to aid in the next phase of the research, which was the participant recruitment. Using graphic design software (in this study, we used Canva), posters were created that could be promoted on social media and around schools, sixth forms, and colleges.
5. The next phase of the research was the participant recruitment, which was carried out over a period of 6 months. For this, schools, sixth forms, and colleges were contacted via email to ask if they could promote the research to their students and display the posters around the institution.

6. Simultaneous to step 5, the questionnaire was promoted online. This was primarily on social media platforms to recruit participants within the demographic. Specifically, social media platforms that could target specific age demographics (Reddit and Twitter) were used. In addition, a participant recruitment website (called 'Call for Participants') was used.
7. When the data collection deadline was reached and the minimum required number of participants had been reached, SPSS was used to carry out statistical analysis of the data to inform us about what the level of cyber security awareness is amongst young adults aged 16 to 18 in the UK.

3.3 Ethics

The demographic for this research was originally for 10- to 13-year-olds, which received ethical approval on 28th January 2021, but after difficulties with participant recruitment an amended ethics application was submitted with the updated demographic of 16- to 18-year-olds with an additional prize draw to aid with participant recruitment. This amended ethics application received full approval from the ethics committee on 9th June 2021 and the approval letter can be seen in Appendix A.

3.4 Participant Recruitment

As described in the methodology steps, participant recruitment was done in two ways. The first way was to contact schools, sixth forms, and colleges via email communication, asking if they could promote the research to their students in the form of displaying the supplied posters around the buildings. Secondly, the questionnaire was posted on the social media

platforms Twitter and Reddit to expand the outreach of participants that the questionnaire could reach (outside of academic institutions, but still within the UK). The questionnaire was also promoted to potential participants through a participant recruitment website called 'Call for Participants', which is a UK-based website for universities who are recruiting participants for their research.

The same questionnaire and questionnaire webpage link was used in all methods of participant recruitment.

A sample of 100 schools, sixth forms, and colleges from across the country were selected from different areas across the UK and invited to take part in this research. A mixture of state, private, single-gender and mixed-gender schools were selected to ensure a diverse range of backgrounds and participants. These educational institutions were contacted via e-mail, with the full participant information sheet (Appendix B), consent form (Appendix C), questionnaire questions (Appendix D), and outline of the research aims included in the correspondence. Unfortunately, this method of recruitment had minimal success, with no response from most institutions. Those that did respond informed us that they do not wish to take part in the research. We believe that this is likely due to the timing, as the invitations were sent out during lockdown in the COVID-19 pandemic, understandably when the schools were extremely busy dealing with the uncertain circumstances. Moreover, as a result of the pandemic, we were not able to visit educational institutions directly to hand out and display poster. As a result of this, we had to alter our method of participant recruitment. We decided that it was most appropriate to recruit solely online due to the circumstances of the pandemic

and the minimal success we had experienced thus far. So, to recruit participants, the questionnaire was posted online to Twitter and Reddit. This is because social media websites have proven to be an effective platform for participant recruitment, helping to recruit participants across a variety of research areas, including clinical trials (Gelinas et al., 2017). Furthermore, social media websites are beneficial for recruiting participants in hard-to-reach areas. For example, one study used social media as a participant recruitment tool to recruit those in the deaf community (Kobayashi et al., 2013). In addition to social media websites, the questionnaire was posted to the participant recruitment website, 'Call for Participants'. This is a website used by academic institutions across the UK to recruit participants for research studies. One study carried out by University College London used this website as a recruitment platform for their research on the human memory with success, and the research has been featured in various publications (Clark, 2015). Screener questions (see Q1 to Q5 in Appendix D) were included in the questionnaire which ensured that all participants were based in the UK, were currently aged 16, 17, or 18, and that they consented to taking part in the research.

In total, we received 811 responses from participants who all met the criteria as defined in the research. Once the time period for our participant recruitment had ended, we used Qualtrics to output the collected data into an SPSS file, which could then be imported into SPSS for analysis.

3.5 Consent

The participants required to take part in this research are aged from 16 to 18 years old. As all participants were at least the age of 16, special considerations for consent were not required, as all participants were able to provide consent for themselves.

Consent was obtained from participants through the questionnaire link that they used to access the research. This was all be done via the questionnaire software, Qualtrics. The first screen that participants were presented with was the Participant Information Sheet, which informed the participants about the research, what they were expected to do, and how the data would be handled. A full participant information sheet can be seen in Appendix B. Once the participant had read the participant information sheet, they could click on the arrow to the next screen, where they were presented with the consent form. The consent form asked participants to agree to seven key statements, which outlined and confirmed that the participant knew what they needed to do, that they could ask any questions they may have had about the research, and that they knew how the data would be collected and how it would be handled. The consent form can be seen in Appendix C.

At this point, the participant was asked to read the consent form and proceed to the next page. On the next page, they were asked whether they agree to the terms and therefore if they provide their consent. The answers to the question were simply ‘yes’ and ‘no’. If the participant answered ‘yes’, then this confirmed that they provided their consent and they were moved on to the next page, where the questionnaire started. If they answered ‘no’, the questionnaire was designed to take them to an end screen, thanking the participant for their

time and consideration. Any participant who did not provide their consent could not complete the questionnaire.

This method of consent was consistent across all methods of participant recruitment. Regardless of whether a participant was recruited via a poster that they saw at their college or whether they saw the research poster advertised online, all participants were taken to the same Qualtrics page where they were provided with the same participant information sheet and consent form that they needed to agree to participate in the research.

3.6 Sample Size

To determine the sample size of the research, we followed the formula developed by Krejcie and Morgan which provides you with the sample size based on your entire population, to enable the sample to statistically represent the population (Krejcie et al., 1970).

In 2020, there were 2,180,873 young adults aged 16 to 18 in the UK (Statista, 2021). Based on this, the recommended sample size according to the Krejcie and Morgan formula is 384. Therefore, this was the minimum number of participants that we required to take part in the research. However, we aimed for as many participants as possible, especially as this research covered the entire geography of the UK.

3.7 Questionnaire Design

The aim of the research was to determine what the level of cyber security awareness amongst young adults is. This means understanding the extent to which young adults understand cyber

security, from both the threat and preventative measure perspectives. Therefore, it was imperative that the questionnaire was designed to reliably capture this information.

Several cyber security awareness studies follow the Likert-scale method in their questionnaire design, which, according to Ahmad et al. has been proven successful in allowing for the gathering of data to analyse the level of cyber security awareness of the participant. Pilots are also regularly carried out to ensure that there are no issues with the questions and that they are all understandable by the participants (Ahmad et al, 2018).

From the findings of Chapter Two, it was clear that a valid and reliable method of surveying participants to determine their level of cyber security awareness was to use the Human Aspects of Information Security Questionnaire (HAIS-Q) (Parsons et al., 2013). Moreover, this appeared to be the most tested method that currently exists in the realms of analysing cyber security awareness. From carrying out the literature review, it was evident that there were minimal alternative options to the HAIS-Q. An alternative would have been to create our own information security awareness questionnaire, however this would then have to be tested for its reliability and validity to ensure an accurate measure of awareness. If this research study was longer, then this would have been a viable option. As we were restricted by time for this research, we decided that the most reliable option was to use the HAIS-Q.

To make the HAIS-Q appropriate for the age demographic of this research (young adults aged 16 to 18 years old), an extra step had to be taken as the HAIS-Q had been created for primarily adults aged 18+ as the target demographic, with a focus on those in employment. The HAIS-Q is comprised of seven sections: password management, email use, internet use, social

networking site use, mobile computing, information handling, and incident reporting (Parsons et al., 2013). Each of these sections has three questions, which are then divided into three further questions to analyse a participant's knowledge, attitude, and behaviour towards the topic. In total, this means that the HAIS-Q has 63 questions. So, to make the questionnaire more appropriate for the age demographic of this research, we had to reduce the number of questions from three questions in each section to one question in each section. By doing this, we were still utilising the theory of the HAIS-Q and the approach that the questionnaire takes (measuring knowledge, attitude, and behaviour), but we were reducing the overall time that the questionnaire took participants to complete and therefore reducing the attention time that a young adult needed to spend completing the questionnaire. As the average attention span of a 16-year-old is 32 to 48 minutes on average (Shakibaie, 2021), this was enough time for the young adult to focus on the questionnaire (as the questionnaire took, on average, no longer than 15 minutes to complete). Furthermore, reducing the time it took to complete the questionnaire made the questionnaire more appealing to take, which may have contributed to improving the outcomes of the participant recruitment. If the questionnaire had been longer, it is likely that we would not have received accurate results as the participants may have become distracted and, as a result, we may have received a higher number of incomplete results. Furthermore, a longer questionnaire could also have caused unnecessary stress for a participant. To minimise this, the questionnaire that was designed for this research was a subset of the HAIS-Q questions, to cause the least stress for the participants and to allow us a better chance of receiving completed (and higher numbers of) questionnaire responses.

3.8 Independent Variables

Independent variables are those variables that are not changed or altered by any factors. These are what this research will be testing against. For this research, there were three independent variables, which were highlighted in each of the three hypotheses. Each of these independent variables was tested against to determine whether they have any effect on a young adult aged 16 to 18's level of cyber security awareness.

The independent variables for each participant were determined from the demographic questions that were asked in the questionnaire. These were the first questions that the participant answered and provided the basis for their responses to the HAIS-Q to be compared against. There were only four demographic questions in the questionnaire. These four questions allowed us to obtain the vital demographic information that was required to inform the independent variables of this research, without being too intrusive or collecting any unnecessary information, in line with GDPR (UK Government, 2018).

The first independent variable was the socioeconomic status of the participant. Within the demographic questions of the questionnaire, the participant was asked two questions which helped us to determine the participant's socioeconomic status. The first question asked the participants to share what level of education their parents had completed. Afterwards, the participants were asked whether they currently receive free school meals (if they were in education). If they were not in education, they were asked to think back to when they were in school and whether they previously received school meals. Taking both the participant's parents' level of education and whether they were eligible for free school meals provided us with an accurate understanding of the participant's socioeconomic status. Significant

research has been carried out surrounding socioeconomic status (SES) and for children, it typically comprises of parental occupation, parental educational qualifications, and family income (UK Government, 2021). The government recommends using these measures when determining a person's socioeconomic status (UK Government, 2021). As this research relies on young adults themselves completing the questionnaire, not their parents or guardians, the parental occupation factor is removed, as young adults may not know their parent's specific occupations. This could have led to inaccurate responses and therefore inaccurate results. Therefore, for this research, socioeconomic status was determined by parental educational qualifications and family income. As it was unlikely that incomes and finance were known by the participants, we can understand family income by whether the young adult has been eligible for free school meals, as this is an accurate indication of household income (those who are entitled to certain benefits are eligible) and is recommended as a measure of socio-economic status by the government (UK Government, 2023).

The second independent variable was the young adult's gender. The digital gender divide is a significant issue in the modern day, with 3% of females choosing a career in technology as their first choice. Moreover, just 5% of leadership positions in the technology industry are held by women. When students were asked to name a famous female in technology, 78% could not (PWC, 2022). This gender divide is a key area of interest for this research, which is why we asked participants to describe their gender, with the option of preferring not to disclose their identified gender if they felt more comfortable not sharing this information.

The third independent variable was the participant's age. In the UK, 16 is the school leaving age (UK Government, 2022). At the age of 18, a young adult has completed their further

education and can go to university. Therefore, these three years are significant in a young person's development as they leave school and determine the next steps for their career. From the findings of Chapter Two, it is evident that young adults are engaging significantly with technology during these years, so it is vital that young adults know what best cyber hygiene practices are and how to prevent becoming a victim of a cyber-attack. Therefore, the final independent variable that we were interested in for this research was age, to determine whether age is a contributing factor to a young adult's level of cyber security awareness. Participants were simply asked to answer whether they are 16, 17, or 18 years old.

These independent variables combined with the dependent variables allowed us to determine whether we could accept or reject the hypotheses of this research. The desired outcome was to be able to determine whether socioeconomic status, gender and/or age have an impact on a young adult's level of cyber security awareness.

3.9 Dependent Variables

Dependent variables are those variables that are being measured. The purpose of this research was to measure the level of cyber security awareness amongst young adults aged 16 to 18 years old. To measure this, a questionnaire consisting of both quantitative and qualitative questions (mixed-methods approach) was used which provided evidence of the level of cyber security awareness of the young adults in the demographic. The specific questionnaire that we used for this research was the Human Aspects of Information Security Questionnaire (HAIS-Q). To determine a participant's level of cyber security awareness, each participant answered questions from the HAIS-Q which analysed a person's level of awareness from three different dimensions: knowledge, attitude, and behaviour. As part of

the HAIS-Q, each of these dimensions has a weighting which has to be applied after the results have been calculated (Kruger et al., 2006). The weightings can be seen in Figure 4.

Dimensions	Weightings
Knowledge	30%
Attitude	20%
Behavior	50%

Figure 4 - Weight and Awareness Scale (Kruger et al., 2006)

Once the weightings had been applied, a person's final percentage level of cyber security awareness has been calculated. This percentage could then be applied to the HAIS-Q scale of information security awareness (see Figure 5), which outlines whether a participant's level of awareness is good, average, or poor (Kruger et al., 2006).

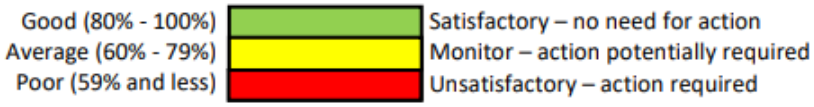

Figure 5 - Scale of Information Security Awareness (Kruger et al., 2006)

In addition to the quantitative HAIS-Q questions, a final qualitative question was asked to participants at the end of the questionnaire. This was an open question that asked participants what they think being a victim of a cyber-attack means. It was clarified to the participant that there is no right or wrong answer; we simply wanted to provide the participants with an opportunity to express their views of cyber-attacks. The responses to this question provided an insight into the reasons behind a participant's HAIS-Q responses, giving participants a voice on an important topic in which they likely do not otherwise have the opportunity to speak openly about.

3.10 Validity

For any research, it is important that validity is considered to ensure that the results gathered from the research are accurate and reliable. The key area of validity for this research is the HAIS-Q questions, as these form the basis of our dependent variable which is the level of cyber security awareness. For this research, both the internal and external validity have been considered and implemented.

3.10.1 Internal Validity

Internal validity is defined as the extent of confidence to which the testing method is trustworthy. It also ensures that the results are not influenced by any factors or variables (Streefkerk, 2021).

The internal validity of the HAIS-Q has been tested throughout multiple research papers, however as the HAIS-Q is typically used for employees and adults over the age of 18, the version of the HAIS-Q that was used for this research was a subset of the original HAIS-Q, with minimal nouns changed to make the questions more relatable for a young adult as opposed to an employee over the age of 18. To test the validity of this version of the HAIS-Q, a small pilot group of five people who fit into the age demographic of this research was formed to test that the questions are understandable, clear, and appropriate for the age demographic. The results from this showed that the questions were all appropriate; all comments from the pilot group were positive and no signs of misunderstanding were displayed.

A key threat that can affect the internal validity of the research results is participant selection. To ensure that the results of the research are valid and can be representative, it is important that there is no influence over a participant's choice as to whether to participate in research. The aim is for the population sample to be as random as possible to ensure the most accurate and representative cyber security awareness level results. To ensure this, we recruited participants through several different means, including posting the questionnaire link to social media platforms and recruiting via participant recruitment websites. By recruiting participants in these several different ways, we aimed to recruit a diverse range of participants who all fit within the specified demographic criteria of this research.

Another internal validity factor to consider is attrition. This is when participants drop out due to the experiment being long and pressured. To be able to analyse the level of cyber security awareness accurately, it is vital that we only collected fully completed responses. Therefore, we adapted the HAIS-Q to make it appropriate for the age demographic and context, reducing the length of the questionnaire down to one third of the original HAIS-Q which is 21 questions. This contributed to prevent the threat of attrition and therefore improved the internal validity of this research.

3.10.2 External Validity

External validity measures the extent to which the results of the research can be applied in a general context to the wider population. For the purpose of this research, as we were aiming to determine the general level of cyber security awareness of all 16- to 18-year-olds in the UK, we needed to ensure that our participant group was representative and reflective of the

general population of 16- to 18-year-olds in the UK. Several measures were taken to ensure the external validity of this research.

Firstly, measures were taken to prevent the external validity threat of sampling bias. This research was focused solely on those who lived in the UK at the time of completing the questionnaire. Therefore, the first question of the questionnaire that participants were required to answer was whether the participant currently lives in the UK. The participant could not continue the questionnaire until they answered this question; there was no option for them to skip the question. If the participants answered 'yes', then they were taken to the following questions. If they answered 'no', they were taken to the debrief page and were not able to proceed with the questionnaire. By designing the questionnaire in this way, we were ensuring that the only participants who could complete the questionnaire were those who currently live in the UK. This contributed to achieving the aim of having a participant group that was representative of the general population of our demographic group.

The age group that we were concerned with for this research was only 16- to 18-year-olds. Therefore, when completing the questionnaire, the participant must have been aged either 16, 17, or 18 years old. This was another question that required a response from the participant with no option to skip. Again, this contributed to our aim of having a participant group that was representative of the general population of our demographic group.

A particular threat to external validation is testing. This is when the participant is aware of the topic and starts to think more consciously about the topic, wanting to get the best results (Streefkerk, 2021). Whilst awareness of the topic is what we are researching, we want the

results to be based on initial instinct as opposed to overthinking of the scenario, as this is more representative of facing a cyberattack situation in reality. To prevent this in our research, the participant information sheet discussed the topic casually, without specifically saying that the participant's level of cyber security awareness is going to be measured. Participants were aware of the topic of the research being cyber security, however the HAIS-Q questionnaire is designed to not put any pressure on the participant in selecting a 'right' or 'wrong' answer. This was reinforced by the fact that every question in the HAIS-Q was answered by using a Likert-scale from 'strongly agree' to 'strongly disagree', enforcing the fact that there is no strict 'correct' answer.

3.11 Chapter Summary

In this chapter, the methods and materials that will be used to carry out this research are discussed. Firstly, the materials that are required are outlined, including both hardware and software. The method is then presented, which shows the steps that have been taken to obtain the results to answer the research question. Participant recruitment is discussed in the next section, which outlines the several methods that were followed to get young adults to participate in this research. Consent is then discussed, outlining how it was obtained from participants. We then look at the optimal sample size, reviewing how we calculated what this was. After, we look at the questionnaire design and what the questionnaire comprises of. The specifics of the independent and dependent variables are discussed next, outlining specifically what variables are constant and what we are testing against. Finally, both the internal and external validity are discussed, outlining how factors that may affect the validity of the results have been identified and tested.

Chapter Four: Results

4.1 Data Cleansing

Due to the nature of the participant recruitment (with participants all being recruited online), thorough checks had to take place to ensure that the collected data was valid and truthful. This is especially important as there was an incentive for participants to take part in the research, this being a chance to win a gift voucher. So, to ensure that the data was valid and could be used in the analysis, data cleansing checks took place.

Firstly, we had to update all the variable names to make the more meaningful, as the default variable names are linked to the question number that they were in Qualtrics. Then, we had to select the data types for each data variable. As the HAIS-Q is based on Likert-Scale questions, the data type of these is numeric. The measure of each data variable also had to be selected, with the choice of nominal, ordinal, or scale measures. Again, as the HAIS-Q is Likert-Scale, which is sequential, the measure of this data is ordinal.

Once the data had been set up and defined correctly in SPSS, we had to cleanse the data. This meant firstly removing any responses from those participants who did not consent to the research. If the participants selected in the questionnaire that they do not consent, then they were taken to the end of the questionnaire, which thanked them for their consideration. Therefore, in SPSS, their questionnaire responses were blank. Those responses were not included in the data analysis; thus, the responses were removed. During initial phase of data cleansing, we have found only one person did not consent to taking part in the research, so their entry was removed. Subsequently, we had a total of 810 responses.

The second phase of the data cleansing was to remove any duplicate entries. The challenge with offering a prize draw entry incentive for participants to take part in the research is that participants want to increase their chances of winning in the prize draw. Therefore, they may respond to the questionnaire enter multiple times to increase their chances. Unfortunately, this is a challenge that we experienced when cleansing the data. However, Qualtrics records the IP address of each participant. Thus, all those entries that were from the same IP addresses with duplicate answers were removed, to ensure that the only data that we had were valid entries from genuine individual participants. After this phase of the data cleansing, we were left with 691 valid responses.

4.2 Cronbach's Alpha

Significant testing of the HAIS-Q has been carried out to test its validity and reliability in measuring cyber security awareness. Cronbach's Alpha has been used on the HAIS-Q to test the reliability coefficient of the questions (McCormac et al., 2016). As the HAIS-Q consists of three constructs (knowledge, attitude, and behaviour) we must carry out the Cronbach's Alpha test on each three of these constructs to test how reliable our dataset is. To do this, we gather each of the constructs' questions across the HAIS-Q and carry out the test. The HAIS-Q is based on a Likert-scale where an answer of one (strongly disagree) indicates a low cyber security awareness and an answer of five (strongly agree) indicates a high cyber security awareness. As some questions are negatively asked (therefore negatively skewed), we must reverse the Likert-scale numerical results to reflect the accurate levels of cyber security awareness. Once this is done, the data could be tested with Cronbach's Alpha.

Cronbach's Alpha tests were carried out on each of the three constructs of the HAIS-Q, which consisted of seven questions for knowledge, seven questions for attitude, and seven questions for behaviour. The Cronbach's Alpha indicates how closely related a set of items are in a group. A high Cronbach's Alpha (0.9 and above) indicates an excellent level of reliability, whereas a low Cronbach's Alpha (0.5 and below) indicates an unacceptable level of reliability (Glen, 2023). The first Cronbach's Alpha test was carried out on the knowledge questions of the HAIS-Q. This returned a result of 0.657. As this is between 0.6 and 0.7, this indicates an acceptable level of reliability (Ursachi et al., 2013). Secondly, a Cronbach's Alpha test was carried out on the attitude questions of the HAIS-Q. This returned a result of 0.780, which shows good reliability. Finally, the behaviour questions were tested, which returned a result of 0.489. This is a low result and suggests questionable reliability.

4.3 Participant Demographics

At the start of the questionnaire, and participants had read the information sheet and consented to taking part, participants were asked to complete four demographic questions. These questions helped us to understand the demography of the participants who took part in the research, and whether this is reflective of the population, and provides us with the independent variable data that we will be using to test the hypotheses in this research.

In total, there were 691 valid participant responses that could be used for statistical analysis. All of these participants provided a response to each of the demographic questions, so there were no missing responses. The full overview of the descriptive statistics for the demographic questions can be seen in Figure 6.

Statistics

		Gender	Parents' Education Level	Free School Meals	Age
N	Valid	691	691	691	691
	Missing	0	0	0	0
Mean		1.58	2.86	1.51	2.15
Median		1.00	3.00	1.00	2.00
Mode		1	4	1	3
Std. Deviation		.822	1.150	.649	.772
Variance		.676	1.323	.421	.597
Range		5	4	2	2

Figure 6 - Descriptive statistics of the demographic questions

The first demographic question was what gender the participant identifies as. The answers that the participant could choose from aimed to be inclusive of all genders, with the options as: male, female, non-binary/third gender, transgender, other, prefer not to say. The participants consisted of 358 males, 311 females, 4 non-binary/third gender, 1 transgender, 7 other, and 10 who preferred not to say. In terms of percentages, the gender split was almost even between male and female participants, with 51.8% of participants identifying as male, 45% of participants identifying as female, and the rest of the genders making up 3.2%. The mean, median and mode all lie within the male category, with a standard deviation of 0.822, showing that the results are not spread far from the average. The full breakdown of responses to this question can be seen in Figure 7.

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	358	51.8	51.8	51.8
	Female	311	45.0	45.0	96.8
	Non-binary / third gender	4	.6	.6	97.4
	Transgender	1	.1	.1	97.5
	Other	7	1.0	1.0	98.6
	Prefer not to say	10	1.4	1.4	100.0
	Total	691	100.0	100.0	

Figure 7 - The full breakdown of responses to the gender question

The second demographic question asked to participants was what education their parents had completed. The answers that participants could choose from included: below secondary school (meaning that secondary school studies were not completed), finished secondary school (meaning that studies ended upon completion of secondary school at 16 years old), further education (meaning that some form of college or apprenticeship was attended until the age of 18), university, and unsure. In total, 13% of participants' parents education level was below secondary school, 30.8% had finished secondary school, 17.2% had completed further education, and 34.9% had completed university. This left 4.1% of participants who were unsure about what level of education their parents had completed. The mean result is 'finished secondary school', with the median being 'further education' and the mode being 'university'. These results have a standard deviation of 1.150, which shows that the results

are spread from the average. The full breakdown of responses to this question can be seen in Figure 8.

Parents' Education Level

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Below secondary school	90	13.0	13.0	13.0
	Finished secondary school	213	30.8	30.8	43.8
	Further education (for example, college)	119	17.2	17.2	61.1
	University	241	34.9	34.9	95.9
	Unsure	28	4.1	4.1	100.0
	Total	691	100.0	100.0	

Figure 8 - The full breakdown of responses to the parents' education level question

Next, participants were asked whether they currently receive free school meals (Figure 9). If participants are not currently in education, they were asked to answer for when they were at school. The results were that 57.2% of participants had received free school meals, 34.3% of participants had not received free school meals, and 8.5% were unsure as to whether they had ever received free school meals. The mean, median and mode all lie within the 'Yes' answer, unsurprisingly as this was the most popular response.

Free School Meals

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	395	57.2	57.2	57.2
	No	237	34.3	34.3	91.5
	Unsure	59	8.5	8.5	100.0
	Total	691	100.0	100.0	

Figure 9 - The full breakdown of responses to the free school meals question

The final demographic question that participants were asked is how old they are (Figure 10). As all participants had to be aged 16 to 18 years old to take part in this research, these were the only three options that participants could choose from. The results are that (at the time of completing the questionnaire), 23.4% of participants were aged 16, 38.2% of participants were aged 17, and 38.4% of participants were aged 18. The mean of this data is 17 and the median is 17, however the mode result is 18. There is a standard deviation of 0.772, which is a low standard deviation, showing that the results are close to the average.

Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	16	162	23.4	23.4	23.4
	17	264	38.2	38.2	61.6
	18	265	38.4	38.4	100.0
	Total	691	100.0	100.0	

Figure 10 - The full breakdown of responses to the age question

H_3 tests the dependent variables against socioeconomic status. To understand the socioeconomic status of our participants (who are aged 16 to 18 years old), we must take into consideration two key factors. These are parents' level of education and household income. For this research, household income is determined by whether a participant is eligible for free school meals. There were some participants who answered 'unsure' for either or both of these questions. The socioeconomic status of these participants cannot be determined as it is vital that we know both parents' education level and eligibility of free school meals. Therefore, those participants that answered 'unsure' for either of these questions are removed from the socioeconomic status variable calculation. In Figure 11 we can see that 81

results are missing; these are the participants that answered 'unsure'. After removing these, we are left with 610 participants that we can calculate the socioeconomic status of.

Socioeconomic Status

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	E	49	7.1	8.0	8.0
	D	162	23.4	26.6	34.6
	C2	142	20.5	23.3	57.9
	C1	186	26.9	30.5	88.4
	AB	71	10.3	11.6	100.0
	Total	610	88.3	100.0	
Missing	System	81	11.7		
Total		691	100.0		

Figure 11 - The full breakdown of responses to the socioeconomic status question

To calculate the socioeconomic status, the values of the parents' education level were combined with the values of free school meal eligibility, to output a value which relates to a socioeconomic status category. In line with the UK Government's measurement of socioeconomic status, participants were coded on a level of 1 to 5 (AB to E statuses) according to the combination of their answers of parental education level and free school meals. The output of the code determined the socioeconomic status of the participant, which the results can be seen in Figure 11 (UK Government, 2021). As defined by the Office for National Statistics, socioeconomic status has five categories. These are: AB, C1, C2, D, and E and can be seen in Figure 12. At the top level, A and B represent higher and intermediate managerial, administrative, professional occupations. C1 represents supervisory, clerical, and junior managerial, administrative, professional occupations. C2 represents skilled manual occupations. D and E represent semi-skilled and unskilled manual occupations, unemployed and lowest grade occupations (ONS, 2022).

Social Grade	Description	% HRP Population (UK)
AB	Higher and intermediate managerial, administrative, professional occupations	22.17
C1	Supervisory, clerical, and junior managerial, administrative, professional occupations	30.84
C2	Skilled manual occupations	20.94
DE	Semi-skilled and unskilled manual occupations, unemployed and lowest grade occupations	26.05

Figure 12 - The socioeconomic status categories as defined by the UK Office for National Statistics (ONS, 2022)

The results of the socioeconomic status variable are that 8% of participants are in the E category, 26.6% in the D category, 23.3% are in C2, 30.5% in C1, and 11.6% in AB. The mean, median and mode all lie within the C1 category. There is a standard deviation of 1.161 and a variance of 1.347, indicating that the results are spread from the average.

4.4 HAIS-Q

After participants had answered the demographic questions, they were taken straight to the HAIS-Q questions. Participants had to answer 21 questions (see Appendix D) based on a subset of the original 63 HAIS-Q questions. These questions were divided into seven different sections: password management; email use; internet use; social media use; mobile devices; information handling; and incident reporting. Each of these sections asks the same target question but in three different ways to establish the participant's knowledge, attitude, and behaviour. All questions are answered using a Likert-scale, from 'Strongly Disagree' to

'Strongly Agree'. Some questions were negatively skewed, so the results had to be reversed. In the data, the higher the score is to 5, the higher the level of information security awareness.

4.4.1 Password Management

The first section of questions was based around passwords. The first question asked was 'it's safe to have a password with just letters', which is an attitude-based question. The mean of this question was 3.44, with a median and mode of 4. For this question, there was a standard deviation of 1.1 and variance of 1.2, which indicates a narrow variation of results.

Secondly, participants were asked to respond to 'I use a combination of letters, numbers, and symbols in my passwords'. This is a behaviour-based question. The mean for this was 3.69, with a median and a mode of 4. The standard deviation and variance were lower for this question than the attitude-based question, at 0.864 and 0.747 respectively. This indicates an even narrower spread of results.

The final question asked in terms of password management was 'A mixture of letters, numbers and symbols is necessary for my passwords'. This is a knowledge-based question. This question had a mean of 4.07, a median of 4, and a mode of 4. The standard deviation and variation were even smaller for this question, at 0.847 and 0.718 respectively.

The full statistics data for the password management questions can be seen in Figure 13.

Statistics

		It's safe to have a password with just letters.	I use a combination of letters, numbers and symbols in my passwords.	A mixture of letters, numbers and symbols is necessary for my passwords.
N	Valid	691	691	691
	Missing	0	0	0
Mean		3.44	3.69	4.07
Median		4.00	4.00	4.00
Mode		4	4	4
Std. Deviation		1.098	.864	.847
Variance		1.207	.747	.718
Range		4	4	4

Figure 13 - The statistics breakdown of the password management questions

To test whether there is any statistical significance between young adults' password management and the independent variables, we used a Kruskal Wallis test against each independent variable (age, gender, and socioeconomic status). We used Kruskal Wallis as this is a nonparametric test used to test for more than two groups, which we have throughout the questions in this research. Kruskal Wallis tests to see whether samples are originated from the same distribution, hence testing for statistical significance (providing us with a p-value) (Xia, 2020).

Firstly, we tested the password management questions against age (Figure 14). For the attitude-based question, the p-value was less than 0.001, which shows high statistical significance. When we compare this with the p-values for the behaviour-based question (0.302) and for the knowledge-based question (0.890), we can see that this is the only statistically significant value to come out of this test against age. Therefore, we can reject the

null hypothesis ($H_{1\_att\_0}$) and accept the hypothesis (H_{1_att}) in terms of attitude towards password management.

Test Statistics[a,b]

	It's safe to have a password with just letters.	I use a combination of letters, numbers and symbols in my passwords.	A mixture of letters, numbers and symbols is necessary for my passwords.
Kruskal-Wallis H	18.160	2.396	.233
df	2	2	2
Asymp. Sig.	<.001	.302	.890

a. Kruskal Wallis Test

b. Grouping Variable: Age

Figure 14 - The Kruskal-Wallis H test results for password management against age

Next, we tested the password management questions against gender (Figure 15). All the p-value results turned out greater than 0.05. The attitude-based question returned a result of 0.687, the behaviour-based question returned a result of 0.638, and finally the knowledge-based question returned a result of 0.168. Therefore, we accept the null hypothesis of the H_{2_0} which shows that a young adult's password management is not affected by gender.

Test Statistics[a,b]

	It's safe to have a password with just letters.	I use a combination of letters, numbers and symbols in my passwords.	A mixture of letters, numbers and symbols is necessary for my passwords.
Kruskal-Wallis H	3.087	3.401	7.799
df	5	5	5
Asymp. Sig.	.687	.638	.168

a. Kruskal Wallis Test

b. Grouping Variable: Gender

Figure 15 - The Kruskal-Wallis H test results for password management against gender

Finally, we tested for statistical significance between password management and socioeconomic status (Figure 16). The result of the attitude-based question was a p-value of 0.006, the behaviour-based question returned a p-value of 0.004, and the knowledge-based question returned a p-value of 0.066. There are two p-values here that show statistical significance. These are the results for both the attitude and behaviour of participants towards password management. Therefore, we reject the null hypothesis and accept the hypothesis (H_{3_att} and H_{3_beh}) that shows that a young adult's attitude and behaviour towards password management is affected by their socioeconomic status.

Test Statistics[a,b]

	It's safe to have a password with just letters.	I use a combination of letters, numbers and symbols in my passwords.	A mixture of letters, numbers and symbols is necessary for my passwords.
Kruskal-Wallis H	14.325	15.390	8.826
df	4	4	4
Asymp. Sig.	.006	.004	.066

a. Kruskal Wallis Test

b. Grouping Variable: Socioeconomic Status

Figure 16 - The Kruskal-Wallis H test results for password management against socioeconomic status

Password Management	*H_1 (Age)*	*H_2 (Gender)*	*H_3 (Socioeconomic Status)*
Knowledge	Reject	Reject	Reject
Attitude	Accept	Reject	Accept
Behaviour	Reject	Reject	Accept

Figure 17 - Hypothesis outcomes for Password Management.

4.4.2 Email Use

The second section of the questionnaire was on the topic of email usage. Specifically, this section targets knowledge, attitude, and behaviour on phishing, one of the most common email cyber-attacks. Participants were firstly asked to respond to 'nothing bad can happen if I click on a link in an email from an unknown sender', which is an attitude-based question. Next, they were asked to respond to 'if an email from an unknown sender looks interesting, I click on a link within it'. This is a behaviour-based question. Finally for this section, participants responded to 'I should not click on a link in an email from an unknown sender', which is a knowledge-based question.

The results for the attitude-based question gave a mean of 3.68, a median of 4.00 and a mode of 4. Furthermore, the responses to this question had a standard deviation of 1.076 and 1.157, which signifies a narrow spread of the results. Comparatively, we have the behaviour-based question, which resulted in a mean of 3.36, a median of 4.00, and a mode of 4. The standard deviation and variance are lower for this question compared to the attitude-based question, at 1.030 and 1.060 respectively. This shows that the results were less spread for the behaviour-based question than they were for the attitude-based question. Finally, we have the knowledge-based question which participants showed the highest level of cyber awareness in. The results of this question were a mean of 4.05, a median of 4.00, and a mode of 4, the highest averages out of the three questions. Moreover, the responses had a standard deviation of 0.847 and a variance of 0.718, the lowest values of the email usage section. This indicates an even narrower spread of the responses. The full breakdown of the descriptive statistics for the e-mail use questions can be seen in Figure 18.

Statistics

		Nothing bad can happen if I click on a link in an email from an unknown sender.	If an email from an unknown sender looks interesting, I click on a link within it.	I should not click on a link in an email from an unknown sender.
N	Valid	691	691	691
	Missing	0	0	0
Mean		3.68	3.36	4.05
Median		4.00	4.00	4.00
Mode		4	4	4
Std. Deviation		1.076	1.030	.847
Variance		1.157	1.060	.718
Range		4	4	4

Figure 18 - The descriptive statistics of the email usage questions

Next, we carried out Kruskal Wallis tests to determine whether the independent variables of age, gender and socioeconomic status affect a young adult's cyber security awareness in terms of email usage.

Firstly, we ran the tests against age (Figure 19). The attitude-based question here returned a p-value of 0.013, which is statistically significant. The behaviour-based question returned a p-value of 0.468 and the knowledge-based question 0.362. Both results are statistically insignificant. Therefore, we can accept the H_{1_att} hypothesis for age having an effect on a young adult's attitude towards email usage. For behaviour and knowledge, we can accept the null hypothesis for $H_{1\_beh\_0}$ and $H_{1\_kno\_0}$ for email usage.

Test Statistics[a,b]

	Nothing bad can happen if I click on a link in an email from an unknown sender.	If an email from an unknown sender looks interesting, I click on a link within it.	I should not click on a link in an email from an unknown sender.
Kruskal-Wallis H	8.700	1.519	2.030
df	2	2	2
Asymp. Sig.	.013	.468	.362

a. Kruskal Wallis Test

b. Grouping Variable: Age

Figure 19 - The Kruskal-Wallis H test results for e-mail use against age

Next, we tested results against gender (Figure 20). Similarly, the p-values were all greater than 0.05, with the attitude-based question resulting in a p-value of 0.362, the behaviour-based question 0.227, and the knowledge-based question 0.062. These were all statistically insignificant and therefore we accept the null hypotheses for $H_{2\_att\_0}$, $H_{2\_beh\_0}$ and $H_{2\_kno\_0}$.

Test Statistics[a,b]

	Nothing bad can happen if I click on a link in an email from an unknown sender.	If an email from an unknown sender looks interesting, I click on a link within it.	I should not click on a link in an email from an unknown sender.
Kruskal-Wallis H	5.465	6.910	10.527
df	5	5	5
Asymp. Sig.	.362	.227	.062

a. Kruskal Wallis Test

b. Grouping Variable: Gender

Figure 20 - The Kruskal-Wallis H test results for e-mail use against gender

Finally, we tested the email usage results against socioeconomic status (Figure 21). The attitude-based question had a p-value of less than 0.001, the behaviour-based question had a p-value of less than 0.001, and the knowledge-based question had a p-value of 0.019. From this, we can reject the null hypothesis and accept the hypothesis H_3 for all areas of email usage, which are attitude (H_{3_att}), behaviour (H_{3_beh}), and knowledge (H_{3_kno}).

Test Statistics[a,b]

	Nothing bad can happen if I click on a link in an email from an unknown sender.	If an email from an unknown sender looks interesting, I click on a link within it.	I should not click on a link in an email from an unknown sender.
Kruskal-Wallis H	19.445	22.880	11.806
df	4	4	4
Asymp. Sig.	<.001	<.001	.019

a. Kruskal Wallis Test

b. Grouping Variable: Socioeconomic Status

Figure 21 - The Kruskal-Wallis H test results for e-mail use against socioeconomic status

Email Use	*H_1 (Age)*	*H_2 (Gender)*	*H_3 (Socioeconomic Status)*
Knowledge	Reject	Reject	Accept
Attitude	Accept	Reject	Accept
Behaviour	Reject	Reject	Accept

Figure 22 - Hypothesis outcomes for Email Use.

4.4.3 Internet Use

The next section that was presented to participants was the 'Internet Usage' section. Specifically, this section asked participants about their knowledge, attitude, and behaviour towards downloading files from the internet onto their computer. The first statement that participants had to respond to according to how strongly they agree with it was 'It can be

risky to download files on my computer', which is an attitude-based question. Next, participants were asked to respond to 'I download any files onto my computer that will help me get my work done, which is a behaviour-based question. The final question in this section is 'I am allowed to download any files onto my computer if they help me to do my work', which is a knowledge-based question.

The results of this section provided us with a mean of 3.74 for the attitude-based question, a mean of 3.23 for the behaviour-based question, and a mean of 3.2 for the knowledge-based question. This shows that, in terms of file downloads, participants were most aware of the fact that it can be risky to download files from the internet. The median result further reinforces this, with values of 4, 3, and 3 respectively. There was a standard deviation of 0.821 for the attitude-based question, which indicates that the results are not as spread for this question as they are for the behaviour and knowledge questions, which have standard deviations of 1.090 and 1.204 respectively. This is further reinforced by the variance, which is significantly less for the attitude-based question compared to the behaviour and knowledge-based questions. The full breakdown of the descriptive statistics for the internet use questions can be seen in Figure 23.

Statistics

		It can be risky to download files on my computer.	I download any files onto my computer that will help me get my work done.	I am allowed to download any files onto my computer if they help me to do my work.
N	Valid	691	691	691
	Missing	0	0	0
Mean		3.74	3.23	3.20
Median		4.00	3.00	3.00
Mode		4	4	4
Std. Deviation		.821	1.090	1.204
Variance		.673	1.188	1.450
Range		4	4	4

Figure 23 - The descriptive statistics of the internet use questions

Next, we ran Kruskal Wallis tests for each question in the internet usage section against the three independent variables of age, gender, and socioeconomic status.

Firstly, we tested the results against age (Figure 24). Both the p-values for attitude and behaviour of internet use against age were greater than 0.05, with the attitude question returning a p-value of 0.127 and the behaviour question returning a p-value of 0.598. However, the knowledge question returned a p-value result of 0.017 which is statistically significant. Therefore, we can accept the null hypothesis for H_1 for attitude $H_{1\_att\_0}$ and behaviour $H_{1\_beh\_0}$ in internet usage and we can reject the null hypothesis and accept the H_{1_kno} for knowledge of internet usage.

Test Statistics[a,b]

	It can be risky to download files on my computer.	I download any files onto my computer that will help me get my work done.	I am allowed to download any files onto my computer if they help me to do my work.
Kruskal-Wallis H	4.130	1.034	8.189
df	2	2	2
Asymp. Sig.	.127	.596	.017

a. Kruskal Wallis Test

b. Grouping Variable: Age

Figure 24 - The Kruskal-Wallis H test results for internet use against age

Next, we ran the tests against gender (Figure 25). Both of the results for behaviour and knowledge returned a p-value greater than 0.05, with 0.205 for behaviour and 0.488 for knowledge. However, with a value of 0.012 for attitude, we can accept H_{2_att} for attitude

towards internet usage. For behaviour and knowledge, we can accept the null hypotheses for $H_{2\_beh\_0}$ and $H_{2\_kno\_0}$ for internet usage.

Test Statistics[a,b]

	It can be risky to download files on my computer.	I download any files onto my computer that will help me get my work done.	I am allowed to download any files onto my computer if they help me to do my work.
Kruskal-Wallis H	14.707	7.211	4.437
df	5	5	5
Asymp. Sig.	.012	.205	.488

a. Kruskal Wallis Test

b. Grouping Variable: Gender

Figure 25 - The Kruskal-Wallis H test results for internet use against gender

Finally for this section, we tested the results against socioeconomic status (Figure 26). This returned a p-value of 0.583 for attitude and a p-value of 0.169 for knowledge. Both of these we can accept the null hypotheses $H_{3\_att\_0}$ and $H_{3\_kno\_0}$ for. However, the p-value result for behaviour is 0.003, which is less than 0.05, so we can therefore accept the hypothesis H_{3_beh} for internet usage behaviour for socioeconomic status.

Test Statistics[a,b]

	It can be risky to download files on my computer.	I download any files onto my computer that will help me get my work done.	I am allowed to download any files onto my computer if they help me to do my work.
Kruskal-Wallis H	2.852	16.167	6.439
df	4	4	4
Asymp. Sig.	.583	.003	.169

a. Kruskal Wallis Test

b. Grouping Variable: Socioeconomic Status

Figure 26 - The Kruskal-Wallis H test results for internet use against socioeconomic status

Internet Use	*H_1 (Age)*	*H_2 (Gender)*	*H_3 (Socioeconomic Status)*
Knowledge	Accept	Reject	Reject
Attitude	Reject	Accept	Reject
Behaviour	Reject	Reject	Accept

Figure 27 - Hypothesis outcomes for Internet Use.

4.4.4 Social Media

Next, participants were asked questions regarding their usage of social media. Again, participants had to respond to the statements using a Likert-scale from 1 (strongly disagree) to 5 (strongly agree). The first statement they responded to was 'It doesn't matter if I post things on social media that I wouldn't normally say in public', which is an attitude-based question. Secondly, they were asked to respond to 'I don't post anything on social media before considering any negative consequences', which is a behaviour-based question. Finally, participants were asked 'I can't be punished for something I post on social media', a knowledge-based question.

The results of this section were a mean of 3.54 for the attitude-based question, a mean of 3.77 for the behaviour-based question, and a mean of 3.41 for the knowledge-based question. As there are five options (and the higher the number, the better the cyber security awareness is), this shows that participants were in the middle in terms of understanding social media. Despite this, the median and mode for all questions is 4, which shows that participants were generally aware of the repercussions that social media usage can have. The lowest standard deviation for this section was 0.808 for the behaviour-based question. The attitude and knowledge questions had standard deviations of 1.008 and 1.188 respectively. This is further reinforced by the lower variance that the behaviour question had at 0.654, with the attitude

and knowledge questions having a significantly higher variance at 1.017 and 1.412 respectively. This shows that the answers for the behaviour-based question were less spread than the attitude and knowledge questions, which indicates an overall higher confidence level in terms of behaviour on social media. The full breakdown of the descriptive statistics for the social media section questions can be seen in Figure 28.

Statistics

		It doesn't matter if I post things on social media that I wouldn't normally say in public.	I don't post anything on social media before considering any negative consequences.	I can't be punished for something I post on social media.
N	Valid	691	691	691
	Missing	0	0	0
Mean		3.54	3.77	3.41
Median		4.00	4.00	4.00
Mode		4	4	4
Std. Deviation		1.008	.808	1.188
Variance		1.017	.654	1.412
Range		4	4	4

Figure 28 - The descriptive statistics of the social media section questions

To test the hypotheses of this research, we ran the social media section questions (attitude, behaviour, and knowledge) through Kruskal Wallis tests against the independent variables of age, gender, and socioeconomic status.

Firstly, we ran the tests for the social media questions against age. All three of the p-values were greater than 0.05, so therefore we accept the null hypotheses of $H_{1\_kno\_0}$, $H_{1\_att\_0}$, and $H_{1\_beh\_0}$. The results of the Kruskal-Wallis H test can be seen in Figure 29.

Test Statistics[a,b]

	It doesn't matter if I post things on social media that I wouldn't normally say in public.	I don't post anything on social media before considering any negative consequences.	I can't be punished for something I post on social media.
Kruskal-Wallis H	2.910	2.710	3.280
df	2	2	2
Asymp. Sig.	.233	.258	.194

a. Kruskal Wallis Test

b. Grouping Variable: Age

Figure 29 - The Kruskal-Wallis H test results for social media against age

Next, we ran the tests against gender to see if there is any statistical significance present. Again, all the p-values were greater than 0.05, so we accept the null hypotheses of $H_{2\_kno\_0}$, $H_{2\_att\_0}$, and $H_{2\_beh\_0}$. The results of the Kruskal-Wallis H test for gender can be seen in Figure 30.

Test Statistics[a,b]

	It doesn't matter if I post things on social media that I wouldn't normally say in public.	I don't post anything on social media before considering any negative consequences.	I can't be punished for something I post on social media.
Kruskal-Wallis H	2.679	2.636	6.536
df	5	5	5
Asymp. Sig.	.749	.756	.257

a. Kruskal Wallis Test

b. Grouping Variable: Gender

Figure 30 - The Kruskal-Wallis H test results for social media against gender

Finally, we tested the questions against socioeconomic status. The behaviour-based question returned a p-value of 0.467, so we accept the null hypothesis of $H_{3\_beh\_0}$ here for social media behaviour. However, the attitude-based question returned a p-value of less than 0.001 and the knowledge-based question returned a p-value of 0.002, so we can accept the hypothesis H_{3_att} and H_{3_kno} for social media usage in terms of attitude and knowledge. The results of the Kruskal-Wallis H test for socioeconomic status can be seen in Figure 31.

Test Statistics[a,b]

	It doesn't matter if I post things on social media that I wouldn't normally say in public.	I don't post anything on social media before considering any negative consequences.	I can't be punished for something I post on social media.
Kruskal-Wallis H	20.914	3.574	17.351
df	4	4	4
Asymp. Sig.	<.001	.467	.002

a. Kruskal Wallis Test

b. Grouping Variable: Socioeconomic Status

Figure 31 - The Kruskal-Wallis H test results for social media against socioeconomic status

Social Media	*H_1 (Age)*	*H_2 (Gender)*	*H_3 (Socioeconomic Status)*
Knowledge	Reject	Reject	Accept
Attitude	Reject	Reject	Accept
Behaviour	Reject	Reject	Reject

Figure 32 - Hypothesis outcomes for Social Media.

4.4.5 Mobile Devices (Public Wi-Fi)

The next section of the HAIS-Q was mobile device usage, testing participant awareness around using technology outside of the home. Specifically, participants were asked to answer questions around their knowledge, attitude, and behaviour around public Wi-Fi networks

(also known as hotspots). Again, the 5-point Likert-scale is used here to determine awareness, with 1 being the lowest level of awareness and 5 being the highest level of awareness. Firstly, participants were asked to respond to 'I send personal files using a public Wi-Fi network', which is a behaviour-based question. Next, participants were asked to respond to 'I am allowed to send personal files via a public Wi-Fi network', which is a knowledge-based question. Finally, participants were asked to respond to 'It's risky to send personal files using a public Wi-Fi network', which is an attitude-based question.

The results of this question were lower than that of previous questions, with a mean of 3.19 for the behaviour-based question, a mean of 3.04 for the knowledge-based question, and a mean of 3.88 for the attitude-based question. This is further reinforced by the median, which resulted in a median of 3 for the behaviour and knowledge-based questions and a median of 4 for the attitude-based question. The mode was also mixed, with a mode of 4 for the behaviour and attitude-based questions and a mode of 3 for the knowledge-based question. The standard deviation was significantly lower for the attitude-based question at 0.823 than it was for the knowledge (1.057) and behaviour (1.080) questions. Furthermore, this is reinforced by the variance, with the attitude question again having the lowest result here at 0.677 compared to the knowledge and behaviour questions at 1.117 and 1.165 respectively.

This indicates that the spread of results was narrower for the attitude-based question. The full breakdown of descriptive statistics for this section of questions can be seen in Figure 33.

Statistics

		I send personal files using a public Wi-Fi network.	I am allowed to send personal files via a public Wi-Fi network.	It's risky to send personal files using a public Wi-Fi network.
N	Valid	691	691	691
	Missing	0	0	0
Mean		3.19	3.04	3.88
Median		3.00	3.00	4.00
Mode		4	3	4
Std. Deviation		1.080	1.057	.823
Variance		1.165	1.117	.677
Range		4	4	4

Figure 33 - The descriptive statistics for the mobile devices section questions

To test the hypotheses, Kruskal Wallis tests were run for the mobile devices section against the three independent variables of age, gender, and socioeconomic status.

Firstly, the tests were run to test whether age affects a person's level of mobile devices cyber awareness. The p-value results for the behaviour and knowledge-based question tests were greater than 0.05, therefore we must accept the null hypotheses of $H_{1\_beh\_0}$ and $H_{1\_kno\_0}$ for this. However, the p-value result of the attitude-based question was 0.008, which is statistically significant. Therefore, we can accept the H_{1_att} hypothesis in terms of attitude towards mobile device usage. The full results of this Kruskal-Wallis H test can be seen in Figure 34.

Test Statistics[a,b]

	I send personal files using a public Wi-Fi network.	I am allowed to send personal files via a public Wi-Fi network.	It's risky to send personal files using a public Wi-Fi network.
Kruskal-Wallis H	3.785	1.411	9.738
df	2	2	2
Asymp. Sig.	.151	.494	.008

a. Kruskal Wallis Test

b. Grouping Variable: Age

Figure 34 - The Kruskal-Wallis H test results for mobile devices against age

Next, we tested to see whether gender affects a person's level of mobile device cyber awareness. The p-value results of these tests also came back all greater than 0.05, so therefore we have to accept the null hypotheses of $H_{2\_kno\_0}$, $H_{2\_att\_0}$, and $H2_{\_beh\_0}$. The full results of this Kruskal-Wallis H test can be seen in Figure 35.

Test Statistics[a,b]

	I send personal files using a public Wi-Fi network.	I am allowed to send personal files via a public Wi-Fi network.	It's risky to send personal files using a public Wi-Fi network.
Kruskal-Wallis H	10.464	5.984	3.287
df	5	5	5
Asymp. Sig.	.063	.308	.656

a. Kruskal Wallis Test

b. Grouping Variable: Gender

Figure 35 - The Kruskal-Wallis H test results for mobile devices against gender

Finally, we tested mobile device usage against socioeconomic status (Figure 36). The p-value result of the attitude-based question is 0.158, which is greater than 0.05 and so we accept the null hypothesis of $H_{3\_att\_0}$ here in terms of attitude towards mobile device usage. However, the p-value results of the behaviour and knowledge-based questions were 0.007 and 0.002 respectively, which are both less than 0.05. This means that they are statistically significant, and we can therefore accept the hypotheses for H_{3_beh} and H_{3_kno} in terms of behaviour and knowledge towards mobile device usage.

Test Statistics[a,b]

	I send personal files using a public Wi-Fi network.	I am allowed to send personal files via a public Wi-Fi network.	It's risky to send personal files using a public Wi-Fi network.
Kruskal-Wallis H	14.030	17.374	6.611
df	4	4	4
Asymp. Sig.	.007	.002	.158

a. Kruskal Wallis Test

b. Grouping Variable: Socioeconomic Status

Figure 36 - The Kruskal-Wallis H test results for mobile devices against socioeconomic status

Mobile Devices (Public Wi-Fi)	*H_1 (Age)*	*H_2 (Gender)*	*H_3 (Socioeconomic Status)*
Knowledge	Reject	Reject	Accept
Attitude	Accept	Reject	Reject
Behaviour	Reject	Reject	Accept

Figure 37 - Hypothesis outcomes for Mobile Devices (Public Wi-Fi)

4.4.6 Information Handling

Participants were asked three questions on the topic of information handling the next section. Specifically, participants were asked to respond to questions that targeted their knowledge, attitude, and behaviour towards discovering an unknown USB. Same as the previous sections,

participants were asked to respond via a 5-point Likert-scale. Firstly, participants were asked to respond to 'If I find a USB stick in a public place, I shouldn't plug it into my computer', which is a knowledge-based question. Next, participants were asked 'If I find a USB stick in a public place, nothing bad can happen if I plug it into my computer', which is an attitude-based question. Finally, participants were asked 'I wouldn't plug a USB stick found in a public place into my computer', which is a behaviour-based question.

The results of this section were higher than previous sections, with a mean of 3.94 for the knowledge-based question, a mean of 3.70 for the attitude-based question, and a mean of 4.07 for the behaviour-based question. Furthermore, the median and mode answers for all these questions is 4. This indicates that, on average, participants have confidence in knowing how to deal with discovering an unknown USB. The lowest standard deviation and variance for this section lies within the behaviour question, with a standard deviation of 0.777 and a variance of 0.603. This is closely followed by the knowledge question which has a standard deviation of 0.896 and a variance of 0.802. This shows that these results are narrowly spread. The question with the most spread results is the attitude question, with a standard deviation of 1.043 and a variance of 1.088. The full breakdown of descriptive statistics for the information handling section questions can be seen in Figure 38.

Statistics

		If I find a USB stick in a public place, I shouldn't plug it into my computer.	If I find a USB stick in a public place, nothing bad can happen if I plug it into my computer.	I wouldn't plug a USB stick found in a public place into my computer.
N	Valid	691	691	691
	Missing	0	0	0
Mean		3.94	3.70	4.07
Median		4.00	4.00	4.00
Mode		4	4	4
Std. Deviation		.896	1.043	.777
Variance		.802	1.088	.603
Range		4	4	4

Figure 38 - The descriptive statistics of the information handling section questions

To test the hypotheses, the information handling section questions were tested against the three independent variables of age, gender and socioeconomic status using Kruskal Wallis tests.

Firstly, the tests were carried out to test whether age affects a young adult's information handling awareness (Figure 39). All the results carried out against age were greater than 0.05, indicating that there is no statistical significance that exists here. Therefore, we accept the null hypotheses of $H_{1\_kno\_0}$, $H_{1\_att\_0}$, and $H_{1\_beh\_0}$.

Test Statistics[a,b]

	If I find a USB stick in a public place, I shouldn't plug it into my computer.	If I find a USB stick in a public place, nothing bad can happen if I plug it into my computer.	I wouldn't plug a USB stick found in a public place into my computer.
Kruskal-Wallis H	3.341	5.908	.837
df	2	2	2
Asymp. Sig.	.188	.052	.658

a. Kruskal Wallis Test

b. Grouping Variable: Age

Figure 39 - The Kruskal-Wallis H test results for information handling against age

Next, tests were carried out to determine whether gender affects a young adult's information handling awareness (Figure 40). Again, all the p-values returned from these Kruskal Wallis tests were greater than 0.05, indicating that no statistical significance exists here. So, we accept the null hypotheses of $H_{2\_kno\_0}$, $H_{2\_att\_0}$, and $H_{2\_beh\_0}$.

Test Statistics[a,b]

	If I find a USB stick in a public place, I shouldn't plug it into my computer.	If I find a USB stick in a public place, nothing bad can happen if I plug it into my computer.	I wouldn't plug a USB stick found in a public place into my computer.
Kruskal-Wallis H	2.121	6.407	8.341
df	5	5	5
Asymp. Sig.	.832	.269	.138

a. Kruskal Wallis Test

b. Grouping Variable: Gender

Figure 40 - The Kruskal-Wallis H test results for information handling against gender

Finally, we ran the Kruskal Wallis tests against socioeconomic status to determine whether this independent variable has an effect on a young adult's level of information handling

awareness (Figure 41). Both the knowledge and behaviour-based question tests resulted in p-values greater than 0.05, indicating that no statistical significance exists for these, so we accept the null hypotheses $H_{3\_kno\_0}$ and $H_{3\_beh\_0}$. However, the p-value result of the attitude-based question is 0.011, which means that we can accept the hypothesis H_{3_att} for socioeconomic status having an effect on a young adult's attitude towards information handling.

Test Statistics[a,b]

	If I find a USB stick in a public place, I shouldn't plug it into my computer.	If I find a USB stick in a public place, nothing bad can happen if I plug it into my computer.	I wouldn't plug a USB stick found in a public place into my computer.
Kruskal-Wallis H	1.178	13.088	6.713
df	4	4	4
Asymp. Sig.	.882	.011	.152

a. Kruskal Wallis Test

b. Grouping Variable: Socioeconomic Status

Figure 41 - The Kruskal-Wallis H test results for information handling against socioeconomic status

Information Handling	*H_1 (Age)*	*H_2 (Gender)*	*H_3 (Socioeconomic Status)*
Knowledge	Reject	Reject	Reject
Attitude	Reject	Reject	Accept
Behaviour	Reject	Reject	Reject

Figure 42 - Hypothesis outcomes for Information Handling.

4.4.7 Incident Reporting

The final section of the HAIS-Q is incident reporting. This section asks participants questions testing their knowledge, attitude, and behaviour towards reporting something that they deem to be suspicious. Again, participants were asked to answer the questions according to

a 5-point Likert-scale, with 5 showing the highest level of awareness and 1 showing the lowest level of awareness. The first question for participants in this section was 'If I ignore someone acting suspiciously at school or work, nothing bad can happen', which is an attitude-based question. Next, participants were asked 'If I saw someone acting suspiciously at school or work, I would do something about it', which is a behaviour-based question. Finally, participants were asked 'If I see someone acting suspiciously at school or work, I should report it', which is a knowledge-based question.

The first tests that were run on this were average tests. The mean of the attitude-based question was 3.47, the mean of the behaviour-based question was 3.49, and the mean of the knowledge-based question was 4.06. Furthermore, the median and mode averages were consistent in this section, with an average of 4 across all questions for both the median and modes. The knowledge-based question had the most confident answers here, with the lowest standard deviation of 0.870 and the lowest variance of 0.758. This is followed by the behaviour-based question, with a standard deviation of 0.919 and a variance of 0.844. Finally, the attitude-based question had the widest spread of results with a standard deviation of 1.023 and a variance of 1.046. The full breakdown of the descriptive statistics for the incident reporting section questions can be seen in Figure 43.

Statistics

		If I ignore someone acting suspiciously at school or work, nothing bad can happen.	If I saw someone acting suspiciously at school or work, I would do something about it.	If I see someone acting suspiciously at school or work, I should report it.
N	Valid	691	691	691
	Missing	0	0	0
Mean		3.47	3.49	4.06
Median		4.00	4.00	4.00
Mode		4	4	4
Std. Deviation		1.023	.919	.870
Variance		1.046	.844	.758
Range		4	4	4

Figure 43 - The descriptive statistics of the incident reporting section questions

The incident reporting questions were then tested using Kruskal Wallis to test the hypotheses and whether a young adult's level of incident reporting awareness is affected by any of the independent variables of age, gender, and socioeconomic status.

Firstly, the Kruskal Wallis tests were carried out against age. All the p-value results of these tests returned values greater than 0.05, indicating that there is no statistical significance. Therefore, we can accept the null hypotheses for $H_{1\_kno\_0}$, $H_{1\_att\_0}$, and $H_{1\_beh\_0}$. The results of this Kruskal-Wallis H test can be seen in Figure 44.

Test Statistics[a,b]

	If I ignore someone acting suspiciously at school or work, nothing bad can happen.	If I saw someone acting suspiciously at school or work, I would do something about it.	If I see someone acting suspiciously at school or work, I should report it.
Kruskal-Wallis H	.296	.064	.915
df	2	2	2
Asymp. Sig.	.863	.969	.633

a. Kruskal Wallis Test

b. Grouping Variable: Age

Figure 44 - The Kruskal-Wallis H test results for incident reporting against age

Next, we tested the questions against gender (Figure 45). The p-value of the attitude question was 0.193, indicating no statistical significance, so we accept $H_{2\_att\_0}$. However, the p-value result of the behaviour-based question was 0.027 and the p-value result of the knowledge-based question was 0.001, indicating statistical significance. Therefore, we can accept the hypotheses for H_{2_beh} and H_{2_kno} that gender affects a young adult's level of incident handling awareness in terms of behaviour and knowledge.

Test Statistics[a,b]

	If I ignore someone acting suspiciously at school or work, nothing bad can happen.	If I saw someone acting suspiciously at school or work, I would do something about it.	If I see someone acting suspiciously at school or work, I should report it.
Kruskal-Wallis H	7.388	12.668	20.356
df	5	5	5
Asymp. Sig.	.193	.027	.001

a. Kruskal Wallis Test

b. Grouping Variable: Gender

Figure 45 - The Kruskal-Wallis H test results for incident reporting against gender

Finally, we tested the results against socioeconomic status (Figure 46). The p-value result of the attitude-based question was 0.188, indicating no statistical significance, so we accept the null hypothesis of $H_{3\_att\_0}$. However, the p-value result of the behaviour-based question was 0.002. Moreover, the p-value result of the knowledge-based question was 0.046. These both indicate statistical significance and therefore we can accept the hypotheses H_{3_beh} and H_{3_kno}

that socioeconomic status affects the level of incident reporting awareness of young adults in terms of behaviour and knowledge.

Test Statistics[a,b]

	If I ignore someone acting suspiciously at school or work, nothing bad can happen.	If I saw someone acting suspiciously at school or work, I would do something about it.	If I see someone acting suspiciously at school or work, I should report it.
Kruskal-Wallis H	6.149	16.483	9.691
df	4	4	4
Asymp. Sig.	.188	.002	.046

a. Kruskal Wallis Test

b. Grouping Variable: Socioeconomic Status

Figure 46 - The Kruskal-Wallis H test results for incident reporting against socioeconomic status

Incident Reporting	*H_1 (Age)*	*H_2 (Gender)*	*H_3 (Socioeconomic Status)*
Knowledge	Reject	Accept	Accept
Attitude	Reject	Reject	Reject
Behaviour	Reject	Accept	Accept

Figure 47 - Hypothesis outcomes for Incident Reporting.

4.5 Qualitative Data

The final question that participants were asked in the questionnaire was not part of the HAIS-Q. Instead, it was an open question that allowed us to gather some qualitative data from participants. The question that participants were asked was 'What do you think it means to be a victim of a cyber-attack?'. The results of this question were varied. Some participants were dismissive of the question, simply answering 'no' or leaving the question blank. On the other hand, several participants openly shared their views of what they believe it means to be a victim of a cyber-attack. One response was 'Someone steals information, files, data etc. from your devices; people are mean to you online e.g., on social media; you click a link, and

your device stops working'. Many of the responses discussed how it would affect their lives and make them anxious about using technology. Several even discussed how this could affect their life offline too, putting their physical safety at risk. Privacy was a common theme amongst responses. One participant detailed how 'if one aspect of your online life is compromised then it has a ripple effect, and you lose everything'. Another common theme across responses was the economic losses in addition to business losses.

4.6 Chapter Summary

Chapter Four presents the results of the research. Firstly, we look at how the data was cleansed before the results could be presented. This involved creating meaningful variable names in the statistical analysis software and removing incomplete entries. The results of the Cronbach's Alpha tests are then presented, which test for the reliability of the collated results. Then, the results of the participant demographics are presented. This includes data about the age, gender, and socioeconomic status of those who participated in this research. The chapter then looks at the results of the HAIS-Q questions, for each section firstly looking at the descriptive statistics (mean, median, mode, standard deviation, and variance) and then running Kruskal Wallis-H tests on the data against age, gender, and socioeconomic status to test the hypotheses. The final section of the chapter discusses the results of the qualitative question that was asked at the end of the questionnaire.

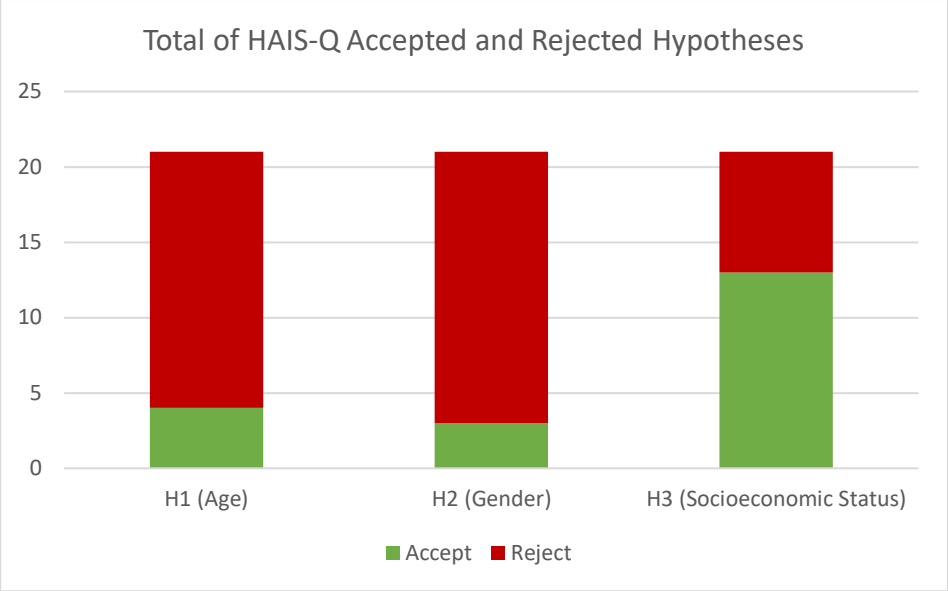

Figure 48 - Bar chart showing the total of accepted and rejected hypotheses across all HAIS-Q categories in this chapter.

Chapter Five: Discussion

5.1 Reliability

Cronbach's Alpha is sensitive to the number of items that are being tested (Glen, 2022). In each of the Cronbach's Alpha tests, seven items were tested (21 in total, making up the full subset of the HAIS-Q questions that were asked). This is a low number of items, which is likely to have affected the results of Cronbach's Alpha. The result of the Cronbach's Alpha shows that the Likert-scale questions asked in this research are of varying degrees of reliability, with the attitude questions being the most reliable questions and the behaviour questions being the least reliable. This is likely because the original HAIS-Q was adapted for the purpose of this research, to make it more appropriate for the age demographic. Due to the average time that participants took to take this questionnaire (10 minutes), it is likely that the full HAIS-Q would be appropriate for this age demographic. In future research, participants of this age demographic could be asked to complete the full HAIS-Q questionnaire. This is likely to be a more reliable measure of cyber security awareness and therefore it is likely that this would return a higher result in the Cronbach's Alpha tests.

5.2 Demographics

The gender split of the participants in the UK is near evenly split, with 50.7% of the population identifying as female and 49.5% of the population identifying as male (Statista, 2021). The gender split of those participants in this research was 51.8% male and 45% female. Moreover, 0.6% of the participants identified as non-binary or third gender, 0.1% identified as transgender, 1% identified as 'other' and 1.4% preferred not to say. Whilst this is a slightly different split to the entirety of the population, it is difficult to accurately measure this data

as the figure is constantly changing and so the gender split for this research is representative of the population, as there is a maximum of 5.7% difference in this research's gender split when compared with the full population. Whilst this is a good result to have organically collected, there were no measures put in place to ensure that a representative gender split was accumulated. This is due to recruiting participants openly on social media, where these factors cannot be controlled. In future research, participant screener tests could be put in place to obtain a more accurately representative pool of participants. These screener tests could ask prospective participants for their demographic information (such as gender) to determine if they are a fit for taking the questionnaire. A count could be implemented to measure the number of participants and their demographic information so that this can be controlled more closely. However, caution would have to be considered to ensure that the participant selection is still random enough to be fully representative of the full population.

The next demographic question was focussed on the level of education that participants' parents had completed. This is one of the factors that made up the socioeconomic status variable of participants, collectively with whether the participant has ever received free school meals. In the UK, it is estimated that around 80% of adults aged 19 to 64 hold a NQF Level 2 or above qualification (equivalent to the completion of secondary school). Moreover, it is estimated that around 60% of adults aged 19 to 64 hold a NQF Level 3 or above qualification (equivalent to further education). Finally, it is estimated that around 40% of adults aged 19 to 64 hold a NQF Level 4 or above qualification (equivalent to university level) (Department for Education, 2019). The full gender breakdown of this data can be seen in Figure 49. Comparing this to the data collected in this research, 34.9% of participants' parents had completed university, which is comparable to the estimated 40% of the population that

holds a Level 4 qualification. Contrastingly, 17.2% of participants parents had completed level 3, which is significantly lower than the 60% of adults who hold a NQF Level 3 qualification. Moreover, 30.8% of participants parents had finished secondary school, which again is lower than the national average. The national data is based on estimates and is also cumulative, so this is a challenge that we face when comparing the data points. However, as the Level 4 national qualification data is in line with the participant data, we can be confident that the data is, on the whole, representative of the general population.

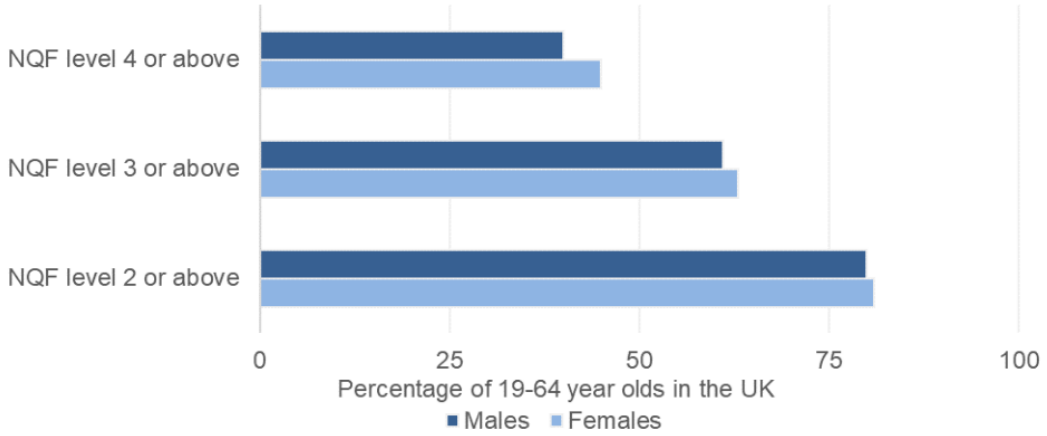

Figure 49 - The level of qualifications held by 19- to 64-year-olds in the UK by age and gender (Department for Education, 2019)

The next demographic data point was whether participants were currently receiving free school meals and if they were not in education, they needed to answer for when they were in school. This question provides the household income element to socioeconomic status. The majority of participants answered that they had received free school meals (57.2%). The national number of pupils who are eligible for free school meals is 19.7% (UK Government, 2021). Therefore, our data is almost three times the national average for those who receive free school meals, which shows that this is not representative of the national population. Despite this, we are not basing socioeconomic status solely on income. This data combined

with the parents' education level will combine to make a more reliable measure of socioeconomic status. In future research, the participant recruitment could be more controlled to ensure a participant pool that is more representative of the general population, for example by providing participants with screener tests to determine what their socioeconomic status is, in addition to using a count to track participant numbers for each level. By doing this, we could more closely control the participant pool so that we have the same percentage of participants for each group so that it is the same percentage of each socioeconomic group within the UK.

The final demographic point was age. All participants in this research had to be aged either 16, 17, or 18 at the time of completing the HAIS-Q questionnaire. This is because the research question is to determine the level of cyber security awareness of young adults aged 16 to 18 years old. The split of the participants was almost equal, with 23.4% 16-year-olds, 38.2% 17-year-olds, and 38.4% 18-year-olds. These are incremental, with the lowest number of participants being 16 years old and the highest number of participants being 18 years old. The number of 16-year-olds in the UK in 2020 was 740,693, the number of 17-year-old was 722,928 and the number of 18-year-olds was 717,252 (Statista, 2021). Whilst all similar numbers (in the 700,000s), the number is 16-year-olds was the highest and the number of 18-year-olds was the lowest, which is the reverse of the results from this data. Despite this, the results were split generally evenly, so we can deduce that these are representative of the population. The demographics of the participants who completed this questionnaire was not controlled; the participants who completed the questionnaire were completely random. As long as a participant was aged 16, 17, or 18 and currently lived in the UK, they were eligible

to complete the questionnaire. In further research, this could be controlled to ensure a completely even split to ensure complete representation of the population.

5.3 HAIS-Q

To test the hypotheses, we used Kruskal Wallis H tests for each of the HAIS-Q questions in each of the sections for each of the hypotheses. As there were 21 HAIS-Q questions asked in this questionnaire and there are three hypotheses to test, this meant that 63 Kruskal Wallis H tests were carried out in total. As there is little research done in the area of cyber security awareness, we did not want to assume a normal distribution for the collected data. Therefore, the Kruskal Wallis H test was appropriate as it is a non-parametric test. The data was run through SPSS to determine the statistical results of the Kruskal Wallis H tests. The Kruskal Wallis H statistic is calculated using the formula that can be seen in Figure 50.

$$H = \left(\frac{12}{n(n+1)} \sum_{j=1}^{c} \frac{T_j^2}{n_j} \right) - 3(n+1)$$

Figure 50 - The calculation for the Kruskal-Wallis H statistic (Glen, 2022)

In the formula, n is the sum of sample sizes for all samples, c is the number of samples, T_j is the sum of ranks in the j^{th} sample, and n_j is the size of the j^{th} sample (Glen, 2022).

5.3.1 Password Management

The question that participants showed the highest level of cyber security awareness of in terms of password management was the knowledge-based question. This was followed by the behaviour-based question and the attitude-based question respectively. We know this as

the average for the knowledge-based question was the highest and the variation in participant responses was the smallest. Interestingly, this could be because participants have the knowledge of what makes a strong password; however, this is challenged more in their practices of creating their own strong passwords in their daily activities (based on their attitude and behaviour towards passwords). There may be a discrepancy that exists between a young adult knowing what a strong password is and then actually applying this knowledge.

In terms of statistical significance of password management against the independent variables of socioeconomic status, gender, and age, there were two tests that resulted in statistical significance. *The first being a young adult's attitude towards password management is affected by age and the second being that a young adult's behaviour towards password management is affected by their socioeconomic status.*

5.3.2 Email Usage

The next section of questions was based around email usage. Again, these tested a participant's awareness in terms of three dimensions: attitude, behaviour, and knowledge. Interestingly, a similar trend occurred in the email usage results as the results of the password management questions. The question that showed the highest level of cyber awareness was the knowledge-based question. This was followed by the behaviour-based question and then the attitude-based question. Several campaigns have been done on the topic of clicking on links in emails that have been sent from unknown senders, with software even being developed that sends out a 'fake' phishing email to test whether its receivers will click on it (KnowBe4, 2022). It is clear from the results that young adults know that they should not be clicking on links in emails from unknown senders. However, due to the results in the attitude

and behaviour-based questions, this indicates that young adults may not be applying this knowledge in their everyday cyber hygiene practices. Similar to password management, there exists some discrepancies here. Further research could be done in this area to identify what the cause behind this is and what needs to be done to get young adults to enforce that knowledge and, most importantly, apply their cyber security knowledge.

5.3.3 Internet Usage

Participants were asked to answer questions on their internet usage next, specifically around their knowledge, attitude, and behaviour towards downloading files. The first question, 'it can be risky to download files on my computer', tests a participant's attitude towards downloading files from the internet. Whenever a person downloads a file from the internet, there is always a level of risk associated with that download. The extent to the risk is dependent on factors such as where the file is being downloaded from, what computer the file is being downloaded to, and the network that the file is being downloaded over (for example, whether the file is being downloaded over a public or a private network). Therefore, this question helps us to understand to what extent participants understand about these risks that are associated with file downloads. The next statement that participants were asked to respond to is behaviour-based: 'I download any files onto my computer that will help me get my work done'. This question directly asks participants whether they will consider downloading anything from the internet, so long as it can contribute to their aim of completing their work. Specifically, this question helps us to understand the extent to which participants can balance the risks associated with downloading files from the internet with the ability to be able to complete their work successfully. The final statement is knowledge-based: 'I am allowed to download any files onto my computer if they help me to do my work'.

Here, participants have to determine to what extent they believe that they are allowed to download files from the internet. Similar to the behaviour-based question, participants are balancing two key factors here: downloading files from the internet and completing their work. If their work depends on them downloading a file, participants may be more inclined to believe that they are allowed to download any files that will help them to achieve this. There are several factors that need to be considered here to determine whether you are allowed to download a file, including the website, the legality of the download, the legitimacy of the file, and the computer that the file is being downloaded to.

The initial statistical results for this section showed that, with a higher mean and lower standard deviation and variance, participants had the best awareness of downloading files from the internet in terms of their attitude towards this. Participants were less aware of file download security in terms of behaviour and knowledge. On the whole, participants had the right attitude towards downloading files from the internet, but they were not sure how to apply this in terms of the act of downloading a file (behaviour) and knowing to what extent it is risky to download files (knowledge). These results indicate that this is a potential area that future cyber awareness work needs to target. When we ran Kruskal Wallis tests against the data to test the hypotheses, we had to accept the null hypothesis for all but one of the results. *The result that showed statistical significance was behaviour against socioeconomic status. This shows that socioeconomic status has an effect on a person's behaviour on how they use the internet (specifically in this case, when it comes to downloading a file from the internet).*

5.3.4 Social Media Usage

Participants were asked to consider their social media usage for the next section of the HAIS-Q questions. Specifically, the questions were focussed on posting to social media. Participants were firstly asked to respond to an attitude-based question that tested participants on how they compare social media to reality. By asking participants this, it is testing their awareness as to whether they believe there is a disconnect between social media and the offline world. Social media has an anonymous feel to it in the sense that anyone can post whatever they like to it (as long as it is within the guidelines); this question is specifically designed to target this and asks participants to consider whether they feel as though they could say the same things that they post on social media as they could offline in reality. Secondly, participants were asked a behaviour-based question, which tests whether a participant thinks of the consequences of their actions before they post to social media. It is quick and easy to upload a post to social media, however depending on the content of what has been posted, there can be repercussions and potentially negative consequences that have to be considered. Finally, participants were asked a knowledge-based question, which asks participants to consider whether they can be punished for something that they post on social media. Again, social media has an anonymous tone to it (especially if an account is made under a pseudonym) and the laws around social media are constantly evolving. Therefore, this question is designed to test participants on the extent to which they feel as though they can be punished for posting something on social media.

The results of this question showed a consistent average. The mean results were slightly lower than the median and mode results, with an overall mean of 3. The best score in terms of cyber security awareness is 5 and the worst score is 1. The mean of 3 therefore indicates that on

average, participants were in the middle ground for this section. Despite this, the median and mode averages had a consistent result of 4, indicating that participants were on average aware of best practices for social media, however as the result was not 5, there is clear room for improvement in this area. The standard deviation and variance were significantly lower for the behaviour-based question than the attitude and knowledge-based questions, indicating that participants are more confident in terms of how they behave on social media as opposed to having the background knowledge of social media best practices. This indicates that knowledge around social media (for example, freedom of speech and social media laws) could be an area of awareness that needs to be targeted in future cyber awareness work for 16- to 18-year-olds.

In terms of statistical significance, we had to accept the null hypothesis for the Kruskal Wallis social media tests against age and gender. However, we could accept the hypothesis that there is statistical significance that exists between social media usage and socioeconomic status. *Specifically, there is statistical significance between socioeconomic status and 16-to-18-year old's attitude and knowledge of social media.*

5.3.5 Mobile Devices

Next, participants were asked to answer questions around their mobile phone usage. Typically, mobile phones are portable and are used out and about, for example at school, coffee shops, and other public spaces. This is why the HAIS-Q questions in this section are around the use of public wi-fi networks. There is a significant amount of public wi-fi networks available that anyone can connect to in order to get access to the internet. The number of public wi-fi hotspots has grown from 94 million in 2016 to 549 million in 2022 (Statista, 2022).

Regardless of what device someone is using, it is important to be aware of the risks associated with using a public wi-fi network. There are several common attacks that target public hotspots, such as the Man-in-the-Middle attack, where the connection can be intercepted by an attacker and unencrypted data can be easily sourced. In these attacks, an unsuspecting victim can connect to a 'fake' wi-fi hotspot that has been set up by an attacker, which diverts all of the traffic from the victim's computer through to the attacker's hotspot. If the data is unencrypted, this can be accessed straight away in plaintext. This makes it especially important to always use websites and services that are encrypted, to ensure that even if you are connected to a cyber attacker's hotspot, your data will have an extra layer of protection. For these reasons, it is important to consider the dangers of public wi-fi networks and unencrypted websites and services when designing cyber awareness training, to ensure that young adults understand how to secure their data whilst in a public space.

The results of this question showed a lower average than previous questions, which indicates that participants were less aware of how to handle public wi-fi networks than other areas of cyber security. This could be due to how common public wi-fi networks are. Due to how common public wi-fi networks are, there may exist a false sense of security. People need to know when they should use public wi-fi networks (if they have to) and the risks associated with them, so that people are well-informed and can make their own decisions about whether they wish to use public wi-fi networks. In terms of averages, the lowest average result was for the knowledge-based question. This shows that there is a potential lack in knowledge around public wi-fi networks. If the knowledge is lacking, then this will have an effect on the correct application and usage of public wi-fi networks. Participants had the most confidence in the attitude-based question, as this result had the lowest standard deviation and variance

compared to the behaviour and knowledge-based questions. This shows that participants were more consistent in their attitude towards using public wi-fi networks.

When it came to testing the hypotheses in terms of cyber awareness of mobile device usage, we had three statistically significant results. The first was mobile device usage attitude against age, the second was mobile device usage behaviour against socioeconomic status, and the third was mobile device usage knowledge against socioeconomic status. *These results show that both age and socioeconomic status can be factors in affecting a person's level of cyber security awareness in terms of their mobile device usage, specifically focused on the usage of public wi-fi networks.*

5.3.6 Information Handling

In the next section, participants were asked to answer questions on the topic of information handling. Specifically, they were asked about their awareness of dealing with an unknown USB stick. There are several dangers associated with finding a USB stick, as it is a tactic commonly used in social engineering. Several cases have occurred where a person has found a USB stick and plugged it into their computer to find out what is on it (or perhaps, to discover who it belongs to). Unfortunately, if this is a malicious attack, the USB could contain software such as viruses or keyloggers, which could track the user's activity and inputs, even when the USB has been removed. Therefore, it is important that people are aware of the risks associated with finding an unknown USB and thus what the best cyber hygiene practices are in terms of information handling. Moreover, if young adults are aware of the risks, this will be greatly beneficial in terms of their future employment, as these types of attacks typically

target the workplace where there is likely to be vast amounts of personal data or financial information.

The results of this section were higher than those of the previous sections, which indicates a promising confidence that young adults know how to deal with finding an unknown USB. The highest result for this section that would indicate the highest level of awareness is 5 and the average of all answers was 4. Therefore, this shows that there is a strong confidence of knowledge, attitude, and behaviour. However, there is still room for improvement to ensure that all young adults are very confident in how to handle a situation in which they discover an unknown USB and that they know the risks that are associated with plugging an unknown USB into a computer. The question with the lowest standard deviation and variance is the behaviour question, which indicates that this is the question that, on the whole, participants were most confident in answering as the results are the most similar and not as spread as the knowledge and attitude questions. This shows that it is potentially more instinctual for a young adult to know what to do upon discovering an unknown USB; the behaviour towards this is most natural for the young adults even when compared to knowledge.

In terms of statistical analysis, there was only one statistically significant result in this section. Both independent variables of age and gender have no effect on a young adult's level of information handling awareness. *However, socioeconomic status does have an effect on a young adult's attitude towards information handling.*

5.3.7 Incident Reporting

Incident reporting is the final section of the HAIS-Q. This section is not specific to technology; however, it is more focussed on the social engineering aspect of cyber security. These questions test a young adult's knowledge, attitude, and behaviour towards reporting something that they deem as suspicious. However, with this, it is also about being aware of and being able to recognise what suspicious behaviour is. Similar to the previous sections, participants were asked questions that tested whether they knew how to deal with the situation (knowledge), whether they would act in the situation (behaviour), and what their general outlook towards the situation is (attitude).

Results of this section showed, on the whole, a good level of understanding and awareness of incident reporting. The result with the lowest average was attitude, with the highest average being knowledge. Similar to other sections, this shows that it is likely that young adults have the knowledge on how to handle a situation that involves reporting an incident, however they are not as confident in their ability to act on this (in terms of behaviour in the HAIS-Q). To reinforce this, the standard deviation and variance results were lowest for the knowledge-based question, which indicates that young adults were most confident in their knowledge on incident reporting as the results were spread less than those in the attitude and behaviour questions. In fact, the question that had the most spread results was the attitude-based question. This shows that young adult's attitude towards incident reporting was the least confident as results were the most varied.

In terms of statistical analysis, the results that showed statistical significance were the behaviour and knowledge-based questions against age and the behaviour and knowledge-based questions against socioeconomic status.

5.4 Qualitative Data

At the end of the questionnaire, participants were asked an open question. This was to gather some qualitative data. The HAIS-Q provided us with quantitative data, however we wanted to take a mixed-methods approach to the research and so providing the participants with an opportunity to share their views allowed us to achieve this mixed-methods goal. The question that participants were asked is 'What do you think it means to be a victim of a cyber-attack?'. This question allows participants to share their views on cyber-attacks to provide us with an understanding of how participants perceive victims of cyber-attacks and the repercussions that being a victim of a cyber-attack can have. The results of this question varied immensely. The fact that some participants were very dismissive of the question indicates that perhaps they are not interested in what it means to be a victim of a cyber-attack. Furthermore, some participants did not answer this question at all. If this research were to be repeated in the future, it would potentially be beneficial to make this question compulsory to answer. Furthermore, further qualitative research could be carried out to understand perspectives of cyber security and lived experiences. Regardless, as the focus of this research was the HAIS-Q, this is why the qualitative question was not compulsory for participants to complete. The key themes that were evident in the responses were the effect it would have on a victim's life (in terms of mental health and physical safety), privacy, economic loss, and business loss. It was promising to see common points being raised in the answers to this question, as this shows a strong understanding amongst participants of the potential damages that being a

victim of a cyber-attack can have. Furthermore, participants had taken this further and discussed the impact that it could have on businesses too (for example, business financial losses). As people are at the root of security, cyber security awareness is vital for employees. The more awareness of cyber security a young adult has, the better foundations of cyber security they will have as future employees.

5.5 Chapter Summary

Chapter Five is a discussion of the results. Firstly, the reliability of the results is discussed, with reference to the results of the Cronbach's Alpha tests. Participant demographics are discussed next, with a comparison of these to the population, to determine the extent to which this participant pool was representative of the population. The different sections of the HAIS-Q are discussed next. Within each section, the results are interpreted, and the wider context of each topic is discussed. Finally, the results of the qualitative data are discussed, with key themes from the collated data being outlined.

Chapter Six: Conclusion and Future Work

The aim of this research was to determine the level of cyber security awareness amongst young adults aged 16 to 18 who currently live in the UK. To achieve this, this research aim was broken down into four sub research questions.

6.1 SQ1

The first sub question, SQ1, asked how age, gender and socioeconomic status affect a young adult's level of cyber security awareness. To answer this question, we divided this into three hypotheses to test whether age, gender and socioeconomic status have an effect individually on a young adult's level of cyber security awareness.

To test the hypotheses, a literature review was carried out in which we discovered the Human Aspects of Information Security Questionnaire, referred to as the HAIS-Q. This questionnaire consists of 63 questions which test participant awareness from three perspectives: knowledge, attitude, and behaviour. This provides us with a holistic understanding of their level of awareness. The HAIS-Q has been previously used throughout research to test employee and university student's levels of information security awareness. As the age demographic for this research is younger than that of which the HAIS-Q has previously been used for, the HAIS-Q was reduced in length for the purpose of this research. The HAIS-Q tests cyber security awareness over seven different categories, which are password management, email use, internet use, social media use, mobile devices, information handling, and incident reporting.

Once the questionnaire had been adapted, the next step was to recruit participants. We aimed to recruit participants directly from schools and colleges from across the UK, however due to the COVID-19 pandemic, we were unable to gain access to the schools as the participant recruitment phase of this research was conducted during one of the UK lockdowns. Therefore, we had to recruit participants in alternative ways. Participants were recruited online, via social media, forums, and participant recruitment websites. In order to test that the participants met the required demographics, this was clearly described in the description of the research and screener questions were asked at the beginning of the questionnaire, which asked if the participant currently lives in the UK and what age they are. If they passed the questions, they were taken through to the HAIS-Q. Otherwise, they were sent to the end of the questionnaire and thanked for their time and consideration. Participant recruitment was open throughout the duration of Summer 2021.

Once the data had been collected, they were collated so that statistical analysis could be carried out to determine the results of the research. Initially, 811 data entries were collected from participants. However, data had to be cleansed to remove duplicate entries (the incentive of the gift cards encouraged participants to submit multiple entries) and those entries that were incomplete. After this had been done, we were left with 691 participant entries that we could analyse. To test the validity and reliability of the collected data, we firstly ran a Cronbach's Alpha test on the data. We used this as it has been successfully used before in previous studies that have used the HAIS-Q. Running the Cronbach's Alpha test gives a reliability coefficient result, which can then be used to determine how reliable the data is. Our data returned a Cronbach Alpha result of 0.657, which in terms of results, is classed as 'acceptable'. We believe that one of the key reasons this result is lower than previous HAIS-

Q studies' results is because we used a subset of the HAIS-Q questions; we used 21 questions instead of the full 63. Cronbach's Alpha is sensitive to this and is affected by the number of questions and data points that are used in a questionnaire. Therefore, to achieve improved reliability in future research, we would recommend that the full HAIS-Q questionnaire is used. Furthermore, one of the reasons why a subset of the HAIS-Q was used was because the participants were younger than those who have completed the HAIS-Q before. The HAIS-Q, at 63 questions, is an intensive time commitment. However, the results of the questionnaires show that on average it did not take participants long to complete the questionnaire, with an average of a 10-minute duration to complete the questionnaire. So, in future research the HAIS-Q is likely to be appropriate for this age demographic. However, for any future research that involves participants who are under the age of 16, it would not be recommended for these participants to take the full HAIS-Q because the questionnaire length must be appropriate for the participant's attention span which is affected by their age. Based on the results of this research, we would recommend that the HAIS-Q is appropriate for participants who are aged 16 and over.

The total number of valid responses that we could analyse for this research was 691. So, we had a total of 691 participants. This was made up of 51.8% male participants and 45% female participants (the remaining percentage did not provide an answer for the gender question). In terms of age, 23.4% of participants were aged 16, 38.2% were aged 17, and 38.4% were aged 18. Despite that no measures were put in place to ensure an accurate representation of the population, the recruitment methods returned participants that were representative of the young adult population. This was further reinforced by socioeconomic status, in which

the results were split so that we had a range of participants from all different backgrounds and socioeconomic statuses.

The first hypothesis that we tested was whether a young adult's level of cyber security awareness is affected by their age. The most common reoccurring factor that was affected by age was a young adult's attitude towards cyber security. In terms of attitude, there were three statistically significant results that showed that age affects a young adult's attitude towards cyber security. This was in terms of password management, mobile device usage, and email usage. A final statistically significant result for H_1 was that age has an effect on a young adult's knowledge towards internet usage. ***So, in total, 4 out of the 21 tests (19.05%) carried out for H_1 were statistically significant.***

The second hypothesis that we were testing was whether a young adult's level of cyber security awareness is affected by their gender. In the Kruskal Wallis tests, 3 of the 21 tests that were carried out for gender were statistically significant. The first was attitude towards internet use, the second was behaviour in incident reporting and the third was knowledge in incident reporting. Whilst these are split across the three domains of the HAIS-Q (one statistically significant result for each domain of attitude, behaviour, and knowledge), it is important to note that two of these results were in incident reporting. This shows a potential area that may need to be focussed on in terms of equal learning and application of learning between genders. ***Overall, 3 of the 21 tests (14.29%) carried out for H_2 were statistically significant.***

The third and final hypothesis that we tested was whether a young adult's level of cyber security awareness is affected by their socioeconomic status. This factor was determined by two questions asked in the demographic section of the questionnaire. The first factor is the young adult's parents' level of education, and the second factor is whether the young adult currently receives or has received in the past free school meals. These two factors determined a young adult's socioeconomic status within this research. Out of the three hypotheses, H_3 returned the highest number of statistically significant results. Socioeconomic status affects a young adult's attitude towards password management, email usage, social media usage, and information handling. It affects a young adult's behaviour towards password management, email usage, internet usage, mobile devices, and incident reporting. Finally, socioeconomic status affects a young adult's knowledge of email usage, social media usage, mobile devices, and incident reporting. The results of this show that socioeconomic status is a significant contributing factor across all seven domains of cyber security awareness and so is a key area for future cyber security awareness work. Overall, 13 out of the 21 tests (61.9%) carried out for H_3 were statistically significant. This shows that socioeconomic status is a majority contributor to affecting a young adult's level of cyber security awareness.

As we can see from the results, gender is the factor that had the least impact on a young adult's level of cyber security awareness, with three results being statistically significant. This is followed by age, with four statistically significant results. The factor that holds the most statistical significance is socioeconomic status, with 13 statistically significant results.

6.2 SQ2

The second sub question asked what cyber security awareness education young adults are currently being provided and to what extent is it effective. To answer this question, we carried out a literature review to determine what education young adults are currently being provided and we could draw upon our results from the questionnaire to determine how effective it is.

From carrying out the literature review, it was evident that minimal research had been published in the area of cyber security awareness education for young adults, with the focus being on education for professionals and employees. Most research studies that were conducted on children and young adults had been carried out in other countries outside of the UK. For example, we discovered that one study carried out in South Africa found that 80% of secondary school students have smartphones but are leaving school with no cyber security education (Ventera et al., 2019). Moreover, in Norway, research is being carried out on gamification of cyber security education, where new tools are being designed to make cyber security education more innovative and engaging for young adults (Quayyum, 2020). Several YouTube videos were also found during our literature review that aimed to educate young adults on cyber security awareness. Whilst these videos could be shown in schools, we could not find evidence of this and so there is a focus here on independent learning either from the young adults or from their parents. The NCSC provides advice and resources for schools and students, with a host of information available on their website. Schools are also gaining recognition for teaching cyber security skills, being rated bronze, silver, or gold for the NCSC's CyberFirst accreditation. However, this is more focused on encouraging young adults into the cyber security industry to reduce the skills gap, as opposed to more general cyber security

awareness training for all (even those who are not looking to pursue a career in cyber security). Despite this, the NCSC has developed a cyber security awareness game called 'Cyber Sprinters' for 7- to 11-year-olds. Moreover, a section of their website is called 'Cyber Aware' and contains vital information for any technology user. However, again we could not find any evidence that shows whether this cyber awareness information is being used in schools, so again there is a focus on independent learning here.

We can use the results of our research to answer the second part of SQ2, which is how effective is the cyber security awareness education that young adults are being provided. For all questions in the HAIS-Q, participants had to answer using a 5-point Likert-scale, ranging from 'Strongly Disagree' to 'Strongly Agree'. Some questions within the HAIS-Q were negatively asked, so when the results were being analysed, these negatively asked questions had to be reversed so that they could be compared to the other questions. The Likert-scale relates to the scale of cyber security awareness, with 1 being the lowest level of cyber security awareness and 5 being the highest level of cyber security awareness. The weightings of the HAIS-Q also had to be applied to calculate the final level of cyber security awareness. The HAIS-Q has been designed with weightings of each domain (knowledge, attitude, and behaviour), so these had to be applied to our results. The weightings are 30% for the knowledge questions, 20% for the attitude questions, and 50% for the behaviour questions. The combined weightings make up the overall 100% of the results. With that in mind, the results of the research that were discussed in Chapter Four can be seen in Figure 51 with the applied weightings.

HAIS-Q Area	Knowledge	Attitude	Behaviour	Total	Percent (%)
Password Management	1.221	0.688	1.845	3.754	75.08
Email Use	1.215	0.736	1.680	3.631	72.62
Internet Use	0.960	0.748	1.615	3.323	66.46
Social Media	1.020	0.708	1.885	3.613	72.26
Mobile Device Use (Public Wi-Fi)	0.912	0.776	1.595	3.283	65.66
Information Handling	1.182	0.740	2.035	3.957	79.14
Incident Reporting	1.218	0.694	1.745	3.657	73.14
Total					72.05

Figure 51 - The cyber security awareness level results with weightings for each section of the HAIS-Q

As you can see, the results were similar for each of the areas of cyber security awareness. We discussed in Chapter Three what the results of the HAIS-Q mean with the weightings applied. A result of 59% or less indicates a poor level of cyber security awareness, which requires action. A result of 60% to 79% is average, with action potentially required. Finally, a result of 80% to 100% indicates a good level of cyber security awareness with no action required (Kruger et al., 2006). The results for every section of the HAIS-Q returned a result that lies in the 'average' category, with the final total result of 72.05% therefore also in this category. The weakest area of cyber security awareness is mobile device use, with the strongest being information handling. Whilst this shows that young adults aged 16 to 18 in the UK have an average level of cyber security awareness, this also indicates that there is potential improvement that needs to be done in terms of the cyber security awareness education that young adults are currently being provided. It is difficult to determine how effective the education that young adults are receiving is, as the literature review highlighted how little

research has been done in this area and so we cannot relate these results to cyber security education. There is significant potential for this research area in future work.

6.3 SQ3

The third sub question, SQ3, asked whether an intervention strategy is required to improve young adults' level of cyber security awareness and, if so, how could this be done. According to the results of this research in Figure 51, and as we have previously established, the level of young adult's cyber security awareness is average at 72.05%, so therefore an intervention strategy is required to improve young adults' level of cyber security awareness. Research carried out in Chapter Two determined how this could be done. Firstly, research is being done in the area of gamification of cyber security awareness for young adults. Whilst there is a focus on this for children, it could also be beneficial to gamify this education for young adults up to the age of 18, too. Furthermore, little cyber security awareness education is taking place in schools and colleges. As it is compulsory for everyone under the age of 18 in the UK to be in some form of education, this would be an excellent starting point for where cyber security awareness education should be provided. Resources such as those on the NCSC 'Cyber Aware' website could be used to design lesson plans around cyber security awareness, especially for young adults aged 16 to 18.

6.4 SQ4

The final sub question asks what the importance of cyber security education is for young adults. From carrying out the literature review in Chapter Two, the importance of cyber security education is immediately clear to see the importance of cyber security education. Firstly, there is a necessity for cyber security education as more young adults than ever are

using the internet (ONS, 2021). Moreover, more young adults are connected to the internet than ever before, with almost all children having their own smartphone by the age of 15 (Ofcom, 2020). Despite that there are significant benefits of using technology, which was highlighted during the pandemic when technology kept young adults connected with their family, friends and teachers, there are a rising number of cybercrimes that target young adults. For example, there are cybercrimes targeting children and young adults that involve the anonymous sharing of images, phishing, and video games (Education Policy Institute, 2017). Furthermore, there is increasing cases of cyberbullying (Cook, 2023), which is especially prevalent with the enabler of social media. The increase in usage of technology by young adults in addition to the number of cybercrimes that target young adults shows the high level of importance that cyber security education is, as it is vital that young adults know how to protect themselves on the internet.

6.5 Future Research

This research has highlighted several different areas that future research can be carried out on. Firstly, in answering SQ1, the HAIS-Q questionnaire that we conducted for this research was a subset of the original HAIS-Q questions, with our questionnaire having 21 questions instead of the original 63. As a result, this impacted the reliability of the results according to the Cronbach Alpha reliability coefficient. This research could be repeated in future with the same age demographic however with the full HAIS-Q, including all 63 questions. This is then likely to improve the reliability of the data. However, the issue is that recruiting participants may be more challenging if they are made aware that they will have to answer 63 questions. This is a more significant time commitment than the 21 questions of this research were, which is likely a contributing factor as to why we were successful in recruiting 691 participants. A

limitation of this research is that participants had to be recruited solely online due to the COVID-19 pandemic. If this research were to be repeated, participants could be recruited in-person at schools and colleges around the UK. This would help to provide a more representative sample of the demographic population.

In terms of answering SQ2, participants could have been asked what cyber security education they have received in the past. This could be quantitative or qualitative; both would be insightful to help us understand the different types of cyber security education that young adults are receiving. Furthermore, participants could be asked how long they have lived in the UK for, as this may have an effect on the type of cyber security education that they have received. Other countries may provide cyber security education in different formats, for example. Future long-term research could also be carried out over the timespan of several years, following groups from children to young adults. This would help us to thoroughly determine the extent to which young adults have received cyber security education throughout their childhood. With short-term research (for example, research being carried out in a single questionnaire), we can only measure what the participants' current level of cyber security awareness.

To conclude, the research carried out in this thesis has contributed to answering what the level of cyber security awareness is amongst young adults aged 16 to 18 in the UK. This is a developing area of research that it is vital to explore further, as our society becomes more reliant on technology and cybercrimes are increasing and becoming more sophisticated. The root of cyber security starts with people which is why cyber security awareness is key for a more secure world.

6.6 Chapter Summary

Chapter Six comprises of sections that answer the research question and sub questions of this research. We look at the results of the research from both Chapter Two and Chapter Four and use this to answer those original research questions that were defined in Chapter One. At the end of the chapter, the limitations of this research are discussed in addition to outlining the future research that needs to be done in this area.

References

Adhikari, M.K., 2018. Cyber Security Awareness Level in Teenage Group of Nepal (Thesis). Central Department of Mathematics and ICT Education.

Adults' Media Use and Attitudes report 2022, n.d. 30.

Ahmad, N., Laplante, P.A., Defranco, J.F., Kassab, M., 2022. A Cybersecurity Educated Community. IEEE Transactions on Emerging Topics in Computing 10, 1456–1463. https://doi.org/10.1109/TETC.2021.3093444

Ahmad, N., Mokhtar, U.A., Fariza Paizi Fauzi, W., Othman, Z.A., Hakim Yeop, Y., Huda Sheikh Abdullah, S.N., 2018. Cyber Security Situational Awareness among Parents, in: 2018 Cyber Resilience Conference (CRC). Presented at the 2018 Cyber Resilience Conference (CRC), pp. 1–3. https://doi.org/10.1109/CR.2018.8626830

Ahmed, N., Islam, Dr.M.R., Kulsum, U., Islam, Md.R., Haque, E., Rahman, S., 2019. Demographic Factors of Cybersecurity Awareness in Bangladesh. https://doi.org/10.1109/ICAEE48663.2019.8975603

Air Force Association, n.d. AFA CyberPatriot [WWW Document]. Air Force Association. URL https://www.uscyberpatriot.org/ (accessed 4.15.20).

Alotaibi, F., Furnell, S., Stengel, I., Papadaki, M., 2016. A Review of Using Gaming Technology for Cyber-Security Awareness. IJISR 6. https://doi.org/10.20533/ijisr.2042.4639.2016.0076

Alzubaidi, A., 2021. Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon 7, e06016. https://doi.org/10.1016/j.heliyon.2021.e06016

Amo, L.C., Liao, R., Frank, E., Rao, H.R., Upadhyaya, S., 2019. Cybersecurity Interventions for Teens: Two Time-Based Approaches. IEEE Transactions on Education 62, 134–140. https://doi.org/10.1109/TE.2018.2877182

Ariffin, M., Letchumanan, M., 2020. Status of Cybersecurity Awareness Level in Malaysia. pp. 343–359. https://doi.org/10.1007/978-3-030-50244-7_17

Azasoo, J., Boateng, K., 2015. A Retrofit Design Science Methodology for Smart Metering Design in Developing Countries. https://doi.org/10.1109/ICCSA.2015.23

Balance, B., n.d. Normal Attention Span Expectations By Age [WWW Document]. URL https://www.brainbalancecenters.com/blog/normal-attention-span-expectations-by-age (accessed 3.6.21).

Bauman, S., Rio, A., 2005. Knowledge and Beliefs about Bullying in Schools Comparing Pre-Service Teachers in the United States and the United Kingdom. School Psychology International 26, 428–442. https://doi.org/10.1177/0143034305059019

Bernard, Z., n.d. YouTube is reportedly pointing kids to thousands of disturbing, violent, and inappropriate videos [WWW Document]. Business Insider. URL https://www.businessinsider.com/youtube-has-thousands-of-disturbing-videos-targeted-at-kids-report-2017-11 (accessed 2.13.20).

Brittan, T., Jahankhani, H., McCarthy, J., 2018. An Examination into the Effect of Early Education on Cyber Security Awareness Within the U.K. pp. 291–306. https://doi.org/10.1007/978-3-319-97181-0_14

Bullying UK, n.d. Cyber Bullying Advice [WWW Document]. URL https://www.bullying.co.uk/cyberbullying/what-is-cyberbullying/ (accessed 2.25.20).

Burrell, D.N., 2020. An Exploration of the Cybersecurity Workforce Shortage [WWW Document]. Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications. https://doi.org/10.4018/978-1-7998-2466-4.ch063

Campbell, M., Whiteford, C., Hooijer, J., 2019. Teachers' and parents' understanding of traditional and cyberbullying. Journal of School Violence 18, 388–402. https://doi.org/10.1080/15388220.2018.1507826

Carroll, F., Legg, P., Bønkel, B., 2020. The Visual Design of Network Data to Enhance Cyber Security Awareness of the Everyday Internet User, in: 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). Presented at the 2020

International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), pp. 1–7. https://doi.org/10.1109/CyberSA49311.2020.9139668

CEOP, n.d. CEOP Education (11-18s) [WWW Document]. CEOP. URL https://www.thinkuknow.co.uk/11_18/ (accessed 4.26.22).

Chandra, N.A., Ratna, A.A.P., Ramli, K., 2020. Development of a Cyber-Situational Awareness Model of Risk Maturity Using Fuzzy FMEA, in: 2020 International Workshop on Big Data and Information Security (IWBIS). Presented at the 2020 International Workshop on Big Data and Information Security (IWBIS), pp. 127–136. https://doi.org/10.1109/IWBIS50925.2020.9255543

Childnet — Online safety for young people [WWW Document], n.d. URL https://www.childnet.com/ (accessed 12.4.22).

Child's Average Attention Span By Age: From Toddler To Teens, 2021. . Ready Kids. URL https://readykids.com.au/average-attention-span-by-age/ (accessed 3.31.23).

Cindana, A., Ruldeviyani, Y., 2018. Measuring Information Security Awareness on Employee Using HAIS-Q: Case Study at XYZ Firm, in: 2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS). Presented at the 2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS), pp. 289–294. https://doi.org/10.1109/ICACSIS.2018.8618219

Clark, D., 2022. UK: population, by age 2020 [WWW Document]. Statista. URL https://www.statista.com/statistics/281174/uk-population-by-age/ (accessed 9.23.21).

Clark, D., 2021. UK: Population women and men [WWW Document]. Statista. URL https://www.statista.com/statistics/281240/population-of-the-united-kingdom-uk-by-gender/ (accessed 3.29.22).

Clark, I., n.d. Using Call for Participants as a Researcher [WWW Document]. URL https://www.callforparticipants.com/blog/2015/11/25/28/case-study-using-call-for-participants-as-a-researcher (accessed 5.24.22).

Cook, S., n.d. Cyberbullying Statistics and Facts for 2023. Comparitech. URL https://www.comparitech.com/internet-providers/cyberbullying-statistics/ (accessed 3.31.23).

Coronavirus impact: global media consumption increase by country 2020 [WWW Document], n.d. . Statista. URL https://www.statista.com/statistics/1106766/media-consumption-growth-coronavirus-worldwide-by-country/ (accessed 12.4.22).

Corron, L., 2020. Social Cyber Threats Facing Children and Teens in 2018 [WWW Document]. Stay Safe Online. URL https://staysafeonline.org/blog/social-cyber-threats-facing-children-teens-2018/ (accessed 2.13.20).

Cyber Security Challenge UK, n.d. Cyber Security Challenge UK [WWW Document]. Cyber Security Challenge UK. URL https://www.cybersecuritychallenge.org.uk/ (accessed 4.15.20).

CyberFirst overview [WWW Document], n.d. URL https://www.ncsc.gov.uk/cyberfirst/overview (accessed 3.31.23).

Cybersecurity Training for Kids, 2020.

De', R., Pandey, N., Pal, A., 2020. Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. Int J Inf Manage 55, 102171. https://doi.org/10.1016/j.ijinfomgt.2020.102171

Definition of CYBER [WWW Document], n.d. URL https://www.merriam-webster.com/dictionary/cyber (accessed 12.4.22).

Department for Education, 2021. Keeping Children Safe in Education 2021 164.

Department for Education, 2019. Education and Training Statistics for the United Kingdom 2019 14.

Department for Education, 2018. Bullying in England, April 2013 to March 2018. Department for Education 21.

Drouin, M., McDaniel, B.T., Pater, J., Toscos, T., 2020. How Parents and Their Children Used Social Media and Technology at the Beginning of the COVID-19 Pandemic and Associations with Anxiety. Cyberpsychology, Behavior, and Social Networking 23, 727–736. https://doi.org/10.1089/cyber.2020.0284

Edwards, S., Nolan, A., Henderson, M., Skouteris, H., Mantilla, A., Lambert, P., Bird, J., 2016. Developing a measure to understand young children's Internet cognition and cyber-safety awareness: a pilot test. Early Years 36, 322–335. https://doi.org/10.1080/09575146.2016.1193723

Fichtner, E., n.d. Cybersecurity 101: Intro to the Top 10 Common Types of Cybersecurity Attacks [WWW Document]. URL https://www.datto.com/uk/blog/cybersecurity-101-intro-to-the-top-10-common-types-of-cybersecurity-attacks?utm_medium=opengraph&utm_source=225 (accessed 4.26.22).

Flinders, K., 2017. UK government wants to give 6,000 teenagers cyber security training [WWW Document]. ComputerWeekly.com. URL https://www.computerweekly.com/news/450423197/UK-government-wants-to-give-6000-teenagers-cyber-security-training (accessed 4.26.22).

Gelinas, L., Pierce, R., Winkler, S., Cohen, I.G., Lynch, H.F., Bierer, B.E., 2017. Using Social Media as a Research Recruitment Tool: Ethical Issues and Recommendations. Am J Bioeth 17, 3–14. https://doi.org/10.1080/15265161.2016.1276644

Glen, S., 2022. Cronbach's Alpha: Definition, Interpretation, SPSS [WWW Document]. Statistics How To. URL https://www.statisticshowto.com/probability-and-statistics/statistics-definitions/cronbachs-alpha-spss/ (accessed 3.29.22).

Gordon, J.U. (Ed.), 2018. Bullying Prevention and Intervention at School: Integrating Theory and Research into Best Practices. Springer International Publishing, Cham. https://doi.org/10.1007/978-3-319-95414-1

Hanif, Y., Lallie, H.S., 2021. Security factors on the intention to use mobile banking applications in the UK older generation (55+). A mixed-method study using modified UTAUT and MTAM - with perceived cyber security, risk, and trust. Technology in Society 67, 101693. https://doi.org/10.1016/j.techsoc.2021.101693

Hart, S., Margheri, A., Paci, F., Sassone, V., 2020. Riskio: A Serious Game for Cyber Security Awareness and Education. Computers & Security 95, 101827. https://doi.org/10.1016/j.cose.2020.101827

Jahankhani, H. (Ed.), 2018. Cyber Criminology, Advanced Sciences and Technologies for Security Applications. Springer International Publishing, Cham. https://doi.org/10.1007/978-3-319-97181-0

Johnson, J., 2021. UK: Internet usage by age 2020 [WWW Document]. Statista. URL https://www.statista.com/statistics/707890/internet-usage-in-the-united-kingdom-by-age-group/ (accessed 9.23.21).

Kapersky, 2022a. Online Video Calls & Conferencing: How to Stay Safe from Hackers [WWW Document]. www.kaspersky.com. URL https://www.kaspersky.com/resource-center/threats/video-conferencing-security-how-to-stay-safe (accessed 4.27.22).

Kapersky, 2022b. What Is a Drive by Download [WWW Document]. www.kaspersky.com. URL https://www.kaspersky.com/resource-center/definitions/drive-by-download (accessed 4.27.22).

Karmakar, S., Das, S., 2021. Understanding the Rise of Twitter-Based Cyberbullying Due to COVID-19 through Comprehensive Statistical Evaluation (SSRN Scholarly Paper No. 3768839). Social Science Research Network, Rochester, NY. https://doi.org/10.2139/ssrn.3768839

KnowBe4, n.d. What is Phishing? Attack Techniques & Examples | KnowBe4 [WWW Document]. URL https://www.knowbe4.com/phishing (accessed 4.27.22).

Kobayashi, Y., Boudreault, P., Hill, K., Sinsheimer, J.S., Palmer, C.G.S., 2013. Using a social marketing framework to evaluate recruitment of a prospective study of genetic counseling and testing for the deaf community. BMC Med Res Methodol 13, 145. https://doi.org/10.1186/1471-2288-13-145

Krejcie, R.V., Morgan, D.W., 1970. Determining Sample Size for Research Activities. Educational and Psychological Measurement 30, 607–610. https://doi.org/10.1177/001316447003000308

Kruger, H., Kearney, W.D., 2006. A prototype for assessing information security awareness. Computers & Security 25, 289–296. https://doi.org/10.1016/j.cose.2006.02.008

Laricchia, F., 2022. Global public Wi-Fi hotspots 2016-2022 [WWW Document]. Statista. URL https://www.statista.com/statistics/677108/global-public-wi-fi-hotspots/ (accessed 4.27.22).

Louis, C., Williams, L., n.d. Protection Poker: An agile game for mitigating risk | Opensource.com [WWW Document]. URL https://opensource.com/article/19/3/protection-poker-agile-security-game (accessed 4.27.22).

Machimbarrena, J.M., Calvete, E., Fernández-González, L., Álvarez-Bardón, A., Álvarez-Fernández, L., González-Cabrera, J., 2018. Internet Risks: An Overview of Victimization in Cyberbullying, Cyber Dating Abuse, Sexting, Online Grooming and Problematic Internet Use. International Journal of Environmental Research and Public Health 15, 2471. https://doi.org/10.3390/ijerph15112471

Mahardika, M.S., Hidayanto, A.N., Paramartha, P.A., Ompusunggu, L.D., Mahdalina, R., Affan, F., 2020. Measurement of Employee Awareness Levels for Information Security at the Center of Analysis and Information Services Judicial Commission Republic of Indonesia. Adv. sci. technol. eng. syst. j. 5, 501–509. https://doi.org/10.25046/aj050362

McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., Pattinson, M., 2017. A Reliable Measure of Information Security Awareness and the Identification of Bias in Responses. Australasian Journal of Information Systems 21. https://doi.org/10.3127/ajis.v21i0.1697

McCormac, A., Calic, D., Parsons, K., Zwaans, T., Butavicius, M., Pattison, M., 2016. Test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q) 10.

Mee, P., 2020. We need to start teaching cybersecurity in elementary school [WWW Document]. World Economic Forum. URL https://www.weforum.org/agenda/2020/03/we-need-to-start-teaching-young-children-about-cybersecurity/ (accessed 4.15.20).

National Cyber Strategy 2022 [WWW Document], n.d. . GOV.UK. URL https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022 (accessed 12.4.22).

National Cybersecurity Alliance, n.d. The State of K-12 Cyberethics, Cybersafety and Cybersecurity Curriculum [WWW Document]. Stay Safe Online. URL https://staysafeonline.org/resource/state-k-12-cyberethics-cybersafety-cybersecurity-curriculum-united-states/ (accessed 4.26.22).

NCSC, 2022. Cyber Aware [WWW Document]. URL https://www.ncsc.gov.uk/cyberaware/home (accessed 4.26.22).

NCSC, 2021. Introducing Young People to Cyber [WWW Document]. URL https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021/ecosystem/introducing-young-people-to-cyber (accessed 4.26.22).

NCSC, n.d. CyberFirst (11 - 19 year olds) [WWW Document]. NCSC. URL https://www.ncsc.gov.uk/section/education-skills/11-19-year-olds (accessed 4.15.20a).

NCSC, n.d. CyberSprinters [WWW Document]. URL https://www.ncsc.gov.uk/collection/cybersprinters (accessed 4.15.22b).

NCSC, n.d. Individuals & families [WWW Document]. URL https://www.ncsc.gov.uk/section/information-for/individuals-families (accessed 4.26.22c).

NCSC, n.d. Schools [WWW Document]. URL https://www.ncsc.gov.uk/section/education-skills/schools (accessed 4.15.22d).

NCSC, n.d. The logic behind three random words [WWW Document]. URL https://www.ncsc.gov.uk/blog-post/the-logic-behind-three-random-words (accessed 4.26.22e).

NCSC, n.d. User education and awareness [WWW Document]. URL https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/user-education-and-awareness (accessed 3.4.21f).

NW, 1615 L. St, Suite 800Washington, Inquiries, D. 20036USA202-419-4300 | M.-857-8562 | F.-419-4372 | M., 2018. A Majority of Teens Have Experienced Some Form of Cyberbullying. Pew Research Center: Internet, Science & Tech. URL https://www.pewresearch.org/internet/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/ (accessed 11.6.20).

O'Driscoll, A., 2022. UK Cyber Security and Cyber Crime Statistics in 2023. Comparitech. URL https://www.comparitech.com/blog/information-security/uk-cyber-security-statistics/ (accessed 3.31.23).

Ofcom, 2020. Children and parents: media use and attitudes report 2019. Ofcom 36.

Ofcom, 2019. Communications Market Report 2019 8.

Office for National Statistics, 2021a. Internet Users, UK 2020 [WWW Document]. URL https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2020 (accessed 4.27.22).

Office for National Statistics, 2021b. Population Estimates [WWW Document]. URL https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates (accessed 4.15.22).

Office for National Statistics, n.d. Remote schooling through the coronavirus (COVID-19) pandemic, England [WWW Document]. URL

https://www.ons.gov.uk/peoplepopulationandcommunity/educationandchildcare/articles/remoteschoolingthroughthecoronaviruscovid19pandemicengland/april2020tojune2021 (accessed 4.27.22a).

Office for National Statistics, n.d. The National Statistics Socio-economic classification (NS-SEC) [WWW Document]. URL https://www.ons.gov.uk/methodology/classificationsandstandards/otherclassifications/thenationalstatisticssocioeconomicclassificationnssecrebasedonsoc2010 (accessed 3.29.22b).

O'Flaherty, K., n.d. Beware Zoom Users: Here's How People Can 'Zoom-Bomb' Your Chat [WWW Document]. Forbes. URL https://www.forbes.com/sites/kateoflahertyuk/2020/03/27/beware-zoom-users-heres-how-people-can-zoom-bomb-your-chat/ (accessed 4.27.22).

Online bullying in England and Wales - Office for National Statistics [WWW Document], n.d. URL https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/onlinebullyinginenglandandwales/yearendingmarch2020 (accessed 12.4.22).

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., Zwaans, T., 2017. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers & Security 66. https://doi.org/10.1016/j.cose.2017.01.004

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C., 2014. Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security 42. https://doi.org/10.1016/j.cose.2013.12.003

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C., 2013. The development of the human aspects of information security questionnaire (HAIS-Q). Proceedings of the 24th Australasian Conference on Information Systems.

PricewaterhouseCoopers, n.d. Global State of Information Security® Survey [WWW Document]. PwC. URL https://www.pwc.co.uk/issues/cyber-security-services/insights/global-state-of-information-security-survey.html (accessed 1.29.21a).

PricewaterhouseCoopers, n.d. Women in tech: Time to close the gender gap [WWW Document]. PwC. URL https://www.pwc.co.uk/who-we-are/women-in-technology/time-to-close-the-gender-gap.html (accessed 3.14.22b).

Quayyum, F., 2020. Cyber security education for children through gamification: research plan and perspectives, in: Proceedings of the 2020 ACM Interaction Design and Children Conference: Extended Abstracts. Presented at the IDC '20: Interaction Design and Children, ACM, London United Kingdom, pp. 9–13. https://doi.org/10.1145/3397617.3398030

Quayyum, F., Cruzes, D.S., Jaccheri, L., 2021. Cybersecurity awareness for children: A systematic literature review. International Journal of Child-Computer Interaction 30, 100343. https://doi.org/10.1016/j.ijcci.2021.100343

Richardson, M.D., Lemoine, P.A., Stephens, W.E., Waller, R.E., 2020. PLANNING FOR CYBER SECURITY IN SCHOOLS: THE HUMAN FACTOR 27, 17.

Sezer, B., Yilmaz, R., Karaoglan, Y.F.G., 2015. Cyber bullying and teachers' awareness. Internet Research 25, 674–687. https://doi.org/10.1108/IntR-01-2014-0023

Simplifying how employers measure socio-economic background: An accompanying report to new guidance [WWW Document], n.d. . GOV.UK. URL https://www.gov.uk/government/publications/understanding-a-workforces-socio-economic-background-for-change/simplifying-how-employers-measure-socio-economic-background-an-accompanying-report-to-new-guidance (accessed 3.31.23).

Statista Research Department, 2022. UK: most popular social media with young adults and teens 2020 [WWW Document]. Statista. URL https://www.statista.com/statistics/1059462/social-media-usage-uk-age/ (accessed 4.26.22).

Statistics How To, n.d. Kruskal Wallis H Test: Definition, Examples, Assumptions, SPSS [WWW Document]. Statistics How To. URL https://www.statisticshowto.com/probability-and-statistics/statistics-definitions/kruskal-wallis/ (accessed 4.15.22).

Streefkerk, R., 2019. Internal vs External Validity [WWW Document]. Scribbr. URL https://www.scribbr.com/methodology/internal-vs-external-validity/ (accessed 3.15.22).

Subedar, A., Yates, W., 2017. The disturbing YouTube videos that are tricking children. BBC News.

Tasevski, P., 2016. It and Cyber Security Awareness-Raising Campaigns. Information & Security 34, 7.

UK Geographics, 2014. Social Grade A, B, C1, C2, D, E [WWW Document]. URL https://www.ukgeographics.co.uk/blog/social-grade-a-b-c1-c2-d-e (accessed 3.28.22).

UK Government, n.d. Data Protection [WWW Document]. GOV.UK. URL https://www.gov.uk/data-protection (accessed 4.29.22a).

UK Government, n.d. Ethnic, socio-economic and sex inequalities in educational achievement at age 16, by Professor Steve Strand [WWW Document]. GOV.UK. URL https://www.gov.uk/government/publications/the-report-of-the-commission-on-race-and-ethnic-disparities-supporting-research/ethnic-socio-economic-and-sex-inequalities-in-educational-achievement-at-age-16-by-professor-steve-strand (accessed 3.14.22b).

UK Government, n.d. Free school meals: Autumn term, Autumn Term 2020/21 [WWW Document]. URL https://explore-education-statistics.service.gov.uk/find-statistics/free-school-meals-autumn-term/2020-21-autumn-term (accessed 3.29.22c).

UK Government, n.d. Get help with technology during coronavirus (COVID-19) [WWW Document]. GOV.UK. URL https://www.gov.uk/guidance/get-help-with-technology-for-remote-education-during-coronavirus-covid-19 (accessed 3.5.21d).

UK Government, n.d. National Cyber Security Strategy 2016-2021 80.

UK Government, n.d. School leaving age [WWW Document]. GOV.UK. URL https://www.gov.uk/know-when-you-can-leave-school (accessed 3.14.22f).

UK Safer Internet Centre, n.d. Resources for 11-19s. URL https://saferinternet.org.uk/guide-and-resource/young-people/resources-for-11-19s (accessed 4.26.22).

Ursachi, G., Horodnic, I.A., Zait, A., 2015. How Reliable are Measurement Scales? External Factors with Indirect Influence on Reliability Estimators. Procedia Economics and Finance 20, 679–686. https://doi.org/10.1016/S2212-5671(15)00123-9

Utica University, 2020. Ten Ways Evolving Technology Affects Cybersecurity [WWW Document]. Utica University. URL https://programs.online.utica.edu/resources/article/ten-ways-evolving-technology-affects-cybersecurity (accessed 4.29.22).

Venter, I.M., Blignaut, R.J., Renaud, K., Venter, M.A., 2019. Cyber security education is as essential as "the three R's." Heliyon 5, e02855. https://doi.org/10.1016/j.heliyon.2019.e02855

Wang, Y., Qi, B., Zou, H.-X., Li, J.-X., 2018. Framework of Raising Cyber Security Awareness. 2018 IEEE 18th International Conference on Communication Technology (ICCT), Communication Technology (ICCT), 2018 IEEE 18th International Conference on 865–869. https://doi.org/10.1109/ICCT.2018.8599967

WCF Cyber Security Awareness Program - #ThinkTalkTeach - Internet Safety for Children (English), 2019.

What is cyber security? [WWW Document], n.d. . NCSC. URL https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security (accessed 3.31.23).

Woods, E., n.d. How Hacker's Use Social Media For Social Engineering Attacks [WWW Document]. URL https://blog.usecure.io/social-media-the-key-ingredients-for-social-engineering-attacks (accessed 4.27.22).

Xia, Y., n.d. Kruskal Wallis Test - an overview | ScienceDirect Topics [WWW Document]. URL https://www.sciencedirect.com/topics/medicine-and-dentistry/kruskal-wallis-test (accessed 3.31.23).

Yunos, Z., Susanty Ab Hamid, R., Ahmad, M., 2016. Development of a cyber security awareness strategy using focus group discussion, in: 2016 SAI Computing Conference (SAI). Presented at the 2016 SAI Computing Conference (SAI), IEEE, London, pp. 1063–1067. https://doi.org/10.1109/SAI.2016.7556109

Zulfia, A., Adawiyah, R., Hidayanto, A.N., Budi, N.F.A., 2019. Measurement of Employee Information Security Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q): Case Study at PT. PQS, in: 2019 5th International Conference on Computing Engineering and Design (ICCED). Presented at the 2019 5th International Conference on Computing Engineering and Design (ICCED), pp. 1–5. https://doi.org/10.1109/ICCED46541.2019.9161120

Appendices

Appendix A: Ethical Approval Letter

Est. 1841 | YORK ST JOHN UNIVERSITY

York St John University,
Lord Mayors Walk,
York,
YO31 7EX

09/06/21

School of Science, Technology, and Health Research Ethics Committee

Dear Melissa,

Title of study: The level of cyber security awareness amongst young adults aged 16 to 18 in the UK (amendment)
Ethics reference: STHEC0027
Date of submission: 08/06/21

I am pleased to inform you that the above amended application for ethical review has been reviewed by the School of Science, Technology, and Health Research Ethics Committee and I can confirm a favourable ethical opinion on the basis of the information provided in the following documents:

Document	Date
Amended Ethical Approval Form and Appendices	09/06/21

Please notify the committee if you intend to make any amendments to the original research as submitted at date of this approval, including changes to recruitment methodology or accompanying documentation. All changes must receive ethical approval prior to commencing your study. You are now free to begin data recruitment and collection for the above approved study.

Yours sincerely,

Dr Sophie Carter
Chair of the School of Science, Technology, and Health Research Ethics Committee

Appendix B: Participant Information Sheet

Melissa Forfitt, York St John University
18th June 2021

Overview:

1. You are being asked to take part in a study that aims to learn about how young adults understand technology and its associated cyber threats.

2. In the study, you will be asked to complete a survey.

3. The study will last up to 15 minutes.

4. This survey will ask you questions about what technology you use and are aware of, your understanding of cyber threats and laws, and some questions to help us understand how you would react in a particular situation. There are also a couple of demographic questions so that we can learn a bit about you, however this will not require you to provide any information that could identify you.

5. If you do not feel comfortable whilst filling in the survey, you can refuse to answer without giving a reason.

6. You are free to leave the study at any time without giving a reason or any further consequences.

7. Your data will only be seen by the group carrying out the study and if necessary, the supervisors, Dr Aminu Usman, Dr Daniel Madigan, and Dr Beth Bell. Your data will always be kept confidential as it will be anonymised; we will not be taking your name and personal information. You will only be asked to provide your email address if you wish to take part in the prize draw and this will only be used to contact you if you are a winner of the prize draw.

8. Any data we collect will be destroyed after we have reported on the results of the study.

9. You will be provided with a debrief after the survey which will provide some useful resources for help and further reading on the topics raised.

10. You can ask us any further questions about the study itself after you have completed the survey.

Contact Information:

Melissa Forfitt: melissa.forfitt@yorksj.ac.uk
Dr Aminu Usman (Supervisor): a.usman@yorksj.ac.uk
Dr Daniel Madigan (Supervisor): d.madigan@yorksj.ac.uk
Dr Beth Bell (Supervisor): b.bell@yorksj.ac.uk

Appendix C: Consent Form

The 7 statements of the consent form are:

By participating in this study, you agree to the following:

1. I have read and understood the information provided to me on the Information Sheet.

2. I understand that the research will involve me participating in a short questionnaire that I can complete online via a questionnaire webpage.

3. I have been given the opportunity to ask questions about the questionnaire.

4. I voluntarily agree to participate in the study.

5. I understand that I can withdraw my participation at any time without giving a reason and there is no penalty for withdrawing.

6. The use of the data for research purposes only has been explained to me.

7. I understand that the information collected from the research will be treated in strict confidence. The information will be anonymous, and no identifiable personal data will be published.

Appendix D: Questionnaire

Q1 Do you live in the UK?

- ○ Yes
- ○ No

Firstly, we are going to be asking some questions so that we can get to know a bit about you. Do not worry, we will not be able to identify you from your survey answers.

Q2 What best describes your gender?

- ○ Male
- ○ Female
- ○ Non-binary / third gender
- ○ Transgender
- ○ Other _____
- ○ Prefer not to say

Q3 What education did your parents complete?

- ○ Below secondary school
- ○ Finished secondary school
- ○ Further education (for example, college)
- ○ University
- ○ Unsure

Q4 Do you receive free school meals? If you are not in education, please answer for when you were at school.

- ○ Yes
- ○ No
- ○ Unsure

Q5 How old are you?

- ○ 16
- ○ 17
- ○ 18

Think about the passwords that you use on a computer. This could be for logging on to a computer, social media, or your favourite website.

Q6 It's safe to have a password with just letters.

- ○ Strongly Disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly Agree

Q7 I use a combination of letters, numbers, and symbols in my passwords.

- ○ Strongly Disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly Agree

Q8 A mixture of letters, numbers and symbols is necessary for my passwords.

- ○ Strongly Disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly Agree

Imagine that you have received an email from someone that you do not know. You are thinking about what to do with the email.

Q9 Nothing bad can happen if I click on a link in an email from an unknown sender.

- ○ Strongly Disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly Agree

Q10 If an email from an unknown sender looks interesting, I click on a link within it.

- ○ Strongly Disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly Agree

Q11 I should not click on a link in an email from an unknown sender.

- ○ Strongly Disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly Agree

Imagine that you are on the internet looking at a file that you can download. You are thinking about what you should do.

Q12 It can be risky to download files on my computer.

- ○ Strongly Disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly Agree

Q13 I download any files onto my computer that will help me get my work done.

- ○ Strongly Disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly Agree

Q14 I am allowed to download any files onto my computer if they help me to do my work.

- ○ Strongly Disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly Agree

Think about when you post things on social media. This could be a text status, a picture, or something else.

Q15 It doesn't matter if I post things on social media that I wouldn't normally say in public.

- ○ Strongly Disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly Agree

Q16 I don't post anything on social media before considering any negative consequences.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

Q17 I can't be punished for something I post on social media.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

Imagine that your device is connected to a public internet network, for example at your school or at a café. You are thinking about sending a personal file to a friend.

Q18 I send personal files using a public Wi-Fi network.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

Q19 I am allowed to send personal files via a public Wi-Fi network.

- ○ Strongly Disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly Agree

Q20 It's risky to send personal files using a public Wi-Fi network.

- ○ Strongly Disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly Agree

Imagine that you are on your way to school or work and you find a USB stick on the floor. You pick it up and think about what you should do with it.

Q21 If I find a USB stick in a public place, I shouldn't plug it into my computer.

- ○ Strongly Disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly Agree

Q22 If I find a USB stick in a public place, nothing bad can happen if I plug it into my computer.

- ○ Strongly Disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly Agree

Q23 I wouldn't plug a USB stick found in a public place into my computer.

- ○ Strongly Disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly Agree

Imagine that you are at school or work, and you see someone behaving in a way that makes you feel unsure of them.

Q24 If I ignore someone acting suspiciously at school or work, nothing bad can happen.

- ○ Strongly Disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly Agree

Q25 If I saw someone acting suspiciously at school or work, I would do something about it.

- ○ Strongly Disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly Agree

Q26 If I see someone acting suspiciously at school or work, I should report it.

- ○ Strongly Disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly Agree

Q27 What do you think being a victim of a cyber-attack means?

Please describe in as much detail as possible what it means to you. There is no right or wrong answer!

_____

Q28 If you would like to be entered into a draw for the chance to win a £20 Amazon voucher, please enter your e-mail address below.

_____