HSBC Portfolio

u5539006

March 2025

Contents

1 Improved Usability Design

This section involves the evaluation and redesign of a movie rental website against basic laws of user experience (UX) (Yablonski, 2020) and the Nielsen Heuristics (Molich and Nielsen, 1990). The website with improved usability is hosted at `https://imogenbartin.github.io/shop.html`.

Nielsen's 10 heuristics are detailed below for reference:

No.	Heuristic	Description
1	Visibility of System Status	Users should always be made aware of what is going on, with appropriate feedback, in a reasonable length of time.
2	Match Between the System and the Real World	The vocabulary of the design should be catered to the audience, rather than using internal jargon. Information should also appear in a logical layout, following real-world conventions.
3	User Control and Freedom	Users should have an easy way to reverse actions should they make a mistake.
4	Consistency and Standards	Follow platform and industry standards in order to avoid confusing users.
5	Error Prevention	Eliminate error-prone conditions in the design, or notify users before they take an action that may result in an error.
6	Recognition Rather than Recall	Reduce memory load by making elements, actions and options visible. Users shouldn't have to remember information from other pages.
7	Flexibility and Efficiency of Use	Shortcuts should exist for experienced users, hidden from novices. Allow users to customise common actions.
8	Aesthetic and Minimalist Design	Interfaces should not contain irrelevant or rarely-needed information. This subtracts from the visibility of relevant information.
9	Help Users Recognize, Diagnose, and Recover from Errors	Errors should present in plain language, indicate the problem, and present a solution.
10	Help and Documentation	Ideally, don't require any extra documentation. However, be sure to include it for complicated actions.

Usability Problem	Description	Heuristic(s)	Rating (/10)
Index Page			
Page does not exist, and user is presented with directory.	Confusing to non-technical users, who may not know how to interact with the website.	1, 5, 8 & 10	9
Login Page			
No formatting examples for login details.	Users may format login details in a non-acceptable manner causing system errors.	5 & 10	3
No input validation on the front-end.	Users may accidentally enter incorrect or ill-formatted details.	1 & 5	6
Shop Page			
Page elements are spread out, and images do not load.	Difficult to quickly understand which movie is which, and what elements relate to it.	4, 5, & 8	7
Similar elements are not aligned.	Duplicate elements that exist for each film are not aligned, and may confuse users when they are selecting a film.	4 & 8	6
No confirmation on button presses.	The "Add to Basket" and "Empty Basket" buttons do not visually confirm that the actions have succeeded, which may cause repeated clicks.	1 & 5	5
The same item can be added to the basket multiple times.	It is possible to add items to the basket that already exist in it, confusing users and causing them to be charged extra.	5	7
Buttons and links to navigate are small and oddly placed.	Buttons to navigate the website are far away from the main content, and take too long to notice, according to Fitt's Law (Yablonski, 2020).	7 & 8	3
Not all relevant information is included.	The cost of films is not displayed on the shop page, and users may add films to basket without viewing the price.	5	5
Genre list is irrelevant and redundant.	Genre list is completely inert, and it is not possible to filter or view genre of films.	8	4

Usability Problem	Description	Heuristic(s)	Rating (/10)
Movie Page			
Film descriptions are not very descriptive.	Some film descriptions contain very little information about the film.	2 & 4	2
No way to return to the shop/home page.	The only way to return is to use the browser back button or to exit then log in again.	3 & 4	8
It is not possible to add the film to the basket.	Users are forced to return to the shop page to add the film to the basket.	7	8
Information is poorly laid out and formatted.	Film details are difficult to quickly read and the price is poorly formatted.	2, 4 & 8	5
Basket Page			
Information is poorly aligned, and formatted badly.	Column data is mis-aligned with column titles, and price is just displayed as a number.	2, 4 & 8	6
Price is not accurate.	The total cost is a number with up to 15 decimal places.	4 & 8	7
"Continue Shopping" button doesn't work.	No action on button press.	5	4
It is not possible to edit/remove items in the basket.	Users are forced to completely clear the basket to edit days to rent, or remove a film.	3 & 7	6
Lack of confirmation of clearing the basket.	Users may either click multiple times unnecessarily or continue to pay after clearing.	1 & 5	7
Checkout Page			
Text boxes do not match with labels, and do not contain example placeholders.	It is unclear which text box relates to what information.	4, 5,	6
No front-end input validation	Users can enter any type of information for any of the fields and they would not be informed of improper input.	1 & 5	5

1.1 Cognitive Walkthrough

The biggest issues discussed during the evaluation of the website template were:

- Index: Page doesn't exist.
- Movie: No way to return to the shop/home page.
- Movie: It is not possible to add the film to the basket from this page.

Below are the cognitive walkthroughs of the pages before/after the redesign of the website, according to the model proposed by Lewis et al. (1990):

1.1.1 Original Index Page: doesn't exist

Stage	Description	Likelihood
User's immediate goal	Access the website to view the available films.	3
How will user access description of action?	No description of action is given.	n/a
How will user associate description with action?	No description of action is given.	n/a
Are all other available commands less appropriate?	It is not clear what the user should do in this scenario.	3
How will the user execute the action?	Select the login.html page from the directory listing. However, they may also select different pages or files.	2
If timeouts, is there time for user to decide before timeout?	The directory listing doesn't timeout.	n/a
Execute the action, describe system response.	If they select a HTML file, they will be redirected to that webpage, and if they select a file, it will be downloaded.	1
Describe the modified goal, if any.	No modified goal.	n/a

Figure 1: Index page pre-redesign

1.1.2 Fixed Index Page: exists

Stage	Description	Likelihood
User's immediate goal	Access the website to view the available films.	3
How will user access description of action?	On-screen message informing the user of a redirect.	3
How will user associate description with action?	They are given a link at the end of the description to use if necessary.	3
Are all other available commands less appropriate?	There are no other commands available.	3
How will the user execute the action?	Wait for the redirect to happen, or click the hyperlink in the message.	3
If timeouts, is there time for user to decide before timeout?	The timeout is the minimum length of time, but there is sufficient time for users to read the given message.	2
Execute the action, describe system response.	User is redirected to the login page for the website.	3
Describe the modified goal, if any.	Sign in or register to the website to access the shop.	3

Figure 2: Index page post-redesign

1.1.3 Index Page Redesign

This redesign stops the user being able to view the directory listing for the web server, which allows them to access any possible webpage or file. This is a security and usability risk, since they can access the source code of the website or any page that they shouldn't have access to, or download arbitrary files, and because it can lead to scenarios that are not possible, such as checking out an empty basket, or trying to open the details for a movie that doesn't exist. This layout also discourages non-technical users as they are unfamiliar with this interface.

After the redesign, the user is promptly informed that they will be redirected in just a moment, and this should happen automatically. A hyperlink is also included if, for any reason, this doesn't happen. Users clicking on the link will be redirected to the home page. This removes the security issue of allowing users to access the directory listing, and also stops users from taking random "paths" through the application, instead having them follow a pre-defined route.

1.1.4 Original Movie Page: no way to return to home

Stage	Description	Likelihood
User's immediate goal	Return to the shop page	3
How will user access description of action?	No description of action.	n/a
How will user associate description with action?	No description of action.	n/a
Are all other available commands less appropriate?	Exit link logs the user out of the system.	3
How will the user execute the action?	Click the link/button to exit, or use the browser back button.	3
If timeouts, is there time for user to decide before timeout?	No timeouts.	n/a
Execute the action, describe system response.	User will get logged out if clicking "Exit" or will return to the shop page using the browser button.	2
Describe the modified goal, if any.	No modified goal.	n/a

1.1.5 Fixed Movie Page: can return home

Stage	Description	Likelihood
User's immediate goal	Return to the shop page.	2
How will user access description of action?	Large labelled button allows the user to go back to the home page.	3
How will user associate description with action?	The button is clearly labelled with the name of the website.	3
Are all other available commands less appropriate?	All other buttons are clearly labelled as to their action.	3
How will the user execute the action?	Click the button.	3
If timeouts, is there time for user to decide before timeout?	No timeouts.	n/a
Execute the action, describe system response.	The user will be redirected to the home page.	3
Describe the modified goal, if any.	No modified goal.	n/a

1.1.6 Movie Page Redesign: Buttons

The movie page was redesigned to allow a user to return to the home page, or to the basket, from it. Previously, this was not doable, and the page only contained information about a specified film, but no way to access the basket or the home page directly without using the browser buttons. This disrupted user flow through the application, and may have caused users to accidentally logout of the application when clicking the "Exit" button. Now, the buttons are clearly showcased as interactable elements, and are clearly labelled. The "Exit" button has been re-labelled to say "Log out" to make its purpose clear to users.

1.1.7 Original Movie Page: can't add film to basket

Stage	Description	Likelihood
User's immediate goal	Add the film to the basket.	3
How will user access description of action?	No description given.	n/a
How will user associate description with action?	No description given.	n/a
Are all other available commands less appropriate?	There is no command to achieve this feature, but there is also no similar buttons.	n/a
How will the user execute the action?	They must return to the home page, then add to basket.	2
If timeouts, is there time for user to decide before timeout?	No timeouts.	n/a
Execute the action, describe system response.	User is redirected to home page, they must then enter days to rent, then add to basket.	2
Describe the modified goal, if any.	Return to the home page, first.	3

1.1.8 Fixed Movie Page: can add film to basket

Stage	Description	Likelihood
User's immediate goal	Add the film to the basket.	3
How will user access description of action?	Button clearly states "Add to Basket".	3
How will user associate description with action?	The labelling is on the button, they just have to click it.	3
Are all other available commands less appropriate?	Other buttons/hyperlinks are clearly labelled, and none are similar.	3
How will the user execute the action?	Click the button to add to basket.	3
If timeouts, is there time for user to decide before timeout?	No timeouts.	n/a
Execute the action, describe system response.	The item is added to the basket, and the user is redirect to the basket page.	3
Describe the modified goal, if any.	Go to checkout	2

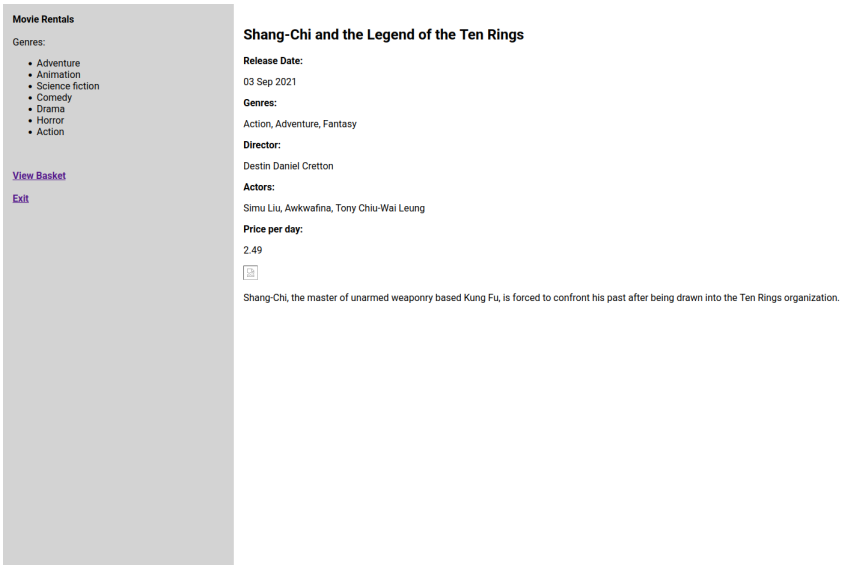


Figure 3: Movie page pre-redesign

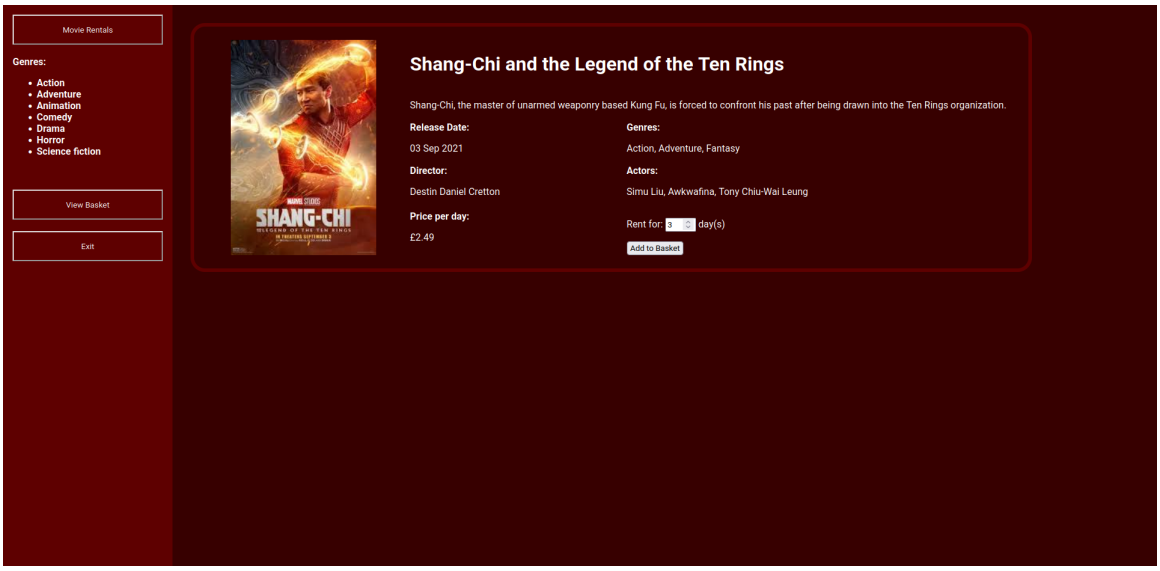


Figure 4: Movie page post-redesign

1.1.9 Movie Page Redesign: Basket

Prior to the redesign, the movie page was inert, and contained details about the given film. These were arranged illogically, and were difficult to read quickly. The lack of picture and the description being at the bottom meant it could be difficult to identify the film. There was also no way to add the film to your basket, despite this being the only page that had the price of the film per day on it.

After the redesign, the information about the film was reorganised into a logical manner, where users could quickly understand what was going on. The information was also correctly formatted, such as the price, which previously had just been a decimal number. Lastly, it is also possible for the user to add the item to the basket from this page where they can see the price, rather than just the home page, which confirms to Nielsen's 6th Heuristic (Molich and Nielsen, 1990), since that information does not have to be remembered.

2 Experiental Reflection

2.1 How has the material taught in the labs affected my understanding of the subject matter?

The labs have, of course, deepened my understanding of the subject content through individual and guided research into the topics, and has brought to my attention the major part that human psychology plays in the cybersecurity space. Through several practical labs (see Appendix A), I have applied the knowledge I have gained to mock scenarios, allowing me to understand how such things would be applied in industry.

I have also been taught to account for the UI/UX considerations in applications to maximise user efficiency and usability, and how subtle things can change a users perspective on an idea or experience of an application.

2.2 What have I learned and how can I apply it in my future work as a cyber security specialist?

The subjects covered in this module are crucial to a variety of cybersecurity specialisms. My present aspirations within cybersecurity involve an offensive specialism, in which ethical obligations are important to consider before taking on any work and to apply the ethical frameworks to. Social engineering can also play a major role in offensive security roles, such as penetration testing, where the principles of nudging and framing are key concepts that one must be able to make use of. This means that any social engineering campaign can be more sophisticated, which is optimal for testing defences.

2.3 How did the material catch my attention?

The material caught my attention through a mixture of understanding malicious psychology, and the principles of UX that go into software engineering. Malicious psychology piqued my interest because of its application in real-world attacks and because deception within cybersecurity has always been an interest of mine.

UX principles and design also caught my attention because of many teenage years spent web developing, and I was excited to see if I'd picked up on the right ideas through intuition. However, I was incredibly humbled, and since then, it has been exciting to be taught the actual proven techniques.

2.4 Are there any unsolved questions or critical issues in my learning?

There is not much in the way of unsolved questions, since the module accurately and comprehensively covers a broad range of subjects involved in the cyber context of human psychology.

Currently however, I am unable to implement a lot of the techniques and ideas we have studied into my own work, since I am unsure how to do so. However, I am positive that this will become clear as my experience grows, and that this is the best way to learn such things.

I would also like to practice the use of previously mentioned malicious tricks in an offensive security sense, to improve those skills before starting a career doing similar things.

2.5 How will the material affect my future thinking?

This module has changed my thinking about technical cybersecurity to be user-centric, and taught me to consider the use cases and UX of users in applications. The module has highlighted the important, and irrefutable, connection between technical cybersecurity, offensive cybersecurity and human psychology, particularly in a malicious sense, and has prompted me to expand my reading and personal study into uses of psychology in offensive security, and somewhat even into just straight psychology.

Secondly, the regular discussion sessions of academic papers has led to others challenging my perspective, which has allowed me to learn to defend my thinking, and also taught me to challenge myself on my thoughts - to think more critically about what I am reading and what it means.

3 Research Paper Selection incl. Textual Reflection

3.1 Summaries of Discussed Research Papers

No.	Paper	Discussion	Leader
1	Kang et al. (2015)	This study investigated the behaviour of technical and non-technical individuals in a Cyber Security scenario. • Technical participants were less likely than others to take simpler advice (antivirus, password changes etc.), instead opting for more technical security such as encryption and Tor. • A large proportion of people felt that their data wasn't important enough to bother securing it.	N
2	Yan et al. (2018)	This study investigates the security behaviours of different demographics to identify the 'weakest link' in Cyber Security. • There was no significant difference between different demographics. • Individuals tend to be more aware of online or computer-based threats, but less aware of physical threats. • Students are better at recognising issues with situations they are commonly exposed to, than other situations.	N
3	Signorelli (2018)	This study investigates the developments of AI towards emulating and overcoming human consciousness. • It was decided that a Turing test is not a reliable test of whether a machine can think, but rather it's ability to mimic previous human thinking. • The paper does not propose an adequate metric to measure the consciousness of Artificial Intelligence, since humans do not understand the concept of consciousness. • Could an AI be conscious without being an emulation of the human brain, instead following a different path?	N

No.	Paper	Discussion	Leader
4	Rodríguez-Priego et al. (2020)	This study investigated the difference between loss- and gain-based framing on the security behaviour of individuals. • Loss-based framing worked best in the short-term, however gain-based was more effective over an extended length of time. • Loss-based framing caused higher emotional impact, and therefore more an influence towards behaviour, however, it can de-motivate individuals. • Gain-based framing is likely to be a better solution in the long-term since people associate the necessary actions with positivity and reward.	N
5	Hatfield (2019)	This study discusses the ethics of deception and social engineering on unaware individuals. • Deception as a training mechanism is useful in the short-term, and with minimal real-world effect. • In order to obtain an accurate report on the security of an organisation, it is necessary to employ deception against the employees while they are unaware of it. • It is however important to let certain high-up individuals aware of the penetration test in order to avoid provoking real-world response. • The use of deception as a test will either create a trust-verified culture within the organisation or cause hostility.	N
6	van Bavel et al. (2019)	This study uses positive and negative framing, similar to Rodríguez-Priego et al. (2020), to influence the online security of individuals. • The study is based on Protection-Motivation Theory, suggesting that a user evaluates the risk of an action and their ability to cope with it before taking said action. • Positive messages (coping messages) were found to encourage more secure behaviour from individuals. • Threat appeals were less effective than any other method, since user's repeated exposure to them reduced their perception of the risk. • Gain-based and positive framing is more effective to the human brain (Xu et al., 2020).	Y

3.2 Discussion Plan Email

A screenshot of the proposed discussion plan, sent on 27/02/2025, can be found in appendix B, Figure 14.

3.3 Textual Reflection

Yan et al. (2018) studied the possibility of various physical characteristics on cybersecurity behaviour in students, including degree subject, gender, and year of study. The aim of this paper was to discuss the splitting of "ordinary people" into categories in order to investigate the "weakest link" phenomena in cybersecurity behaviour. However, they concluded that these factors did not significantly affect individual's cybersecurity behaviour, and instead suggested the grouping of individuals into three categories: low, moderate, and high cybersecurity judgement.

However, a more recent study (Hull et al., 2021) suggested the variables by which individuals should be evaluated into these groups. It was found that knowledge and awareness of cybersecurity and cyber threats was the biggest contributor to high cybersecurity judgement, alongside motivation, confidence, risk and sex-related characteristics. Some of these characteristics are objective between situations, however, some are not.

It is reasonable, and even intuitive, therefore, to say that an individual's cybersecurity behaviour is dependent largely on both their perception of threats, and their perceived ability to deal with cyber threats. Kovacevic et al. (2020) and Alanazi et al. (2022) support this conclusion, largely, with the added result that previous experience also affects behaviour. We know that these factors affect human behaviour as a whole (Maslow, 1954), but they appear to be the leading factors in affecting cybersecurity behaviour.

However, it is impossible to educate everyone on the nature, threat vectors, and techniques of cyber threats, and how to deal with them in a confident but secure way. Therefore, there is always going to be a group with low cybersecurity judgement (the "weakest link").

However, I do not believe that research into discovering the so-called "weakest link" is sufficient, and afterwards, should focus on the methods by which personal security for those in this group could be improved.

With this in mind, I believe that the best course of action is, instead of only attempting to educate ordinary people about the dangers of cyber attacks and the importance of high cybersecurity behaviour, changing the environment in which ordinary people encounter cyber threats. This would fall onto the shoulders of popular service providers e.g. Google, Microsoft etc. to subtly influence the behaviour of individuals using their services to promote personal security.

A study (Dolan et al., 2012) conducted into the environmental factors that can automatically or subconsciously affect the behaviour of individuals found several key factors: physical environments, societal norms, default options, framing, subtle cues, timing, loss aversion and commitment.

Further research into this subject is required, but this is likely to mean that it must be easier and more convenient for users to act securely, such as by having many notifications, pop-ups, and confirmations to act insecurely within an application. Users should also be notified of what other users are doing, a parallel with the idea of peer pressure, and users should have to actively choose to act insecurely. By default, secure functions should be selected and used. Finally, users should have threat-messages displayed prominently when acting insecurely, as humans tend to be more prone to loss aversion than gain-based nudging.

In this context, it is difficult to implement measures to control commitment, and timing. However, by controlling most of the factors, a noticeable increase in secure cybersecurity behaviour should be possible.

4 Critical Reflection

> *"Cybersecurity should be included in the culture of an organization and be a priority of management. Establishing culture in a cybersecurity organization depends predominantly on individuals, technology, organizational behaviour, and several facets of information security. The most vulnerable aspect of cybersecurity is the human that needs to be trained to be more cybersecurity aware. Diversity in the workplace is also increasing a person's individual cultural background needs to be considered to communicate effectively cross-culturally. A combination of cybersecurity culture and employee ethnic culture consideration is needed to successfully maintain consistent effective practices of cybersecurity. Creating cybersecurity culture needs to be communicated along with the recognition that human aspects of cybersecurity is an on-going learning experience that expands cybersecurity awareness."*

It is incredibly important for cybersecurity to be considered and integrated into the culture of an organisation, and to be made the priority of not only the management, but also every employee. It is necessary for employees to have the education and for management to enforce security policies and regulations, to ensure that taking appropriate security measures isn't viewed as a "chore". This education allows employees to understand the organisation needs, and as such, they feel more of a personal stake in the security of it (Rumble et al., 2010).

It is foolish to believe that the "*the most vulnerable aspect of cybersecurity is the human*". This can be the case, however, it is not always. Effective implementation of a cybersecurity culture within an organisation significantly reduces the risk of human factors affecting cybersecurity incidents. It is important to remember that the two sides of this argument have different characteristics. People tend to be trusting and more gullible than a computer, which cannot empathise with scenarios. However, it can be much more difficult to exploit a human. Humans are very unique compared with one another, and exploiting them consumes far more mental effort than exploiting a bug in software - which will be similar on similar systems.

It is clear, however, that phishing scams are the most lucrative attack vector for malicious actors, since 84% of cyberattacks on businesses in the UK in 2024 were the result of phishing scams (Department for Science, Innovation & Technology, 2024). It is therefore of paramount importance that employees are trained to not only be "aware" of but also be able to practically identify and report them. It is also important that training is catered to the context of the business needs, and to that of the individual.

Creating a cybersecurity culture is very important, but, as stated, it must be balanced with employee ethnic culture consideration and more general employee consideration, to "*successfully maintain consistent effective practices of cybersecurity*". Reports have shown that employees that are unhappy, stressed, or tired are more susceptible to phishing and other scams (Which?, 2022). There is also the risk of disgruntled employees becoming insider threats. It is therefore crucial to employ measures to maintain employee wellbeing in order to maintain good cybersecurity, alongside the training that employees should receive.

Cybersecurity is constantly evolving, and scams are becoming more sophisticated, as well as more general cyberattacks. This means that the only effective cybersecurity culture is one that evolves alongside the field itself. Therefore, it is of paramount importance that employees undergo regular training and practical exercises to test and revise their cybersecurity awareness and knowledge. This will cause less employees to fall victim to social engineering strategies, and to report suspicious activity / contact. Lastly, it is important to not punish employees who facilitate a cyberattack unwittingly, as this creates a hostile environment where employees do not want to admit to potential

improper cybersecurity behaviour.

In conclusion, a cybersecurity culture can only be implemented and fostered through ongoing practical training and an environment in which employees are not penalised.

5 Behaviour Change Intervention

5.1 Identify and Review

Humans may be the biggest cybersecurity risk to organisations. As mentioned previously, 84% of data breaches in 2024, surveyed by the NCSC (Department for Science, Innovation & Technology, 2024), identified phishing as the attack vector. This survey also identified that only 18% of organisations had received cybersecurity awareness or training in the last 12 months.

However, those that do implement cybersecurity training, generally do not offer any kind of adaptive training, instead opting for static training. A report from HornetSecurity (2024) found that fewer than 8% of organisations have adaptive cybersecurity training courses, and 45% of organisations believe their cybersecurity training is outdated.

Even despite training, users are often found to demonstrate insecure behaviour in real-world scenarios, affected by a multitude of factors: fatigue, lack of focus, ego, or complacency. This intervention aims to increase the engagement and retention of a cybersecurity course with users, to improve their day-to-day behaviour.

Studies into learning techniques have concluded that active techniques (those that *"actively [engage] the students in contributing, collaborating, discussing, discovering, reflecting, and sharing."*) are more effective to long-term retention that passive training techniques Minnick et al. (2022). However, this does come with downsides: passive training techniques tend to have a stronger effect on knowledge immediately after the training course. Therefore, it would be imperative to combine regular cybersecurity training and revision courses with active learning techniques to have the greatest effect.

It is also suggested by many, and supported with evidence (Kincaid and Westerlund, 2009), that simulation training is highly effective. Since cybersecurity threats are more prevalent in organisations with higher reliance on IT infrastructure, it is likely that organisations will have the facilities and capabilities to run simulation-based training, particularly in a gamified form, which has been proven to increase student engagement with the content (Smiderle et al., 2020).

5.2 Logic Diagram

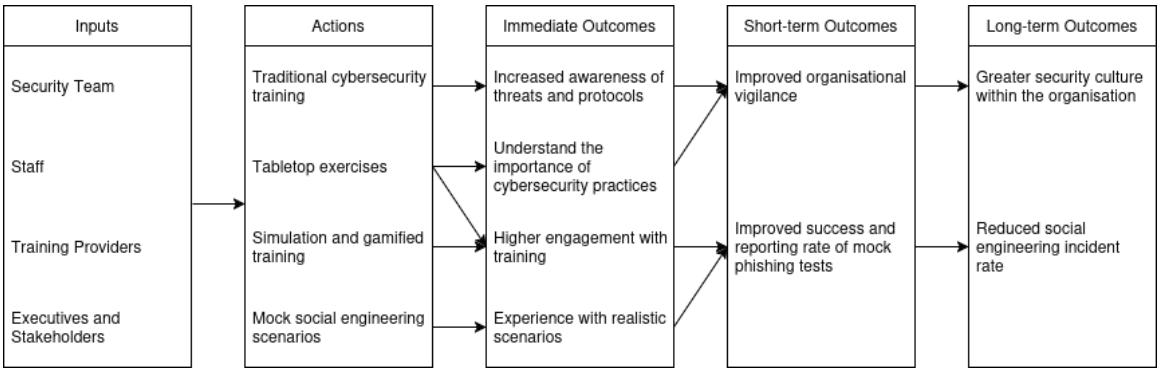


Figure 5: Logic diagram of proposed intervention

5.3 Developing the intervention

The intervention itself is a mixture of redeveloping traditional training courses with active learning strategies, and including gamified and simulation elements, and performing mock social engineering tests on users.

Redeveloping existing training courses

Training courses will be redesigned to be more of a discussion and collaboration session for users, since these type of active activities promote a greater retention of the material. This should include group work, such as on password rules and creation, internet browsing and viruses, and on phishing scams. By encouraging the discussion of each of these topics, a greater security culture should be achieved.

This would involve the collaboration and discussion on what kind of rules should be implemented for password creation, and why, including a visual demo of the strength of the password using a tool such as `https://nordpass.com/secure-password/`. Password managers should also be discussed to discourage password reuse. It may be useful to also include a live demo of a password-cracking attack to demonstrate the speed and power of computers.

Secondly, there should be discussion on internet browsing and viruses, covering HTTPS, payment details, and what to download or not, followed by a group task on evaluating potential phishing emails.

Lastly, there should be a quiz to test short-term retention of the email in an interactive, silly, and fun way. This promotes people to try what they think, because of the lack of consequences. For example, a 'Kahoot!' (`https://kahoot.com/`).

Mock social engineering tests

It is of the utmost importance that this part of the course is delivered without any consequence, judgement, or humiliation. Users must be able to flag what they believe to be scam and phishing emails and receive feedback on their choices. They should be informed about key signs of a scam email, and be able to refer back to these, such as an intranet resource - this also serves to inform users about where they can find information.

It is then necessary for users to read through a list of emails, flagging the emails they believe to be phishing attempts, and also identifying the reason - such as by clicking on the relevant part of the email. This increases interactivity by gamifying the exercise, which will increase engagement. Having a points system for tell-tale sign accuracy would also contribute to this aspect of the course.

By having users physically identify the suspicious parts of the email, it should help to consolidate the red flags for phishing in their mental models of email client, which should reduce the incident rate.

This should be performed at random intervals, in an ongoing process.

References

J. Yablonski. *Laws of UX: Using Psychology to Design Better Products & Services*. O'Reilly Media, 2020. ISBN 9781492055280. URL https://books.google.co.uk/books?id=BuneDwAAQBAJ.

Rolf Molich and Jakob Nielsen. Improving a human-computer dialogue. *Commun. ACM*, 33(3): 338–348, March 1990. ISSN 0001-0782.

Clayton Lewis, Peter G Polson, Cathleen Wharton, and John Rieman. Testing a walkthrough methodology for theory-based design of walk-up-and-use interfaces. In *Proceedings of the SIGCHI conference on Human factors in computing systems Empowering people - CHI '90*. ACM Press, 1990.

Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. "my data just goes everywhere:" user mental models of the internet and implications for privacy and security, 2015. URL https://www.usenix.org/system/files/conference/soups2015/soups15-paper-kang.pdf.

Zheng Yan, Thomas Robertson, River Yan, Sung Yong Park, Samantha Bordoff, Quan Chen, and Ethan Sprissler. Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Comput. Human Behav.*, 84:375–382, July 2018.

Camilo Miguel Signorelli. Can computers become conscious and overcome humans? *Front. Robot. AI*, 5:121, October 2018.

Nuria Rodríguez-Priego, René van Bavel, José Vila, and Pam Briggs. Framing effects on online security behavior. *Front. Psychol.*, 11:527886, October 2020.

Joseph M Hatfield. Virtuous human hacking: The ethics of social engineering in penetration-testing. *Comput. Secur.*, 83:354–366, June 2019.

René van Bavel, Nuria Rodríguez-Priego, José Vila, and Pam Briggs. Using protection motivation theory in the design of nudges to improve online security behavior. *Int. J. Hum. Comput. Stud.*, 123:29–39, March 2019.

Sihua Xu, Mohan Wang, Qingqing Liu, Cencen Wang, and Can Zhang. Exploring the valence-framing effect: Gain frame enhances behavioral and brain sensitivity to the failure of decision-making under uncertainty. *Int. J. Psychophysiol.*, 153:166–172, July 2020.

Matthew Hull, Leah Zhang-Kennedy, Khadija Baig, and Sonia Chiasson. Understanding individual differences: factors affecting secure computer behaviour. *Behav. Inf. Technol.*, pages 1–27, October 2021.

Ana Kovacevic, Nenad Putnik, and Oliver Toskovic. Factors related to cyber security behavior. *IEEE Access*, 8:125140–125148, 2020.

Marfua Alanazi, Mark Freeman, and Holly Tootell. Exploring the factors that influence the cybersecurity behaviors of young adults. *Comput. Human Behav.*, 136:107376, November 2022.

Abraham Maslow. *Motivation and Personality*. Harper & Row, 1954.

P. Dolan, M. Hallsworth, D. Halpern, D. King, R. Metcalfe, and I. Vlaev. Influencing behaviour: The mindspace way. *Journal of Economic Psychology*, 33(1):264–277, 2012. ISSN 0167-4870. URL https://www.sciencedirect.com/science/article/pii/S0167487011001668.

Ann C Rumble, Paul A M Van Lange, and Craig D Parks. The benefits of empathy: When empathy may sustain cooperation in social dilemmas. *Eur. J. Soc. Psychol.*, 40(5):856–866, August 2010.

Department for Science, Innovation & Technology. Cyber security breaches survey 2024, 2024. URL `https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024`.

Which? The psychology of scams: Understanding why consumers fall for appo scams, 2022. URL `https://media.product.which.co.uk/prod/files/file/gm-c66f3d70-3928-4dee-bb8b-481405be2b5e-the-psychology-of-scams-understanding-why-consumers-fall-for-app-scams.pdf`.

HornetSecurity. Urgent training gap exposed: a quarter of organisations unprepared for cyber-attacks, 2024. URL `https://www.hornetsecurity.com/en/blog/company-security-awareness-survey-2024/`.

Wanda Minnick, Tracey Cekada, Luz Marin, Majed Zreiqat, Bryan Seal, and John Mulroy. The impact of active learning strategies on retention and outcomes in safety training. *Creat. Educ.*, 13(02):526–536, 2022.

J Peter Kincaid and Ken K Westerlund. Simulation in education and training. In *Proceedings of the 2009 Winter Simulation Conference (WSC)*. IEEE, December 2009.

Rodrigo Smiderle, Sandro José Rigo, Leonardo B Marques, Jorge Arthur Peçanha de Miranda Coelho, and Patricia A Jaques. The impact of gamification on students' learning, engagement and behavior based on their personality traits. *Smart Learn. Environ.*, 7(1), December 2020.

A Lab tasks

A.1 Lab 1: Identifying HFs

What did you learn today and why is it important?
We learnt how common a technique phishing is in perpetrating cyberattacks, and facets of it, such as whaling and spear-phishing. This is important because it is necessary to understand a threat vector before it is possible to analyse and prevent it.

How does this activity link to areas you have covered in lectures?
This activity is linked to lectures that covered social engineering as a whole, and also phishing in more depth.

How has this activity changed the way you understand the underlying topic?
It has deepened my understanding of the actual threat vector itself, and the factors that contribute to its success (lack of training / greed / curiosity).

How did you feel about this activity?
It is a good starting point for investigating social engineering, and gaining insight into the causes of cyberattacks. This was particularly useful in later labs as well, as context.

What did you like about this activity? Why?
I enjoyed mapping out the steps involved in a cyberattack and reading about many different cyber-attacks, since none are ever the same, and it is interesting to break down the attack into small steps in order to gain a deeper understanding of it.

How did your group work together?
We split the task between the members of the group, in order to accurately record what we researched about the cyberattacks in depth, and reconvened to share what we'd learnt.

What did you learn about yourself by doing this activity?
There was not much opportunity for personal development during this activity, however, it did allow us to gain a good foundation for future lectures/labs, and get us comfortable with working in a group for research.

What did you learn as a group that you might not have learned alone?
It allowed us to efficiently study cyberattacks in great depth, but also share the key knowledge from those attacks, which meant we managed to cover more information in the given time, as well as disregarding any filler information.

Give an example of a challenge you had and what you did to solve it?
It was difficult to find cyberattacks that had taken place recently, since more recent cyberattacks have less information about them - but we eventually started referring to papers and news outlets for better information that search engines.

Describe a professional situation where you might need the skills/knowledge you have learned today.
It helped form a foundation for knowledge about phishing, which is incredibly useful for educating

others e.g. through training programs and how to research effectively using trustworthy sources.

1 Week 1: Identifying HFs

Company	Year	Variables	Citations
Arup	2024	Phishing and deepfake video call	Milmo 2024
UK Government	2024	Spear-phishing	Elena Courea 2024
Ofgem	2022	Phishing	McCallum 2022
Crelan	2022	Whaling (phishing)	Anon 2021
NHS	2021	Phishing	Kay 2022
Microsoft 365	2021	Phishing	Gatlan 2021
Redcar & Cleveland Council	2020	Phishing with malicious attachment	ITV 2023
Sony	2015	Phishing	Bisson 2015
Facebook & Google	2013-2015	Phishing	Romo 2019

Table 1: Examples of cyber-attacks employing social engineering techniques in the UK in the last decade

Figure 6: Table of cyberattacks from lab 1

1.1 Timeline

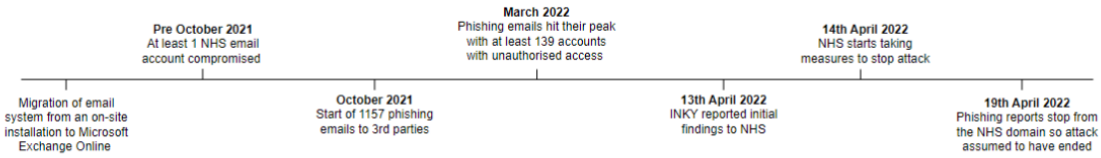


Figure 1: Timeline showing the NHS email phishing attack from 2021-2022

Figure 7: Timeline of NHS cyberattack from lab 1

Company	Events	Consequences	Causes	Human Factor Lessons	Citations
NHS	Two compromised NHS email accounts sent at least 1,157 emails mostly containing fake new document notifications from Adobe or Microsoft with a few being advanced fee scams	139 accounts were found to be compromised and these account credentials will likely be recycled in further attacks	The two initial compromised accounts were likely accessed through similar credential harvesting attacks	Check the sender's email address as many of the emails claimed to be from Adobe or Microsoft despite coming from an NHS email	Kay 2022
Redcar & Cleveland Council	Council systems were encrypted and unusable for at least three weeks due to ransomware. Systems were irrecoverable.	Staff were forced to use pen and paper for records, 135k residents couldn't use council systems for up to 8.5 months while they were rebuilt, cost about £8.7m.	"Lax" cyber security awareness training, employee downloading malicious email attachment on council laptop, no cyber insurance.	Email attachments should be treated with high suspicion unless expected and from a trusted contact, employees should be more aware of cyber security risks.	Tidy 2020, Pidd and Robinson 2020, ITV 2023, Arnold 2023, Jeraj 2022, zync. 2020
Arup	Starting with a phishing email and a deepfake video call, employees were tricked into sending a £20 million bank transfer to a criminal's account.	Large financial loss of £20 million.	Poor training and lack of awareness caused employees at Arup to believe an AI deepfake of senior employees and send a bank transfer of £20 million to the criminal's account.	Make employees aware of deepfake scams and show them what to look out for (e.g. an account from outside the company). Also implement multiple security checks before transferring money.	Guardian 2024, Realtyme 2024, CNN2024 2024

Table 2: Caption

Figure 8: Detailed report of three cyberattacks from lab 1

A.2 Lab 2: Mental Models and Warning Response Behaviour

What did you learn today and why is it important?
We learnt how users assess danger and how they will interpret warning messages - this is useful for writing constructive warnings on applications and how to accurately convey the danger level of a something.

How does this activity link to areas you have covered in lectures?
This links to lectures that covered the idea of nudging, particularly in a negative sense, and to the UX laws.

How has this activity changed the way you understand the underlying topic?
I understand the factors that play into individual's interpretation of warning messages and their perceptions of danger.

How did you feel about this activity?
It was very interesting and exciting even to dive into the psychological ideas of how humans interpret messages differently.

What did you like about this activity? Why?
We enjoyed working through the redesign and evaluation as we considered how we and others might react, and how to heighten other's responses.

How did your group work together?
We discussed together how one might improve the template, and bounced ideas off each other.

What did you learn about yourself by doing this activity?
I learnt about the way my mental model works, through how I interpreted the messages.

What did you learn as a group that you might not have learned alone?
Other examples of how messages could be interpreted and what others considered to be important factors in determining the interpretation of the message.

Give an example of a challenge you had and what you did to solve it?
Because of our lack of psychological knowledge, we struggled with deciding on the best general course of action for a warning - should it be a notification-type alert to catch the user's attention, play into the user's fear etc.? We discussed and decided fear was the best option, but in hindsight, this would likely only work in the short term.

Describe a professional situation where you might need the skills/knowledge you have learned today.
This will allow me to design warning messages that convey sufficient danger and alert users properly, with the necessary information, such as for error messages in an application.

2 Week 2: Mental Models and Warnings

2.1 Mental Models

Problem: when approached with the warning, novice users tend to assess the severity of the warning by considering the 'look' of the popups and the severity of the text. Considering all warning popups look the same whether the downloaded software contains a vulnerability or not this is not good. This is not severe when experts are confronted with this same problem however it will still help to point 'experts' to reliable sources so that they can exercise educated caution.

2.1.1 Improvements

Improvements suggested:

- Change the background colour or text to red as it is associated with danger
- fsweonhigsdrflkjnaswdrpjkovdslnjksefoijngfrsojinnawepijn – this text is good because it makes the average user think they've already been hacked and therefore are more likely to do something about the situation
- Add resources both novice and expert users could search in order to determine if the software they have downloaded is actually safe

2.1.2 Notes

Novice users tend to consider the look and message of the warning before deciding how they feel about it red associated with danger so if not already used make more red

Look at maybe adding good links to easy documentation that helps explain what could be going on

If novice users can't find what the problem is, they either assume there's no problem and carry on or find a different way to do what they want to

—

Novice users seem a lot less cautious, and are more likely to run a program if they do not understand it.

Make warning text clear

Add error code / warning code (something to make it easy to search about)

Add a risk number (how important the warning is) – they will ignore anything other than 5

About 50% of the time novice users end up running the software anyway

Figure 9: Notes on discussion of template redesign from lab 2

A.3 Lab 3: Interaction Design

What did you learn today and why is it important?
I learnt to critically evaluate the usability of a system, and to identify shortcomings, but also useful features.

How does this activity link to areas you have covered in lectures?
This links back to UI design and UX, and increasing the usability, and intuitiveness of a system.

How has this activity changed the way you understand the underlying topic?
I learnt about some factors that I wouldn't have otherwise considered by myself, and just how important some of those things are.

How did you feel about this activity?
I enjoyed this activity.

What did you like about this activity? Why?
It was fun to consider since it involved evaluating a device that plays a fundamental role in everyone's day to day life.

How did your group work together?
We bounced ideas off each other, and did preliminary research into what parts of mobile phone operating systems serve to increase your engagement with the device, then shared that information with each other.

What did you learn about yourself by doing this activity?
It allowed me to reflect on all the things that cause me to spend time beyond necessary actions on my mobile phone, and has since allowed me to reduce the amount of time I am spending on it.

What did you learn as a group that you might not have learned alone?
We were able to do more research than we would've managed individually, and come up with more ideas.

Give an example of a challenge you had and what you did to solve it?
We struggled to consider how to improve such a system, since a lot of UX laws and psychological tricks to keep attention were already complied with, but ended up managing to think of some generic suggestions in the end, that involve less common actions, that are still required.

Describe a professional situation where you might need the skills/knowledge you have learned today.
It may be necessary to evaluate the usability of an application and how to increase users focus on it in order to maximise engagement. This could be in a professional setting e.g. for training, or for software development.

3 Week 3: Interaction design

3.1 good and bad about the way the device works

good:

- physical buttons - intuitive, two for volume next to each other
- color coding - power button and volume buttons are different colours and sizes
- touchscreen - easy and intuitive to use
- symbols - pretty universal
- icons - colourful, big, obvious
- home screen layout - can be personalised to suit the user and easy-access location for most used apps
- Search - search for apps
- control centre - central hub for other functions e.g. torch, volume, brightness etc
- notification centre - to display all notifications
- how notifications displayed - banners make it hard to miss, sounds
- status indicators - easy to check battery, WiFi, bluetooth etc.
- lock screen - key information and notifications available without unlocking phone for quick view
- SD/SIM slot - easy to understand and use with new phones coming with removal tool
- Fingerprint Scanner - easy to log in for users, in an ergonomic position
- Facial Recognition - no effort to log in while still providing good security

bad:

- power and volume buttons are on either side of the phone but level with each other so I'm constantly taking screenshots when trying to turn down the volume.
- no headphone jack
- ability to take screenshots
- hard to figure out how to restart
- randomly has slow moments, even if it is not being overwhelmed

3.2 description of the user experience resulting from interacting with it

Often the only problems are with varying designs between phones meaning when someone buys a new one they have to relearn any physical shortcuts with buttons. Also rivalry OS's and their abilities.

3.3 Compile a set of usability and user experience goals. Decide which are the most important ones and explain why

- easy to navigate - standard expectation between models and differing OS's.
- Comfortable to hold - keep sizing of hardware to be hand-sized.
- easy to use buttons - easy to use buttons to perform specific actions, should be easy to reach while holding

Figure 10: Notes from discussion of mobile device interaction from lab 3

3.4 Translate each of your sets of usability and user experience goals into two or three specific questions. Then use them to assess how well your device fares

- Is the device easy to navigate? Yes
- Is the device comfortable to hold? Depends on model
- Is the device usable without being frustrating? Overall yes but features/moments that are annoying. For example slow loading times and lack of features.

3.5 Repeat (c) and (d) but this time using the design principles outlined in the lecture

3.5.1 Compile a set of usability and user experience goals

- Visibility: users should be able to find different functions they require easily
- Feedback: the phone should provide instant feedback, for example opening apps as soon as they are selected
- Constrains: the phone should minimise the margin for human error
- Mapping: apps should be easy to find
- Consistency: the phone should have a consistent layout, where all apps function similarly with the same sized icons/buttons and should also look consistent, e.g. font size
- Affordances: Users should be able to identify how the phone should be used easily

3.5.2 Translate each of your sets of usability and user experience goals into two or three specific questions. Then use them to assess how well your device fares

- Visibility: Can a user find the different functions they require easily?
- Feedback: Does the phone provide instant reactions (e.g. does it open an app as soon as it is selected?)?
- Constrains: Does the phone allow a user to make mistakes easily?
- Mapping: Can a user find apps easily? Does the layout of the apps make sense?
- Consistency: Is the interface consistent in the design?
- Affordances: Can a user easily identify how the phone should operate and how to use certain functions?

3.6 propose improvements to the interface based on the answers obtained for (d) and (e)

Improvements:

- make buttons clearer (e.g. to restart phone)
- have a different method of taking screenshots (separate button or swipe action)
- improve processing speed

Figure 11: Notes from discussion of mobile device interaction from lab 3 (continued)

A.4 Lab 4: Human Processor Model

What did you learn today and why is it important?
We learnt to predict how users will choose to interact with a system according to the Human Pro-

cessor Model.

How does this activity link to areas you have covered in lectures?
This, again, links to lectures on UX design and nudging.

How has this activity changed the way you understand the underlying topic?
Now that I have practiced, I feel comfortable with assessing how a user will interact with a system, despite being the one developing it.

How did you feel about this activity?
I struggled with the concept initially, but once I got a grasp on it, it was very interesting.

What did you like about this activity? Why?
The breakdown of interaction into perception, processing, and retrieval was very interesting, including the parallels of AI and human processing to a red stop light. This demo and real-world application really helped me to understand the idea.

How did your group work together?
We worked together to share ideas with one another, and to collectively expand our knowledge. We then collaboratively wrote up our work.

What did you learn about yourself by doing this activity?
I learnt about how short and long-term memory functions, and how I might "trick" myself into storing certain things in certain places.

What did you learn as a group that you might not have learned alone?
We discussed ideas in-depth and it allowed us to build a comprehensive idea of the concept and answers to the questions, that one person could not do alone.

Give an example of a challenge you had and what you did to solve it?
We struggled with the amount of content in the lab, and formulating and collecting ideas in the time we had. We decided to focus on the preliminary parts of the lab to be written up, and instead verbally discussed the later sections, before writing them up in brief outside of the lab.

Describe a professional situation where you might need the skills/knowledge you have learned today.
When developing software, it is necessary to consider user stories: the sequence of actions a user may perform to achieve an end goal. By predicting how a user will interact with a system, it is possible to consider the main user stories at a very accurate level.

4 Week 4: Human Processor Model

4.1 Main Elements

The purpose of the model is to help designers predict how users will interact with a system, this is done by drawing parallels between how humans perceive and remember information. The model is broken down into three interactive systems all having their own memory.
The perceptual processor, simulating the senses, focuses on the inputs from audio and visual sources storing them in the appropriate storage.
The cognitive Processor, is a substitute for the brain, it creates an output into working memory. This memory access includes both short and long term storage, this comes with all the features of memory types.
The third and final is the motor processor, this is what carries out actions. Translating the rest of the body to being the output aspects of a computer system.

4.2 How the model can be used to show time taken to perform an elementary task

When taking the example of processing a visual stimulus, the model can showcase the time taken. This is done through initially breaking it down into the three processors, the eye movement in the perceptual process showcases a time delay in the user finding the elements needed to be interacted with. Then the cognitive process running in parallel recognising if the current focus of the peripherals is the correct match, this includes retrieving information from long-term memory and then storing recently processed stimulus in the working memory (RAM equivalent). From this once a match has been established then the motor processor will make the appropriate action output.

4.3 AI car example breakdown

As soon as the light turns red then the visual processing of the driver will need to find and recognise that there has been a change in colour. This is the main job of the perceptual processor in the model this change is then passed along to the cognitive processor, this is done by storing the fact that the light changed to red in the visual image store (VIS) of the working memory. Where long term memory is accessed to recall the meaning behind the change of colour for the light, the colour changed to is gained from the VIS. The motor processor then makes the appropriate call to action with the rest of the body to take control of the vehicle. Over all this will take at least 310 ms for the reaction to be completed.

With the assumption that together the reaction time and time taken to move hands to the steering wheel with pedals being pressed takes 2 seconds. In this time the car has moved 40 metres meaning that at that point where the breaks are engaged the car will take 50 meters to stop. This takes up 90 of the possible 100 before collision. In this case then the car would be safe but only just, if other factors that effect reaction speed for example tiredness then the same can not be said.

Figure 12: Discussion on questions regarding the HPM from lab 4

A.5 Lab 7: CyberSafe

What did you learn today and why is it important?
We practiced applying techniques we had learnt to create a comprehensive, engaging cybersecurity awareness course.

How does this activity link to areas you have covered in lectures?
I would go as far as to say this links to practically every other lab and lecture, to some extent. There is particular focus on UX, social engineering, nudging, and human processor model.

How has this activity changed the way you understand the underlying topic?
A strong method of applying what we've learnt into one place, and for understanding the work that

goes into the creation of a course like this.

How did you feel about this activity?
It used the contents of previous labs very well, but did not cover any new content unfortunately.

What did you like about this activity? Why?
I enjoyed putting the ideas we'd learnt into practice, for something that will have real consequence.

How did your group work together?
We discussed the activity, split into several smaller groups, and completed individual sections. Other groups reviewed these sections afterward.

What did you learn about yourself by doing this activity?
I learnt how to communicate cybersecurity concepts effectively in a way that the average person could understand.

What did you learn as a group that you might not have learned alone?
It helped us identify weaknesses with our work, and also bounce our ideas off each other to check they were suitable and appropriate.

Give an example of a challenge you had and what you did to solve it?
Making the course engaging was difficult, with the lack of resources Moodle provides. However, we ended up gamifying the course, and provided clear links to interactive elements such as password strength checkers, and phishing simulations.

Describe a professional situation where you might need the skills/knowledge you have learned today.
Useful in a management scenario, where it is necessary to train others about cybersecurity.

7 CyberSafe

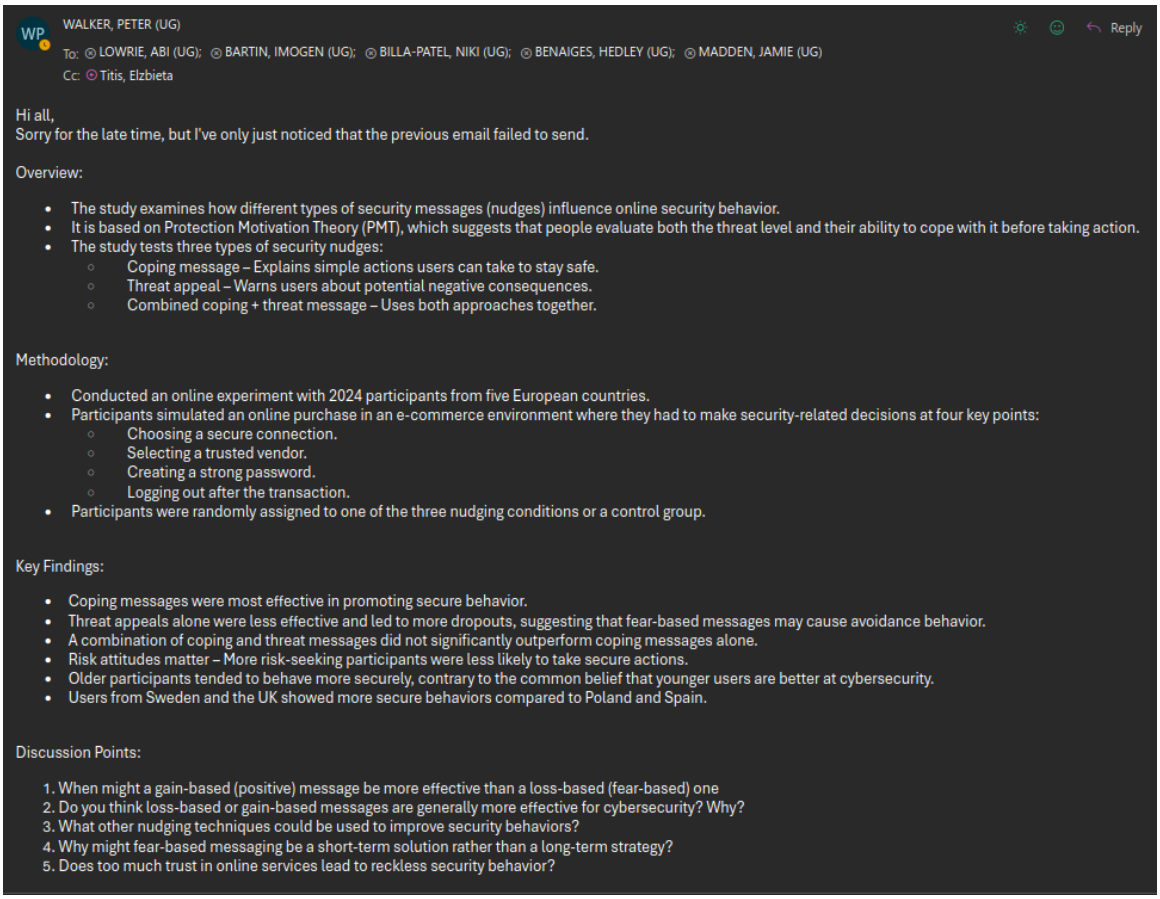
7.1 FeedBack

- Incentive of vouchers so good

- Does not mention password reuse anywhere (VERY IMPORTANT)
- In the password example, it swaps e-¿3, a-¿4, o-¿0, i-¿1, which are very common techniques that hackers will know, and thus not good practice
- The strong password example 'Sw33tBlueW!ne' has a strength of 'medium' and takes about 33 hours to crack according to 'password monster', which is not good for a secure example. To improve, suggest a 4 word phrase instead of 3.
- A link to interactive sites, like 'password monster' so users can estimate password strength would be good
- Visually Uninteresting
- Long title sections
- A lot of words on, too much for mobile - not engaging - not concise - exceeded word count, grade capped at a pass - 4 paragraph intro
- A lot of repetition - makes it boring to read
- Grammatical errors
- There is no explanation of consequences (distinct lack of scaremongering)
- Add a summary at each stage
- No images have a description of the images
- People should earn badges to gameify the process (keep people interested)
- Language used is vague e.g. 'Encrypt your computer/laptop' – – either explain specifically, or link to a tutorial
- VIDEOS to engage the user
- Staff taking all the credit, students not on 'meet the team'
- Different learning paths

Figure 13: Notes for CyberSafe implementation from lab 7

B Discussion Plan



WALKER, PETER (UG)

Reply

To: LOWRIE, ABI (UG); BARTIN, IMOGEN (UG); BILLA-PATEL, NIKI (UG); BENAIGES, HEDLEY (UG); MADDEN, JAMIE (UG)

Cc: Titis, Elzbieta

Hi all,
Sorry for the late time, but I've only just noticed that the previous email failed to send.

Overview:

- The study examines how different types of security messages (nudges) influence online security behavior.
- It is based on Protection Motivation Theory (PMT), which suggests that people evaluate both the threat level and their ability to cope with it before taking action.
- The study tests three types of security nudges:
  - Coping message – Explains simple actions users can take to stay safe.
  - Threat appeal – Warns users about potential negative consequences.
  - Combined coping + threat message – Uses both approaches together.

Methodology:

- Conducted an online experiment with 2024 participants from five European countries.
- Participants simulated an online purchase in an e-commerce environment where they had to make security-related decisions at four key points:
  - Choosing a secure connection.
  - Selecting a trusted vendor.
  - Creating a strong password.
  - Logging out after the transaction.
- Participants were randomly assigned to one of the three nudging conditions or a control group.

Key Findings:

- Coping messages were most effective in promoting secure behavior.
- Threat appeals alone were less effective and led to more dropouts, suggesting that fear-based messages may cause avoidance behavior.
- A combination of coping and threat messages did not significantly outperform coping messages alone.
- Risk attitudes matter – More risk-seeking participants were less likely to take secure actions.
- Older participants tended to behave more securely, contrary to the common belief that younger users are better at cybersecurity.
- Users from Sweden and the UK showed more secure behaviors compared to Poland and Spain.

Discussion Points:

1. When might a gain-based (positive) message be more effective than a loss-based (fear-based) one
2. Do you think loss-based or gain-based messages are generally more effective for cybersecurity? Why?
3. What other nudging techniques could be used to improve security behaviors?
4. Why might fear-based messaging be a short-term solution rather than a long-term strategy?
5. Does too much trust in online services lead to reckless security behavior?

Figure 14: Discussion Plan Email