HOW CAN INCENTIVES BE USED TO CHANGE CYBER SECURITY BEHAVIOURS?

A STUDY SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN

CYBER SECURITY AND TECHNOLOGY

INDUSTRY PROJECT IN COLLABORATION WITH CYBERSMART

ESTHER PEARSON

C1547074

PRIFYSGOL CAERDYDD

CARDIFF UNIVERSITY

SCHOOL OF COMPUTER SCIENCE AND INFORMATICS

SUPERVISORS: DR EIRINI ANTHI FOR CARDIFF UNIVERSITY

ANETE PORIETE FOR CYBERSMART

SEPTEMBER 2022

Abstract

The hypothesis of this study is to help ascertain whether incentives will be useful in encouraging individuals to embrace cyber security best practises. The cyber security best practises are defined, and the reasons why an individual would choose not to adopt these options are studied. Various previously explored incentive approaches will be evaluated and discussed, and one technique will be selected and further investigated in the implementation phase. Data is collected from members of the public to help further understand reasons why individuals are not adopting effective practises in cybersecurity. Existing related works will be explored and debated during this study. The data collected from the survey will be analysed. 87 responses are gathered from participants aged 18 – 69. The most significant result of the survey was that 83.9% of participants stated they would prefer to encounter an immediate inconvenience for a shorter period of time, versus being inconvenienced at another point in the future over a longer period of time. No significant correlation between age, education level or digital background and cyber secure behaviour is found.

Acknowledgements

First and foremost, I would want to express my heartfelt gratitude to everyone who took the time to partake in the survey related to this research, especially those who went above and beyond to invite their own friends and family to participate in order to contribute to my work. I am astounded by the outpouring of support from everyone who came to my aid; your generosity has helped to motivate my studies and make me feel as if I have not been alone while writing this!

Thank you to Cardiff Capital Region who in conjunction with PwC fully funded my studies on the master's course. I would particularly like to thank Dr Yulia Cherdantseva for offering me a place on the course, and for continuing to support my growth and development both throughout and after the course had concluded.

Thank you to my supervisors, Eirini and Anete, for your encouragement, patience, and support throughout this project. It has been a delight to learn from you both, and your guidance has been fundamental to my success in completing this project.

Finally, I want to thank all of my family and friends who have always encouraged me to pursue my dreams and ambitions, especially my partner Levi, who has always been by my side and supported my decisions no matter what.

Contents

List of Figures

List of Tables

1 Introduction

Technology is becoming more intertwined and essential in our daily lives in the digital age, leading many to become reliant on it. Despite the numerous benefits of being connected on the go, such as convenience, entertainment, and seemingly limitless access to information, using technology is not without risks. Individuals are increasingly more vulnerable to cybersecurity attacks than ever before (Saravanan & Bama, 2019), and protective safeguards to protect them are continuously being developed. Regardless, humans continue to be the weakest link in the security chain (Kimpe, et al., 2022). Despite the advancements in technology such as biometrics being used to replace passwords, cyber attackers continue to prevail in overcoming these obstacles via the human-factor. The relevance of this research stems from its purpose of discovering whether humans may be favourably "hacked" in order to permanently secure the chain.

Incentives have been used throughout history to encourage certain behaviours and to stimulate motivation. In a corporate setting, incentives include monetary rewards, 'work perks', gifts, and much more. During the mid-nineteenth century, psychologist Clark Hull established 'incentive theory', which proposed that individuals are attracted towards behaviours that lead to rewards and repelled by behaviours that may lead to negative consequences (Hull, 1949). With this in mind, why are people unwilling to form cybersecurity habits that in turn will protect them from negative consequences? Is the incentive of being secure from cyber-attacks not enough? Habits are formed when an individual is confident about completing the task, without needing to use substantial amounts of cognitive effort, according to (Hong & Furnell, 2021). Cyber awareness does not come naturally to everyone, making it more difficult for some to form cyber secure habits. This paper will explore how an incentive could be used to motivate individuals to form and continue to develop these habits, and in turn help to strengthen the weak link in the security chain.

Existing incentive approaches will be examined, and their faults and strengths will be explored. The ideal cybersecurity practises will be defined, and the reasons why an individual may not follow them will be investigated. Data will be collected from survey participants in order to better understand the psychology behind why people choose to skip secure practises in favour of less secure routines, as well as to give insight into people's thoughts and feelings about adopting specific activities.

The sections in this report are organised as follows: Section 3 will examine existing literature, specifically around cybersecurity behaviours, and explore different proven methods of incentive. Section 4 will describe the methodology approach and design and justification of the survey. Section 5 will present the findings and results of the survey data. Section 6 will discuss and evaluate the survey in depth, and present any correlations discovered. Section 7 will discuss future work, and Section 8 will present the overall conclusion of the research. Section 9 contains the authors personal reflection on the project.

2 Background

Many existing approaches and studies around helping people to become more cyber aware are heavily reliant on the teaching and awareness aspect. While it is arguable that being informed around the risks serves as its own incentive to protect oneself, many continue to follow bad practices, including professionals (Sulaiman, 2021).

To be regarded as an incentive, the individual must believe that they are receiving some kind of advantage or reward in exchange for completing an action. While there are several advantages to being secure online, these gains are not immediately apparent, and in practice may feel like a burden or a chore. Bad habits emerge from this state of mind.

The goal of this study is to investigate the psychological underpinnings behind these bad habits and determine which incentive strategy may be most effective in combating them. Short-term, immediate incentives such as monetary rewards will be explored, as will delayed gratification incentives such as nudges. Financial incentives for cyber security have yet to be tested, thus their implications in different contexts will be investigated. While nudges have begun to be trialled in an attempt to affect user behaviour, the concept is still relatively new. Many of these trials focus on compelling the user to do an action in the present instant rather than influencing the user's thought process and behaviour over a longer period.

This chosen topic was also personal to the author, with the researcher of the project wanting to understand the in-depth reasons for digital security complacency and the way individual behaviours could be influenced to improve cyber security amongst the public.

3 Literature Review

The initial problem statement is explored in this chapter by reviewing concepts and hypotheses obtained from current literature. The best practices of cyber security are researched and established, while discussing why individuals may choose not to adopt these behaviours. In order to identify and study relevant material, Cardiff University's Library Search and Google Scholar were used, and relevant phrases were searched, such as 'Cybersecurity Behaviour Incentives'. For reliability, a great emphasis was placed on using peer-reviewed articles and journals. Because technology is rapidly evolving and changing, using as much recently written literature was a priority.

3.1 Cybersecurity Best Practices

While there is no end to the lengths one can take to keep themselves safe online, experts have proposed the following ten best practices that everyone should adopt (Coventry, et al., 2014). Alongside these, the positive and negative consequences of choosing to follow and not follow these best practices has been explored.

Using complex passwords may be off putting, as it is more difficult to remember than a simple password. Many may also choose to use the same password across many platforms. The perceived benefit of simple passwords is that it will be less effort to set up and memorise, causing less stress for the user. Another suggested strategy discussed by (Kävrestad, et al., 2020) is to create longer passwords made up of multiple, simpler, and pronounceable words, as studies have shown these to be easier to remember than shorter, more complex passwords. With the surge in popularity of password managers, the need to memorise passwords may become obsolete, and they can provide significant peace of mind if used correctly. However, in a 2019 study where 30 participants were surveyed around password managers, some participants expressed their misgivings about password managers, with many being sceptical about their security and finding the fact that they have a single point of failure to be unsettling (Pearman, et al., 2019). The consequence of using weaker passwords increase the likelihood of it being compromised through data leaks, brute force attacks etc (Curran, et al., 2011). An event like this would in fact result in more overall effort and stress by having to deal with the consequences.

Anti-virus and firewalls may be perceived as time consuming and requiring effort to set up and can also be a nuisance as many will display warning alerts while the user is browsing the web. Many anti-virus software also comes with an upfront cost, or an ongoing subscription to continue to use the service. Properly configured AV software and firewalls significantly reduces the likelihood of viruses, malware, and spyware which can lead to loss of availability or financial loss (Zare, et al., 2018). Preventing these risks means less effort and time spent fixing the issue, being less likely to encounter financial loss through knock on effects such as ransomware, phishing scams, or compromised bank card information.

Installing updates can take a while, especially if it's a significant OS update. Many people can also be reluctant to update the system they are accustomed to because they worry that the UI or functionalities will change. Users may decide to forego updates in order to save time and effort in the short term (Crossler, et al., 2019). Failure to apply updates causes vulnerabilities in the system, making the user susceptible to attacks from which it will be difficult and time-consuming to recover (National Cyber Security Centre, 2021). Skipping updates may potentially result in programmes ceasing to function entirely or may force the system to perform a significant update, leading to increased downtime in the long term.

It's perceived as being convenient to keep websites open, or the computer in standby mode so one can start up where they left off and avoid having to log in again. Many might not be aware that they are leaving themselves vulnerable to attacks by doing so. If the site in question is vulnerable, CSRF and XSS attacks could be used to compromise sessions. If the application uses weak or predictable session tokens, these could be brute forced (Baitha & Vinod, 2018). All currently active logged-in sessions may be accessible in the event of a physical attack, such as the theft of a device. Financial loss, considerable stress, and time spent fixing problems could be the outcome of dealing with the effects of the aforementioned attacks.

Home networks should always be secured using a password, which should not be shared with anyone. If an attacker gains access, they may be able to snoop on any activity occurring on the network (Information Commissioner's Office, 2022). Using free public Wi-Fi may be appealing since it could boost download speed or simply save money on data usage on cellular plans. However, public Wi-Fi access points may not be properly configured or secured. As a result, attackers have an easier time accessing and stealing the private information and files of anyone connected to the network. Using a VPN can help prevent cybercriminals from intercepting data, and when accessing a public network, users should avoid using certain websites, such as social networking, email, or banking services (Kaspersky, 2022). Regardless of the cost and difficulty of adopting a VPN or simply avoiding public networks entirely, the consequences of a third-party acquiring passwords, personal information, and credit card information will result in significantly more time and money spent addressing these issues.

Online shopping has made it easier than ever for customers to get the best discounts on the things they want to purchase. While searching for an item, a user may discover it for sale on a website at a significantly lower price than elsewhere. They might also find an item in stock that is completely sold out everywhere else! However, there is a chance that these sites are fake, and designed to steal credit card information. Online streaming sites also allow customers to watch their favourite movies or television episodes with the touch of a button. There are also many torrenting and piracy sites where this content may be downloaded for free and may offer films that are not yet available to the general public. Being able to watch a show or film for free is an incentive – especially where others have had to wait and pay for the same privilege. Regardless of these advantages, they are generally illusory and can quickly lead to compromised bank accounts, malware, and disappointment. In these situations, the saying "if it's too good to be true, it probably is" is important, and users should exercise caution when navigating an unfamiliar website.

Users can easily stay in touch with everyone they know, or even people they do not know, thanks to social media. The desire to overshare when sharing happy news and life events to followers can be strong, and updates about new jobs, house moves, or even frustrated posts about how their bank has let them down are not unusual. While this type of action may appear to be harmless, it is exactly what an attacker requires for a social engineering attack, and the results can be disastrous (Masood, 2022). Someone who posts about a new job one day may get a call the following day from their new HR department asking them to send in some identification documents for the internal screening procedure. The victim agrees because they believe nothing is out of the ordinary, until their identity is stolen to open credit card accounts. The pleasant emotions that come from creating new connections and establishing a digital community are the incentives for oversharing on social media. Many may also choose to make their profiles public in order to increase the reach of their posts. In doing so, users should be very wary of what they share, and keep any personally identifiable information to a minimum.

Many may prefer to make use of daily commute to catch up on work, or to simply browse social media and emails. Devices, especially smartphones, hold a plethora of private information that many would be unwilling to share with anyone. 'Shoulder-surfing' is a technique used to steal PINs, passwords, and other sensitive information by physically seeing an unsuspecting user's device screen. Many gadgets now offer biometric authentication, reducing the risk of password theft. However, if a shoulder-surfer obtains enough personally identifying information from the user's screen, social engineering attacks may still be possible. While catching up during the commute may feel productive or entertaining, the repercussions of a successful shoulder surfing attack will take time to resolve and will most likely be quite distressing.

It can be difficult to keep up with all of the scams that appear to be emerging on a daily basis. When an individual is subjected to impersonation scams, the fraudsters are taught how to gain the customer's trust, exert pressure on them, and create a sense of urgency. The victim will believe that if they do not comply right away, their lives would get more stressful and challenging in the future, yet the reality is quite the reverse. Many people could decide not to notify the police after learning about, or even after becoming a victim of a cybercrime. They could believe that including all the information required for the authorities to investigate will take a lot of time and effort. Many people might also be discouraged or untrusting of this method since they think it will not accomplish anything or aid in the capture of offenders. Crime victims could feel humiliated by the fact that they were deceived. The incentive to report is because in doing so, law enforcement will have a chance of apprehending criminals since without these reports, they would not be aware that a crime had been committed and would not look into it. These reports can act as an alert for businesses and individuals, allowing them to take the precautionary measures.

New patterns in scams will not be proactively identified if people do not report them. Another motivation is the possibility that the victim's bank will reimburse them as a gesture of goodwill if they report a crime that has caused financial loss, such a scam. Without a police report, many banks will not give refunds or compensate victims.

3.2 Existing Incentive Methods

While the long-term benefits of adhering to cybersecurity best practises may outweigh the short-term gains, many individuals opt to disregard them. Some people may want to prioritise their time and effort in the present moment, while others might simply be unaware of the full implications of their actions. Incentives for adopting these behaviours have been studied and tested in an effort to strengthen security on their employees and the general public.

3.2.1 Reward Based Incentives

While the definition of an incentive is something that inspires or urges someone to do something, it is strongly associated with there being some form of reward at the end. One of the most common forms of reward-based incentive is a workplace bonus scheme, where employees are rewarded with money or gifts in return for hitting a certain quota. Numerous studies and evidence have proven that financial incentives do work as a motivator to increase performance and output.

According to (Lazear, 2018), incentive compensation is classified into three types: discrete, in which a worker is paid a fixed amount per hour, continuous, in which a worker is paid per completed piece of work, and relative, in which a worker is given a financial incentive when a promotion or target is met. In regard to their overall efficacy, Lazear suggests that incentives have a differing effect depending on the employee's base salary and position on the corporate ladder. For example, a $5000 bonus is going to feel more appealing to a worker earning $25,000 than to a CEO who earns $300,000. The report also references Safelite Auto Glass installers, who switched from paying their employees hourly to paying them per completed piece, with a minimum wage guarantee. By doing so, productivity instantly shot up by 44%.

However, while financial incentives might be quite helpful in some instances, they are not always beneficial in influencing behaviour. When bus drivers in an Asian city were granted financial incentives in 2013 for ensuring that their bus routes arrived on time, the drivers began failing to stop at designated stations during peak periods where customers were waiting, in order to avoid arriving late and therefore losing out on their incentive (Shaw & Gupta, 2015). While one could argue that the incentive structure in this case needs to be reconsidered, it also illustrates that incentives may affect behaviour for the wrong reasons.

The most significant financial incentive for businesses is to guarantee that their operations are cyber secure. This will assist to protect against cyber-attacks that may result in the theft of assets or intellectual property, or the payment of funds due to ransomware. Large fines are also enforced on firms who fail to appropriately secure sensitive data. While the expense of implementing these steps may be substantial, can businesses afford the risk of threats if they do not take these precautions? Furthermore, it can be maintained that developing a cyber safe culture in the workplace begins at the top, and the duty should not be placed primarily on the employees.

3.2.2 Awareness Campaigns

Cybersecurity campaigns have been launched by a variety of organisations, including the Government, charities, and financial institutions such as banks, in an attempt to alter behaviour. These can take the form of literature, digital media, or in-person courses. The perceived purpose of these efforts is to increase awareness of new fraud techniques or scams, measures for staying secure online, and the consequence of not doing so. This is done with the belief that improved awareness would lead to behavioural changes, resulting in fewer occurrences of fraud, scams, and other cyber-attacks. While these efforts can be educational about generic cyber security measures, their efficiency is debated. Many campaigns address the general public as a whole, rather than focusing on specific groups. For example, a campaign around romance scams may be best targeted at older, more lonely people than at school children (Steen, et al., 2020). Using a generic approach may also result in a lack of underlying knowledge or ability to undertake certain best practices, as is corroborated by Bada et al (2019).

In one study, a group of researchers used media to try to encourage users to keep their antivirus software up to date. They produced and deployed an interactive comic in which the characters created would fight and solve cybersecurity crimes while also protecting the public from 'Hack,' a villain used as a metaphor for computer security crimes. The comic's goal was to teach the reader about computer security, particularly anti-virus, in a pleasant fashion that would help them overcome the "intimidation-factor" of standard awareness training. One week after reading the comic, 88% of those who took part could describe how anti-virus works, compared to 13% who could beforehand. While this demonstrated a 677% change in respondent awareness of antivirus following the study, when questioned a week later, less than a third of respondents had gone on to make specific routine cybersecurity improvements, such as installing or updating their anti-virus software (Zhang-Kennedy, et al., 2014). While this research has helped demonstrate that knowledge and education may be sufficient to motivate some people to change their behaviours, it remains to be seen why the other two-thirds of the participants did not act, despite the evident impact that reading this comic had on their abilities.

3.2.3 Targeted Learning

With cyber threats becoming more sophisticated, many companies are opting to have their employees undergo specific cyber awareness training based on their role. This can be conducted in house, or from an external training provider, and it will analyse the most common threats found in the specific job role and tailor the training around that. This method can be more beneficial than generic awareness campaigns, as employees may become frustrated with having to learn information that is not relevant to them and end up 'switching off' when it comes to needing to do any type of training, rendering it useless. An example of this training may include test phishing emails that are relevant to the persons role – for example, a payment request being sent to the accounts team is a highly likely scenario that could occur, as opposed to a generic mass phishing test email which is sent to all employees, regardless of their role.

One study with over 19000 participants sought to determine the efficacy of integrated phishing exercises and to uncover any ways to enhance these efforts (Siadati, et al., 2017). This survey was carried out on behalf of a medium-sized business, and those who took part were employees. Participants were divided into departments and job functions to analyse the differences in answers from each group and to help in targeted phishing activities. Some phishing emails contain a link that entices the reader to click, directing them to a phishing awareness training exercise if they do so. Emails might be sent out at random, targeted, or repeated throughout the campaign to test their impact. During the eight-month campaign, 28 separate test emails with differing levels of persuasion were deployed amongst the 32 different groups of employees.

The recipient's clicks on any embedded links, as well as whether or not they completed the training provided after clicking a link, were all tracked. It also contained a statistic for measuring how convincing the email was depending on whether the email's content influenced the 'click-through' rate, such as utilising sports or celebrity news to pique the user's interest and see whether they are more likely to click a link than an email with less engaging content. While total click-through rates dropped by only 2.77%, the email's substance and persuasiveness dictated its overall performance.

The improvement in a non-persuasive email's total click-through rate is insignificant because the email was unlikely to mislead readers in the first place. Furthermore, those who were deceived by non-persuasive emails may be more difficult to educate with phishing awareness training in general. However, a link between the more convincing emails' click-through rates and completion of the consequent phishing awareness training reveals a reduction in click-through rates over time, suggesting that the training does make a substantial difference in this area.

3.2.4 Nudges

A nudge is the choice architecture that alters people's behaviour in a predictable way without forbidding any options or significantly changing their economic incentives. For example, banning junk food is not a nudge, but offering free fruit and vegetables is (Thaler & Sunstein, 2008). In recent years, nudges have been adopted as part of studies aimed at changing behaviours around cybersecurity.

A study was conducted on groups of people from varying backgrounds, ages and from different parts of the world, which consisted of asking the users to participate in a simulation of making a purchase on an e-commerce website. The participants scored higher points if they adopted more cyber secure behaviours, such as opting to connect to a secure network, using a complex password, and logging out at the end of the session. Different participants were subject to various styles of nudges – some were given warning nudges about possible threats. Others were given 'coping messages' with information on how to best complete that stage in a more cyber secure manner. A combination of both threat nudges and coping messages were also tested. The study found that the participants who received more threat warnings would drop out of the session without completing, possibly due to fear of not being able to complete the process securely, while those given coping information were able to use that to guide them to successfully completing the transaction and score well overall (Bavel, et al., 2019).

Another study using nudges was conducted using a mock registration process, where a password was auto generated for the user. The user was then randomly assigned one of five nudges: Incentive, Norm, Default, Salience and Ego. The study found that the most effective nudge was Salience, which contained both a warning and an incentive to change the auto generated password. Contrary to the study conducted by Bavel et al (2019), is believed that this nudge was the most effective thanks to the fact that it tapped into user's fear (Kankane, et al., 2018).

3.3 Summary

The literature review has concluded that while there are many tried and tested approaches to incentivisation and awareness around cybersecurity, there is still a shortfall between peoples understanding and knowledge versus adoption of secure behaviours.

When considering how to establish positive habits and behaviours, one major hurdle is when the individual believes they lack the confidence or capacity to adopt that habit. To break past that barrier, they must have a strong desire to do so - an incentive.

Awareness campaigns can be valuable to some, but they are so broad and generalised that they only make modest impacts to specific groups when explicitly targeted at them.

While no previous trials where participants were paid to be more cyber secure were discovered, it is arguable whether a study like this would be effective based on existing monetary based incentives in other domains. Would a monetary incentive cause people to modify their behaviours consciously over time, or would they merely learn how to best obtain the reward? When it comes to corporate sales incentive programmes, the results are varied. Would rewarding security-conscious staff with a monetary incentive assist to influence behaviour for the right or wrong reasons? Would it result in a more aware, secure workforce? What effect would this have on the company's cyber security spending, and how much would it offset? Is output better driven by other variables if individuals are paid well in the first place? Cyber security is a culture that begins at the top, and if the superiors are not behaving optimally, the rest are not likely to follow suit.

A fundamental issue is a lack of understanding of cyber threats, or more especially, a lack of awareness of the implications. Users will always click on dubious links since they do not know any better and are not cyber specialists. It's the defence in depth that should be limiting them once they click the email, and it's not really their fault they were duped; threat actors' methods are so sophisticated now.

Nudges are another strategy that has recently been investigated, with different degrees of success in experiments and inconsistent outcomes. Could a nudge that did not give a reward but emphasised the risk of not completing the advised action be as successful as one that gave a reward if you completed the suggested action? Tapping into the users fear of cyber threats had mixed results amongst the studies performed by Bavel et al, 2019 and Kankane et al, 2018, and requires further exploration.

A nudge that provided a time and effort-based incentive may likewise be researched further and tested. While understanding of cyber risks may motivate some to act out of fear, some may opt not to act because they are in denial that these events will occur. Would the prospect of having to spend less time and effort in the future be a worthwhile motivator for these individuals?

4 Methodology

This chapter investigates the methodologies and tactics that will be utilised to address the central issue of 'How can incentives be used to influence cybersecurity behaviours?' Using the knowledge gained from the literature review, a research methodology will be explored and chosen, as well as its design and structure implemented.

4.1 Research Methodology

Based on the research conducted thus far, the planned direction is to explore the effectiveness of nudges which offer a time and effort incentive. This is based on the presumption that if humans were given the upfront choice whether they would prefer to spend slightly longer on a task now to save time in the future, versus putting in no effort and time now but being inconvenienced later, they would prefer to avoid later inconvenience. Could a nudge that gives the user this upfront choice, for example 'spend 10 minutes now setting up your password manager and you'll never need to reset a password again' help us consider the consequences of our actions in the moment, rather than after the fact? Would this type of nudge make the user more conscious of their actions and be an incentive to help to improve habits and behaviours long term?

One method for studying the efficacy of nudges would be to observe users' activities when they use the internet for ordinary tasks like reading emails or shopping. Nudges might show at critical points when there are likely to be greater threats, such as on a shopping website's checkout page or when a user wants to download a file. There have been studies, such as (Kankane et al., 2018), in which participants were brought in for an experiment in which they would utilise a mock up website and complete a transaction. However, the reliability of these results is debatable because the participants would have already been 'on guard' and on the lookout for potential threats due to the setting and conditions they were under. When users are aware that they are being observed or will be scrutinised, they are more inclined to adopt better behaviours out of fear of being criticised or caught out. In an ideal world, users may be given software to put on their devices that would nudge them and track whether or not the nudges were effective in changing their behaviour. Over time, once the user has gotten accustomed to such software, this should provide some insight into the influence the nudges have on the user's behaviour.

Due to the constraints of time, ability, and finances, an experiment like this was not feasible to conduct. In place of this, a survey was designed, aimed at individuals of all backgrounds, ages, and abilities.

The original survey that was planned aimed to mimic the above proposed experiment, by creating simulated 'scenarios' of the types of cyber threats that may occur in a workplace environment. The user would be presented with a scenario, then given a list of options on what action they would take next. If the user selected a less secure option, it would generate a nudge which would show on the screen. The user would then have the option to continue with their choice, or to go back and choose again. Different styles of nudges would be used at random – some nudges would provide an effort-based incentive, for example 'using a password manager will save you less work in the long run, which will outweigh the effort it takes to set it up in the short term'. Other nudges would offer a time-based incentive – 'Installing updates sooner rather than later could save you more time overall, as updates may help to optimise your software and programs and help them to run quicker'. Some nudges could also be a hybrid of the two. The aim of this survey would be to see which nudges were most effective, if at all, in making the participant go back and change their answer.

Concerns around this method were that respondents would treat this like a test rather than choosing the answer that they were more likely to go for if the scenario were real. In turn, they would be looking to choose the 'correct' answer, as they felt they were being monitored. There is also the added fact that they are under conditions of an experiment or test, so they are very aware of the actions they are taking. There were also concerns around the time and effort it would take for respondents to take the survey. It is likely that a survey like this could take upwards of 15 minutes and may become confusing or frustrating enough to cause the user to quit halfway through, resulting in their responses not being recorded. As we are asking respondents to take part of their own accord and in their own time, with no compensation offered for taking part, a simpler, streamlined approach is necessary. It is also crucial that the data from the survey is easy to process and understand.

4.2 Survey Design

For the final design of the survey, a simple multiple-choice model was decided upon, for speed and ease of use for the participant. Google Forms (Google, 2022) was used to create and host the survey. There were some options that allowed the user to type their response in text where necessary. The survey takes less than 10 minutes to complete.

The survey consisted of five stages, as detailed further below.

4.2.1 Socioeconomic Background Questions

In this stage, facts around the participants were gathered such as age range, education level, current occupation, and questions about their current level of internet access. Facts about their social background such as parents' education level, and whether they had access to the internet during their childhood were also gathered. The rationale for acquiring this information was to see whether there is any correlation between the participants upbringing and socioeconomic background, and their responses to the upcoming scenario questions.

4.2.2 Password Questions

In this section, the participant is presented with some multiple-choice questions around password management. The questions asked what type of passwords they generally use when setting up their accounts and were given options such as 'the same one used for all your other accounts' or 'a really long and complicated password. There was also an option for 'other', where the user could type in their answer if none of the available options were suitable. Participants were prompted at every stage to be as honest as possible, to hopefully deter them from choosing the answer they feel is most 'correct'. In another attempt to sway this, a follow up question was asked where the user was given the chance to choose what they feel is the type of password which is the most secure. The participant was then asked how they would store and manage their passwords, with multiple choice options such as 'by memory' or 'using a password manager', with the opportunity to choose as many options as they wish. As a follow up question, again to encourage honesty from participants, the user is then asked what they feel is the best approach to password management, regardless of the previous question. As a final question to this part of the survey, there is an opportunity for the participant to write any comments they feel are relevant to the questions in an optional text box field.

4.2.3 System Updates

The questions in this section are asked a little differently to the previous stage, as there are no repeated questions. These questions surround software updates and ask the respondent whether or not they have ever skipped an update. To further encourage honestly, the question allows multiple options to be selected, and includes types of devices such as PC/Laptop, Smartphone etc. The respondent is then asked their feelings as to why so many decide to forego installing important updates, and what they believe will happen as a result of installing updates. They are again provided with a range of responses to choose from. As a final question to conclude this section, the participant is provided with a hypothetical ultimatum – 'While delaying an update may save the user time in the short term, they may end up spending more time/effort dealing with the consequences in the long run. If you were given the choice upfront, do you think you would prefer to be inconvenienced in the immediate term but for a shorter period of time, or inconvenienced in the future but for a longer period of time?'. The participant may answer either yes, no, or unsure, but there is also the option to select 'other'. The purpose of this question is to attempt to identify whether nudges based around time and effort would likely have any effectiveness in a real-life situation, by gauging the respondents' feelings.

4.2.4 Phishing

The first part of this section contains an image of an email, and the participant is asked to write in their own words what their initial reaction is, and how they would respond to the email. No further information or questions are presented until this section has been completed, and it is not revealed that this email is likely a spoofed phishing email. The purpose of this is to identify whether the respondent is likely to be able to identify when something does not feel quite right when receiving an email like this. Once the respondent has written an answer, they can progress to the next stage where it is revealed that the email was not genuine. They are then asked two multiple choice questions – what they would do after receiving a phishing email, and what they feel prevents themselves and others from taking these actions. Both of these questions have multiple options, and they also have the option of 'other' where they can include some extra information. Again, the purpose of this is to see whether their answer has changed at all since the initial question of this round, and whether being given a subconscious 'nudge' has affected their judgement and response.

4.2.5 Final Thoughts

An optional text box appears which gives the opportunity for the user to record any final comments or thoughts around the survey or scenario. Any information captured here may be useful and helpful towards the conclusion of this study.

4.3 Ethical Considerations

Because the survey will rely on human respondents and gather their data, the Cardiff University COMSC Ethics policy (Cardiff University COMSC, 2022) needed to be adhered to. This ensures that the participants and their data are safe, and that the research is conducted in a fair, straightforward, and honest manner. Before being able to begin gathering survey responses, an application for ethical approval had to be completed and approved by the school's ethics committee. Research Integrity Training (Cardiff University, 2022) was also completed, and each module was passed, with proof given in the application. As part of the application, several factors were discussed and addressed.

There must be a legitimate rationale for collecting all parts of survey data. The reason for gathering socioeconomic data was to examine if there was a link between background, age, education level, and demonstrated cyber security behaviours. Any acquired data must also be anonymised, and any direct quotes included in the report must be altered or deleted to eliminate any potentially identifying information.

It was agreed that respondents under the age of 18 would be excluded from taking part in the study. This would have complicated matters further due to safeguarding concerns and the necessity of parental/guardian agreement, and responses from this demographic was not a key requirement for the purpose of the survey. In order to communicate this to participants, the first question of the survey was “Are you over 18 years old?”. If the respondent selected “No”, they would be given the message “Unfortunately, you must be over 18 to participate. Thank you for your time.”. Selecting “Yes” progresses onto the next part of the survey.

Participants were then required to provide informed consent by reading the Information Form (Appendix B) and ticking the option “I have read and understood the above Participant Information Form.”. They are then directed to the Consent Form (Appendix A), and select the option “By checking this box, I am confirming that I have read and agreed to all points detailed in the above consent form.”. This was on the opening page of the questionnaire, and users were greeted by it before being able to proceed to the survey questions. This phase also captures the participants' email addresses, which they may use to get an electronic copy of their survey replies at the conclusion if they desire. Obtaining the email address also ensures that the data of the responders may be easily recovered if they request that it be destroyed.

The goal was to receive 50 answers. The poll would be promoted on social media "stories," group chats like WhatsApp or Discord, or email distribution lists in order to acquire these. Participants could not be approached directly since it may be perceived as aggressive. It was also made plain that there would be no compensation for participating in the study, and the estimated amount of time it would take to complete was communicated. Individually targeting certain categories of people would be against ethical guidelines since it might affect data integrity. An example of the wording used to advertise the survey detailed below:

"Hello everyone. I'm looking for people to take part in my survey about cyber security behaviours. My project's goal is to shed some insight on the reasons why we choose not to adopt cyber secure behaviours online, and to investigate whether there is a way to incentivise us to make better choices and habits. The survey is open to anybody over the age of 18, and I urge replies from people of all ages and backgrounds - regardless of how 'cyber aware' you feel you are! The survey is mainly multiple choice with some optional text box questions. It should only take a few minutes to complete and works on mobile browser for your convenience. There is no reward or payment offered for completing the survey. If you have any questions or comments, please contact me at pearsonEM@cardiff.ac.uk. Thank you very much!"

Finally, any data collected needed to be kept safe, and not shared with anyone unless it was necessary. In this case, this included the project supervisors. The data gathered from the completed Information and Consent forms also needed to be securely stored in line with ethics policy guidelines. The data from the survey was shared with the project supervisors by granting access via the options on Google Forms. The data was analysed by importing the .csv file into Microsoft Excel, which was saved as a password-protected file, and never shared or moved to any other devices.

5 Results

The purpose of this section is to explore the responses to the survey and identify underlying trends and correlations within the data. The purpose of gathering this data was to try and determine the respondent's current cyber security behaviours and knowledge levels, and the reasons behind why respondents may or may not choose to follow best practices. The survey consisted of a mixture of quantitative and qualitative questions. The responses for each section will be fully discussed and analysed.

5.1 Socioeconomic Questions

5.1.1 Age, Employment and Education

The survey concluded with 87 responses. The majority of the respondents were aged 25-39, and the fewest responses were received from 55–69-year-olds. Nobody 70 or older participated in the survey, and under 18s were excluded from taking part due to ethical considerations.

More than half of the respondents were in full-time employment, followed by full-time students. The minority of respondents were self-employed, or homemakers (Table 1).

Age Range	Employed full-time	Full time student	Employed part-time	Self employed	Self-employed and employed	Homemaker	Grand Total
18 - 24	9	8	1				18
25 - 39	38	6	6	2	1	1	54
40 - 54	6		2	1			9
55 - 69	2		1	3			6
Grand Total	**55**	**14**	**10**	**6**	**1**	**1**	**87**

Table 1 - Age, Employment and Educational Statistic

Almost half of the respondents were educated up to bachelor's level or equivalent, and a quarter up to Postgraduate. Only one respondent had no educational background (Figure 1).

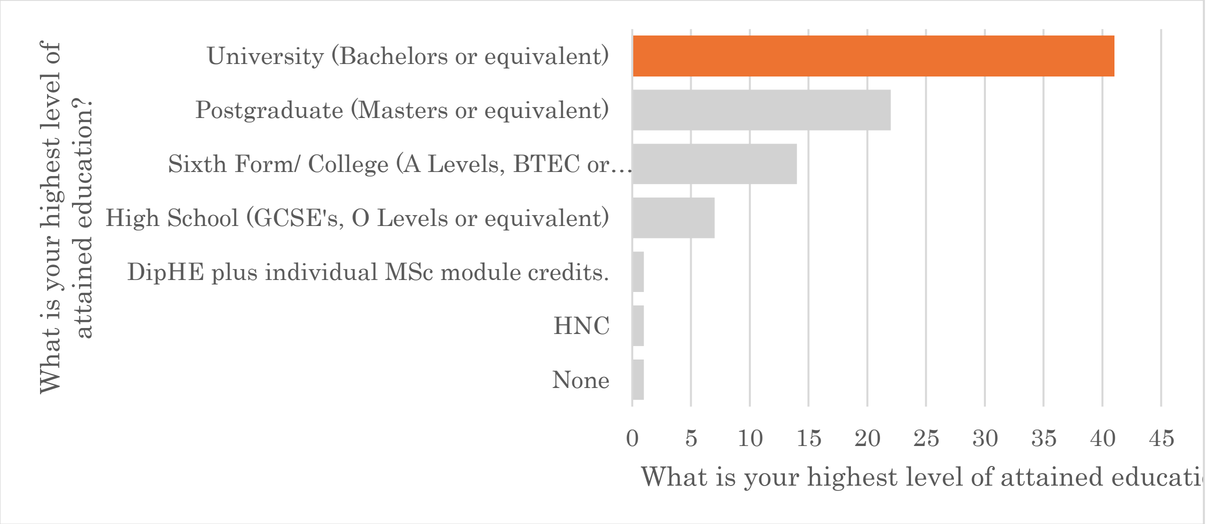


Figure 1 - Education level of respondents

Respondents were given the optional chance to provide details about their employment or study. 16 of the 63 people who chose to respond to this section have an employment background in either IT, Software or Cybersecurity. There were also 3 individuals studying a technical subject (Table 2).

Accountancy, Banking and Finance	Accountant	1
	Finance	3
	Management	2
Arts and Design	Artist	1
	Fashion	1
Charity	Clerical	3
	Managerial	1
Consulting and Management	Consultant	1
	Project Manager	1
Education	Teaching	2
	Support	1
	Other	3
Health and Beauty	Hair	1
	Beauty	1
Information Technology	Cyber	4
	Software	8
	IT	4
Office Work	Admin	5
	Managerial	2
Other		5
Property and Construction	Manual	1
	Clerical	1
Public Services	Emergency	1
	Social	2
	Civil	1
	Health	2
Student	Cyber	2
	Economics	1
	Software	1
	Other	2
Unspecified		23
Total		**87**

Table 2 - Employment Backgrounds

The responses surrounding the parent’s level of education were varied. While the majority had at least one parent educated up to Bachelor’s level, the second highest trend was High School education, followed by Sixth Form, and Postgraduate respectively. This differs from the responses relating to the participants own level of education, where Postgraduate was the second most common response. Four respondents had at least one parent who had completed a Doctorate, while four separate respondents had both parents without any educational background. Finally, three respondents chose not to disclose this information, or were unsure (Figure 2).

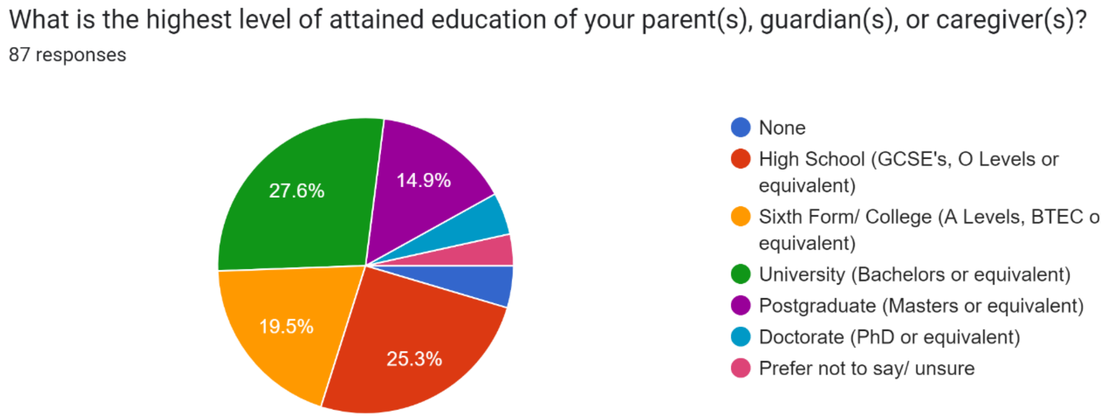


Figure 2 - Parental Education Level

To better comprehend the participants' technological backgrounds, they were divided into two groups: "digital natives" (DN) and "digital immigrants" (DI). A digital native is someone who was born into the technological age and is thought to be inherently technologically skilled, whereas a digital immigrant is someone who had to learn how to use technology at a later point in their life and is assumed to find some difficulty in using and understanding technology (Wang, et al., 2013).

In the context of this survey, digital natives are those aged up to 39, who had regular access to the internet up until the age of 18. Anyone falling outside of this category would be classed as a digital immigrant. 72 of the respondents were 39 or younger, and only 6 of these had no access during their childhood and teenage years. This could be because technology usage increased and became more generally available and affordable after the dawn of the new millennium, thus anyone beyond the age of 30 may have missed out. The lack of access could also have been due to financial constraints. Therefore, the respondents of this survey consisted of 66 digital natives, and 21 digital immigrants.

5.1.2 Internet Access

All 87 respondents have regular access to the internet, with the majority having access at home. All respondents owned at least one device which enabled them to access the internet, with a great majority owning both a PC/ Laptop as well as a smartphone (Figure 3).

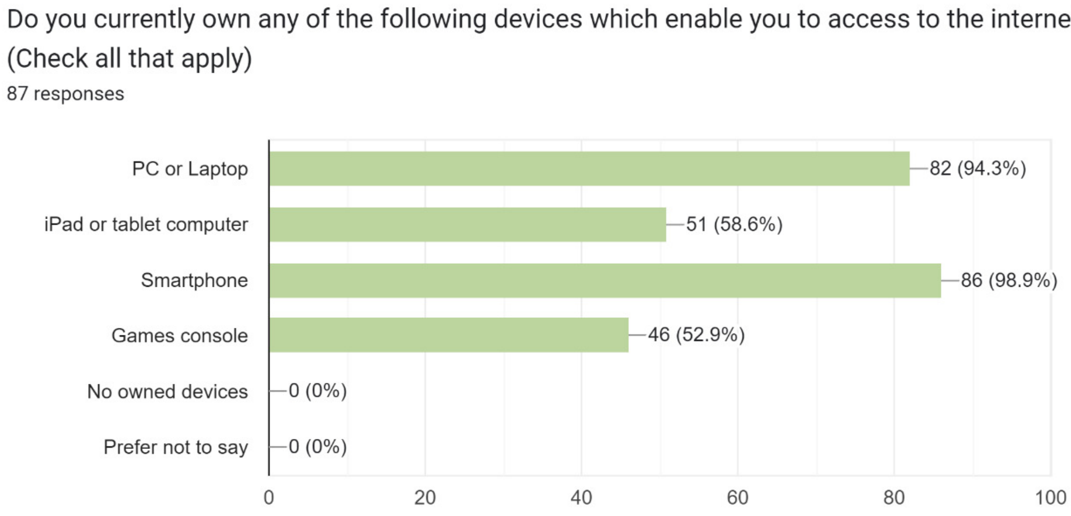


Figure 3 - Owned Devices

Just over half of the respondents had regular access to the internet both at home and at school from a young age. 15 did not have access as the internet was not widely used or available at the time, which correlates with the age range they have provided. Of the 7 respondents who selected that they had no access to the internet, 5 of these are between the age range of 40-69. This suggests that these responses may have been chosen in error or misunderstood, and that the reason these respondents had no internet access was in fact due to the internet not yet being widely available in households or schools. The remaining two respondents who selected this option are between the ages of 25-39 and may not have had internet access due to other factors.

5.1.3 Scam and Cybersecurity Behaviour Questions

Nineteen respondents revealed that they had previously been a victim of a scam in the past, with fourteen respondents opting to share further details of these scams. Eight of these scams involved the users account being compromised. Three resulted in monetary loss, and another three resulted in data loss. The cause of two of these scams are believed to have happened as a result of a data breach, and one was due to a virus. Finally, two respondents have experienced a cyber-attack of a personal nature, involving cyber stalking and harassment. One of these respondents shared the following details of the event:

'When I was younger, I had my account details compromised by an ex-partner. He managed to access my account by using my security questions and my email login. He changed my password and gave the account details out to a load of people online, and they posted a load of horrid stuff and contacted my family. The police were involved, and my ex was given a police warning in relation to the Computer Misuse Act.'

When asked about the precautions they take to protect themselves online, 56 of respondents stated that they take some precautions, while 19 claimed to be very secure online. One respondent felt no need to do so, while another felt that they did not use the internet enough to be concerned. One respondent admitted that they should do more. 9 respondents were unsure how to answer (Figure 4).

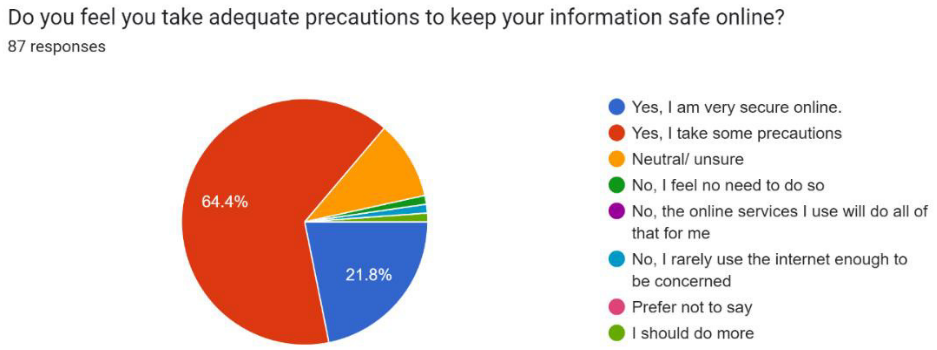


Figure 4 - Respondents attitude towards safety online

79% of the respondents who shared that they had been a victim of a cyber-attack stated that they felt they were secure online, with a third of these respondents claiming to be very secure online. Whether or not this is as a consequence of previously experiencing a cyber attack remains to be seen.

5.2 Scenario Questions

5.2.1 Creating Passwords

Participants were asked what style of password they would likely choose when setting up a new account. The most popular choice was a variation of a password that they use elsewhere, followed by using the same password that is used for all other accounts, and something completely unique taking third place. 3 respondents would choose a long and complicated password, while 2 would opt for a simple password that is easy to remember. The remaining respondents opted to write their own answers here, with 4 respondents saying they use the auto generated options from their password managers (Figure 5).

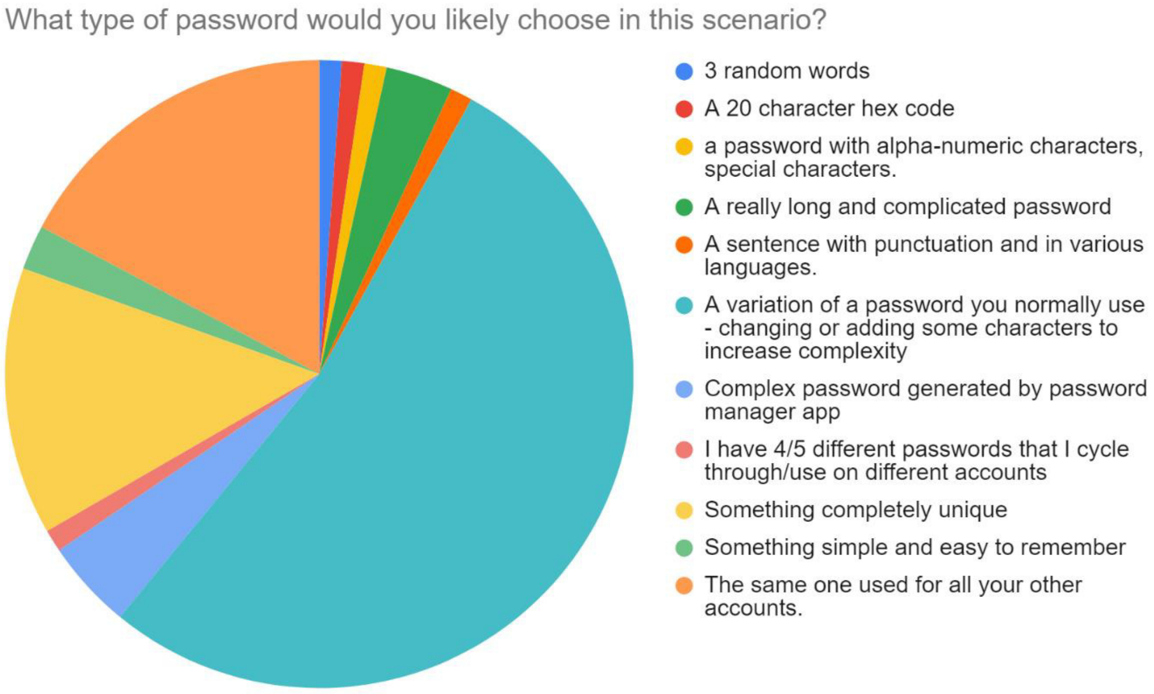


Figure 5 - Chosen password creation option

When asked what kind of password they would use to register for a new account, 53% said they would probably use a variation of a password they currently use elsewhere. Despite this, when asked what kind of password they thought was the most secure, regardless of the type they chose in the preceding question, 59% of respondents said a completely unique password is the preferable choice. Using a long and complicated password was the second most popular choice, followed by using a variation of an existing password (Figure 6).

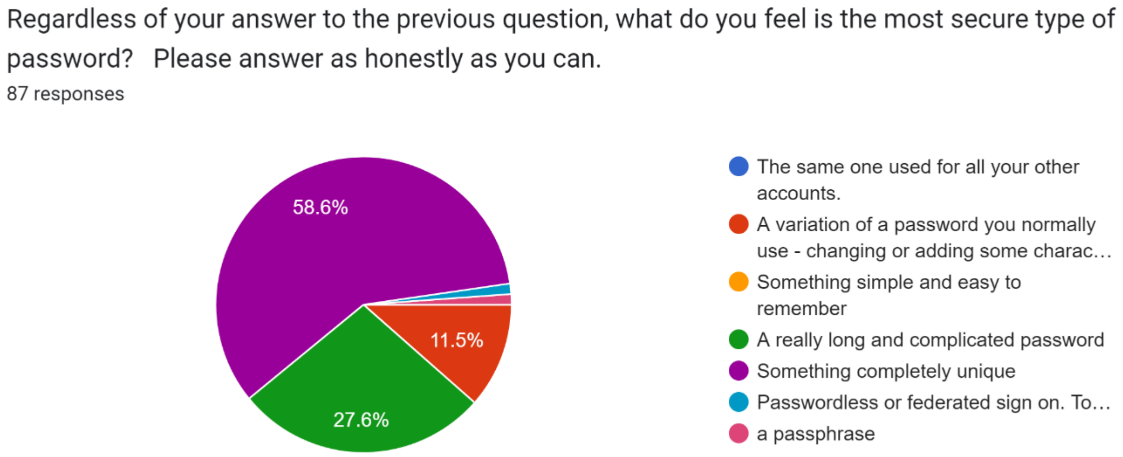


Figure 6 - Perceived securest option of password creation

When examining this further, 14% of DIs believed that using a variation of their existing password was the most secure choice. 66% opted for a unique password, while the remaining 20% would suggest that a long and complicated password is the more secure approach. Of the DNs, 56% would choose a completely unique password, 30% chose a long and complicated password, 11% suggested a variation of their own password, while the remaining 3% made other suggestions.

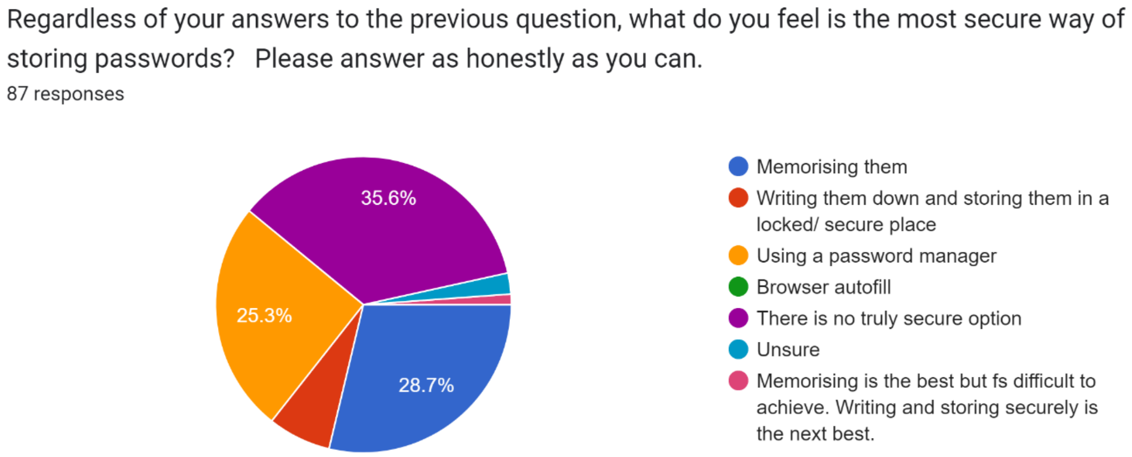
5.2.2 Storing Passwords

Participants were asked how they keep track of the passwords they have and were permitted to select as many options as they needed. The most popular choice was memorising the passwords, and password managers and autofill came in at joint second place. The least popular choices were to write them down, and one person stated that they used a secured spreadsheet to note down their passwords.

When asked to share their opinion on which method of password storing is the most secure, there was not a large overall majority for any method, and choices were split roughly three ways between using password managers, memorising, and the view that there is no truly secure option.

Of the DNs, 38% felt there is no truly secure option, 30% think memorising is best, 24% suggest a password manager, 6% would write them down while 2% were unsure.

Between the DIs, there was an equal 3 way split of 29% between memorising, using a password manager, or the feeling that there is not a secure option. 10% think writing down is most secure, while 3% are unsure which option is most secure (Figure 7).



Regardless of your answers to the previous question, what do you feel is the most secure way of storing passwords? Please answer as honestly as you can.

87 responses

Figure 7 - Perceived securest option of password storage

Participants were given the opportunity to share in their own words what they felt prevented themselves or others from utilising secure password creation and management. When collating this data, the given sentiments were organised into categories (Figure 8).

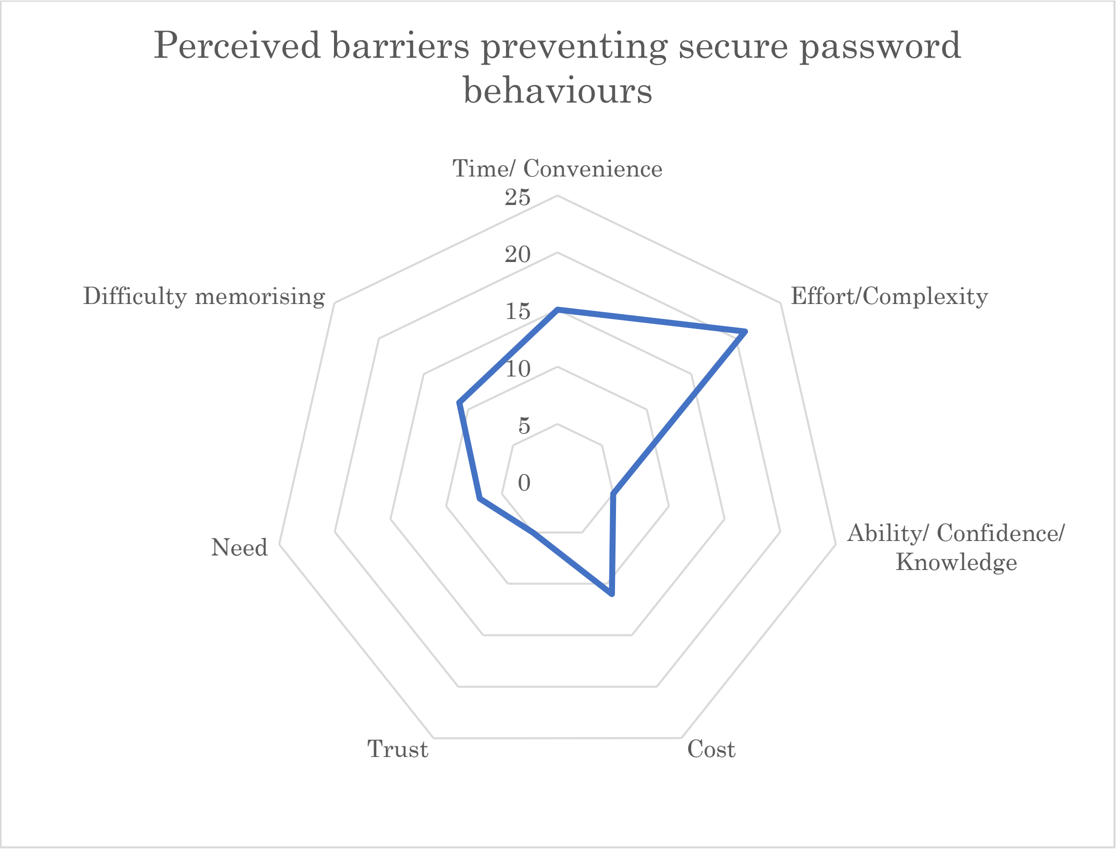


Figure 8 - Perceived barriers to secure password behaviours

In order to better visualise the data, a WordCloud Generator (MonkeyLearn, 2022) was used to display the most frequently used words and phrases from the responses (Figure 9).

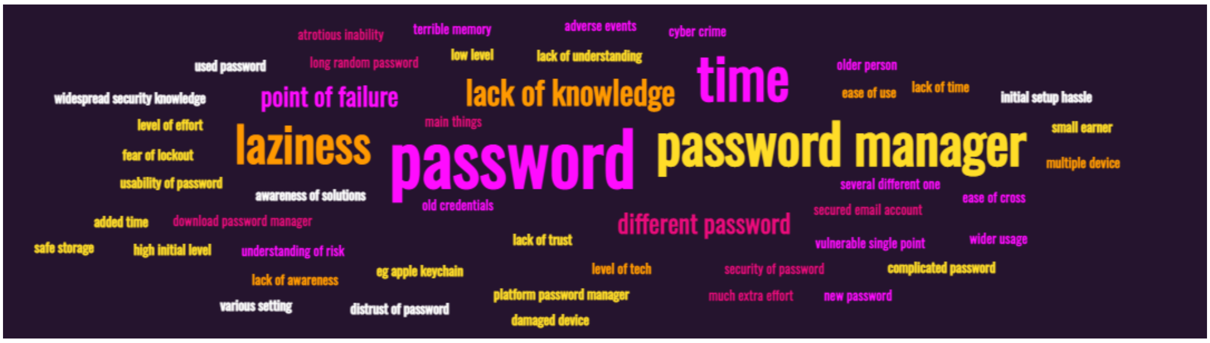


Figure 9 – Word cloud data displaying most frequent words used in responses.

The most common issue expressed by participants was the time and effort required to set up what they considered secure password management, such as utilising unique passwords or password managers. The phrases 'lazy' or 'laziness' featured in around one-sixth of the written comments, and several respondents felt that users would not see the benefit or need in investing time and effort to set up a password manager, as indicated in the following comment from one participant:

'Convenience taking precedence over security, i.e., not perceiving the risk as worth taking the time to remember new passwords, download password manager etc.'

The disparities indicated between participants choosing their own passwords and determining the most secure way of password creation show that the difficulties faced by these individuals are most likely not connected to knowledge and understanding, but rather to the time and effort required to follow these specific cyber secure practices.

5.2.3 System Updates

The goal of this component of the survey was to determine respondents' attitudes toward installing software updates, as well as their understanding of how these updates influence their systems and the implications of not updating them. One-quarter of those polled claimed to have never missed an update. The most popular response among the remaining respondents was having skipped updates on home PCs/laptops and smartphones. Over a third of those polled admitted to skipping updates on their work computer (Figure 10).

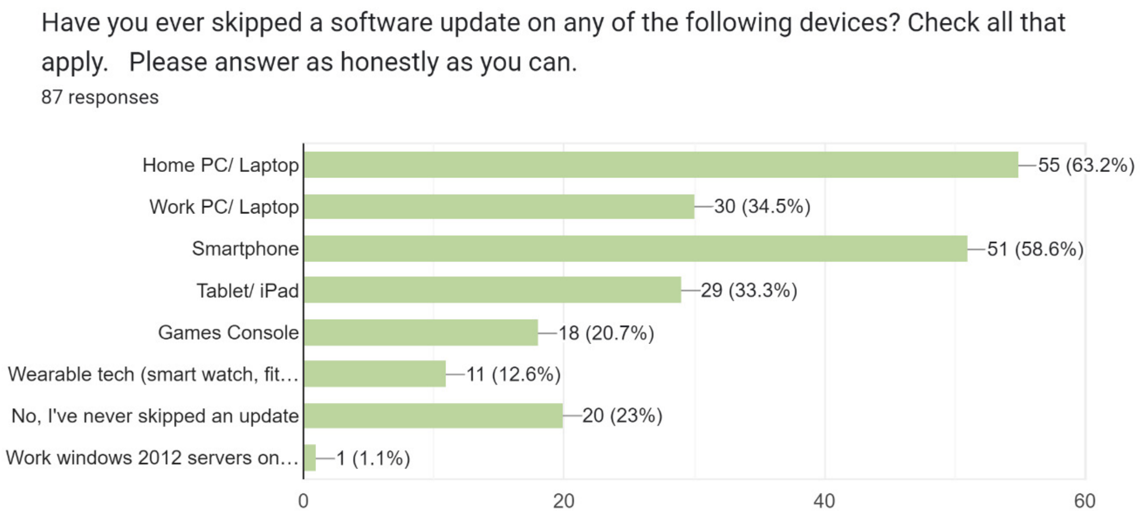


Figure 10 - Skipped Updates

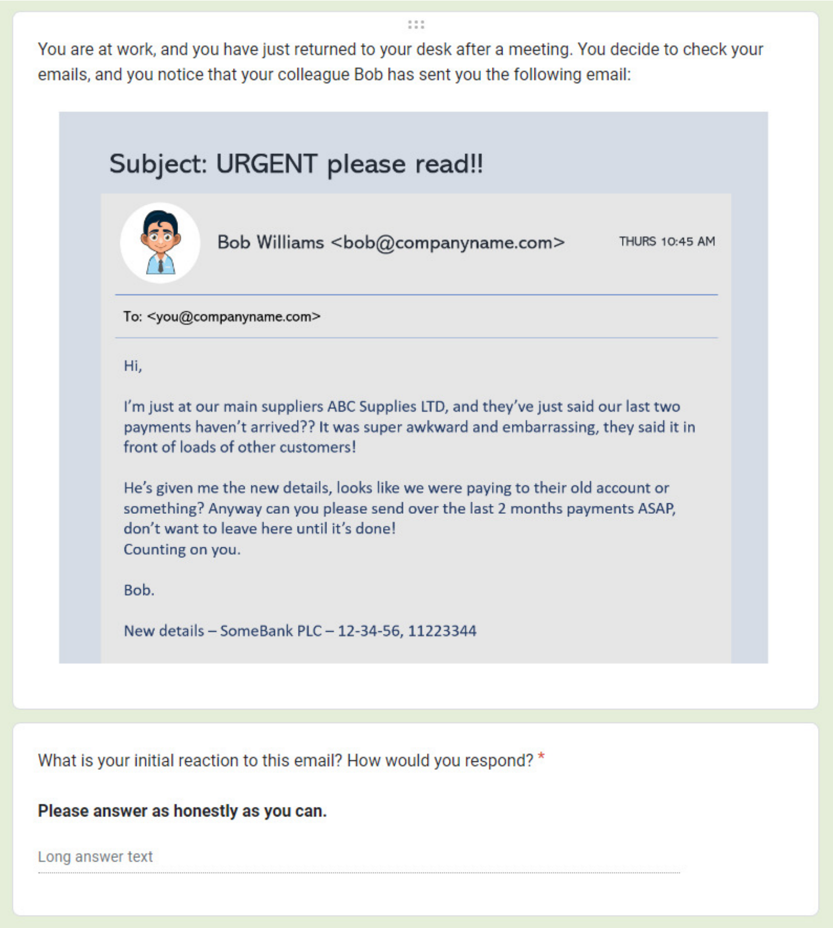
Regarding the reasons for skipping these updates, 7 out of 10 users felt that they would interfere with a task that the user was attempting to do at the time. 62% thought the updates took too long to finish, and slightly more than a third were concerned that it would cause substantial changes to the device or system. 18% did not believe software updates were important.

To gain a better grasp of the participants' overall cyber awareness, they were asked what they felt the potential consequences of missing key updates would be. While 65% acknowledged that it could lead to security vulnerabilities and 48% said it could lead to parts of the system failing to function until updated, the main concern which was selected by 77% of participants was that the system would bombard the user with reminders and prompts to start the update until it was completed. One in every seven people believed that skipping an update would have no major consequences; however, many of the respondents who chose this option also selected a number of other options, implying that the respondent meant that no major incidents would occur from skipping the update in the short term, but they would intend to complete the update at a later time.

Finally, participants were asked how they felt about a hypothetical situation: would they rather be inconvenienced temporarily by completing a software update, or expend less time and effort now but be inconvenienced in the long term by not having to install software updates and having to deal with potential consequences such as slower/obsolete systems, security vulnerabilities, and constant reminders to update? An overwhelming 84% of respondents said they would rather be inconvenienced in the short term and benefit long term. 7% disagreed, stating that they would rather avoid upgrades and cope with the consequences, while 6% were unsure. The remaining respondents said that more information about the situation was needed before they could decide.

5.2.4 Phishing

In the final section of the survey, participants were presented with an image of an email from one of their colleagues, Bob (Figure 11). They were asked how they would initially react to this email. At this point, no further hints or cues were provided, and no multiple-choice options were provided in an attempt to elicit a genuine response.



You are at work, and you have just returned to your desk after a meeting. You decide to check your emails, and you notice that your colleague Bob has sent you the following email:

Subject: URGENT please read!!

Bob Williams <bob@companyname.com> THURS 10:45 AM

To: <you@companyname.com>

Hi,

I'm just at our main suppliers ABC Supplies LTD, and they've just said our last two payments haven't arrived?? It was super awkward and embarrassing, they said it in front of loads of other customers!

He's given me the new details, looks like we were paying to their old account or something? Anyway can you please send over the last 2 months payments ASAP, don't want to leave here until it's done!
Counting on you.

Bob.

New details – SomeBank PLC – 12-34-56, 11223344

What is your initial reaction to this email? How would you respond? *

Please answer as honestly as you can.

Long answer text

Figure 11 - Spoofed phishing email

As this data is in written text, the most frequently used words have been displayed below in an attempt to quantify (Figure 12).

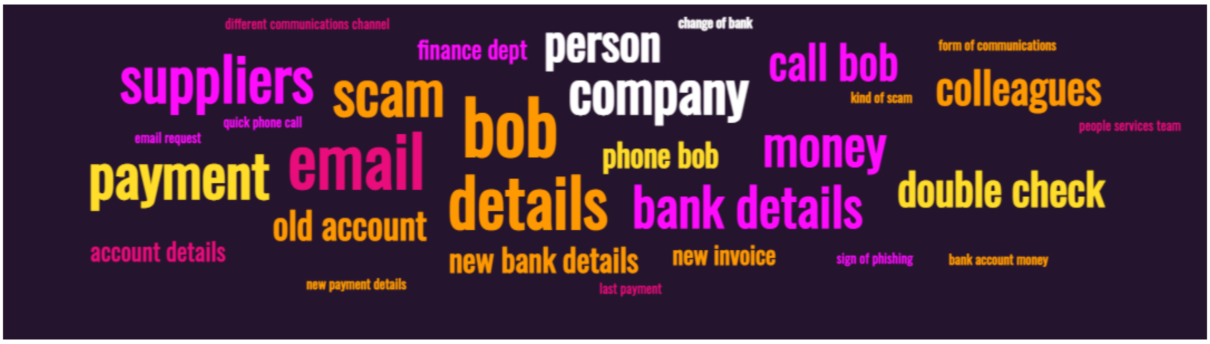


Figure 12 - WordCloud generated from survey responses.

On closer analysis of the answers, only two respondents felt the email was genuine and that they would action the request and send the money. One of these respondents' main concerns was to ensure the bank details were correct, and another said they would send the money immediately before calling Bob to confirm that the transfer had gone through. The remaining respondents confirmed they would take some other action first – 30 said they would want to speak with Bob directly to confirm if the email was genuine.

As the data from the previous question is difficult to quantify, respondents are asked via multiple choice to confirm how they would actively respond to a phishing email. 87% said that informing the relevant team that they had received this email would be the most beneficial approach. 66% would delete the email, while 43% would report it to appropriate authorities such as ActionFraud. Only two respondents believed that any action they took would have no overall impact, while 4 stated that they were unsure.

To complete this part and identify potential barriers, respondents were asked what stops them from carrying out the previously indicated actions. Despite only two participants expressing this sentiment in the previous question, 54% believed that their efforts would make no effect. And, despite only four persons professing to be unclear in the previous question, just under half of respondents chose that not knowing the right course of action to take would prohibit them or others from acting. This could be due to respondents having good intentions and being aware of what action they should take, but still believing it will make no difference. Since this question asks why others may not take the same step, it could also be alluding to other people's apathy or uncertainty toward reporting fraud.

Despite the fact that the vast majority of respondents were suspicious of this email, this may not be indicative of how these same people would react to a phishing email in real life. The reasons for this observation include the fact that the participants were under 'test conditions' of completing a cyber-security-based survey, and as a result were on the lookout for cyber threats. Some respondents also took a more literal approach to the email by basing it on their real-life work situation, and remarking that someone in their position would be unlikely to receive an email like this, such as the following response:

'Phishing, I'm just a software engineer not an accountant'

From the research conducted in the literature review, it was found that participants were more likely to fall for phishing emails that contained relevant and compelling content (Siadati, et al., 2017). Therefore, it is unknown whether respondents such as this one would be tricked by a phishing email that was more specifically targeted at them and contained information relevant to their personal situation, such as a phishing email appearing to come from their bank.

5.3 Final Comments

Participants were invited to offer any final views they had about any aspect of the survey at the end. This stage was optional, and while it was not necessary for the data collection, some insightful remarks were offered.

One participant expressed the following:

'I think that for a lot of people, not being secure enough online is down to the belief that 'it won't happen to me' and not understanding the devastating impact of identity theft or phishing emails to a company.'

Another respondent made a comment that echoed a similar sentiment:

'Some of these lessons are unfortunately learned the hard way no matter how much briefing/ training is given. My employer's ITSEC team occasionally sends out "fake" phishing emails to try to catch out unwary employees'.

The issues raised by these two comments are that many people may be in denial that anything will happen to them until it is too late. While 19 respondents claimed to having been a victim of a scam in the past, the majority of these respondents continued to engage in insecure behaviours such as using the same or similar password across several accounts, skipping updates, and failing to report or act on phishing emails. While one may argue that this is a knowledge issue, the responses indicate otherwise. Ten of the prior scam victims use a variation of the same password, three use the same password, and six use secure passwords. When asked what the most secure choice is, 13 suggest a unique password, 5 suggest a long and complicated password, while 1 felt that a variation of the same password was best. In spite of their knowledge and previous bad experiences, these individuals continue to follow bad practices. Despite all of this, these respondents believed that they took adequate precautions to keep themselves secure online.

Is this evidence that denial exists independent of experience? Is it the assumption that nothing bad will happen, regardless of whether it has happened before? Is it denial that bad practices are being followed, leading to a false sense of security? Or is it indifference and laziness toward adopting secure behaviours rather than denial?

6 Evaluation and Discussion of Survey

The survey's goal response was 50 respondents, but 87 responses were obtained, resulting in a response rate of 174%. This was unanticipated since the survey took more than a few minutes to complete, which may have put off participants. Time restrictions were also a concern, since there was only around one week to collect these replies, which decreased expectations.

At least 16 of the participants had a technical background, either through employment or education. It's possible that this influenced the survey's overall results, as these respondents are likely to have more in-depth understanding of cyber security due to their professions.

With technology being so widely used and relied upon, many of the other respondents working in non-technical roles may also be kept up to date with the latest common scams and threats. As the risk of cyber-attacks increases, companies of all types are beginning to make an effort to educate and equip their staff with preventative skills and knowledge.

Aside from individuals with technical backgrounds, the vast majority of respondents were digital natives who grew up with internet access. Being digitally literate may assist an individual to have better cyber security behaviours and awareness since they are naturally more confident with technology. However, the user's confidence and effortless ability to operate technology may lead to overconfidence and a false sense of security. Is it advantageous to be a digital immigrant if it causes the user to doubt and distrust the technologies they use? When grouping the data and comparing the responses of DIs vs DNs, the ratio split of answers were very similar across both groups. There was no clear majority or indications that one group was more cyber aware than the other. 14 of the 21 DIs shared that they worked in roles that would be reliant on some form technology, such as office work. As DIs only made up around one third of the responses, surveying more people from different backgrounds would offer more insight into the general public's cyber knowledge and behaviours, especially those in roles that are not reliant on technology, and those who have retired.

Life experience may also play a role in an individual's cybersecurity awareness – even having a bank account could influence this, with many high street banks running awareness campaigns in an effort to educate their customers. Owning assets or having funds that one wishes to keep secure is also a motivator for increasing cyber awareness. In future research, surveying those under 18 may provide additional insight and findings around cyber secure behaviours. Due to ethical considerations and time constraints, it was not possible to do so in this study.

No direct correlation was found between education level and cyber awareness. The answers from respondents who had an educational background of high school equivalent or lower showed the same variety as those with a higher education level. Only one out of this group of respondents had been a victim of a scam. Does this demonstrate that cyber security is something that is accessible and learnable by all? Or is it down to the fact that cyber awareness is unavoidable?

7 Future Work

In order to further explore the results of this study, more participants from a variety of backgrounds could be surveyed. This would include those who work in roles that are not reliant on technology, individuals over the age of 70 and under 18, and a higher level of digital immigrants. Diversifying the pool of respondents and comparing the results may reveal different patterns and correlations to be explored.

In this study, the responses from those who had been victims of scams were conflicting. Surveying more individuals who had previously experienced a scam would be beneficial, as well as asking for more information around whether the experience had led them to changing their behaviour in the long term. This could help to determine whether or not a bad experience could be used to help develop nudges around scams and cyber-attacks.

Although most people chose that they'd rather be inconvenienced short term, only one question touched on this point, making it hard to determine how accurate this is and whether or not it would apply in real life. The survey needed to be kept short as it was being completed on a voluntary basis, and it was crucial to keep respondents engaged to ensure completion of the survey. A longer survey may have led to dropouts due to boredom or frustration. Future research could involve obtaining some funding that could be used to pay or reward participants in exchange for spending more time completing the survey or conduct research through other means such as live simulations or interviews.

Despite the high rate of uptake, the sample size is still small and unvaried. More research is required to see whether nudges could be utilised as an incentive to change behaviour. In addition to surveying or interviewing a larger number of people, nudge trials might be a useful strategy. These might be performed in a test environment; however, respondents' behaviour in a test setting is likely to differ. Future study might include long-term experiments in which participants are monitored to evaluate if nudges influence their behaviour when utilising their own devices to do daily tasks.

8 Conclusion

This project's investigation is complete, and the initial problem statement may now be revisited and reflected on. What does this study show regarding the use of incentives to impact cyber security behaviour? This study, along with other previous studies on nudges and incentives, has just scratched the surface of solving the problem.

Because incentives in cybersecurity are a relatively new concept, there were few existing resources and experiments to investigate. Experiments with time and effort-based nudges have yet to be investigated in cyber psychology. Many of the research including nudges focused on leveraging consumers' fears of the accompanying risks, and the outcomes were mixed. The findings of this study also indicated that fear only motivates certain people, while others are motivated by other factors. Based on the survey, even individuals who had direct experience with the repercussions of cyber-attacks failed to exercise sufficient care online.

Some novel findings were uncovered as a result of this study, which could pave the way for future research. The survey's most clear finding was that the majority of respondents are aware of cybersecurity best practises and the dangers associated with failing to implement them. The most significant reason for not doing so was the time and effort involved, in addition to the belief that a cyber-attack would never happen to them. Regardless of past knowledge or experience, many people continue to practise unsecure behaviours because it is the simplest option at the time. To overcome the first barrier of not wanting to spend the time or effort completing an action, an incentive is required. Would a gentle nudge in the right direction suffice to help create new habits? Participants answered that they would rather save time and effort in the long run even if it meant doing more work in the short term. What would individuals do if they could be prompted of the time and effort implications of their decisions before making them?

If time and effort are the most significant barriers, technological advancements may be able to help. Adopting cyber safe behaviours is becoming easier, and it frequently happens automatically as a result of built-in password managers or keychains, biometrics, multi-factor authentication, and spam detection. Will technology handle our cyber security on our behalf, or will the user always bear responsibility? If the latter assertion is always true, additional research is needed to determine the best strategy of persuading people to be cyber secure.

9 Reflection

While I have no background in psychology, the human aspect of cybersecurity has piqued my interest since I began my studies. I also worked at a high-street bank for nearly 7 years, where I spent the majority of my time talking with customers face to face. A large part of my job was to keep these customers safe by looking for indicators of common scams including intimidation, romance, and investment scams. I soon realised that, despite the bank's numerous warnings, campaigns, and safeguards, customers continuously opted to disregard them, resulting in financial or data loss. My purpose for choosing this topic was to try to understand the causes underlying these behaviours and what might be done to overcome them.

Although it was apparent that my approach would require human input, the decision to develop a survey was not reached until several weeks into the project. Obtaining ethical approval took significantly longer than expected, which delayed the project. Fortunately, with the aid of my family and friends, I was able to obtain the majority of my survey replies in one weekend, which helped to get things back on track.

Another challenge was analysing the survey data, which was foreign territory for me. The inbuilt pie and bar charts in Google Forms made a lot of the data self-explanatory and easy to read and comprehend, but the cross-referencing and patterns were detected by manually reviewing and analysing the data rather than using any specialised tools. Despite the initial setback, I believe this went well and that no significant insights were missed.

This project has sparked my curiosity in cyber psychology, which I hope to pursue more in the future. I am really interested in future research and advancements in this sector since it has triggered a chain reaction of questions and hypotheses about human behaviour and how it is impacted.

If I could repeat this project, I would spend more time planning my strategy and methodology from the start and give more time to complete the ethical approval procedure. This would have allowed for more responses and, as a result, more diverse data to investigate. I would also change some of the survey questions to emphasise nudges and delayed incentives in order to acquire a better insight of people's thought processes.

Overall, I am pleased with the outcome of the project, and I am glad I chose to research this topic.

Bibliography

Bada, M., Sasse, A. M. & Nurse, J. R., 2019. Cyber Security Awareness Campaigns: Why do they fail to change behaviour?.

Baitha, A. K. & Vinod, S., 2018. Session Hijacking and Prevention Technique. *International Journal of Engineering & Technology,* 7(2.6), pp. 193-198.

Bavel, R. v., Rodríguez-Priego, N., Vila, J. & Briggs, P., 2019. Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies,* Volume 123, pp. 29-39.

Cardiff University COMSC, 2022. *School of Computer Science and Informatics School Research Ethics Committee.* [Online]
Available at: https://www.cs.cf.ac.uk/ethics/
[Accessed August 2022].

Cardiff University, 2022. *Research Integrity Online Training Programme.* [Online]
Available at: https://intranet.cardiff.ac.uk/students/study/postgraduate-research-support/integrity-and-governance/training/research-integrity-online-training-programme
[Accessed August 2022].

Coventry, L., Briggs, P., Blythe, J. & Tran, M., 2014. Using behavioural insights to improve the public's use of cyber security best practices. *Government Office for Science.*

Crossler, R. E., Bélanger, &. F. & Ormond, D., 2019. The quest for complete security: An empirical analysis of users' multi-layered protection from security threats. *Information Systems Frontiers*, Volume 21, pp. 343-357.

Curran, K., Doherty, J., McCann, A. & Turkington, G., 2011. Good Practice for Strong Passwords. *The EDP Audit, Control, and Security Newsletter*, 18 November, 44(5), pp. 1-13.

Google, 2022. *Google Forms.* [Online]
Available at: https://docs.google.com/forms/
[Accessed August 2022].

Hong, Y. & Furnell, S., 2021. Understanding cybersecurity behavioral habits: Insights from situational support. *Journal of Information Security and Applications,* Volume 57.

Hull, C. L., 1949. *Behavior Postulates and Corollaries.* s.l.:Yale University.

Information Commissioner's Office, 2022. *Wi-Fi Security.* s.l.:s.n.

Kankane, S., Buckley, C. & DiRusso, C., 2018. *Can We Nudge Users Toward Better Password Management? An Initial Study.* Montreal, Association for Computing Machinery.

Kaspersky, 2022. *Public WiFi Security.* s.l.:AO Kaspersky Lab.

Kävrestad, J., Lennartsson, M., Birath, M. & Nohlberg, M., 2020. Constructing secure and memorable passwords. *Information and Computer Security,* 22 June.28(5).

Kimpe, L. D., Walrave, M., Verdegem, P. & Ponnet, K., 2022. What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology,* 41(8), pp. 1796-1808.

Lazear, E. P., 2018. Compensation and Incentives in the Workplace. *Journal of Economic Perspectives,* 32(3), pp. 195-214.

Masood, H., 2022. *A Technique for Identification of Information Severity Levels for Facebook User Profiles,* Islamabad: Capital University of Science and Technology.

MonkeyLearn, 2022. *WordCloud Generator.* [Online]
Available at: https://monkeylearn.com/word-cloud/
[Accessed August 2022].

National Cyber Security Centre, 2021. *Keeping devices and software up to date.* s.l.:s.n.

Pearman, S. et al., 2019. *Why people (don't) use password managers effectively.* Santa Clara, CA, s.n.

Saravanan, A. & Bama, S. S., 2019. A Review on Cyber Security and the Fifth Generation Cyberattacks. *Oriental Journal of Computer Science and Technology,* 12(2), pp. 50-56.

Shaw, J. D. & Gupta, N., 2015. Let the evidence speak again! Financial incentives are more effective than we thought.. *Human Resource Management Journal,* 25(3), pp. 281-293.

Siadati, H., Palka, S., Siegel, A. & McCoy, D., 2017. *Measuring the Effectiveness of Embedded Phishing Exercises.* s.l.:10th USENIX Workshop on Cyber Security Experimentation and Test (CSET 17).

Steen, T. v., Norris, E., Atha, K. & Joinson, A., 2020. What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use?. *Journal of Cybersecurity.*

Sulaiman, N., 2021. *A Study on Password Security Awareness in Constructing Strong Passwords.* Delhi, ICICC 2021.

Thaler, R. & Sunstein, C. R., 2008. Nudge. In: *Improving Decisions About Health, Wealth and Happiness.* s.l.:Yale University Press.

Wang, Q. (., Myers, P. M. D. & Sundaram, D., 2013. Digital Natives and Digital Immigrants. *Business & Information Systems Engineering*, 8 November.

Zare, H., Olsen, P., Zare, M. J. & Azadi, M., 2018. *Operating System Security Management and Ease of Implementation (Passwords, Firewalls and Antivirus).* Las Vegas, Springer Verlag, pp. 749-755.

Zhang-Kennedy, L., Chiasson, S. & Biddle, R., 2014. *Stop clicking on "update later": Persuading users they need up-to-date antivirus protection.* Padua, Italy, Springer, pp. 302-322.

Appendix

A Consent Form

I confirm that I have understood the information sheet dated 11/08/2022 version 2 for the above research project and that I have had the opportunity to ask questions and that these have been answered satisfactorily.

I understand that my participation is voluntary, and I am free to withdraw at any time without giving a reason and without any adverse consequences (e.g. to medical care or legal rights, if relevant). I understand that if I withdraw, information about me that has already been obtained may be kept by Cardiff University.

I understand that data collected during the research project may be looked at by individuals from Cardiff University or from regulatory authorities, where it is relevant to my taking part in the research project. I give permission for these individuals to have access to my data.

I consent to the processing of my personal information (age group, employment status, education level, socioeconomic background) for the purposes explained to me. I understand that such information will be held in accordance with all applicable data protection legislation and in strict confidence, unless disclosure is required by law or professional obligation.

I understand who will have access to the personal information provided, how the data will be stored and what will happen to the data at the end of the research project.

I understand that after the research project, anonymised data may be made publicly available via a data repository and may be used for purposes not related to this research project. I understand that it will not be possible to identify me from this data that is seen and used by other researchers, for ethically approved research projects, on the understanding that confidentiality will be maintained.

I understand that anonymised excerpts and/or verbatim quotes from my survey response may be used as part of the research publication.

I understand how the findings and results of the research project will be written up and published.

I agree to take part in this research project.

By checking this box, I am confirming that I have read and agreed to all points detailed in the above consent form.

B Information Form

PARTICIPANT INFORMATION SHEET

Research Project Title:

'How can incentives be used to change cybersecurity behaviours?'

You are being invited to take part in a research project. Before you decide whether or not to take part, it is important for you to understand why the research is being undertaken and what it will involve. Please take time to read the following information carefully and discuss it with others, if you wish.

Thank you for reading this.

1. What is the purpose of this research project?

The purpose of this student project is to help understand what factors could influence someone's cyber security behaviours and decisions. With cyber-attacks against individuals and businesses on the rise, there is a necessity for everyone to do their part to keep themselves and their data safe online. Despite this, many are not taking the required precautions, and are still using weak passwords, insecure wi-fi networks etc. This research aims to identify whether this is due to a lack of knowledge, or a lack of incentive.

2. Why have I been invited to take part?

You have been invited because this survey is open to everyone over the age of 18 who uses the internet on a regular basis, whether it is for work, school, or personal use. We welcome people from all backgrounds to take part.

3. Do I have to take part?

No, your participation in this research project is entirely voluntary and it is up to you to decide whether or not to take part. If you decide to take part, we will discuss the research project with you and ask you to sign a consent form. If you decide not to take part, you do not have to explain your reasons and it will not affect your legal rights. If you are Cardiff University student, please rest assured that involvement in this research project will have no effect on your education or progression through a degree course. If you are receiving care, your decision to take part or not to take part will not affect the care you receive.

You are free to withdraw your consent to participate in the research project at any time, without giving a reason, even after signing the consent form.

4. What will taking part involve?

You will take one survey, which will take no more than 15 minutes to complete. The survey will be multiple choice, and there will occasionally be a box to add optional extra comments if you wish to do so. The survey will ask for some personal, non-identifiable information such as which age group you fit into, employment status, education level and socioeconomic background, however you will have to option to refuse to answer this if you wish. The main part of the survey will consist of some hypothetical scenario questions, where you will choose an answer based on the action you are most likely to take if you were in that scenario.

5. Will I be paid for taking part?

No. You should understand that any data you give will be as a gift and you will not benefit financially in the future should this research project lead to the development of a new method/test/assessment.

6. What are the possible benefits of taking part?

There will be no direct advantages or benefits to you from taking part, but your contribution will help us understand the psychology behind why individuals choose to/ not to take precautions to protect themselves online.

7. What are the possible risks of taking part?

There have been no identified risks of participating in this survey. The survey will not be timed, and participants are welcome to take as many comfort breaks as they wish while completing the survey.

8. Will my taking part in this research project be kept confidential?

All information collected from (or about) you during the research project will be kept confidential and any personal information you provide will be managed in accordance with data protection legislation. Please see 'What will happen to my Personal Data?' (below) for further information.

9. What will happen to my Personal Data?

The personal data that will be collected will consist of two parts: The first is the completed consent forms, which will contain your name and signature. In order for you to participate in the survey, this information must be collected. The second will be the survey responses, which will ask for your age group, employment status, education level, and socioeconomic background, however you will be given the option to refuse this information if you do not wish to share. The data collected from the consent forms will be collected separately from the survey responses, and therefore any survey responses will not be able to be linked to names given on the consent form.

Cardiff University is the Data Controller and is committed to respecting and protecting your personal data in accordance with your expectations and Data Protection legislation. Further information about Data Protection, including:

- your rights
- the legal basis under which Cardiff University processes your personal data for research
- Cardiff University's Data Protection Policy
- how to contact the Cardiff University Data Protection Officer
- how to contact the Information Commissioner's Office

may be found at https://www.cardiff.ac.uk/public-information/policies-and-procedures/data-protection

After 29/09/2022, the research team will anonymise all the personal data it has collected from, or about, you in connection with this research project, with the exception of your consent form. Your consent form will be retained for 5 years and may be accessed by members of the research team and, where necessary, by members of the University's governance and audit teams or by regulatory authorities. Anonymised information will be kept for a minimum of 5 years but may be published in support of the research project and/or retained indefinitely, where it is likely to have continuing value for research purposes.

All data from completed survey responses will be securely stored, and not be able to be viewed by anyone other than the researcher, and the project supervisor. Please note that it will not be possible to withdraw any anonymised data that has already been published, or from the point at which it has been anonymised.

10. What happens to the data at the end of the research project?

Any collected data that may appear in the final research report and will be fully anonymised and unidentifiable. The data in its raw form will never be shared and will be safely stored on a password protected repository. Once the research has been completed, all survey responses will be safely destroyed.

11. What will happen to the results of the research project?

It is our intention to publish the results of this research project in academic journals and present findings at conferences. Participants will not be identified in any report, publication, or presentation. There is no intention to use verbatim quotes from participants.

12. What if there is a problem?

If you wish to complain, or have grounds for concerns about any aspect of the manner in which you have been approached or treated during the course of this research, please contact – Esther Pearson pearsonEM@cardiff.ac.uk, or Eirini Anthi anthiES@cardiff.ac.uk. If your complaint is not managed to your satisfaction, please contact COMSC School Research Ethics Committee at comsc-ethics@cardiff.ac.uk .

If you are harmed by taking part in this research project, there are no special compensation arrangements. If you are harmed due to someone's negligence, you may have grounds for legal action, but you may have to pay for it.

13. Who is organising and funding this research project?

The research is organised by Esther Pearson and supervised by Dr Eirini Anthi in Cardiff University. This project will be co-supervised by our industry partner Anete Poriete from Cybersmart. The research is not funded.

14. Who has reviewed this research project?

This research project has been reviewed and given a favourable opinion by the School of Computer Science and Informatics School Research Ethics Committee, comsc-ethics@cardiff.ac.uk .

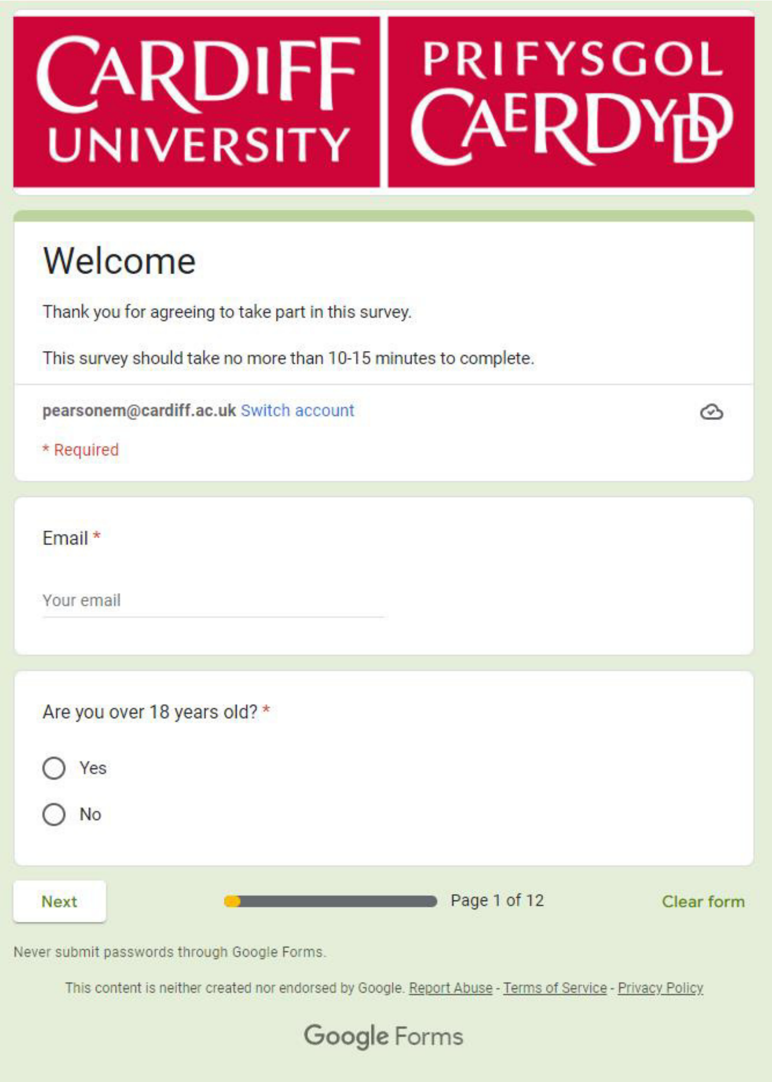
15. Further information and contact details

Should you have any questions relating to this research project, you may contact us during normal working hours:

Esther Pearson
pearsonEM@cardiff.ac.uk
+44 (0)7753337654.
Cardiff School of Computer Science and Informatics,
Abacws Building,
Senghennydd Rd,
Cardiff
CF24 4AX.

Thank you for considering to take part in this research project. If you decide to participate, you will be given a copy of the Participant Information Sheet and a signed consent form to keep for your records.

C Survey



Welcome

Thank you for agreeing to take part in this survey.

This survey should take no more than 10-15 minutes to complete.

pearsonem@cardiff.ac.uk Switch account

* Required

Email *

Your email

Are you over 18 years old? *

○ Yes

○ No

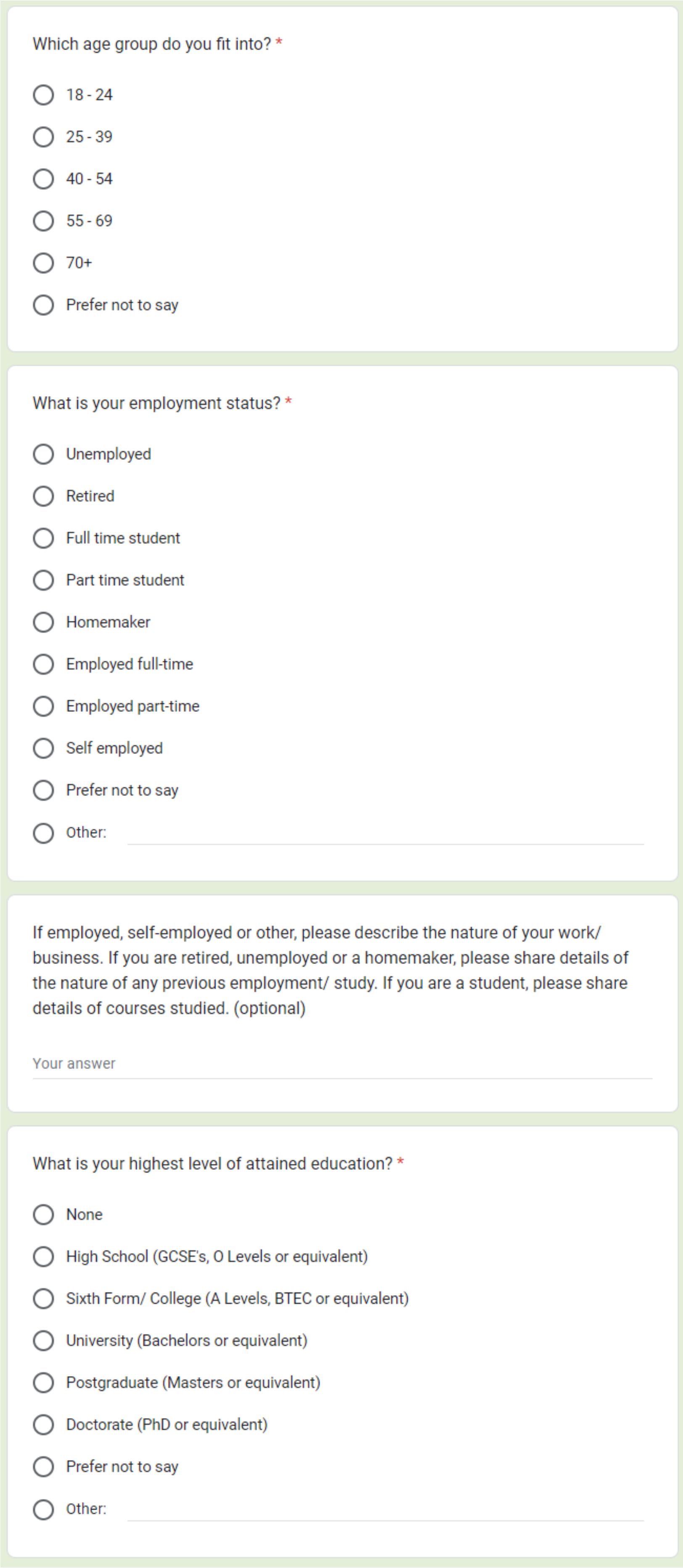
Next

Page 1 of 12

Clear form

Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. Report Abuse - Terms of Service - Privacy Policy



Which age group do you fit into? *

○ 18 - 24

○ 25 - 39

○ 40 - 54

○ 55 - 69

○ 70+

○ Prefer not to say

What is your employment status? *

○ Unemployed

○ Retired

○ Full time student

○ Part time student

○ Homemaker

○ Employed full-time

○ Employed part-time

○ Self employed

○ Prefer not to say

○ Other: ____________________

If employed, self-employed or other, please describe the nature of your work/ business. If you are retired, unemployed or a homemaker, please share details of the nature of any previous employment/ study. If you are a student, please share details of courses studied. (optional)

Your answer

What is your highest level of attained education? *

○ None

○ High School (GCSE's, O Levels or equivalent)

○ Sixth Form/ College (A Levels, BTEC or equivalent)

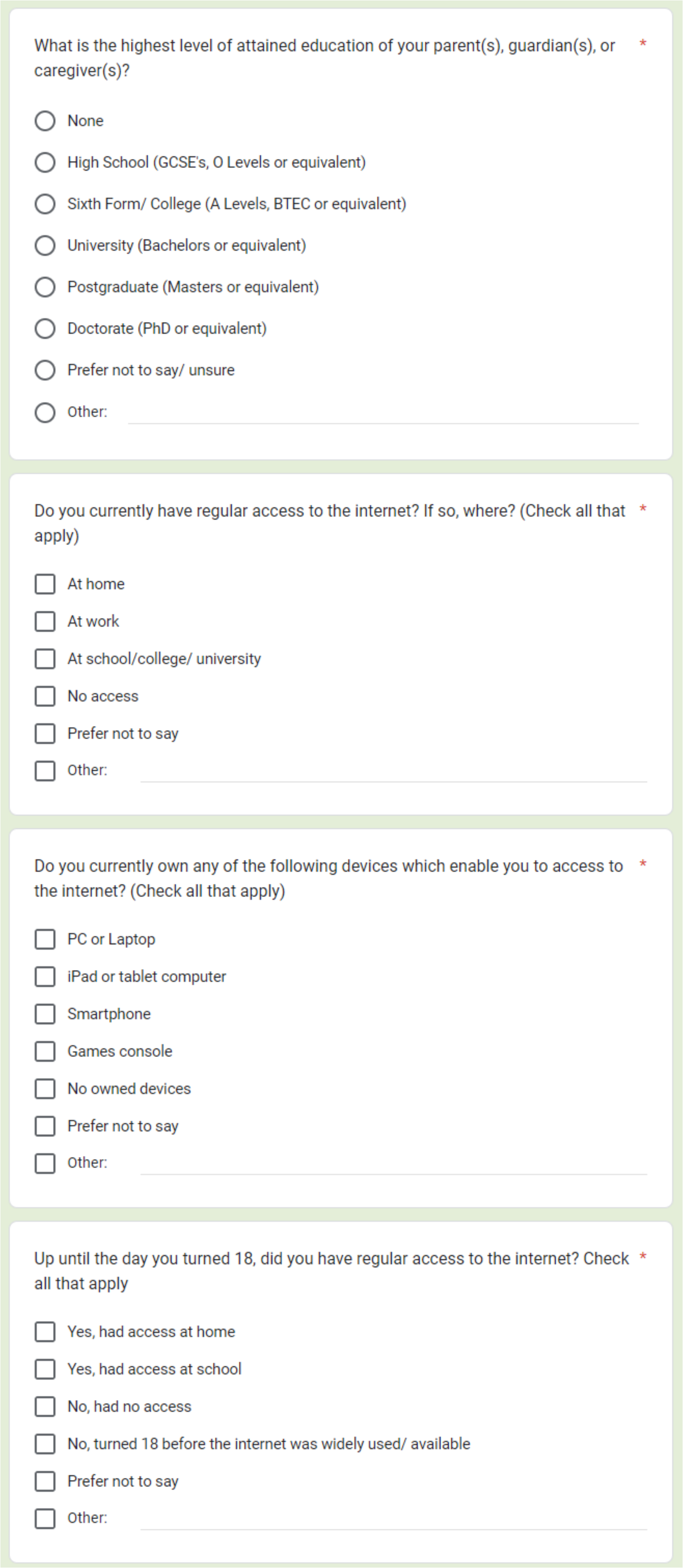
○ University (Bachelors or equivalent)

○ Postgraduate (Masters or equivalent)

○ Doctorate (PhD or equivalent)

○ Prefer not to say

○ Other: ____________________



What is the highest level of attained education of your parent(s), guardian(s), or caregiver(s)? *

○ None

○ High School (GCSE's, O Levels or equivalent)

○ Sixth Form/ College (A Levels, BTEC or equivalent)

○ University (Bachelors or equivalent)

○ Postgraduate (Masters or equivalent)

○ Doctorate (PhD or equivalent)

○ Prefer not to say/ unsure

○ Other: ____________________

Do you currently have regular access to the internet? If so, where? (Check all that apply) *

□ At home

□ At work

□ At school/college/ university

□ No access

□ Prefer not to say

□ Other: ____________________

Do you currently own any of the following devices which enable you to access to the internet? (Check all that apply) *

□ PC or Laptop

□ iPad or tablet computer

□ Smartphone

□ Games console

□ No owned devices

□ Prefer not to say

□ Other: ____________________

Up until the day you turned 18, did you have regular access to the internet? Check all that apply *

□ Yes, had access at home

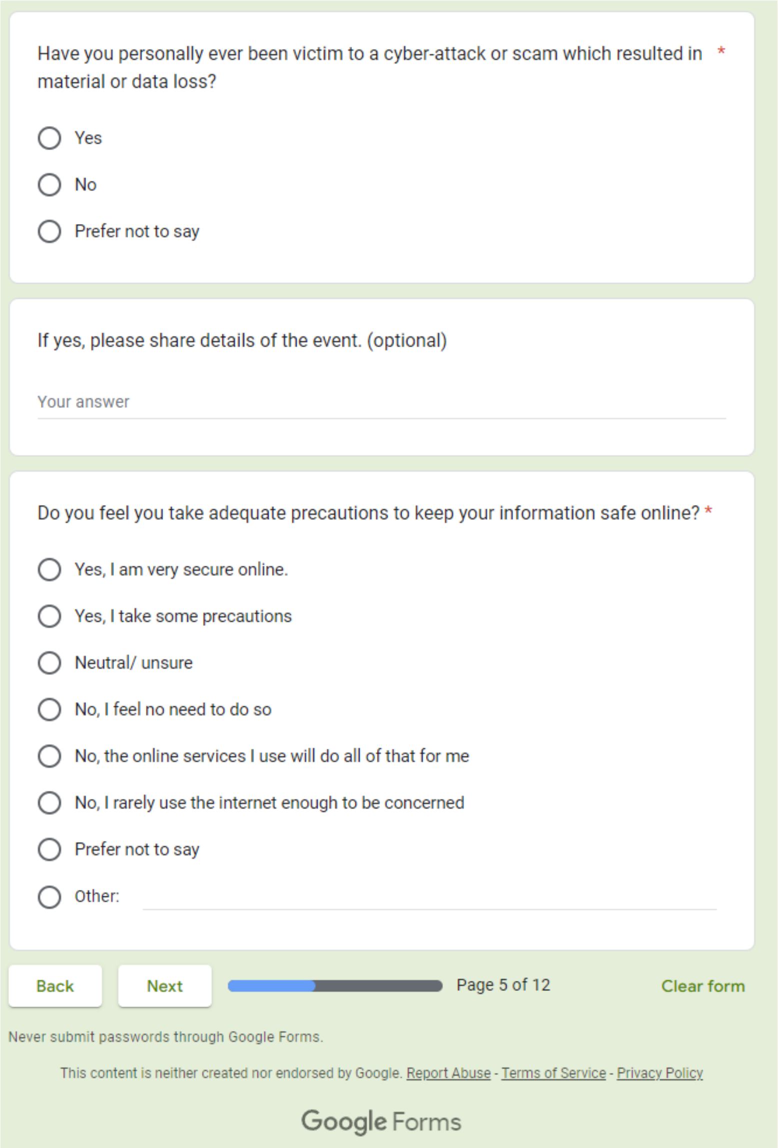
□ Yes, had access at school

□ No, had no access

□ No, turned 18 before the internet was widely used/ available

□ Prefer not to say

□ Other: ____________________



Have you personally ever been victim to a cyber-attack or scam which resulted in material or data loss? *

○ Yes

○ No

○ Prefer not to say

If yes, please share details of the event. (optional)

Your answer

Do you feel you take adequate precautions to keep your information safe online? *

○ Yes, I am very secure online.

○ Yes, I take some precautions

○ Neutral/ unsure

○ No, I feel no need to do so

○ No, the online services I use will do all of that for me

○ No, I rarely use the internet enough to be concerned

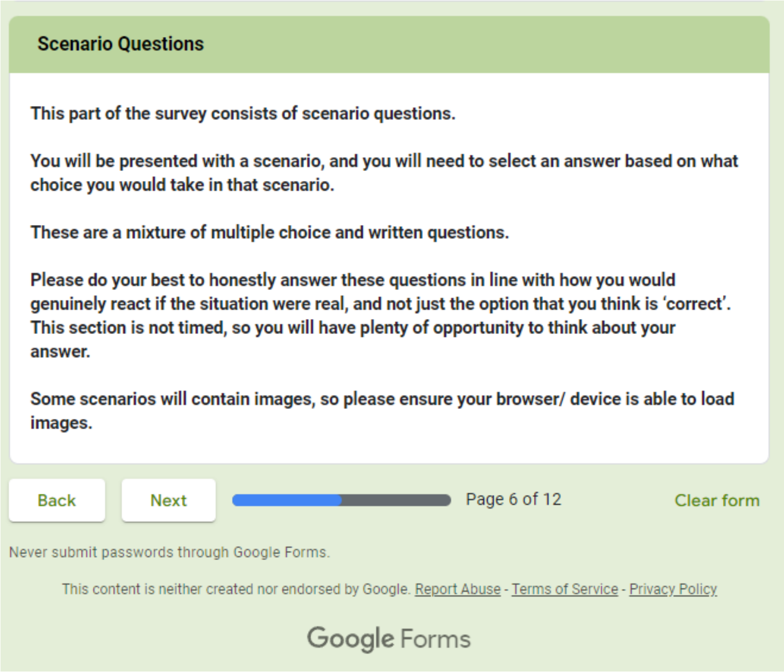
○ Prefer not to say

○ Other: ____________________

Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. Report Abuse - Terms of Service - Privacy Policy

Google Forms



Scenario Questions

This part of the survey consists of scenario questions.

You will be presented with a scenario, and you will need to select an answer based on what choice you would take in that scenario.

These are a mixture of multiple choice and written questions.

Please do your best to honestly answer these questions in line with how you would genuinely react if the situation were real, and not just the option that you think is 'correct'. This section is not timed, so you will have plenty of opportunity to think about your answer.

Some scenarios will contain images, so please ensure your browser/ device is able to load images.

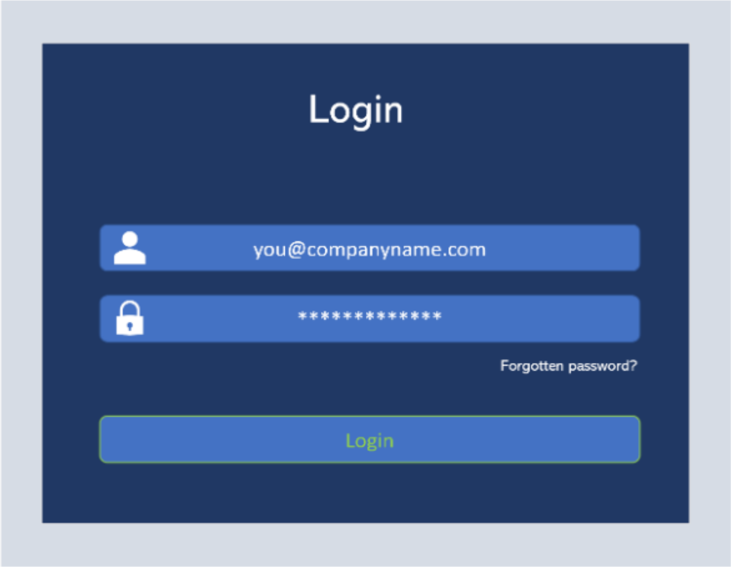
Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. Report Abuse - Terms of Service - Privacy Policy

Google Forms

Passwords

The company you work for has invested in some new software, all employees have been asked to create a new account.



What type of password would you likely choose in this scenario? *

Please answer as honestly as you can.

○ The same one used for all your other accounts.

○ A variation of a password you normally use - changing or adding some characters to increase complexity

○ Something simple and easy to remember

○ A really long and complicated password

○ Something completely unique

○ Other: ____________

Regardless of your answer to the previous question, what do you feel is the most secure type of password? *

Please answer as honestly as you can.

○ The same one used for all your other accounts.

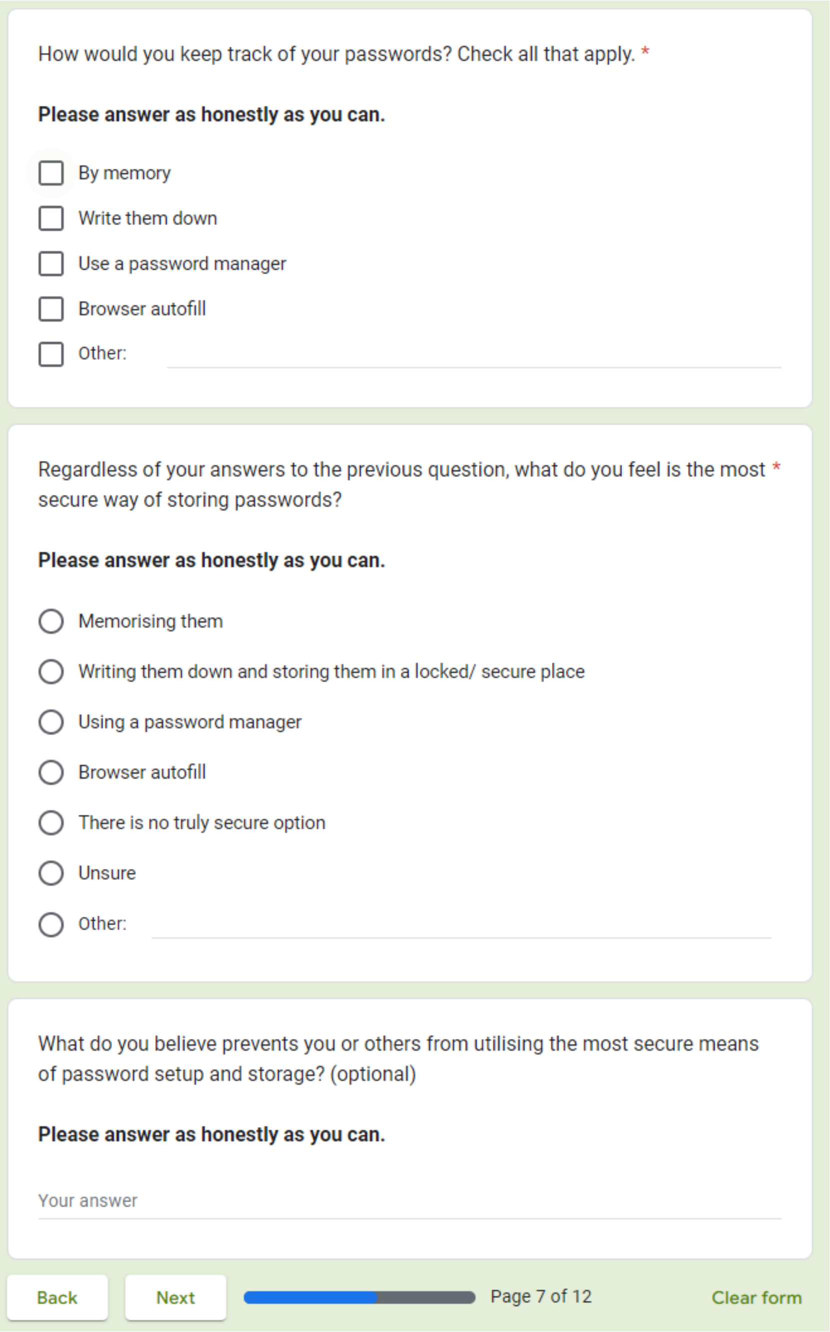
○ A variation of a password you normally use - changing or adding some characters to increase complexity

○ Something simple and easy to remember

○ A really long and complicated password

○ Something completely unique

○ Other: ____________



How would you keep track of your passwords? Check all that apply. *

Please answer as honestly as you can.

□ By memory

□ Write them down

□ Use a password manager

□ Browser autofill

□ Other: ____________________

Regardless of your answers to the previous question, what do you feel is the most secure way of storing passwords? *

Please answer as honestly as you can.

○ Memorising them

○ Writing them down and storing them in a locked/ secure place

○ Using a password manager

○ Browser autofill

○ There is no truly secure option

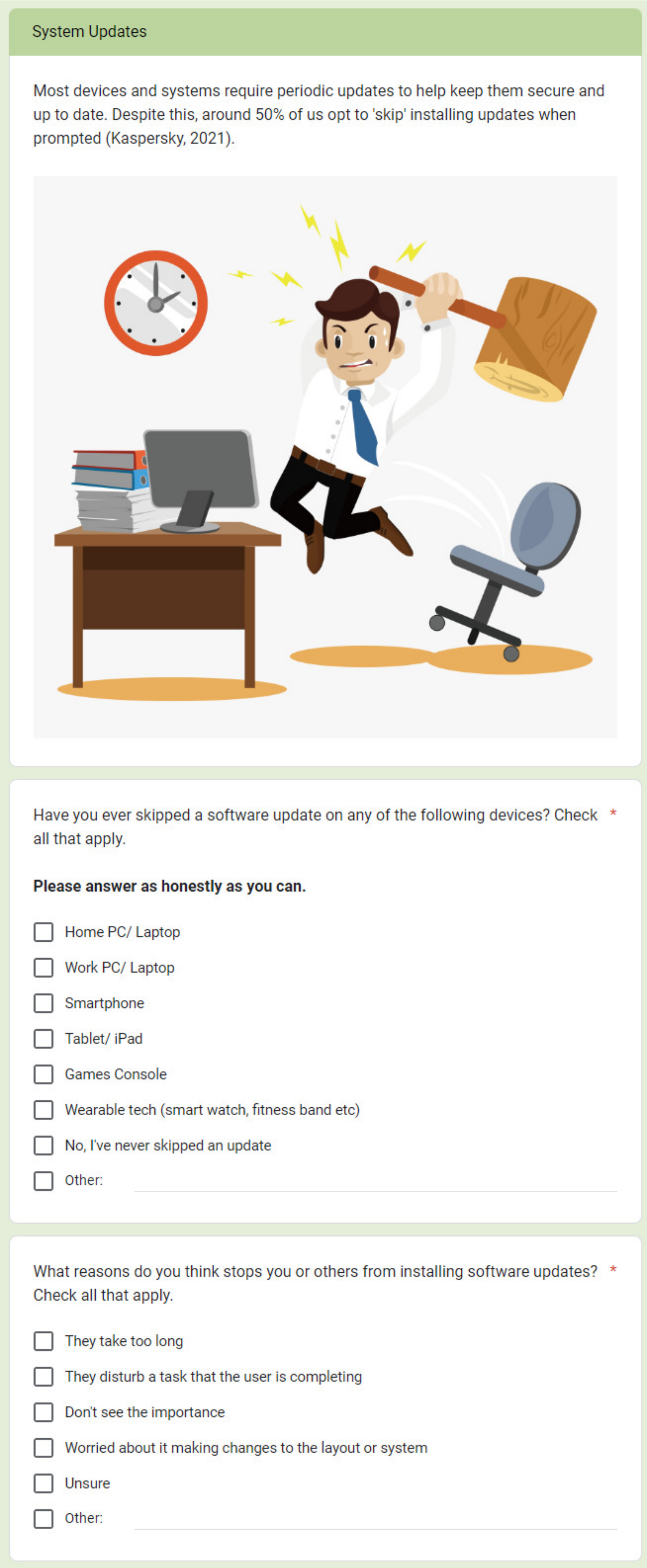
○ Unsure

○ Other: ____________________

What do you believe prevents you or others from utilising the most secure means of password setup and storage? (optional)

Please answer as honestly as you can.

Your answer



System Updates

Most devices and systems require periodic updates to help keep them secure and up to date. Despite this, around 50% of us opt to 'skip' installing updates when prompted (Kaspersky, 2021).

Have you ever skipped a software update on any of the following devices? Check all that apply. *

Please answer as honestly as you can.

□ Home PC/ Laptop

□ Work PC/ Laptop

□ Smartphone

□ Tablet/ iPad

□ Games Console

□ Wearable tech (smart watch, fitness band etc)

□ No, I've never skipped an update

□ Other: ____________________

What reasons do you think stops you or others from installing software updates? Check all that apply. *

□ They take too long

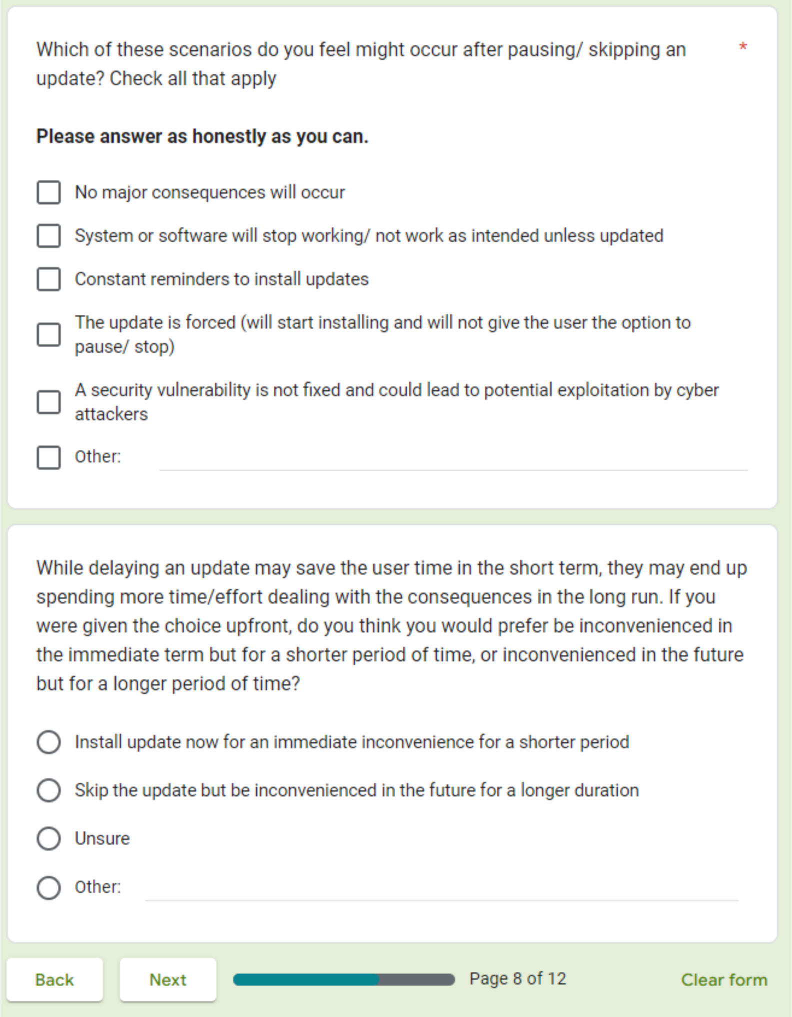
□ They disturb a task that the user is completing

□ Don't see the importance

□ Worried about it making changes to the layout or system

□ Unsure

□ Other: ____________________



Which of these scenarios do you feel might occur after pausing/ skipping an update? Check all that apply *

Please answer as honestly as you can.

□ No major consequences will occur

□ System or software will stop working/ not work as intended unless updated

□ Constant reminders to install updates

□ The update is forced (will start installing and will not give the user the option to pause/ stop)

□ A security vulnerability is not fixed and could lead to potential exploitation by cyber attackers

□ Other: ____________

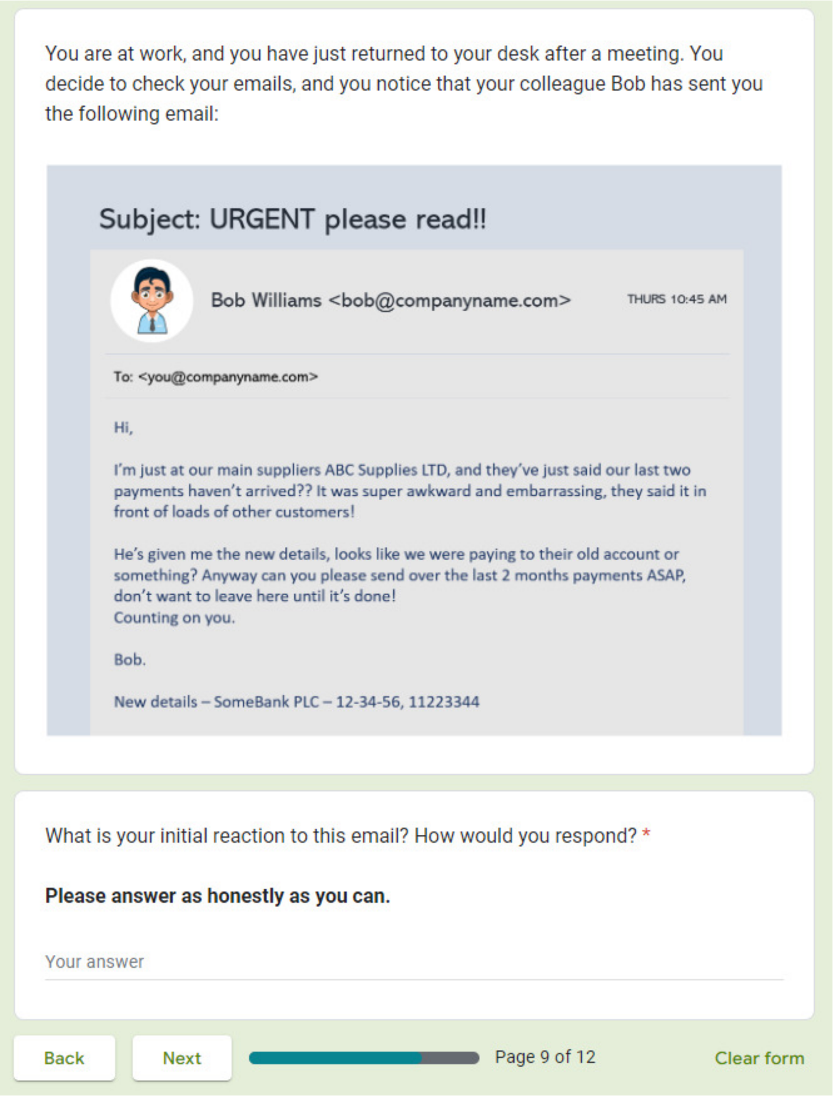
While delaying an update may save the user time in the short term, they may end up spending more time/effort dealing with the consequences in the long run. If you were given the choice upfront, do you think you would prefer be inconvenienced in the immediate term but for a shorter period of time, or inconvenienced in the future but for a longer period of time?

○ Install update now for an immediate inconvenience for a shorter period

○ Skip the update but be inconvenienced in the future for a longer duration

○ Unsure

○ Other: ____________



You are at work, and you have just returned to your desk after a meeting. You decide to check your emails, and you notice that your colleague Bob has sent you the following email:

Subject: URGENT please read!!

Bob Williams <bob@companyname.com>

THURS 10:45 AM

To: <you@companyname.com>

Hi,

I'm just at our main suppliers ABC Supplies LTD, and they've just said our last two payments haven't arrived?? It was super awkward and embarrassing, they said it in front of loads of other customers!

He's given me the new details, looks like we were paying to their old account or something? Anyway can you please send over the last 2 months payments ASAP, don't want to leave here until it's done!
Counting on you.

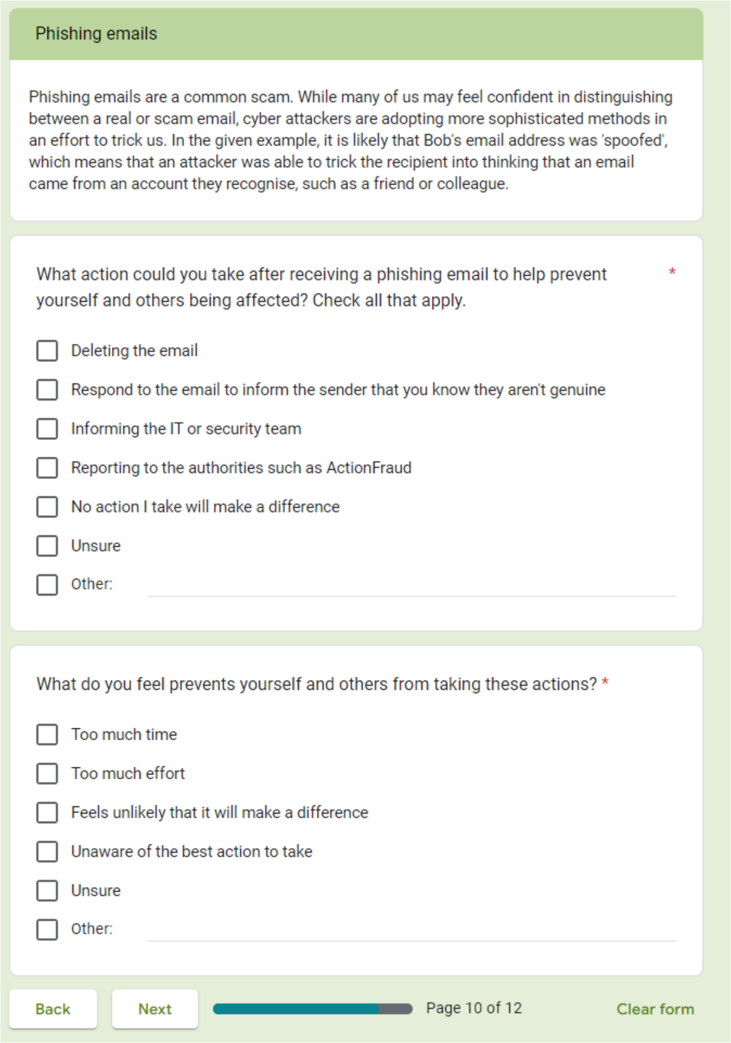
Bob.

New details – SomeBank PLC – 12-34-56, 11223344

What is your initial reaction to this email? How would you respond? *

Please answer as honestly as you can.

Your answer



Phishing emails

Phishing emails are a common scam. While many of us may feel confident in distinguishing between a real or scam email, cyber attackers are adopting more sophisticated methods in an effort to trick us. In the given example, it is likely that Bob's email address was 'spoofed', which means that an attacker was able to trick the recipient into thinking that an email came from an account they recognise, such as a friend or colleague.

What action could you take after receiving a phishing email to help prevent yourself and others being affected? Check all that apply. *

□ Deleting the email

□ Respond to the email to inform the sender that you know they aren't genuine

□ Informing the IT or security team

□ Reporting to the authorities such as ActionFraud

□ No action I take will make a difference

□ Unsure

□ Other: ____________________

What do you feel prevents yourself and others from taking these actions? *

□ Too much time

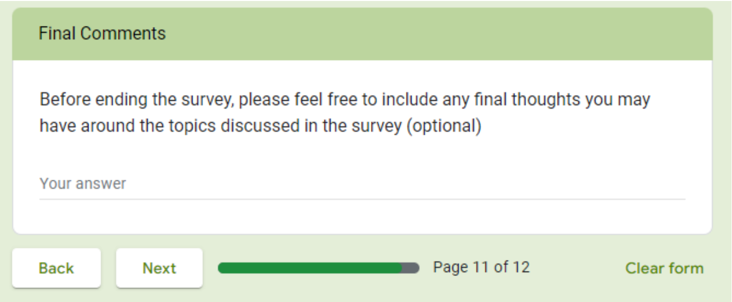
□ Too much effort

□ Feels unlikely that it will make a difference

□ Unaware of the best action to take

□ Unsure

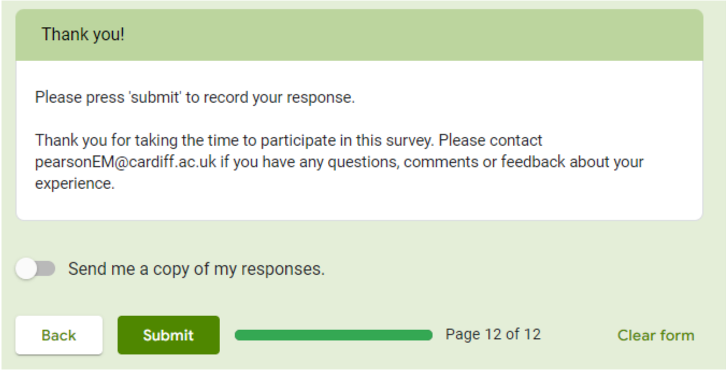
□ Other: ____________________



Final Comments

Before ending the survey, please feel free to include any final thoughts you may have around the topics discussed in the survey (optional)

Your answer



Thank you!

Please press 'submit' to record your response.

Thank you for taking the time to participate in this survey. Please contact pearsonEM@cardiff.ac.uk if you have any questions, comments or feedback about your experience.

Send me a copy of my responses.