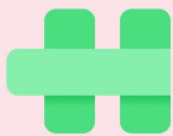


Utilizing user centered design to mitigate security threats

Emmy Edfors and Albin Sverreson

DEPARTMENT OF DESIGN SCIENCES
FACULTY OF ENGINEERING LTH | LUND UNIVERSITY
2022

MASTER THESIS



Homepal



Utilizing user centered design to mitigate security threats

Emmy Edfors
em4146ed-s@student.lu.se

Albin Sverreson
al5826sv-s@student.lu.se

October 3, 2022

Master's thesis work carried out at Homepal AB.

Supervisor: Günter Alce, gunter.alce@design.lth.se

Examiner: Joakim Eriksson, joakim.eriksson@design.lth.se

Utilizing user centered design to mitigate security threats

Copyright ©2022 Albin Sverreson, Emmy Edfors

Published by

Department Design Sciences
Faculty of Engineering LTH, Lund University
P.O Box 118, SE-221 00 Lund, Sweden

Subject: Interaction Design MAMM01
Division: Ergonomics and Aerosol Technology
Supervisor: Günter Alce
Examiner: Joakim Eriksson

Abstract

As technology advances and is more and more intertwined with our everyday lives, the security of these systems becomes very important. Abraham Maslow famously put safety needs as the second level of his hierarchy of needs, its importance second only to physical needs such as air, food and sleep[33]. To make sure technological systems are as safe as possible there exists threat modeling frameworks and processes. These are made to find possible threats and make sure they are mitigated to a wanted extent. The mitigations realized during these processes often involve code related and cryptographical solutions as they are carried out by software development teams. However, some threats stem from human error and can be hard or impossible to develop code based solutions to. An example of this, which is discussed in this thesis, is the threat of phishing where an adversary tricks a user into performing some harmful action.

This thesis aims to explore the possibility to use design and user centered design process to mitigate threats found in one of these threat modeling processes. A threat modeling process was performed on the Homepal data platform and a threat was chosen with possible design related mitigations to focus on. A literature study was conducted to find mitigation alternatives and a survey was made to investigate the user base's opinions on them. After the requirements were set, lo-fi alternatives were then created and evaluated and the results turned into hi-fi prototypes. The hi-fi prototypes were then subject to a more extensive evaluation, resulting in one poster being recommended as well as several guidelines for how to effectively convey security tips on posters.

Keywords: Educational reminders, Posters, Phishing, Security Education, STRIDE, Threat Modeling, User Centered Design

Sammanfattning

I takt med att teknologin blir en större och större del av vårt vardagsliv ökar även vikten av att säkerställa att dessa system har en hög säkerhet. Säkerheten blir en större del av vår vardag och har alltid varit viktigt för människan. Abraham Maslows placerade säkerhet på andra steget i hans hierarki av behov för en människa, precis under fysiska nödvändigheter som luft att andas, mat att äta och sömn. För att säkerställa att teknologiska system är så säkra som möjligt används olika modeller för att hitta, analysera och hitta lösningar för att mildra potentiella säkerhetsshot. De lösningar som hittas innefattar ofta kodbaserade eller kryptografiska lösningar då säkerhetsshoten ofta är kopplade till själva utvecklandet av produkten. Dock är det viktigt att poängtera att det ibland inte går att koppla en lösning till kod eller kryptografi, utan att säkerhetsshot ibland har en relation till mänskliga utförda fel. Ett exempel på detta är phishing, ett hot som diskuteras i detta examensarbete, där användaren luras att utföra en skadlig handling.

Detta examensarbete utforskar möjligheterna att använda design och en användarcentrerad process för att mildra konsekvenserna av funna säkerhetsshot efter genomförandet av en säkerhetsanalys. Säkerhetsanalysen gjordes på Homepals dataplattform och ett av säkerhetsshoten valdes att fokusera på, då detta visade potential att kunna ha designrelaterade åtgärder. Även en litteraturstudie genomfördes för att hitta alternativ på åtgärder, samt två enkäter skickades ut för att förstå användarnas åsikter gällande dessa alternativa åtgärder. Efter att kraven på produkten var satta skapades en lågnivåprototyp, som sedan utvärderades och itererades till en högnivåprototyp. Högnivåprototypen genomgick sedan en omfattande utvärdering som resulterade i att en affisch rekommenderades som en potentiell lösning på åtgärder för säkerhetsshotet, samt några riktlinjer kring hur man effektivt kan förmedla säkerhetstips genom att använda affischer.

Nyckelord: Affischer, Användarcentrerad design, STRIDE, Phishing, Säkerhetsutbildning, Säkerhetsshotsanalys, Utbildningspåminnelser

Acknowledgements

Firstly, we would like to thank all the people who have provided us with valuable input throughout the thesis - without you this thesis would not have been possible. An especially big thank you to our supervisors, Daniel Åhlin at Homepal AB and Günter Alce at Design sciences at LTH who has followed us closely in every bit of the thesis. Not to forget, thank you to all test participants and survey responders, without you it would be impossible to complete this user centered design thesis.

A big thank you is also directed to Homepal AB for letting us spend our time at your company. Thanks for bringing us in, believing in us and providing us with many fun and inspiring moments.

Emmy Edfors, Albin Sverresson

Lund, September 2022

Contents

1	Background	4
1.1	Background	4
1.2	Purpose and goals	5
1.3	Homepal AB	6
1.3.1	Homepal's platform	6
1.4	Scope and limitations	6
1.5	Global goals	7
1.6	Related work	7
2	Theoretical background	8
2.1	Interaction design	8
2.1.1	User centered design	9
2.1.2	Brainstorming	9
2.1.3	Prototyping	10
2.1.4	Usability evaluation strategies	10
2.1.5	Test plan	14
2.2	Security: Threat modeling	15
2.2.1	STRIDE	15
3	Identify requirements	17
3.1	Security awareness	18
3.1.1	Slips and mistakes	18
3.1.2	Tools for security awareness	18
3.1.3	Security awareness and design	20
3.2	Applying STRIDE	21
3.2.1	STRIDE and user awareness	23
3.2.2	STRIDE analysis conclusion	23
3.3	Public user survey	24
3.3.1	Initial part	24
3.3.2	Security on-boarding part	24

3.3.3	Poster part	25
3.4	User base survey	28
3.5	Main takeaways	28
4	Create alternatives	30
4.1	Lo-fi prototype	31
4.2	Evaluation	34
4.3	Main takeaways	35
5	Produce prototypes	36
5.1	Graphical profile	37
5.1.1	Text elements	37
5.1.2	Graphical elements	37
5.2	Poster information	37
5.3	Hi-fi prototype	39
6	Usability evaluation	42
6.1	Test plan	43
6.2	Pilot test	48
6.3	Test results	48
6.3.1	SUS-evaluation	49
6.3.2	General observations	51
6.3.3	Main takeaways	52
7	Discussion	53
7.1	The design phases	53
7.1.1	Identify requirements	53
7.1.2	Create alternatives	54
7.1.3	Produce prototypes	54
7.1.4	Evaluation	55
7.2	Research questions	56
7.3	Future work	57
8	Conclusion	58
Appendix A		64
A.1	Public survey	64
A.2	Usability evaluation	71
A.2.1	Form of consent	71
A.2.2	Manuscript	72
A.2.3	Pre-test survey	73
A.2.4	SUS-survey	74
Appendix B Prototypes		76
B.1	Lo-fi	77
B.2	Hi-fi	82

Chapter 1

Background

1.1 Background

This chapter aims to give a general background of the thesis and presents its purposes and goals as well as its scope. Further, a background is given on Homepal and their data platform. Lastly some related works are presented.

Interactive technology in our every day life is increasing by the minute. The burst in technology causes a chain reaction for multiple connected factors to increase in magnitude, an example being an increased complexity of the products produced. As the complexity rises, so does the demands on the user to increase their knowledge, as well as the demands on the producer of the product to ensure a maintained usability in an evolving product. A user centered design process is a core element in ensuring usability and a decrease of frustration for the user [41].

Another factor that increases in magnitude with advancing technology is the importance of security. Abraham Maslow famously put safety needs as the second level of his hierarchy of needs, its importance second only to physical needs such as air, food and sleep. To make sure technological systems are as safe as possible there exists threat modeling frameworks and processes made to find possible threats and make sure they are mitigated to a wanted extent. The mitigations realized during these processes often involve code related and cryptographic solutions as they are carried out by software development teams. However, some stem from human error and can be hard or impossible to develop code based solutions to. The users role in the security process is crucial to ensure a secure system, were both the data and the user is safe from threats. In 1994 Jakob Nielsen defined a set of usability heuristics regarding how to evaluate and think while designing a usable product, and while 1994 is a long time ago these theorems are still applicable to this day. One of the heuristics were to ensure that the product helps the users to recognize, diagnose and recover from errors [37], a subject that this thesis wanted to explore in combination with security awareness.

Thus, as the technology advances so does the curiosity for the relationship between se-

curity, design and the user. This thesis explores the possibilities of this relationship, more specifically if the use of a user centered design process in combination with increased user security awareness could achieve a proactive security position for the user, and whether this would increase the security for a system.

1.2 Purpose and goals

This thesis aims to investigate how design and user experience could be used to mitigate security threats.

For a young company such as Homepal, dealing with such sensitive data that housing companies generate, it is very important to work towards as secure a platform as possible. Because of this we would like to investigate the possibility of using design and user experience to increase the security for the user of the system. Below are the research goals and questions we established.

Goals:

- Get a theoretical background of known security threats to similar platforms such as Homepal's
- Get a theoretical background of design concepts that could be used in order to mitigate the threats found.
- Evaluate Homepal's platform in relation to the concepts found. The scope of the evaluation could be broadened to e.g. Homepal's website if time allows.
- Test possible improvements on users, preferably Homepal's customers.
- Conclude some tangible suggestions in visual and written form for Homepal on how to move forward in the work with increasing the safety of their system.

Research questions:

- Which security threats are most prominent for a platform such as Homepal's?
- Which design concepts exist that could help in mitigating the threats?
- How are these design concepts best utilized to achieve a more secure system/platform/product?

1.3 Homepal AB

Homepal's main platform and business model is data aggregation for housing companies. The problem that they have identified is that a lot of housing companies is struggling with handling and utilizing their data, especially since as a lot of their data comes from legacy systems, physical sources and local files [21]. The view that housing companies struggle with data handling and utilization is supported by a report on digitalization by the Swedish Agency for Economic and Regional Growth where housing companies is ranked as one of the worst industries in terms of digitalization [47].

1.3.1 Homepal's platform

The Homepal platform is built to collect data from systems, databases and file and then rearranged and remodeled to fit modern systems in a better way. The data can for example be forwarded to storage in modern databases, used in analytic tools by the customers or utilized in one of Homepal's own apps. The platform and apps are run on AWS, letting companies start using the platform without having to invest in hardware.

Homepal then provides products that allows the user to use the gathered and modeled data in different ways. At the time when this thesis was written, the developed product was *Explore*. *Explore* is a property search engine, made for housing companies to easily find all the information about a property by searching for any piece of information linked to that property. This is in contrast to manually having to search through multiple legacy systems and/or local files in order to find what you're looking for. They also have products that allows the user to set up API's and reports based on the processed data. [21].

1.4 Scope and limitations

In relation to the purpose and goals, as well as time and resource factors, a scope and limitations for the thesis was formed.

Most importantly the scope for the thesis was limited to looking into how the users knowledge of security could be improved and not on the security factors surrounding how the product was developed and maintained. This choice was a crucial decision in order to limit the scope of the security analysis and resulted in a high-level, design and end-user focused, point of view throughout the analysis.

Another important limitation of this thesis is the fact that Homepal is a relatively new company, with an ever changing platform with new features and apps, and it is therefore important to point out that this thesis has focused on the system version available at the time.

1.5 Global goals

In 2015 a set of global goals was set by 193 world leaders for the year 2030, with the purpose of aiming political focus on 17 different areas of interest. The goals purposes stretch from ending poverty and hunger to encourage and support innovation and economic growth. All 17 goals, with corresponding information about sub targets, can be found in [45].

The goals that were found to be contributed by this master thesis were *Goal 4: Quality education* [16] and *Goal 9: Industry, innovation and infrastructure* [17]. As technology innovation is an ever growing part of our every day life the need for easily accessible education is and will be a crucial part of eliminating discriminational grounds in order to take part of the technology based society. Thus, these goals are the most relevant to this thesis as it aims to increase the knowledge for the users of the ever growing technology innovation, here especially within IT security, and make education easily accessible for the users.

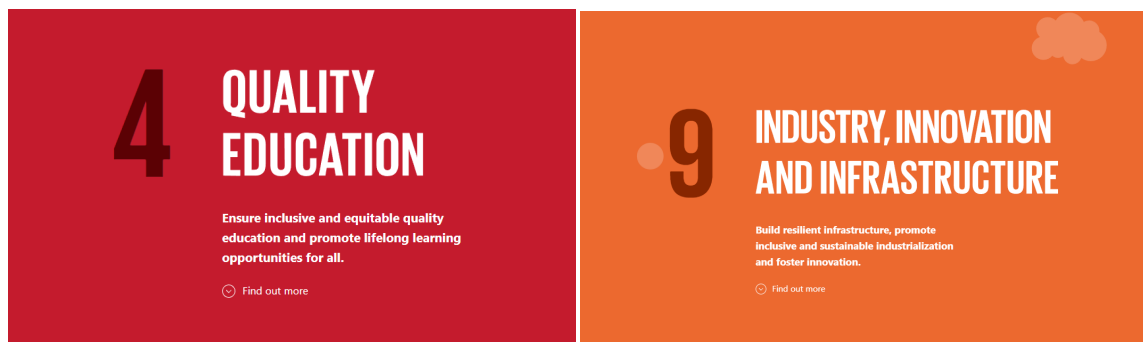


Figure 1.1: The two global goals [16] [17] found to be contributed to by this thesis.

1.6 Related work

Dhamija et al. [10] explored which strategies work when spoofing a website. While it was published in 2006 it is still relevant and the paper as a whole has contributed with inspiration and ideas throughout this thesis. The paper only investigates what makes attacks work and not which mitigations that work but it gives a good background to the subject of phishing as a whole and some good insight into the minds of the victims.

In the case of user security awareness Leach [28] points out the importance of motivate the user to take the right decisions and understand their importance in the security chain. This in combination with findings by Eminağaoğlu et al. [13] as well as Ilic and Rowe [23], and real life examples such as Folkhälsomyndighetens Covid-19 posters [14], created a spark of curiosity to explore the subject and use posters for security awareness purposes. The papers brings up some dos and don'ts in the security awareness and poster production and has been a great contribution towards this thesis.

Chapter 2

Theoretical background

This chapter aims to give the reader a theoretical background to different subjects that is brought up in this the master thesis. The chapter will start with interaction design and its corresponding theory, with user centered design and usability evaluation strategies in focus. It will then move on theory related to security threat modeling and give a deeper explanation of the STRIDE model.

2.1 Interaction design

The interaction design process is an iterative process that learns from previous iterations, through evaluation and user involvement, with the goal to produce a usable product. The different phases of the interaction design cycle, seen in figure 2.1, could be seen as different stages of a process. Though, due to the fact that it is an iterative process it is not quite that simple as a

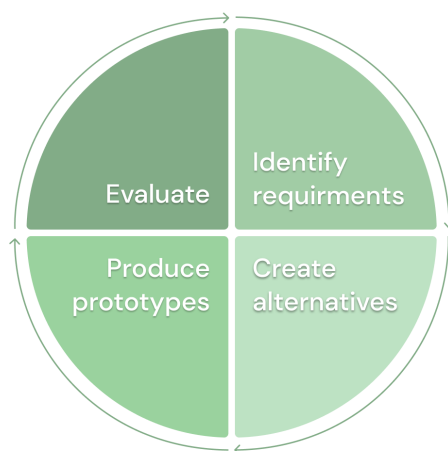


Figure 2.1: The iterative interaction design process.

step-by-step process, the phases are often intertwined with each other because of its iterative nature and contributes to each other. The stages use each other to work forward in the iterative cycle, whereas evaluation should be seen as a crucial part used throughout the whole process [41].

The difficulty with this loop is, like any other loop, is to find a point where the result is good enough to stop the iteration. In order to find this point there is a couple of possible evaluation strategies available, some of which will

be presented below together with some evaluation strategies to use throughout the process. Prior to this, in order to understand the syllabus surrounding interaction design and why the user is such a central part of the process, the user centered design process will be presented.

2.1.1 User centered design

User centered design (UCD) is the focal point in the interaction design process. The aim of UCD is to understand the needs and demands of the real users, that is those who will use the product after release. User centered design emphasises to incorporate the users early on in the process, as well as take in user feedback throughout the process that contribute to the iterative process [41].

User experience

User experience (UX) is nowadays one of the biggest buzzwords in the design industry, and perhaps one of the most commonly used expressions to describe the user centered design process. Of course, user experience is a crucial part of user centered design, otherwise it would not attract such attention. User experience is, as the name implies, how the user experiences the use of a product, e.g. how they use it and how pleased they are of the end result. It could be seen as an emotional and describing statement from the user that analyses not only the product, but the impression of the whole environment surrounding the use of the product [41].

Usability

In order to express the user experience into requirements for designing one could turn to the definition for usability. The definition for usability is standardized in ISO 9241-11 as

Extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use [25].

To translate the definition into practise, it is often turned into goals that can be used as questions that the designer could ask themselves throughout the whole design process to challenge and evaluate the products usability. The goals can be viewed in figure 2.2, some of which can seem a bit confusing and of a broader nature. Regardless, they could be used to bring perspective when aiming to understand the users' experience. Thus, the goals works as an inspiration to challenge the designers perspective in the user centered design cycle and could be a use full approach to try to make sure that the product is *usable* for the end user [41].

2.1.2 Brainstorming

With the usability goals and the user experience in mind, a good design process often contains one or more brainstorming sessions. The main point of brainstorming is to collect ideas and concepts that can be used in the design. During the brainstorm it is important to keep an

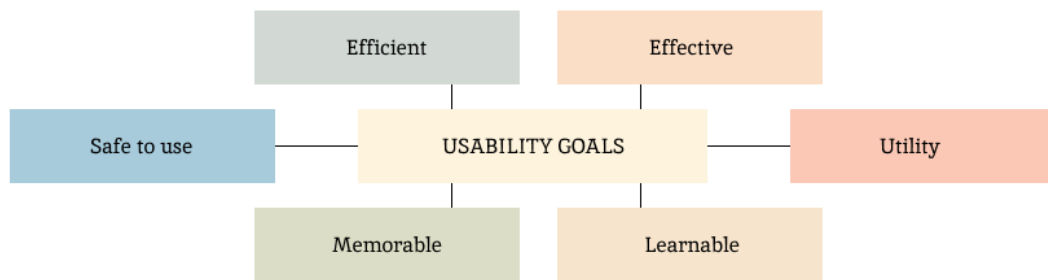


Figure 2.2: The usability goals.

open mind and encourage all the participants to share their thoughts and ideas and later on boil it down to a few concepts. This technique could be used in multiple stages of the process to increase and broaden the design and hopefully results in finding more user requirements to use in the design process[32].

2.1.3 Prototyping

In order to meet the requirements found, or to use the ideas produced in a brainstorm or another idea generating activity, designers often turn to prototyping to realise their concepts. The prototypes could have different levels of complexity, from simple sketches to real software. This step is often used before moving on to the real development of the product, to test a concept's liability and usability without risking failure in production [41].

Low fidelity prototype

A low fidelity (lo-fi) prototype is often created as sketches or simple interactive paper prototypes that shows the design concepts in a very simple way. It could be used to explain or illustrate where the current thought process is, and is an effective way to easily compare different alternatives without having to put a lot of effort and work into it[41].

High fidelity prototype

A high fidelity (hi-fi) prototype is a higher level design prototype, often produced in a digital environment. It is a more detailed and realistic prototype, used to mock up the real end product and enables more complex testing on real end users in the thought user environment. This implies that there is a lot of elements that needs to be produced in the prototype, for example the design, colour decisions etc, and does not only focus on the functionality of the product, as lo-fi, but rather the whole user experience [41].

2.1.4 Usability evaluation strategies

As mentioned in section 2.1, there is a need to know when the product is good enough to stop the iteration and move on to release. This, in relation to user centered design, is a process that needs to be conducted throughout the whole design cycle with different evaluation methods

to ensure the users involvement at all stages, as well as a way of moving forward in the process cycle. The evaluation strategies are sometimes time or process stage dependent, but that does not mean that the chosen evaluation method can not contribute later on in the cycle. For example, early and mid process evaluation activities could potentially work as a reflection points for the later stages of evaluation [41]. Below some different evaluation methods that has been relevant for this master thesis are presented.

Interview

Interviews is an evaluation method that can be used throughout the whole design process to explore a specific topic. The structure of the interview is based on a spectrum of level of control, stretched from an open discussion of a non structured interview to structured interviewed with short and concise questions. A non structured interview aims to develop deeper and broaden understanding of the subject and the users relation to it, and could be used to find new perspective in the process with qualitative data. Structured interviews on the other hand, as mentioned before, has a more concise approach to questioning. It is often used in combination with predetermined answer alternatives to choose from and aims to collect quantitative data surrounding specific subjects. Both has its advantages, and therefore it is often profitable to find a middle ground in using semi structured interviews. Semi structured interviews uses structured questions in combination with more open minded questions to both achieve quantitative data collection in a specific subject, as well as gaining a more deep understanding with qualitative directed discussions. A common approach is to use a concise question with a follow-up question connected to the same subject that can be used if needed to guide the user towards a deeper answer. Though, it is important to keep in mind not to form the questions with an obvious answer, but to analyse each question in relation to the purpose of the interview with an objective mind[41].

Survey

Surveys are another way of evaluating the users thoughts and feelings at a point in the design process. The structure is quite similar to interviews and should, as interviews, therefore be practised in the structure that fits the particular situation. How the questions are formulated and the orders of the questions depends on the purpose of the survey and could follow the structured, semi structured or non structured approach presented in *Interviews*. Surveys often has a structure of starting with demographic questions, or other questions that can be used to divide the users in to group that can contribute to an easier analyse the data in a later stage. The division could also mean that there is a need for using different surveys on different groups depending on the purpose of the survey [41].

As mentioned in *Interviews*, it is important to analyse the questions in regard to what data is meant to come from the answers. To keep frustration and question marks out of the game, it is also important to introduce and explain the process of how and why the survey is being conducted. This also contributes to ensure that the user understands the relevance for them, especially in order to keep the motivation up to complete the survey [41].

Usability Heuristics

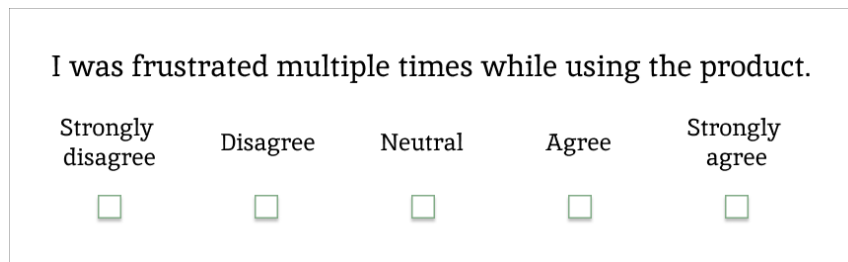
Usability Heuristics were introduced in 1994 by Jakob Nielsen, who defined a set of directives on how to find usability problems while analysing a product. As mentioned in section 2.1.1 *Usability*, the definition for Usability rises from the goals seen in figure 2.2, but Nielsen gave a more definite suggestions that has been used in multiple different contexts throughout the years [37]. The directives are often mentioned as heuristics and consist of, as defined in [37]:

1. **Visibility of system status:** Give the user uncomplicated and direct feedback throughout the interface. This to bring awareness to where the user is located in the process, as well as works as an indicator of the consequences of an interaction.
2. **Match between system and the real world:** Design the system to fit the users cultural background, such as their language and known concepts within the community.
3. **User control and freedom:** Create ways for the user to undo or exit an action and make sure that it is easy accessible actions.
4. **Consistency and standards:** Use norms and user expectations from similar products to decrease the cognitive burden on the user as well as decrease the time needed to learn the ways of the product.
5. **Error prevention:** Ensure that the product is designed for slips or mistakes, e.g. that it contains multiple steps of confirmation and/or warnings when interacting with crucial parts of the system.
6. **Recognition rather than recall:** Design the interface to visibly remind and inform the user of previous steps as the process moves forward to reduce the need for recalling.
7. **Flexibility and efficiency of use:** Use multiple different ways to reach the same action goal, to ensure that there is a way that fits multiple different users.
8. **Aesthetic and minimalist design:** Keep information and elements that are relevant in focus, do not clutter the interface with unnecessary components.
9. **Help users recognize, diagnose, and recover from errors:** Emphasize and explain the errors that arises, preferably in relation with an explanation of how to solve it.
10. **Help and documentation:** Have understandable, simple and easy accessible instructions to use if necessary.

These 10 heuristics are still applicable to this day, and is one way to evaluate usability in a product. Even though, the context of the application could complicate the level of applicability, a fact that has expanded the heuristics to multiple different side approaches. In some context there is a need for a combinational approach to the evaluation due to the complexity of the system structure. An example of this could be found in [26], where it is recommended to use the heuristics together with their combinational approach based on the heuristics as well as activity theory, a theory that emphasises to use the contextual course of action, in order to ensure a broad analyse of IT security management tools.

System Usability Scale

System Usability Scale (SUS) is one of the most commonly used evaluation strategies in the industry to determine the usability of a product. SUS is based on the Likert scale, where the user needs to consider multiple statements and their stand point in relation to the statement based on a 1-5 scale [8, 41, 42]. An example of a Likert scale can be viewed in figure 2.3, where the scale of 1-5 is translated to how applicable the statement is on the user's experience.



I was frustrated multiple times while using the product.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 2.3: An example of using a Likert scale.

The most common approach to use SUS is to use 10 Likert statements divided into five positive and five negative statements about the subject. [27, 31]. The order of the statements needs to follow a particular order in order to work as intended while calculating the SUS score. The statements are, according to [8]:

1. I think that I would like to use this system frequently
2. I found the system unnecessarily complex
3. I thought the system was easy to use
4. I think that I would need the support of a technical person to be able to use this system
5. I found the various functions in this system were well integrated
6. I thought there was too much inconsistency in this system
7. I would imagine that most people would learn to use this system very quickly
8. I found the system very cumbersome to use
9. I felt very confident using the system
10. I needed to learn a lot of things before I could get going with this system

The number of the statement then corresponds to a particular way of calculating. As seen in equation 2.1, all the statements with an odd number (1, 3, 5, 7, 9) the score should be subtracted with 1 and for the even numbers (2, 4, 6, 8, 10) the score should be subtracted from 5. The total sum is then multiplied with 2.5 to achieve the individual score and the process then needs to be reproduced for each participant in the evaluation. When all these steps are complete, the overall SUS score can be calculated from the average score of the participants, as seen in equation 2.2 [8, 31].

$$\begin{aligned}
SUS_{userX} = & 2.5 * ((Score_1 - 1) + (Score_3 - 1) + (Score_5 - 1) + (Score_7 - 1) \\
& + (Score_9 - 1) + (5 - Score_2) + (5 - Score_4) \\
& + (5 - Score_6) + (5 - Score_8) + (5 - Score_{10}))
\end{aligned} \tag{2.1}$$

$$SUS_{total} = \frac{SUS_{user1} + SUS_{user2} + \dots + SUS_{userN-1} + SUS_{userN}}{N} \tag{2.2}$$

N = number of participants

The total score ends up as a number between 0-100, but important to note is that it should not be seen as a percentage of usability. Due to its industry wide use, SUS is a great way of comparing the score between similar products and find the benchmark for usability for the product's specific context [27]. With this in mind, there is some more accepted benchmark used, where a score of 68 or above is considered average, and a score of 80 or above is considered good usability wise [27, 30].

2.1.5 Test plan

To conduct a good usability evaluation it is important to keep a good structure and maintain a consistent test procedure which contributes to make it easier to analyse the results. Therefore it is a good idea to produce a test plan before the testing starts, as well as conduct a pilot test to test the structure before moving on to the real test. Pilot test should not focus on the usability testing, but rather testing and evaluating the test plan with its corresponding material [43]. A good test plan should contain:

- **Purpose** - A short description of why the test is conducted and how.
- **Research questions** - The questions that is searching for answers.
- **Selection of participants** - Defines if there are any requirements on the test participant, and how many test is wished to be conducted.
- **Test procedure** - A description of how the test is conducted and the material used for each step. Includes everything from greeting the test participant until the test is completed.
- **Test scenarios** - Contains a description of the scenario, a list of task, with corresponding sub tasks. Often also includes maximum time accepted and Successful Completion Criteria.
- **Test environment and supplies** - List where the test is carried through as well as the supplies needed for the test.
- **Division of roles** - Describes the division of roles within the test group, for example test leader, secretary and responsible for timing.

- **Data collection** - Defines which data is collected corresponding to the research questions.
- **Presentation of results** - Defines how the results will be processed and published [43].

2.2 Security: Threat modeling

Threat modeling is the process of identifying and assessing possible threats that some type of system might face. It is often applied to software systems, but can be applied to a wide array of things [11].

A threat model typically starts with a system description to get a collectively agreed upon view of what the threats will be directed at. This description is then used to define what security requirements exist for the system in question [35]. Not all systems have the same requirements and a simple example of this is a website with a regular front page for regular visitors and another page for administrators to control the site. A security requirement for the admin page would be that no unauthorized users could access it, while this requirement would not exist for the normal front page as it is made for random visitors.

With security requirements in place threats can be found that might jeopardize these requirements. The threats can then be ranked by their likelihood, severity or some other metrics [49]. Mitigations for the threats can then be found and implemented. Finally you should validate that the mitigations actually work as intended and thereby prove that the system is secure.

To effectively and reliably increase security, threat modeling should be made for all parts of a system as well as continuously and iteratively during the development and lifespan of the system[46]. Since this thesis focuses on using design to mitigate threats the regular threat modeling method will be deviated from slightly to stay within scope.

2.2.1 STRIDE

For this thesis we've chosen to employ the STRIDE model, a model developed at Microsoft in 2009. It is not a complete threat modeling framework, from system description to mitigation validation, but a way to find common threats posed against software systems with a system description and security requirements in place. Although the STRIDE model has received a fair bit of critique [29] it will hopefully give us sufficiently advanced results for our purposes.

It consists of six parts, one for each letter in the name. The parts are spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege [34], all of which will be given further explanation below.

Spoofing refers to pretending to be something one is not. This could be impersonating another person or entity, both in the sense of pretending to be someone else over phone or e-mail, or in the sense of having a computer impersonate another computer or server by interfering in some protocol as well as creating a fake website to impersonate a real one.

Tampering is, as defined by The National Institute of Standards and Technology of the US, "*An intentional but unauthorized act resulting in the modification of a system, components of systems, its intended behavior, or data.*"[44]. In other words, an act of tampering aims to change

a system or its components with the intention of causing damage or change the behaviour of it.

Repudiation, to reject as unauthorized or as having no binding force,[48] is in the sense of computer security the threat that a user could deny performing a harmful action towards the system. This could be due to a lack of logging user activity or that the logging system is susceptible to tampering [40].

Information disclosure is simply that a user or adversary could get their hands on information that they should not have access to.

Denial of service is when a system can not be accessed by a user due to some malicious action by an adversary. The action could be e.g some sort of exploit that causes the system to crash or by sending a flood of traffic/requests to keep the system completely busy and unable to handle legitimate requests [1].

Elevation of privilege refers to vulnerabilities that allow a user to gain higher privileges than it should. This could be used by a malicious user or leveraged by an adversary who has gained user access to gain further access to the system.

For each of these threats you can look at the system for which you are performing the threat modeling and analyse how they might affect your particular system and what their implications are. Following this contributes to more structured threat analysis, and could be good step before moving on with the regular threat modeling process and rank the threats, find mitigations etc.

Chapter 3

Identify requirements

This chapter aims to explain how the user requirements of the design process were found. Firstly a literature study in security awareness methods and its corresponding practises is presented. This is followed by the application of STRIDE on Homepals platform as well as the results that came out of it. After this we present a survey that was conducted aiming to investigate opinions about experience with security awareness education and opinions about using posters to mediate information, as well as a survey conducted on Homepals users. These surveys were conducted to find out what the users think about it in the every day working life to add a dimension to our user requirements analysis. Lastly, the main takeaways from this phase will be presented.

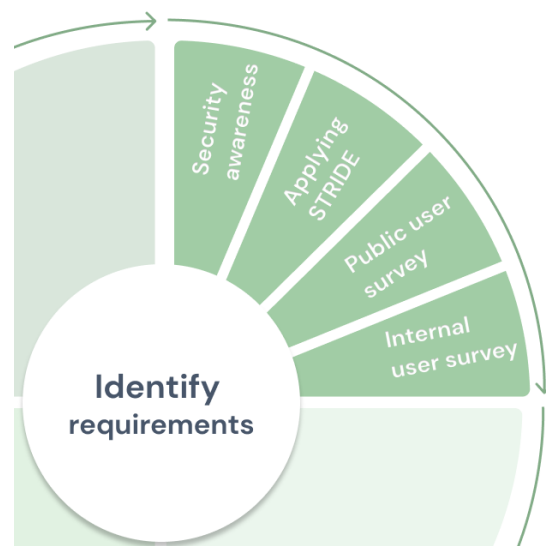


Figure 3.1: The current state of the process, to identify requirements.

3.1 Security awareness

In order to increase the security awareness within a company is important to not only look on outside threats, but also to evaluate usage strategy for the everyday users. This is due to the fact that many security threats for a company could come from within the company routines or work models. Users could be taking unnecessary risks in their every day work due to lack of awareness of the importance of security procedures, but also in their lack of knowledge of their position in the decision chain in case of a critical security situation [3] [28]. All these factors are not always connected to the users wrongdoings, but could rather be connected to underlying problems within the organisational work structure [2].

In this section the underlying theory about user behaviour in relation to making wrong decisions is presented, as well as some of the possible strategies that can be used in order to address security awareness problems - both in relation to the individual and the organisation.

3.1.1 Slips and mistakes

In order to understand the users intentions and actions it is important to understand the underlying factor of an errorogenous decision. According to Norman [38] an error could be divided into two categories: slips and mistakes. The difference between the two is that slips could be traced to a situation where the action performed has a good intention but ends up being the wrong one, whereas mistakes are based in a inaccurate plan or a faulty goal target. Important to point out is that both could be the result of a faulty memory based action, as simple as the user forgetting the course of action to use in a situation.

Mistakes is this case the most interesting one, as a mistake could possibly be traced to the user choosing the wrong approach, even though the user has the correct overview of the problem, or it could be traced to the fact that the user lacks the knowledge to analyse the situation correctly [38]. In order to address the errors performed by users it is important not to blame the individual, but rather analyse the process and try to aim the focus on changing the environment, the user interface, and routines surrounding the users every day actions [2].

3.1.2 Tools for security awareness

In the security case it is important to aim the focus on changing the users behavior connected to security critical actions, as well as creating a positive security culture [2, 28]. In the company perspective there is a need to see the user as an asset in increasing the security situation and work towards a culture that aims to encourage the increase the user security awareness [3, 9]. Furthermore, it is important to look into both the users knowledge of the demands on their security position as well as the users will and motive to keep their actions within these demands [3, 28]. The motivation and knowledge of the user is a complex pattern with both personal opinions and background at stake as well as company culture and limitations, a fact that is important to keep in mind while developing a solution for a company [28]. Some of these factors are not possible to effect due to its personal nature, as mentioned in section 3.1.1, but instead it is important to focus the work on the security culture around the users every day work, their position in the security decision chain and also the need for increasing the users security decision making [3, 28]. Some of the found approaches to achieve an impact

on these factors are presented below.

Education

One of the strategies in order to achieve an increased security awareness for the user is to develop an adequate security awareness education for the company [3]. To ensure that the education is received positively within the user group it is important not to overflow the user with information to avoid cognitive overload due to the complexity of cyber security [7], a fact that was brought up in the 2021 World Conference on Information Security Education (WISE) [12].

The educational process could instead be an iterative and agile process with activities that at different occasions points increases the user knowledge, both with tangible examples and with contextual knowledge in mind. The educational process should then be followed up and iterated to maintain the users awareness and educational level and increase their knowledge layer by layer [28, 36]. Once again it is important not to focus on the wrong-doings of the users, but instead shine light on possible strategies on giving the user tools for solving upcoming situations. In addition to learning about a tangible situation in their context it's important to include parts of education for the user to achieve a good understanding of the users security position and the influence that the user has in the company security structure and to understand the importance of the security awareness across the company [3, 36].

Gamification

A way of conducting the security awareness training could be through educational gamification, an increasing concept in many educational areas. Multiple different games exists with the purpose of increasing the security awareness for employees at companies. These games could vary between video games, story telling, card games and regular board games, aiming for different purposes in different situations [20]. The gaming environment creates a creative and interactive environment for the user and could often be adjusted to fit multiple users and scenarios [4].

Poster

Another approach to increase the security awareness is through visual elements presented within the company's physical environment. An example of such an element is a graphical poster placed in the office environment. This poster could work as a supplement to another element in a security awareness process, e.g. as an ongoing reminder to maintain the awareness after an educational element [13, 23].

The issue with a poster or similar graphical reminders is the risk of it being overseen after some time [6]. This increases the demands on it to be graphically pleasing, user friendly [13] and even humorous, as well as being iterated and changed on a regular basis, e.g. every 90 day to maintain the user interest. The length of an iteration and the design of the poster should be, as many other elements in the security awareness domain, develop specifically for the company and their users in question, to fit and contribute to their specific security awareness culture [6].



Figure 3.2: Poster (in Swedish) of *Folkhälsomyndighetens* advices during Covid-19 [14].

One current example of using posters as a way of spread awareness can be seen in figure 3.2. This is a tangible example of one of the awareness campaign carried through by *Folkhälsomyndigheten* in Sweden during the Covid-19 pandemic and could often be found at public and corporate toilets. The poster aims to increase the awareness in possible measurements that could be practised by a citizen in order to decrease the spread of Covid-19 [14].

3.1.3 Security awareness and design

The main subject within both user perspective and security awareness is using tools to change the user behavior through making it an easier choice to change a routine and/or a behaviour and focus on develop educational element that is based in the particular environment of use for the user. It is therefor crucial to use an user centered design approach, with the users need in focus, in order to achieve a good security awareness within a company.

In relation to education, design elements can be integrate throughout the whole learning cycle, for example in the presentation of tangible examples through using interactive elements for the user to interact with. In the gamification approach user centered design is a crucial part, as the main focus for the concept is for the user to use interactive elements in the learning process.

Furthermore, posters also has a need for using user centered design in order to ensure their usability. The need for a design process is also crucial for ensuring a kept interest and provide an attractive and up-to-date information. Thus, it is an interesting concept to use for reminding users of their security awareness and to move forward with in this master thesis.

3.2 Applying STRIDE

The threat analysis is based on the system description in section 1.3.1, which is a high-level description based on information gathered from their website. In addition to this, additional information was collected from interviewing developers and product owners at Homepal, and the complete analysis will be presented below.

Spoofting

Spoofting, in the sense of creating a fake website that mimics the Homepal platform in order to trick users to give up their credentials is definitely a possibility. The Homepal platform login site is, much like Facebook, Google and a lot of other modern login sites, pretty much just a box with inputs for username and password as well as the company logo somewhere on the site [22]. This is very easy to replicate, especially since most modern browsers have built in developer tools which allows a user to conveniently view the HTML and CSS of a website, the parts that dictates what the page looks like [18]. Adding more, as well as more complicated, elements to the site could increase a users feeling of safety but might not make it much harder for an adversary as they could still use the same technologies as described before to easily replicate the look of a website [10].

If a spoofed website is in place, an adversary still needs the victims to go to the site to actually perform the attack. This is often done using spoofed communication such as emails, text messages or some sort of voice communication, called phishing. Phishing can both be used to get a user to outright send their credentials to the adversary or enter their credentials in a fake website. An easy way to identify a fake website is the URL, as the URL can not be spoofed with https in use [19]. While spoofing is more or less impossible with https, getting another URL certified is not difficult at all [15]. A common workaround for an adversary trying to spoof a website is to register and use a URL that is similar to the original in some way. This could mean switching letters for similar ones or adding typos that are hard to notice.

Since spoofing/phishing attacks are by far the most common attack[24] and users do not always know how URLs work[10] it's obvious that checking the URL needs to be as easy as possible. With Homepal's platform however, as well as for instance Google's login site, the login URL is on a subdomain, very long and contains seemingly random strings containing some kind of information for the back-end system. This makes it much harder to identify a fake URL imitating a real one as there is a lot of other text in the address field.

Tampering

Tampering is a very present threat as Homepal's main business idea concerns data handling. *Explore* allows users to add missing data or correct faulty data. If an adversary were to gain access to a user account they could easily tamper with the data. Gaining access to the backend AWS service instead of a user account could lead to an adversary being able to tamper with the data for all customers using the platform, not only the company to which a compromised user account is registered. As the Homepal platform is meant to create APIs and make data usable by modern applications the severity of a tampering attack differs heavily depending on what kind of applications are using the data in the end. If, for example, the data is sent to an

application handling billing and invoices an attack could conceivably lead to huge losses for both housing companies and tenants. If the data is sent to an application handling vacancies tampering could lead to occupied real estate being published as possible to rent, leading to costs in administration as well as damage control for a housing company and stress and uncertainty for affected residents.

Repudiation

The threat of repudiation is closely linked to that of tampering. This is because repudiation attacks often come in two different types. One involves an adversary tampering with logs meant to protect from repudiation attacks to create fake logged actions or delete valid ones to hide some form of tampering. The other one involves a malicious user who uses the lack of logging to tamper with the system for some personal gain. Although not an attack, complete lack of logged user actions can make it harder to find out what went wrong and reevaluate design to avoid future mistakes if a user makes an honest mistake and affects the system in an unintended way. This threat is also very present since most of Homepal's apps do not log user actions at all. This makes it harder to detect tampering or unauthorized usage by an adversary and harder to undo the actions performed. It also makes it harder to detect and undo slips and mistakes made by regular users.

Information disclosure

Information disclosure could happen in many ways, from adversaries gaining illegitimate access to the applications or databases or legitimate users by mistake gaining access to data they should not have access to. As with tampering the severity of this depends heavily on the information disclosed.

Denial of service

The Homepal platform and applications are hosted on the AWS cloud computing platform. This gives them the advantage of using already implemented DDoS protection services to protect from the traffic flood type of DoS attacks [5]. While it is possible to protect against Application-bug type attacks, with for example anomaly detection, a system with well built applications and updated dependencies and services is resilient in and of itself [39]. A successful DoS attack would affect all of Homepal's customers potentially costing them and Homepal money as well as damaging Homepal's reputation.

Elevation of privilege

Elevation of privilege would mean a low end user account gaining more access than intended, either by mistake or with malicious intent. A successfully leveraged elevation of privilege attack would in turn lead to information disclosure and tampering possibilities, with their respective consequences.

3.2.1 STRIDE and user awareness

With these high level threats applied to Homepal's platform and applications there are some possibilities to relate the result to design or user experience in some way.

Spoofing is the threat where design and user experience has most potential to be used. While there are mitigations such as TLS and other authentication schemes to make sure you are communicating with the correct website or person it still often comes down to the user to detect spoofing. Because of this it's extremely important that the users know how to detect spoofing attempts, how they work, what the consequences are and what to do when an attempt is detected.

While stopping an adversary with system access from tampering or stopping a repudiation attack using design is probably impossible, accidental tampering made by regular users can probably be mitigated in several ways through increasing the security awareness. Furthermore, logging user action to both control tampering and repudiation could be used to find slips and mistakes made by legitimate users to help improve the overall design and user experience of the platform and applications.

Information disclosure, denial of service and elevation of privilege are all very tied to implementation and configuration and therefore the possibilities to mitigate these threats using design or user experience to mitigate them are very small. Due to the fact that these threats need to be assessed during the development of the platform it falls outside the scope for this master thesis.

3.2.2 STRIDE analysis conclusion

In conclusion, the result of the analysis is to focus on the threat of spoofing. While accidental tampering definitely could be prevented with good design Homepal's applications and their designs are ever changing, making the task sisyphian. Since spoofing might could be mitigated with user knowledge and behavioural change the security aspects of the educational on-boarding process at companies as well as reinforcement of the things employees are taught during that process was chosen as a subject for further investigation.

3.3 Public user survey

To join the two subjects of spoofing and security awareness the thesis moved on to exploring the thoughts and opinions of real life users. To begin the investigation a survey was created. This survey aimed to collect opinions in relation to user experiences within security on-boarding elements, as well as opinions related to using posters as a potential way to inform and remind people of something. This to see if these two subjects had something to move forward in the master thesis and hopefully add another dimension to the identification of requirements process.

The survey consisted of both quantitative questions, with statements and Likert scales to consider in relation to the participants own experiences within the scope of the statement, as well as qualitative questions, by adding follow up questions to statements as well as giving the participants the opportunity to motivate their statement answers. The complete survey can be seen in Appendix A.1.

The survey was discussed with our supervisors prior to release and pilot tested by three participants to get feedback and ensure that the answers were relevant for the thesis. An approximate time to complete the survey was also recorded and used to motivate the future participants. The feedback from the pilot test participants consisted of to correct a couple of spelling mistakes, as well as to adjust the approximated time to complete the survey from eight to five minutes. The pilot test also got the wanted reflection of ensuring that the questions asked seemed relevant, as well as rewarding, for the thesis. Upon release, the survey was distributed to our friends and family through social media, and generated 85 responses.

3.3.1 Initial part

The first part of the survey consisted of a couple of background questions regarding age, gender, employment and self estimated level of technical competence.

Since our main way of distributing the survey was through social media channels and by word of mouth most of the responses were by engineering students and people working in IT. This skewing of course is not optimal since Homepal's users are not likely to be computer science engineers, but it gives us a lot of data regarding security on-boarding which brought a lot of value to the thesis and will be presented more in detail below.

The people who took the survey was mostly men in their twenties with 64 responders being between 20 and 27 years old and 62 of them male, the different ages of the responders can be seen in figure 3.3. Two thirds of responders were studying and one third working, the working part mostly being in IT. Most people considered their technical competence to be good.

3.3.2 Security on-boarding part

The security on-boarding part of the survey meant to show what people have thought of the security on-boarding experiences they've had and how they could have been improved. If the participants did not have any previous security on-boarding experience their general view on security education was still interesting and therefore was included in the questions regarding the designing of educational elements.

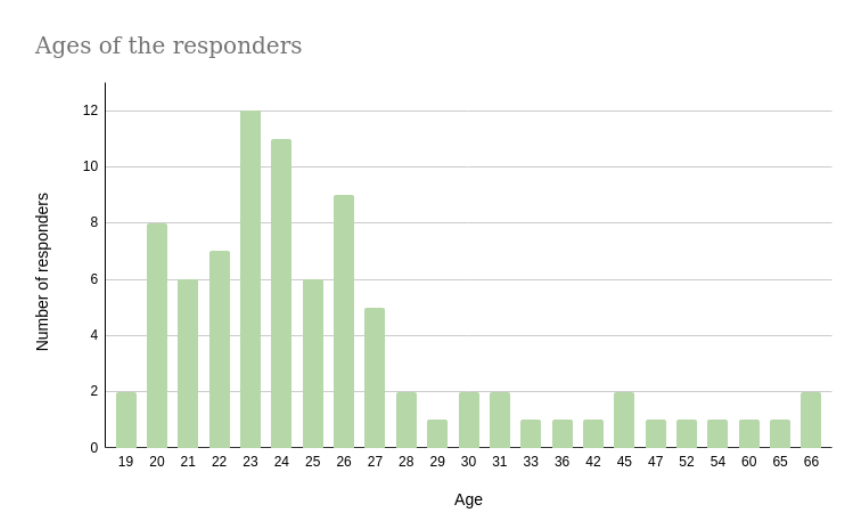


Figure 3.3: Graph over the respondents different ages.

Half of responders had gone through a security on-boarding process, either a digital education or a physical lecture. The things that people found negative with their educations were that they were too simple, even boring, and lacking in good examples that made you understand why things were insecure and how attacks actually worked, a fact that seemed important to many of the responders regardless if they had completed a security education or not, as seen in figure 3.4. The things that people found positive was that the education did not take a long time if you already knew the things being taught, but it was pointed out a need for using different levels of difficulty based on previous IT security knowledge. Overall there was a general consensus that the educations were very important in order to increase the awareness in IT-security, see figure 3.5.

Although almost all responders agreed that it was very important to follow up an education only 30% reported that their education had been followed up in some way. Most of the people who had had some sort of follow up had it immediately after the education in the form of a quiz and a few had to take the same education again some time afterwards.

3.3.3 Poster part

The poster part of the survey meant to investigate how well the Covid-19 reminder posters have worked and why. This to further find out what the users thought about the use of it as a reminder, and find out whether to use posters as a way of increasing security awareness was a direction in which this thesis could go.

All but one of the responders had seen the Covid-19 posters during the pandemic. Most people thought the posters were a good way of conveying information regarding the pandemic and even more considered them to be a good reminder of important information, as seen in figure 3.6.

Generally the responders attributed the success of the Covid-19 posters to them being clear and concise as well as placed in appropriate places. When asked if they had found that they disregarded the posters after having seen them a lot of times most of the responders agreed that this happened to some extent, but a lot of them said that even though they started

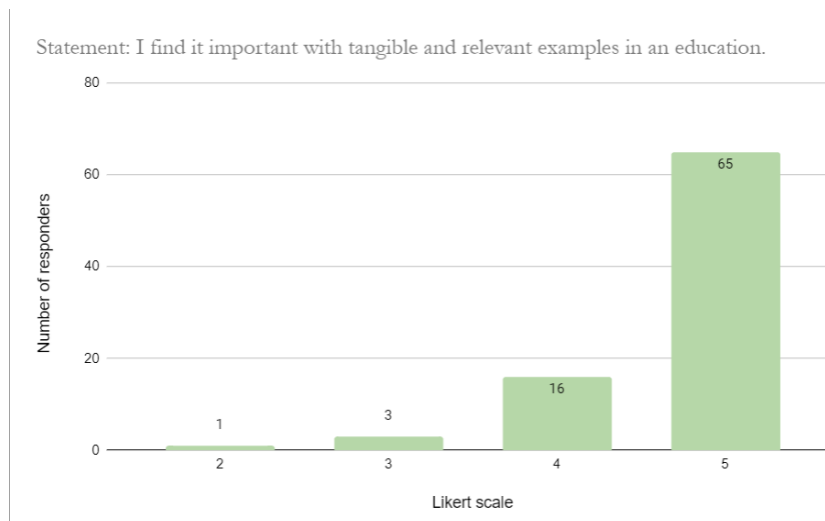


Figure 3.4: Survey results of the statement *"I find it important with tangible and relevant examples in an education."*

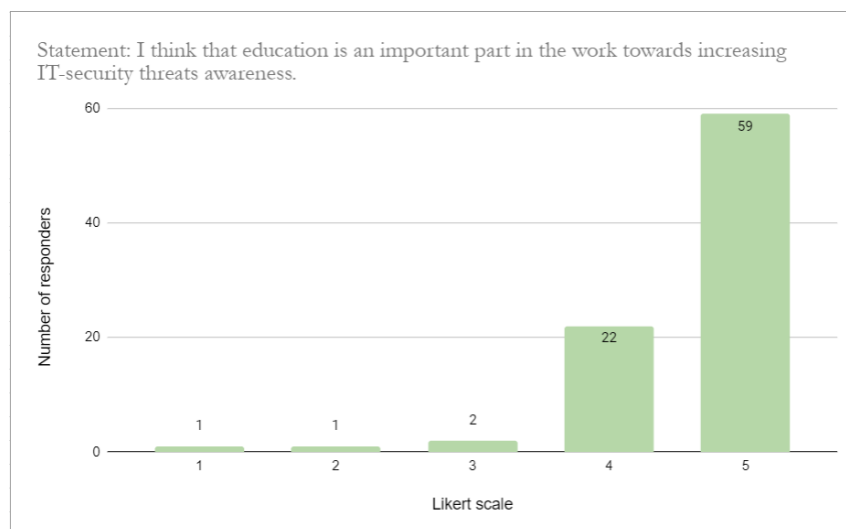


Figure 3.5: Survey results of the statement *"I think that education is an important part in the work towards increasing IT-security threats awareness."*

to look past the posters they were still reminded about what they knew was on them just by noticing them.

When choosing three different qualities that makes a poster effective almost all, 93%, chose that the poster should have a simple and straight forward design. Furthermore 66% of responders said that the poster had to be eye-catching and 32 and 34% respectively thought that it should be apparent who made the poster and how to find more information on the subject. The alternatives making a poster effective that the responders could choose from were:

- Simple and straightforward design
- Contains detailed information about the subject

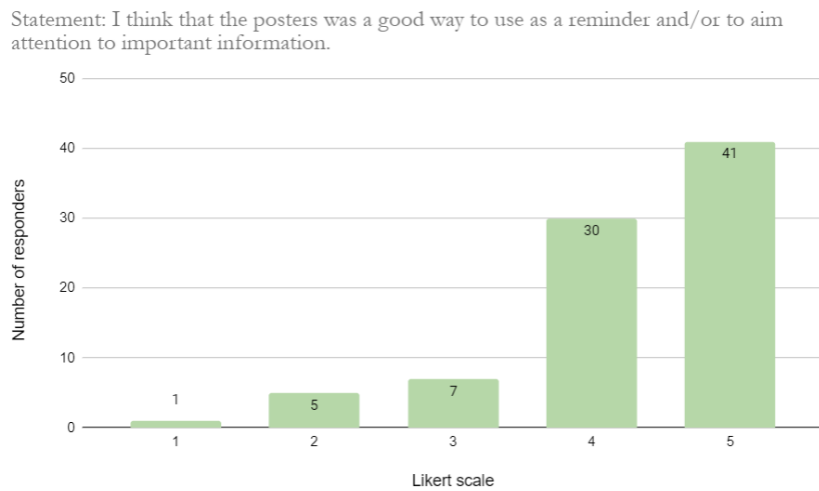


Figure 3.6: Survey results of the statement " I think that the posters was a good way to use as a reminder and/or to aim attention to important information."

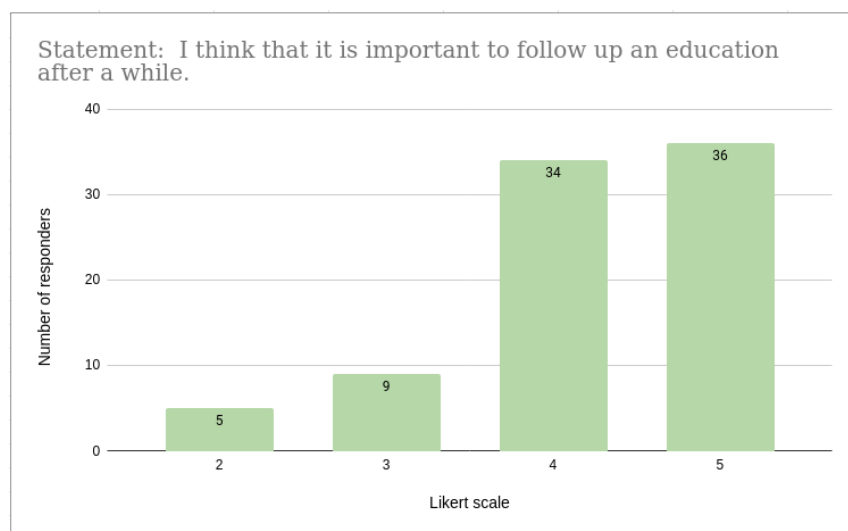


Figure 3.7: Survey results of the statement " I think that it is important to follow up an education after a while."

- Has a nice colour scheme
- Clearly shows who made the poster
- Is eye catching
- Gives the viewer the option of finding more information
- Contains humorous elements
- Looks nice
- Is replaced regularly

These alternatives were chosen from brainstorming different aspects of a poster, inspired from previous experiences with posters, the examples of Covid-19 posters, as well as the usability goals. The result was an important step in order to understand the users point of view in an early design stage and resulted in requirements used later in the process.

3.4 User base survey

To add a layer to our user requirements the general opinion about security awareness in Homepal's user base was investigated to see how the current users of Homepal felt about the subject. Therefore, the survey created in the previous section was narrowed down and distributed to Homepal's user base.

The goal of the survey was to reach out to the users of the platform, but it should be reserved that the users that participated and answered the survey were all in some form of management position. Therefore it was chosen to modify the survey parts and collect data about the educations that were/were not conducted rather than the personal opinions of the participants.

In the final survey the poster specific parts were removed as the answers to that section from the general survey probably would be representative of the general population. The shortening of the survey would also make it easier for the companies to take time out of their day to fill it in. The question *"Have you ever undergone an IT-security education at a workplace?"* was changed to *"Have you ever undergone an IT-security education at your current workplace?"*. This affects all the questions in part 3 so that they are about the security education at the users current workplace and this was done to better get an understanding of the situation regarding security education at Homepal's customers. Two questions were added as well, one about the users current role at their workplace and one about their preferred way of follow up to an education. The possible answers to the latter of the two were examples taken from the general survey, with the alternative of a poster added.

The survey got responses from four companies, which makes up half of Homepal's user base. The results showed that all of the responding companies had some sort of security education. Three of them had digital educations, were one of the three had a digital education during the employee on-boarding and physical educations periodically. The fourth company only had physical educations. Three out of the four did not follow up the education other than repeating it annually or biannually. The only one following up the education in some way did it by sending out fake phishing emails and checking if the employees fall for it. All respondents were positive towards using education as a way of increasing security awareness and thought it was important to follow up the education after some time.

3.5 Main takeaways

To sum up the requirements found in this chapter, the following conclusions were made:

- Spoofing, especially in the form of phishing, is the threat were design can be most utilised for Homepal. The possibility to use design here corresponds to the need of educating the user and furthermore utilising design within education.

- There are many different type of ways to integrate design elements in increasing the security awareness for employees, but a physical/digital education seems to be one of the most common approaches. Responders of the public survey emphasised the need for follow up security education, but was in reality missing for many of the responders.
- Many responders had a positive approach of using posters as a way of reminding of important information. This, together with the positive approach to the importance of following up a security education aimed the thesis in the direction of investigating the combination of the both.
- Responders found simplicity, eye-catching, facts about who made the posters and a possibility to find more information about the subject to be the most important elements in designing a poster.
- The companies using Homepal's platform all have some sort of security education, but most of them do not follow up their educations in a meaningful way.

Chapter 4

Create alternatives

This chapter aims to explain the thought process behind the design alternatives created, in this case lo-fi prototype posters. Below, each poster is described along with an explanation of the design process as to why it was chosen to design the poster and arrange the elements in this certain way. Lastly in the chapter, the evaluation of the lo-fi prototypes that was carried out will be presented.

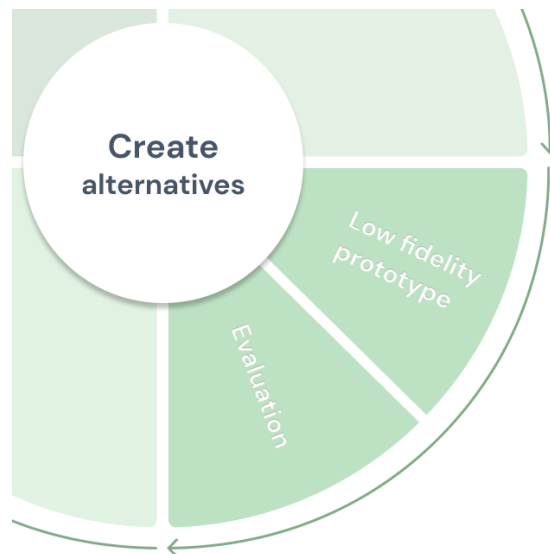


Figure 4.1: The current state of the process, to create alternatives.

4.1 Lo-fi prototype

As concluded in the last chapter, four main requirements were important to the responders: simplicity, eye-catching, facts about who made the posters and a possibility to find more information. With the requirements in place a few lo-fi posters were created through using colour pens and paper, as the purpose of creating a lo-fi prototype was to test concepts and ideas. The top 4 qualities found in the survey were used as starting points for brainstorming of different concepts to be developed into sketches, with design elements that satisfied those qualities.

The first quality, simplicity, permeated all parts of the design while the other qualities had more specific elements tied to them. To keep the posters simple only white backgrounds and a minimal colour scheme were used. The elements were also kept as simple as possible and all elements were made sure to be relevant to the information or to the understanding of the poster as a whole. The second most important quality, for a poster to be eye-catching, both had specific elements and a more general effect on the design. The specific elements used to catch the eye were big titles and interesting shapes. To satisfy the quality of conveying who made the poster the Homepal logo as well as their name in different combinations were used. To make it easy to find more information links and QR-codes with text in different combinations were used. All posters can be viewed below in figure 4.2, as well as in a bigger scale in Appendix B.1.

Poster 1

Poster 1 has a very large title covering most of the space catching the eye, with the Homepal logo and a QR-code sharing the space at the bottom. With only three simple elements and a minimal colour scheme the poster is very simple and it's impossible to miss any of the elements. However there is not a lot of information on the poster and up to the viewers to follow the QR-code if they want to. Hopefully it should have some effect on the viewer, as some responders wrote in the survey, they found that it took very little to be reminded of something they already knew. Since most responders felt they already knew a lot of the basics they were supposed to learn in their on-boarding even a poster this simple could work as a quick reminder (figure 4.2).

Poster 2

Poster 2 has a medium sized title sharing the top space of the poster with an illustration meant to catch the eye. In the lo-fi prototype the illustration is a light bulb, often used to express remembering something or getting an idea. Below the title there are two tips with a bolded title part and a non-bold body of text explaining or reminding the viewer of something. Beside each tip is a check mark to illustrate that these are steps that can be taken to achieve something. At the bottom there is a small Homepal logo with their name next to it as well as a small QR-code. This poster can contain a bit more information than poster 1 but is a little bit more cluttered which could lead to viewers disregarding the poster due to too much visual information making the poster less easy to quickly read (figure 4.2).

Poster 3

Poster 3 has no title but has three tips in the same manner as poster 2. While it is less eye-catching it can contain more information and has a simpler more straight forward look. The only thing with the tips that's different from poster 2 is that each individual tip has a small frame around it to clearly show where one ends and the next one starts. This gives the poster a bit more structure as well and helps the poster feel less cluttered with a lot of text. At the bottom there is a small Homepal logo and a shortened link to more information (figure 4.2).

Poster 4

Poster 4 has a small title at the top along with the Homepal logo. Below there are four tips or pieces of information staggered, each with their own unique medium sized illustration of some sort. The illustrations are meant to catch the eye and in the lo-fi prototype they are different shapes in slightly different colours. Later, they might change to better represent the specific information they are connected to. At the bottom Homepal's name is stated. This poster has a different type and style of eye-catching elements to the previous posters, the effectiveness of which will be evaluated later. While there are no frames around the pieces of text the bigger more complicated illustrations next to the text will hopefully make clear that the texts are separate, as well as draw attention to different facts using both text and graphical illustration (figure 4.2).

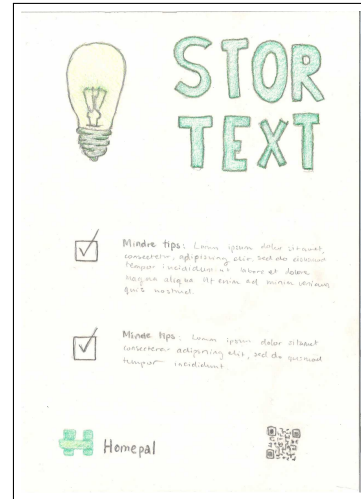
Poster 5

Poster 5 has no title but a big illustration dominating the whole poster. The illustration is supposed to be linked to some part of spoofing or phishing and has a small explanatory text below it. At the bottom of the poster is the Homepal logo with Homepal written next to it. This poster contains almost no information but the illustration is more interesting and eye catching than a large title and might still remind the viewer of something important. A poster that only reminds the viewer of something small is still better than a poster with a lot of important information that everyone disregards (figure 4.2).

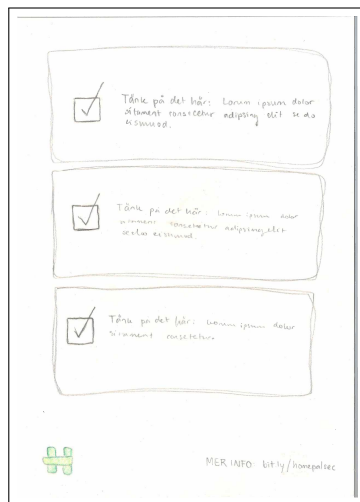
Overall we've tried to mix up the combinations of name/logo, QR-code/link as well as having different types of eye catching elements and different amounts of information to more clearly be able to see what works when evaluating our designs later.



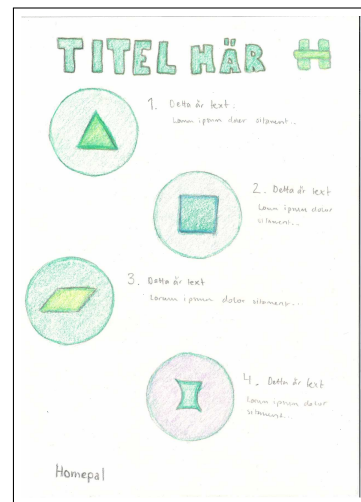
Poster 1



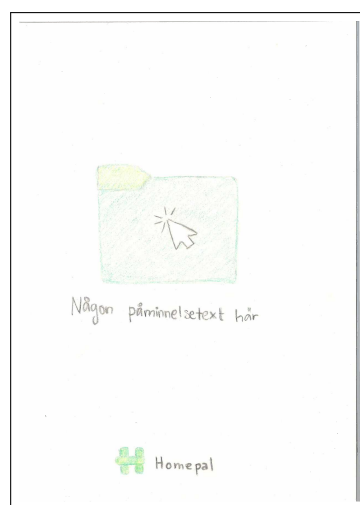
Poster 2



Poster 3



Poster 4



Poster 5

Figure 4.2: All 5 lo-fi posters

4.2 Evaluation

As the lo-fi prototypes were finished it was time to move on to perform an evaluation, with the purpose to give ground for the hi-fi prototypes. As the posters were a result of the survey, it was in our interest to make sure that the posters had satisfied the most important requirements mentioned found before moving on to the hi-fi prototype. The evaluation was made to find the best versions of specific elements as well as make sure that the reasoning regarding some elements were sound. The versions of elements that were tested were QR-code versus bit.ly link as well as the combinations of the Homepal logo with and without text. The reasoning that the evaluation was made to check was that of the eye catching elements. The evaluation was also made for us to get some general pointers that could be used to further improve the posters before hi-fi and testing.

The evaluation was carried out by performing semi-structured interviews where subjects would be presented with all lo-fi posters and asked to answer a few questions with plenty of room for discussion to achieve qualitative data. The questions, in order, were

1. *Which elements catch your eye?*
2. *If you decided to find more information, which of the options would you prefer? QR or link?*
3. *Which of the posters do you prefer and why?*
4. *All posters contain Homepal's logo. Which of the combinations with logo and text do you prefer?*
5. *Do you have any other thoughts of the posters or the elements contained within them?*

Due to the fact that the evaluation was carried out during the peak summer vacation in Sweden there was a need for conducting some of the interviews digitally for logistical reasons. All in all four physical interviews and three digital interviews were completed and all of the participants had taken part in the original evaluation. This meant that their answers would represent if the requirements from the first evaluation were satisfied. The participants in the physical interviews were all people between 20 and 25 years old studying computer science, one of them male and three of them female. The participants in the digital interviews were of mixed ages and backgrounds, all of them male.

Firstly, all of the interviewees said that qr-codes were preferred to links and that the Homepal logo with text made it much clearer who made the poster without making it more cluttered.

Regarding general preferences, most of the interviewees preferred poster 1 or 2 and the light bulb was specifically mentioned several times as a good graphical element that signified learning or remembering as well as being eye-catching. Poster 3 was critiqued for only having information without a clear beginning, contrary to poster 2 and 3 which were described as having a "good flow" when viewing or reading them. Poster 4 still received some critique about reading flow as the graphical elements connected to the information were more eye catching than the title, making the user start reading somewhere in the middle of the poster instead of at the top. Regarding flow as well, one of the interviewees mentioned that they felt that the logo in poster 4 should have been at the bottom instead of the top and another interviewee mentioned that the fact that the logo and qr code or link was at the bottom

made the posters easier to read as you would not care for more information before you had consumed the information contained on the poster.

The posters were overall considered simple and straight forward but one interviewee felt that while the green colour was nice and obviously related to Homepal, it did not always feel like the user was being warned of something and that a red colour could be used in some way to signify malice.

4.3 Main takeaways

From this part the following conclusions were drawn:

- It is important to have a good reading flow both in the design and the information. This to guide the user to read the poster in the order that is intended.
- The use of QR-code seems to be a good way to mediate a way of getting more information about the subject and should be investigated further.
- The use of eye-catching elements in the form of illustrations and titles seems to be a good concept, but need further investigation within its thought context.
- The graphical concepts and colours was over all perceived as positive and should be used in future iterations, perhaps in combination with using more contrast colours such as red or black.

Chapter 5

Produce prototypes

This section will consist mainly of a description of the ideation, creation and evaluation of the hi-fi prototype. Firstly the underlying graphical profile will be presented, which will be followed by the collection of the information on the posters. Lastly, there will be a presentation of the hi-fi prototypes produced.

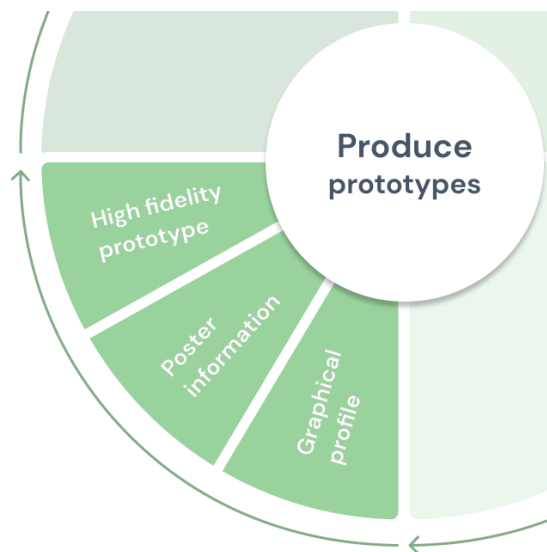


Figure 5.1: The current state of the process, to produce prototypes.

5.1 Graphical profile

After completion of the lo-fi prototype evaluation we moved on to start the ideation of the hi-fi prototype posters. As the posters are produced for Homepal it was needed to keep the design within their graphical guidelines and choose to produce a graphical profile that later both could be used as a template to pick and choose from in the production of the posters, as well as contributing towards ensuring a consistency in the design. The complete graphical profile can be seen in figure 5.2 and 5.3.

5.1.1 Text elements

The first part of the production of the graphical profile consisted of setting the standard for titles and body text. Homepal uses the font *DM Sans*¹ for external purposes, and since the posters are meant to be used and located at Homepal's customer's location it was given to use this font in the posters as well. The chosen text elements can be seen in figure 5.2. The choice of colours for the titles will be further explained in 5.1.2 Graphical elements, but is combination of the different main colours that hopefully will work as an attention drawer in the posters.

5.1.2 Graphical elements

In order to graphically present different subjects in the posters a profile for the graphical elements was developed, which can be seen in figure 5.3. Firstly the colours were collected from Homepal's graphical guidelines, together with two different versions of their logotype. These components seemed pretty straight forward in their design and an obvious choice to use in regards to producing these posters for Homepal. Furthermore, the colour pallet was complemented with a red colour with the purpose of representing malicious intents in the illustrations. The check boxes and the example illustrations components also has their origin in Homepal's graphical guidelines and was collected from their chosen tool for history telling illustrations *unDraw*². The illustrations were post collection modified to fit the colour scheme as well as the purpose needed for the different posters in mind. As noted in the graphical guidelines of Homepal, they are only examples of illustrations and subject for change if needed.

5.2 Poster information

As the design stage has moved the design process one step further, the example text in the lo-fi prototypes were switched to headlines and information that was more applicable to phishing and security awareness.

Information to fill the posters was gathered online, and the decision to keep the posters in Swedish was made due to the fact that Homepal's platforms are mainly in Swedish. For the security tips on the posters the ones from The Swedish Civil Contingencies Agency were

¹DM Sans <https://fonts.google.com/specimen/DM+Sans>

²*unDraw* <https://undraw.co/illustrations>



Figure 5.2: Graphical profile part 1: Text elements.

used directly. Other information on the posters was put together from the sources listed below.

Another way of finding relevant information to fill the posters with would have been to reach out to companies and asked them to share their security on-boarding educations and taken the information from there instead. However companies might be reluctant to share such information publicly as knowledge of shortcomings in their security education might pose a threat to their organizations. In some posters the fact that everybody makes mistakes was emphasized since a lot of victims feel embarrassed about falling for scams and therefore avoid reporting them even though reporting an incident is extremely important. The sources used for information were *Säkerhetskollen*³, *Sentor*⁴, *Polisen*⁵ and *MSB*⁶

The information on the posters was chosen to try to meet the following usability heuristics:

4. **Consistency and standards:** The information on a poster need to reflect what the users are taught during their security education for it to effectively remind users of the steps they should take to stay safe.
6. **Recognition rather than recall:** The information should be concise and quickly remind the viewer of all the relevant information by just reading a bit. This is also done in design by printing key words in bold.
8. **Aesthetic and minimalist design:** A poster shouldn't contain any unnecessary information as this could waste precious seconds of viewing time and make the poster as a whole less credible.
9. **Help users recognize, diagnose, and recover from errors:** Incident reporting is extremely important and viewing the company utilizing the posters as one big system

³<https://tanksakert.sakerhetskollen.se/fordjupning-natfiske-phishing/>

⁴<https://www.sentor.se/artikel/10-tips-fran-experten-sa-undviker-du-natfiske/>

⁵<https://polisen.se/utsatt-for-brott/skydda-dig-mot-brott/bedrageri/natfiske-phishing-/>

⁶<https://www.msb.se/sv/rad-till-privatpersoner/informationssakerhet/skydda-dig-mot-natfiske-och-skadlig-kod/>

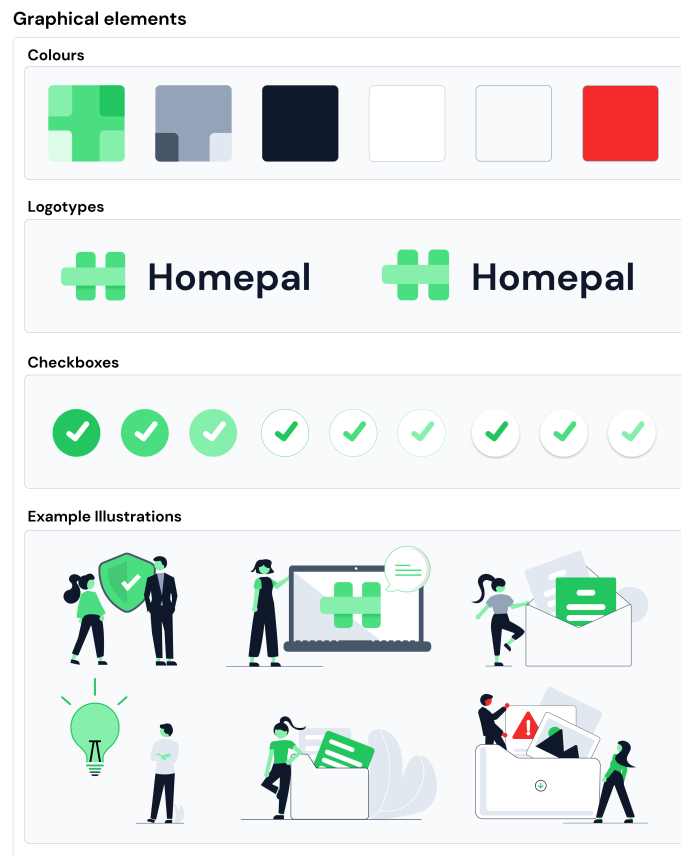


Figure 5.3: Graphical profile part 2: Colours and graphical elements.

the reporting is needed to control damages and prevent future incidents. Therefore information about incident reporting was prioritized quite high.

5.3 Hi-fi prototype

When the graphical profile felt complete it was time to move on to produce hi-fi prototypes of the posters. They were developed in *Figma*⁷, a tool that is used for producing digital prototypes in an easier way. All the posters uses the graphical profile mentioned in section 5.1 and contains information collected in section 5.2. The number of posters were kept the same, as we wanted to further investigate different elements as well as try some new ideas with using background colours to make certain elements pop. The posters can be seen in figure 5.4 as well as in Appendix B.2, and will its corresponding design decisions will be explained further below.

⁷*Figma* <https://figma.com/>

Poster 1

The hi-fi prototype of poster 1 is very similar to the lo-fi prototype poster 1 since it was regarded as eye catching and intriguing by the participants of the lo-fi test. To maintain the eye catching effect, but aim the purpose of the title to be more directed at security awareness, it was decided to use the sentence "Är du säker?" as a title which translates to "Are you secure?".

Poster 2

Poster 2 also mostly resembled the lo-fi prototype version of poster 2. In the evaluation of the lo-fi prototype, the light bulb was considered a good, eye catching element that signified a reminder and were therefor adapted to the graphical profile and kept in the hi-fi version. The information on the poster was given a green background to make it stand out a bit more and aim the focus to the information.

Poster 3

The lo-fi version of poster 3 was considered not very eye catching and therefore the check boxes were replaced with more interesting illustrations, which corresponds to the information given in the corresponding text. The middle piece of information with its corresponding illustration was given a green background to further separate the sections of text which are a bit longer than in the other posters and create a better flow to guide the user through the poster.

Poster 4

The logo in poster 4 was moved to the bottom, in comparison to the lo-fi prototype, to give the poster a better reading flow and a QR-code was added as well to make sure the viewer could find more information. The illustrations and text sections were put in a straight line instead of a staggered one as the staggered layout created unnecessary confusion, made for large unused sections of space as well as squashed the text sections which became very thin and long.

Poster 5

Poster 5 was the one that the lo-fi evaluation interviewees liked the least and was therefore replaced with a poster similar to poster 2, but with different illustrations to further investigate what made poster 2 the most liked one during the lo-fi testing.



Poster 1



Poster 2



Poster 3



Poster 4



Poster 5

Figure 5.4: All 5 hi-fi posters

Chapter 6

Usability evaluation

In this chapter the hi-fi prototype will go through a usability evaluation. Firstly the test plan will be presented, with the purpose of the test together with the structure of the data collection and the structure of the test. The decisions made in the test plan, for example which questions to use, will also be presented together with its corresponding test plan section. Lastly the main takeaways of the evaluation will be presented, which will lay ground for part of the master thesis conclusions.



Figure 6.1: The current state of the process, to evaluate.

6.1 Test plan

To keep a good structure to the usability evaluation a test plan was created with the structure described in section 2.1.5. The components were produced by the authors to fit the purpose of the testing and was originating from the requirements set in the public user survey, as well as the lo-fi evaluation. All and all, there was a desire to see if the new hi-fi versions were a better solution from the user perspective, and if not, how they could be improved even better.

Purpose of testing

To evaluate the hi-fi prototypes produced in relation to achieved usability and previous set requirements. The evaluation will be carried out with a SUS-scale evaluation and interview questions.

Test research questions

To concretize the purpose into more tangible examples, the following research questions were produced:

1. Which usability score does the posters achieve?
2. How are the elements on the posters received? Illustrations/texts/titles.
3. Are any of the posters more eye-catching than the other posters?
4. What do the test participants think about the effectiveness of providing information through using posters?
5. What do the test participants think about using the QR-code?
6. Is it clear for the test participants who have produced the posters?
7. Is it a good idea to use posters as reminders of security information?

Selection of participants

The total number of participants were 10 people, all of which studied, or had studied for a Master of Science in computer science or information and communication technologies degree. Some of the participants had graduated and had since worked approximately a year within software development. Eight out of the ten participants were male, two were female and the average age was 25,7 years. The participants were recruited through the authors social network, were the potential participants chose a time slot with a booking system in excel.

The participants needed to have completed a security education within the last 5 years in order to participate, which was controlled while booking a time slot with the test person. This was also more defined while answering background questions in the pre-test survey, seen in Appendix A.2.3, where the test person will define how long ago the security education was conducted. All of the participants had completed a IT-security education within the last 2 years, six of them within the last year.

Test procedure

To have an consistent layout to the test, a test procedure scheme was created and can be seen in table 6.1. The form of consent, the manuscript and the pre-test survey can be seen in Appendix A.2.1, A.2.2 and A.2.3 respectively. The test scenarios, which lays the ground for the observation protocol and is the main part of the manuscript is presented in section *Test scenarios* below. If the test participant (TP) did not agree with the first part of the test and signed the form of consent, the test was canceled.

Table 6.1: Table of the different stages conducted in the test, which corresponding material is needed, and the expected time to complete the stage.

Stage	Sub stages	Material needed	Time
Pre test	Meet and greet of test person (TP) Present form of consent Background questions of TP	Manuscript Form of consent Pre-test survey	10 min
During test	1. Fast test 2. Individual tests 3. All posters	Test scenarios Observation protocol	20 min
Debriefing	Supplementary questions	Interview questions	2-3 min

Test scenarios

Based on the research questions a couple of test scenarios were created and can be seen in detail in table 6.2 below. The test was conducted in three different stages, with three different scenarios. Some of the test scenarios are influenced by the lo-fi evaluation, as there were a curiosity for evaluating the set requirements even more. For example, task 3 b) asks the test participant to find out more information (using the QR-code or link), which originates from the lo-fi evaluation task 2. The difference is that this task, in the hi-fi evaluation, investigates and observes the interaction made, as well as the thoughts surrounding the interaction to make, whereas the test participant in the lo-fi test needed to imagine the interaction. The first part of the test was designed to try to find out what the first impression were of the posters, and that's why it was chosen to present them only for a short moment before answering the questions. The thought was to see if any of the posters were eye catching enough to be interesting while only being able to see the posters for a short period of time.

The second part of the test aimed to let the test participant formulate their thoughts about the individual posters in their own time through using a SUS-survey, which can be seen in Appendix A.2.4. The posters were presented in a randomized order between the test participants in order to try to avoid to much influence between the different posters. The main difference to a more traditional usability evaluation was the fact that the SUS and its questions, described in 2.1.4, was adapted to better fit an evaluation of the posters.

In all questions the word system was replaced with poster since the evaluation only regards a poster and not some big technical system. Questions regarding use of the system were modified in different ways where the word *use* was replaced in some way with understanding the information contained within the poster as this is how a viewer would "use" the poster. Modifying the questions might make the SUS results and benchmark less reliable. However, not modifying them might make them hard to understand in the case of evaluating the poster and if the test participant taking the survey interpret the questions wrongly their answers and the resulting SUS score would be completely useless, a fact that weighted heavier than keeping the original questions.

Our modified questions were:

1. I think the poster is a good way to frequently remind the viewer about information.
2. I found the poster unnecessarily complex.
3. I thought the poster was easy to understand.
4. I think that I would need support to understand the poster.
5. I found the various parts of the poster worked together.
6. I thought the poster contained inconsistencies.
7. I would imagine that most people would find the poster easy to understand.
8. I found it cumbersome to take part of the information contained on the poster.
9. I felt confident that I understood the information on the poster.
10. I needed to learn a lot of things to understand the information on the poster.

The third part of the test aimed to get an even deeper understanding of the test participants thoughts surrounding the posters. Here all posters were presented at the same time and the test participant was given time to reflect in relation to the questions asked, and got a chance to interact with the poster, more than visually, through the task of finding out more information.

Test environment and supplies

Locations used: E-huset LTH, Homepal's office and in one of the authors home. The decision to use multiple location were made to reach out to more test participants. The test environment tried to be kept as similar as possible to avoid disturbances in the environment and effects of outside factors on the test. Supplies needed in the testing:

- Computer for notes.
- Computer for surveys.
- Pre-test survey.

Table 6.2: Table of the test tasks conducted in the test, as well as the successful completion criteria.

Task	Scenario	Sub task	Successful completion criteria
1. Fast test	All the posters will be presented in 30 seconds for TP, and then covered.	a) Posters are presented. b) Which elements do you remember? c) Which company has produced the poster?	TP has answered the questions.
2. Individual test	Each poster is presented for TP in a randomized order and SUS evaluated individually.	a) Present poster. b) Fill in SUS-survey.	SUS-survey is filled in for every poster.
3. All posters.	All 5 posters are presented for TP at the same time.	a) Do you recognize anything from your previous IT-security education? b) Find out more information. Thoughts? c) To you prefer any poster? Why? d) What are your thoughts regarding the illustrations? e) Would any of the posters work better if combined with another one? If so, which ones?	1. TP found the QR-code scanned it or found the link and followed it. 2. TP has answered the questions.
Debriefing		a) Do you have anything else you would like to add?	

- Manuscripts.
- Form of consent.
- Observation protocol.
- Timer.
- Recording supplies.

Division of roles

To conduct a good test there was a need for division of roles to make sure that the test participant is given the best possible opportunity to participate in the test. Before the test was conducted the authors divided the roles between each other, and the roles needed are as following:

- **Test manager** - overall responsible for the test, makes sure that the division of roles are clear and that every needed material is in place.
- **Test leader** - guides the test person throughout the test. Presents the test scenarios and asks the interview questions.
- **Responsible for recording and timing** - responsible for making sure that recording is on and times the test.
- **Secretary** - Responsible for taking notes during the test.

Due to the fact that the number of roles are bigger than the number of available authors, there was a need for taking more than one role during the test. Both authors were test managers, whereas the role of test leader were assigned to Emmy as she had a profitable background in usability testing and therefor could optimize the test to achieve the best possible test environment for the test participant. Albin was responsible for recording and timing, as well as secretary.

Data collecting

In table 6.3 the different data that was hoped to be collected in the evaluation is defined. As the evaluation does not contain any clear objective and quantitative data, for example minimum time of completion or number of errors, the column is left empty. Thus, the evaluation had a heavy focus on the users thoughts and experiences while interacting with the posters rather than quantitative and objective data, which is shown in the table through the fact that the main part of data collection is subjective. The objective data collection parts is incorporated through test observation, which will be conducted through taking notes and audio recording the tests.

Table 6.3: Table of collection of data corresponding to research question.

Research question number	Objective /quantitative	Objective /qualitative	Subjective /quantitative	Subjective /qualitative
1			SUS-survey	
2		Test observation	SUS-survey	Task 1; 3c), 3d)
3		Test observation		Task 1b); 3c)
4		Test observation	SUS-survey	Task 3a), 3b), 3e)
5		Test observation		Task 3b)
6		Test observation	Task 1c)	Task 1c)
7		Test observation	SUS-survey	Task 1; 3a)

6.2 Pilot test

The pilot test was conducted on a student that studies within similar educational as the authors, and with a good knowledge and understanding of usability testing and interaction design.

The pilot test gave several insights about the evaluation and modifications were made. The biggest change was the fast poster assessment switching places with longer individual assessment of the posters. This was due to the test subject being able to recall almost all parts of all posters after having looked at them individually for a prolonged period of time.

The pilot test also showed that while shuffling the order in which the posters are shown is probably a good idea poster 2 and 5 are very similar and should not be shown directly after each other or with just one poster in between. This is because when shown consecutively to our pilot test subject he answered the exact same for both posters. Showing them further apart from each other might give some insight to how the test subjects are biased depending on how many posters they were previously shown.

The last insight that was drawn was that numbering the posters visually would help both the participants and us in knowing which poster is currently being looked at.

6.3 Test results

Below, the test results for the usability evaluation will be presented together with the analysis originating in the test research questions from the test plan in section 6.1.

Firstly the SUS-score for each individual poster will be presented, followed by an analysis of the score and related comments made by the test participants. Lastly more general test observations will be presented, with focus on the overall impression of the components of the posters.

6.3.1 SUS-evaluation

In this section the mean SUS-score for each poster will be presented, discussed and analysed. The score for the individual poster per test participants can be seen in table 6.4, whereas the mean SUS-score for the posters can be seen in table 6.5.

Table 6.4: SUS-score for each test participant.

Test participant	Poster 1	Poster 2	Poster 3	Poster 4	Poster 5
M25	27.5	100	77.5	92.5	100
M27	42.5	92.5	82.5	100	100
M24	35	72.5	75	100	52.5
M26	87.5	97.5	97.5	90	82.5
F24	75	62.5	55	82.5	80
M25	22.5	87.5	65	85	87.5
M27	95.5	100	100	100	100
M27	30	75	95	97.5	95
M26	85	62.5	72.5	70	80
F26	32.5	90	75	100	97.5

Table 6.5: mean SUS-score for the posters.

Poster	mean SUS-score
Poster 1	53.25
Poster 2	84
Poster 3	79.5
Poster 4	91.75
Poster 5	87.5

Poster 1

Poster 1 got a mean SUS-score of $M=53.25$, which is a number that is below the accepted benchmark of 68 points, a score that is considered to be the average accepted score for usability. This could mean that this poster is not considered good, but rather bad, usability wise and should be investigated if it should be used in further iterations of the posters.

While the QR-code was very big and according to most participants signified that there was more information to find, they also pointed out that a lot of interest in the subject would be needed from their part in order to try and scan the code.

The participants often mentioned that while the poster was very eye-catching it suffered greatly from not having any information on it and that the title text could be interpreted, or even misinterpreted, in many ways. Some mentioned that they interpreted the title that could be part of a work environment campaign, for example for sexual harassment in the workplace or similar. The fact that the title was ambiguous and the poster was lacking in information affected the scoring of several of the SUS-questions as many of them consisted of statements regarding understanding in some way. One of the participants summarized this lack of information making the poster hard to understand as the poster being "*Unnecessarily complex in its simplicity*".

Poster 2

Poster 2 got a mean SUS-score of $M=84$ making it the third highest rated one. While it was deemed as one of the more eye-catching ones it was often referred to as a worse version of poster 5.

The biggest critiques of poster 2 was that the illustration were perceived as to signify getting an idea rather than being reminded of something. Another critique point was the fact that the title was hard to read when it was broken up in two lines and could rise confusion for the observer.

As with most other posters the content of the information was considered good and the fact that the information had bold parts conveying the most important parts helped in quickly understanding the purpose of the poster as a whole.

Poster 3

Poster 3 received a mean SUS-score of $M=79.5$ which is right on the border between good and very good. It was generally praised for having good design, especially with the poster being divided into three segments. Important to point out though is that the participants often thought it was the least eye catching of the posters as it was missing a title. However, many of them thought that three pieces of information was superior to two, a fact that was proved to be true in poster 4 as well.

The illustrations connected to the information were over all thought to represent the information in a good way, but one participant felt that the green colour of the illustrations did not signify warning enough. Two participants pointed out that they thought the middle illustration to not represent the text connected to the illustration and would rather see a more representative illustration connected to "*Do not click*". This was also pointed out by the same two participants in their evaluation of poster 4.

As most of the participants preferred QR-codes to links almost all of them noted the absence of a QR-code on this poster.

Poster 4

Poster 4 received the highest SUS-score of the posters, a total score of $M=91.75$. This was also reflected in when the participants were asked about which poster they thought was the best

due to the fact that many of them answered poster 4.

When reflecting about the poster almost all participants mentioned the numbers to be a contributing factor to the good usability and during the quick glance test many remembered *"a poster with three steps on it"*, a fact that proves its eye catching effect. Another part of the poster that received praise was the title which had white text on a green background and was deemed more eye-catching than the titles with green text on white backgrounds.

Poster 5

Poster 5 got a SUS-score of $M=87.5$, a bit higher than the very similar poster 2. When comparing the two, most participants attributed poster 5 being better to the more easy to read title as well as a better illustration which the participants felt signified Homepal telling or teaching you something. One participant however felt that the illustration did not convey that the information on the poster was about safety. This poster was also mentioned as the favourite by several test participants.

6.3.2 General observations

The overall impression of the design of the posters were good. Many test participants found the posters to be visually pleasing, but one test participant found the green colour to not signify warning enough. The illustrations were commented to be a good eye catcher without taking attention from the purpose of the text, with the reservation of the facts brought up in the individual posters analysis above.

All test participants used a QR-code when asked to retrieve more information. When asked about their opinions about it some liked the combination of both QR-code and link, but most found the QR-code to be the easiest way to fast get to know more about the subject. When discussed further some pointed out that iOS-users have a more easily accessible QR-scanner in their phone camera, whereas the Android-users need to use an external app. However, non of the participants found the need for using a external app to be frustrating because of their every day encounter of QR-codes. Some pointed out that they thought that an older generation might not find the use of the QR-code to be as easily accessible as for them self, and therefor would like a combination of both QR-code and link.

To archive a first impression from the test participants the first part containing of a short viewing of the posters was included. This due to test the eye catching effect of the elements in the different posters, the result of which is explained in the individual poster evaluating above. Another factor investigated in this part were the fact if the participant observed the creator of the poster, in this case Homepal. All except two had observed who had produced the poster, one of which had observed the green theme of the logo but not the name of the organisation.

Possible combinations

The question of combining posters sparked very different answers. Four of the participants wanted to combine the elements of different posters. These participants often wanted to combine the more extensive information from poster 3 with the title and numbers on poster

4. Another common combination was the numbers and information of poster 4 with the design of poster 5.

When asked about combining the posters by having two next to each other the answers differed a lot but could be summarized as choosing one of the posters with more information and combining it with one of the more eye catching ones. This often resulted in either combining poster 3 with the participants favourite poster or poster 1 with any of the others.

6.3.3 Main takeaways

To summarize the test result the following conclusions were made:

- Poster 2-5 all have an above average SUS-score, which makes them suitable for future use. Poster 2, 4 and 5 stands out even more and have a score above the benchmark considered to be good usability wise.
- It is important to not let the eye-catching effect overpower other factors such as understanding the context in order to achieve a good usability.
- A combination of being eye-catching, using bold headlines and or colours, and still give the observer step-by-step information about the subject as well as give the observer a chance to find more information is a good approach usability wise while designing a poster.
- QR-code is a common and usable approach for the user to find more information.
- Illustrations is a fruitful way of balancing the text on the posters and give even more context to the observer.
- Posters are a good approach usability wise to remind and provide security information.

Chapter 7

Discussion

In this chapter the work of the master thesis' different parts will be discussed. Firstly the four different interaction design phases, identify requirement, create alternatives, create prototypes and evaluation, will be discussed. After this the research questions will be answered and lastly in this chapter the possible future work will be presented.

7.1 The design phases

7.1.1 Identify requirements

The identify requirements phase was one of the longest and most complex phases of the thesis as this formed the thesis' direction. The phase consisted of a lot of researching, both through literature studies and threat modeling but also through discussing and exploring the user's needs.

To identify which threats to focus on the threat model STRIDE was employed. It was argued that while STRIDE is very simple it would give us sufficiently advanced answers. It felt like this was the case as the process resulted in two clear threats, one of which could be mitigated somewhat using design. While this process as a whole was a success it was definitely influenced by the fact that the authors knew that only potential threats that could be mitigated with design were relevant. This resulted in threats not being pursued further when design mitigation felt improbable and some threats possibly being undiscovered and therefore not investigated properly.

Upon entering the exploration of the user's needs phase the experienced mindset was that there would be extensive possibilities to interact and interview the users of Homepal's platform. Sadly this was not the reality of the user base, both due to the fact that Homepal is a small and growing company that just recently brought users into their apps, but also due to the fact that it was not easy to reach the current users of the system due to summer vacation. The lack of possibilities to talk and investigate the user base made it clear that the thesis

needed data from other sources, in this case Homepal's employees as well as external input on the concept as a whole. The external source in this case was the public survey, where one of the most interesting results of both the public and the user base survey was the fact of the wide spread and commonly use of a security education within the workplace and the need for it to be followed up in some way. The surveys and the input of Homepal's employees, in relation to the literature study, resulted in valuable insights for the thesis and shaped the process towards the end result of exploring security awareness posters as a concept.

Even though the focus was aimed towards posters, the education of the users is a crucial part of the security awareness process, a fact that was backed to be important by both surveys conducted as well as the literature study, and is still a big part of this thesis. The fact that the thesis aimed the graphical work to posters was a result of a curiosity in previous use of posters as a reminder of education, especially in relation to the requirements found in the survey of the users graphical and content demands. This decision was also made in combination with the reality of the time resources available, as an extensive work with a graphical education would not be possible within the time frame of the thesis.

7.1.2 Create alternatives

The main goal of the create alternative-phase was to concretize the concepts found in the identification of the requirements. This phase involved a lot of brainstorming and using the authors knowledge in design and usability to interpret the requirements found in the previous phase. The concepts were translated into lo-fi posters and evaluated, which gave the thesis valuable input on the concept of using posters as well as a confidence boost that the concept was something worth looking into further.

The use of a prototype made by paper and colour pens was an easy approach to concretize the concepts of the posters, but had its downsides. The use of example text and example illustration sometimes made it hard for the evaluation test participants to really understand the thoughts behind the posters, a fact that made it important to include real text and relevant illustrations in the hi-fi prototype. Also, as this phase was conducted during peak summer vacation in Sweden it resulted in the fact that the evaluation did not having as many participants as intended at first. This was solved by introducing a digital version of the test, which gave the additional input needed to move forward in the design process.

7.1.3 Produce prototypes

When entering the produce prototype stage the project had a good base to stand on. The design process brought together the identified requirements and the knowledge from the lo-fi prototype evaluation and translated these into a hi-fi prototype using to the digital tool called Figma. To interpret the results and evolve from the lo-fi prototype a lot of brainstorming was conducted in this phase as well, similar to the create alternative-phase.

In contrast to the lo-fi prototype the hi-fi prototype aimed to have a more specific security awareness approach to both colours, illustrations and text content. As Homepal provided their graphical profile, which was extensive, there was not really any difficulties in choosing the graphical profile and from that design the posters using it. In regards to the text content a lot could be found using trusted Swedish governmental sites in combination with the usability heuristics, which made it easier to ensure that the info provided was legitimate.

The hardest part of producing the hi-fi prototype was to ensure the eye-catching effect before printing the posters, as it was not possible to pre-print every iteration due to economical reasons. After brainstorming and evaluating the posters internally a couple iterations it was found to be crucial to for example increase the thickness of the frames and the size of the titles to ensure the eye-catching effect. Even though, it should be pointed out that the printed version did not really reflect the correct colours but was reasoned to be good enough for evaluating as the test participant would not be familiar with the digital version and did not affect the eye-catching elements or any other factors to an extent worth re-printing.

7.1.4 Evaluation

To evaluate the changed concepts and the more specific information an user evaluation was conducted of the hi-fi posters. The evaluation was carried out on ten different participants as semi-structured interviews where the participants answered questions and performed tasks in relation to the posters.

While planing the test procedure it was realized that the usability evaluation method of SUS-scoring needed to be altered to fit this evaluation. The standard SUS-scoring uses statements regarding the interaction between a user and a system, but in the poster case the interaction is not that obvious as for example between a user and a interactive system. An alteration choice was therefor made to decrease the complexity for the test participant and increase the chance of understanding the statements in the given context better and as a result get a better evaluation.

In relation to the fact that there is not a clear interaction between the user and the product resulted in not having any timed and/or other quantitative data to analyse. The SUS-part provided some quantitative data, but was also mainly subjective as it was provided by the test participant. Though, in this evaluation case it was not that relevant to need a lot of quantitative objective data as the evaluation focused mainly on qualitative data with the test participants' opinions in focus. This in combination with the SUS-score was found to provide a high quality evaluation of the posters.

One of the biggest reflection points from the evaluation was the fact that ten different test participants could have such different opinions in some cases and very similar in other. Some had very strong opinions regarding details such as the placements of elements or the content of the text, which resulted in a lot of interesting insights. The fact that the evaluation did not only contain positive feedback, but also constructive examples of change, was a nice surprise in order to achieve a good evaluation of why or why not a concept works.

The most complex aspect of the evaluation was the fact to tackle the participants' comparison between the posters. The choice to randomize the order of the posters presentation helped some, but many participants remembered the posters from the quick viewing of the first task or compared to the previous viewed posters. This is a fact that is hard to prevent as it is human to compare interactions to previous experiences and a conclusion was made that it did not affect the over all result of the evaluation enough to be a big problem.

In summary, the evaluation phase gave the thesis interesting and important content in order to conclude and finish the project, as well as contributed towards the discussion of future work in the area.

7.2 Research questions

Which security threats are most prominent for a platform such as Homepal's?

The threats against the platform was modeled using STRIDE and the most prominent threats found were spoofing, mainly in the form of phishing, and tampering. Spoofing is relevant since it is not the Homepal employees using their products, which puts a lot of the responsibility of detecting phishing attempts on the customers. Tampering is relevant since some of their products are designed to complement missing data, which is then used to make different decisions, making the system prone to tampering and the potential damages quite extensive. It was decided that spoofing was the threat where design and user experience could be utilized to mitigate the threat in the most meaningful way.

Which design concepts exists that could help in mitigating the threats?

There are multiple different possible design concepts that could be utilized for mitigating different threats. The combination of education and interaction design elements is a common approach, one that could be varied in many ways with for example video games, board games or interactive educational elements.

As security threats evolve, so does the need for maintaining a proactive security position by the employees at a company. To ensure a high security awareness the employee needs to keep their knowledge up to date, and therefor a reminder could be utilized as a way of repeating the education. In this thesis the use of a poster as a reminder was explored even further, a design element that been used before in Covid-19 purposes and could be a possible approach to mitigate phishing security threats.

How are these design concepts best utilized to achieve a more secure system/platform/product?

In Homepal's case a poster could be a good way to mediate the importance for the user to keep alert while using their system. This since they are not able to remind the user in person post security awareness education and therefor needs a way of mediate the information.

As the user base survey confirmed that Homepal's current customers already have a security awareness education the current situation for Homepal would be to collaboration with the customer to ensure a good translation from their education to the reminder of the poster. If the customer does not have an education, for example in the case that Homepal has a new customer and/or the customer did not answer the user base survey, the process of security awareness would needed to start with an education. A possible future case would perhaps be for Homepal to develop an own security awareness education using interactive design elements, a product that would ensure Homepal that the users of the system has an adequate education and standardize it in relation to the posters.

7.3 Future work

To continue the research regarding security awareness education there are multiple approaches that could be chosen. The fact that the process of security education could be intertwined and adapted to the specific company and/or workplace in question could be developed into multiple different interesting future research area.

A dream scenario would be to test the effectiveness of using posters as a reminder after a security awareness education in the thought environment of an office. A possible approach to this is using two departments and test the effectiveness of reminding the employees after a security awareness education. One of the departments would use the posters as reminders and the other department would not be exposed to the posters and/or any other reminding element. The approach would then be evaluated and analysed after a certain amount of time to see if there were any differences in the achieved awareness by the employee. A requirement for this approach would be that the company in question is big enough to ensuring that the employees do not encounter a reminder by mistake. This could be avoided by for example using different geographical locations or restrictions in the work place building.

Another future research approach could be to test the need for exchanging the posters and how long the posters stay relevant for the users. It would be interesting to evaluate if the users stop looking at the posters after a certain amount of time and how a frequent change of the posters would affect the effectiveness of the providing of information for the user.

Additionally, it would be interesting to explore the effects of the chosen placement of the posters. In the Covid-19 poster cases the posters were often placed in connection to the need of the information, for example if the poster informed about washing your hands it was placed in connection to the sink. In the security awareness poster case, the placement would be in connection to the users computer and/or desk. The more general Covid-19 posters informing about staying at home etc has been seen to be placed on the toilet door in height of the person sitting on the toilet, on a coffee machine or on an entry door, an approach that perhaps could be interesting thing to try out in a future research study in relation to the security awareness posters.

Chapter 8

Conclusion

This thesis explored the possibility of using design and user experience to mitigate security threats. The threat model STRIDE was used to identify possible threats against the Homepal data platform. The threat modeling was done in a high-level fashion as it was argued that going deep and investigating implementation details would take an unnecessary amount of time and result in threats that could not be mitigated using design. The high-level threat modeling process resulted mainly in two threats, tampering and phishing. Phishing was chosen as a focus as it was argued to be the most promising in being mitigated using design.

Having found a threat to focus on possible mitigations were investigated by reading about phishing and different things related to design and user experience that could be used to combat it. Since phishing often is mitigated by educating a user base of a system in detecting and avoiding phishing attempts it was decided to look further into education. A survey was created to investigate the thoughts on security education by the general public and the survey was modified to investigate the presence of security education at Homepal's customers. The survey showed that most people go through some sort of security education in their workplace, but that their education is rarely or never followed up. This is in contrast to the general opinion that following up an education is very important. The results from the survey sent to Homepal's customers also matched that of the general survey.

With these results in mind the possibility of following up an education using posters to remind the users of the things learned during the education was investigated. This idea originated from the informational posters used during the Covid-19 pandemic.

The final conclusion was that posters is a prominent way to use user centered design to remind the users of a system about security critical things and several poster alternatives were created. Therefore the thesis recommends Homepal to use posters as a complement to education to remind their users of the importance of security awareness, as well as help them to resolve and act on suspicious activities.

Bibliography

- [1] Cybersecurity & Infrastructure Security Agency. *Understanding Denial-of-Service Attacks*. Original date: 2009-11-04. URL: <https://www.cisa.gov/uscert/ncas/tips/ST04-015>.
- [2] Roland Akselsson. *MÄNNISKA, TEKNIK, ORGANISATION OCH RISKHANTERING*. Institutionen för Designvetenskaper, Lunds Tekniska Högskola, 2014.
- [3] Hussain Aldawood and Geoffrey Skinner. “Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review”. In: *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*. 2018, pp. 62–68. DOI: 10.1109/TALE.2018.8615162.
- [4] Faisal Alotaibi et al. “A review of using gaming technology for cyber-security awareness”. In: *Int. J. Inf. Secur. Res.(IJISR)* 6.2 (2016), pp. 660–666.
- [5] Amazon. *AWS Shield: Managed DDoS protection*. Accessed: 2022-06-16. URL: aws.amazon.com/shield/.
- [6] Duncan Ki-Aries and Shamal Faily. “Persona-centred information security awareness”. In: *Computers & Security* 70 (2017), pp. 663–674.
- [7] Leon Bernard et al. “Minimizing Cognitive Overload in Cybersecurity Learning Materials: An Experimental Study Using Eye-Tracking”. In: *IFIP World Conference on Information Security Education*. Springer. 2021, pp. 47–63.
- [8] John Brooke. “SUS: a ‘quick and dirty’ usability scale”. In: *Usability evaluation in industry* 189.3 (1996).
- [9] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. “INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS.” In: *MIS Quarterly* 34.3 (2010), 523–A7. ISSN: 02767783. DOI: 10.2307/25750690.
- [10] Rachna Dhamija, J. D. Tygar, and Marti Hearst. “Why phishing works”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Apr. 2006. DOI: 10.1145/1124772.1124861.

- [11] Victoria Drake. *Threat Modeling*. Accessed: 2022-06-16. URL: https://owasp.org/www-community/Threat_Modeling.
- [12] Lynette Drevin et al., eds. *Information Security Education for Cyber Resilience. 14th IFIP WG 11.8 World Conference, WISE 2021, Virtual Event, June 22-24, 2021, Proceedings*. IFIP Advances in Information and Communication Technology: 615. Springer International Publishing, 2021. ISBN: 9783030808648.
- [13] Mete Eminağaoğlu, Erdem Uçar, and Şaban Eren. “The positive outcomes of information security awareness training in companies—A case study”. In: *Information security technical report* 14.4 (2009), pp. 223–229.
- [14] Folkhälsomyndigheten. “Undvik att bli Smittad och att Smitta Andra (affisch) - folkhälsomyndigheten”. In: Article number: 20087, Accessed: 2022-05-12. 2021. URL: <https://www.folkhalsomyndigheten.se/publicerat-material/publikationsarkiv/u/undvik-att-bli-smittad-och-att-smitta-andra-affisch/>.
- [15] *Getting Started*. Accessed: 2022-05-17. URL: <https://letsencrypt.org/getting-started/>.
- [16] *Goal 4: Quality education*. Accessed: 2022-07-14. 2022. URL: <https://www.globalgoals.org/goals/>.
- [17] *Goal 9: Industry, innovation and infrastructure*. Accessed: 2022-07-14. 2022. URL: <https://www.globalgoals.org/goals/>.
- [18] Google. *Chrome devtools*. Accessed: 2022-05-17. URL: <https://developer.chrome.com/docs/devtools/>.
- [19] Google. *Secure your site with HTTPS*. Accessed: 2022-05-17. URL: https://developers.google.com/search/docs/advanced/security/https?hl=en&visit_id=637883051488150489-80896169&rd=1.
- [20] Stephen Hart et al. “Riskio: A Serious Game for Cyber Security Awareness and Education”. In: *Computers & Security* 95 (2020), p. 101827. ISSN: 0167-4048. DOI: <https://doi.org/10.1016/j.cose.2020.101827>.
- [21] *Homepal| Samla in, hantera och använd fastighetsdata*. Accessed: 2022-05-17. URL: homepal.se.
- [22] *Homepal platform*. Accessed: 2022-05-17. URL: platform.homepal.se.
- [23] Dragan Ilic and Nicholas Rowe. “What is the evidence that poster presentations are effective in promoting knowledge transfer? A state of the art review”. In: *Health Information & Libraries Journal* 30.1 (2013), pp. 4–12.
- [24] Federal Bureau of Investigation. *Internet Crime Report 2021*. Accessed: 2022-05-17. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.
- [25] *ISO 9241-11:2018(en) Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts*. Accessed: 2022-09-21. 2018. URL: <https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-2:v1:en>.
- [26] Pooya Jaferian et al. “Heuristics for evaluating IT security management tools”. In: *Proceedings of the Seventh Symposium on Usable Privacy and Security*. 2011, pp. 1–20.

- [27] Page Laubheimer. “Beyond the NPS: Measuring Perceived Usability with the SUS, NASA-TLX, and the Single Ease Question After Tasks and Usability Tests”. In: Accessed: 2022-05-17. 2018. URL: <https://www.nngroup.com/articles/measuring-perceived-usability/>.
- [28] John Leach. “Improving user security behaviour.” In: *Computers & Security* 22.8 (2003), pp. 685–692. ISSN: 0167-4048. DOI: 10.1016/S0167-4048(03)00007-5.
- [29] David LeBlanc. *DREADful*. Original date: 14.08.2007. URL: https://docs.microsoft.com/en-us/archive/blogs/david_leblanc/dreadful.
- [30] James R Lewis and Jeff Sauro. “Item benchmarks for the system usability scale.” In: *Journal of Usability Studies* 13.3 (2018).
- [31] James R. Lewis. “The System Usability Scale: Past, Present, and Future.” In: *International Journal of Human-Computer Interaction* 34.7 (2018), pp. 577–590. ISSN: 10447318.
- [32] Charlotte Magnusson et al. “User Study Guidelines”. In: *Hapti Map Consortium* (2009).
- [33] Abraham Maslow and KJ Lewis. “Maslow’s hierarchy of needs”. In: *Salenger Incorporated* 14.17 (1987), pp. 987–990.
- [34] Microsoft. *The STRIDE Threat Model*. Original date: 12.11.2009. URL: [https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878\(v=cs.20\)](https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)).
- [35] Microsoft. *Threat Modeling*. Accessed: 2022-06-16. URL: <https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling>.
- [36] Erik L Moore et al. “A Layered Model for Building Cyber Defense Training Capacity”. In: *IFIP World Conference on Information Security Education*. Springer. 2021, pp. 64–80.
- [37] Jakob Nielsen. “10 Usability Heuristics for User Interface Design”. In: Updated Nov. 15, 2020, Accessed: 2022-05-17. 1994. URL: <https://www.nngroup.com/articles/ten-usability-heuristics/>.
- [38] Donald A. Norman. *The design of everyday things*. Basic Books, 2013. ISBN: 0465072992.
- [39] Opeyemi Osanaiye, Kim-Kwang Raymond Choo, and Mqhele Dlodlo. “Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework”. In: *Journal of Network and Computer Applications* 67 (2016), pp. 147–165. ISSN: 1084-8045. DOI: <https://doi.org/10.1016/j.jnca.2016.01.001>. URL: <https://www.sciencedirect.com/science/article/pii/S1084804516000023>.
- [40] OWASP. *Repudiation Attack*. Accessed: 2022-05-17. URL: https://owasp.org/www-community/attacks/Repudiation_Attack.
- [41] Jennifer Preece, Yvonne Rogers, and Helen Sharp. *Interaktionsdesign bortom Människadator-interaktion*. Translation by Lena Svensson and Maria Drangel. Studentlitteratur AB, 2016. ISBN: 978-91-44-09207-2.
- [42] Maria Rosala. “Rating Scales in UX Research: Likert or Semantic Differential?” In: Accessed: 2022-05-17. 2020. URL: <https://www.nngroup.com/articles/rating-scales/>.

-
- [43] Jeffrey Rubin and Dana Chisnell. *Handbook of usability testing: how to plan, design and conduct effective tests*. John Wiley & Sons, 2008.
- [44] *Security and Privacy Controls for Information Systems and Organizations*. Tech. rep. Sept. 2020. DOI: 10.6028/nist.sp.800-53r5.
- [45] *The Global Goals*. Accessed: 2022-07-14. 2022. URL: <https://www.globalgoals.org/goals/>.
- [46] *Threat Modeling Manifesto*. Accessed: 2022-06-16. URL: <https://www.threatmodelingmanifesto.org/>.
- [47] Tillväxtverket. *Digitalisering i svenska företag*. Original date: 2018-06. URL: <https://tillvaxtverket.se/vara-tjanster/publikationer/publikationer-2018/2018-06-21-digitalisering-i-svenska-foretag.html>.
- [48] Merriam Webster. *Repudiate*. Accessed: 2022-05-17. URL: <https://www.merriam-webster.com/dictionary/repudiate>.
- [49] Jackson E. Wynn. *Threat Assessment and Remediation Analysis (TARA)*. Original date: 2014-10. URL: <https://www.mitre.org/publications/technical-papers/threat-assessment-and-remediation-analysis-tara>.

Appendices

Appendix A

A.1 Public survey

* = mandatory question

Part 1 of 6

Introduction

Hello! We are two students who are currently finishing our studies, and are therefore writing our master thesis at Lunds Tekniska Högskola. The master thesis explores how design can be utilized to increase the security awareness within IT-security and this survey is an important step in our process towards getting a hold of what different people thinks about the subject.

The survey will consist of 3 steps, whereas the first step includes background questions, the second step includes questions about experience in IT-security education, and lastly the last step contains questions about using posters as an informational tool. The survey can be completed regardless of previous experience in the subjects.

Some of the questions will be designed as statements with a scale from 1-5 to take in to consideration, whereas 1 = strongly disagree and 5 = strongly agree. 3 can be seen as a neutral answer.

The survey is anonymous and takes approximately 5 minutes to complete. Thank you for your participation!

Questions

How old are you? *

Which gender do you identify as?*

- Woman
- Man
- Non binary
- Other...

My current occupation is: *

- High school student
- Post high school student (University/College)
- Unemployed
- Employed
- Employed within the IT sector
- Other...

Statement: I think that I have a high level of technical competence. *

- | | | | | |
|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| 1 | 2 | 3 | 4 | 5 |
| <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Strongly disagree | | | | Strongly agree |

Part 2 of 6 IT-security education

Introduction

IT security is an more and more topical subject within both the working and the every day life sector. This fact encourage many companies to choose to educate their employees within the subject. With IT-security we mean the general subject of security surrounding computers and internet, external and internal digital security threats, spoofing etc.

Questions

Have you ever undergone an IT-security education at a workplace? *

- Yes
- No
- Do not remember

Part 3 of 6 Specific for education

If the participant answered "Yes" in the previous part, they will be sent to this page.

Introduction

Since you have undergone an IT-security education we would like to hear more about your opinions about the experience. With IT-security we mean the general subject of security surrounding computers and internet, external and internal digital security threats, spoofing etc.

Questions

How was the IT-security education designed? *

- Digital education
- Attendance of lecture/education in person.
- Board or card game
- Computer or video game
- Other...

What did you find positive with the education?

What did you find negative with the education?

Was something missing?

Statement: I found the education to be worthwhile. *

- | | | | | |
|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| 1 | 2 | 3 | 4 | 5 |
| <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Strongly
disagree | | | | Strongly agree |

Statement: I found the information in the education to be assimilative. *

- | | | | | |
|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| 1 | 2 | 3 | 4 | 5 |
| <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Strongly
disagree | | | | Strongly agree |

Was the education followed up in some way? *

- Yes
- No
- Other...

If yes, how was it designed and how long after was it followed up?

Enter text here...

Do you have anything else you would like to add about your previous experience in IT-security education?

Enter text here...

Part 4 of 6 General about design of educational elements.

If the participant answered "No" or "I do not remember" in the part 3, they will be sent directly to this part. If they answered "Yes" they will be sent here after completing part 4.

Introduction

Regardless if you have gone through an IT-security education we would like your opinion in the following statements regarding a potential design of an education. With IT-security we mean the general subject of security surrounding computers and internet, external and internal digital security threats, spoofing etc.

Questions

Statement: I think it is important with tangible and relevant examples in an education. *

1	2	3	4	5
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Strongly disagree				Strongly agree

Statement: I would like interactive elements in an education. For instance clickable elements or drag-and-drop questions. *

1	2	3	4	5
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Strongly disagree				Strongly agree

Statement: I think that education is an important part in the work towards increasing IT-security threats awareness. *

1	2	3	4	5
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Strongly disagree				Strongly agree

Statement: I think that it is important to follow up an education after a while. *

1	2	3	4	5
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Strongly disagree				Strongly agree

Do you have any additional opinions regarding the design of educational elements and/or it's connection to IT-security?

Enter text here...

Part 5 of 6

Introduction

Using posters as a way of increasing the awareness surrounding a subject is a more and more common approach in our every day life. For instance, it could be adds for a music festival, political messages or governmental information.

During the Covid-19 pandemic posters has been used as a tool for increasing awareness and spreading information about the importance of washing ones hands, stay at home while sick etc. This phenomenon has made us curious if there is a way of applying this on IT-security, more specifically increasing the awareness on IT-security.

Two examples of Covid-19 posters from Folkhälsomyndigheten is presented below.



Figure A.1: Posters retrieved from Folkhälsomyndigheten's web page.

Questions

Have you seen these, or similar, posters during the Covid-19 pandemic? *

- Yes
- No

Part 6 of 6 Specific for education

If the participant answered "Yes" in the previous part, they will be sent to this page. If they answered "No" they will be asked to send in the survey.

Introduction

Since you have seen these, or similar, posters we would like to know more about your opinions about using the posters as a way of spreading information. This part will mainly consist of statements, but since we want to know more about your opinions there will be space for sharing your potential motivation to your answer in between the statements.



Figure A.2: Posters retrieved from Folkhälsomyndigheten's web page.

Questions

Statement: I found the posters to be an effective way to spread information. *

1	2	3	4	5
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Strongly disagree				Strongly agree

Possible motivation:

Statement: I found the posters to be a good way of reminding and/or bring awareness to important information. *

A.2 Usability evaluation

A.2.1 Form of consent

This is a written form of consent for participating in this test session. The test will be conducted in Swedish and consist of different tasks and/or reflective questions. We encourage you to speak your mind out loud and not to hesitate to ask questions during the test. The purpose of our thesis is to investigate how design and user experience could be used to mitigate security threats. Throughout the thesis we have aimed our research towards an investigation using posters as a way to remind and bring awareness to cyber security issues, and today we want to use our time with you to evaluate our results.

Before we start we need you to agree to the following:

- I understand that this is not a test of my skills and/or knowledge but rather a test of the product presented.
- If I at any time want to stop the test and/or skip any part of the test I am entitled to do so.
- I agree that my test will be audio recorded and documented in written text. Any audio records will be deleted upon completion of the thesis.
- I understand that the results and documentation of this test will be anonymised and presented in our master thesis.
- I understand that if I at any time want the test data deleted or ask any questions I can contact em4146ed-s@student.lu.se or al5826sv-s@student.lu.se
- I understand the purpose of the thesis and my participation.

Date & Place:

Name:

Signature:

A.2.2 Manuscript

This is the manuscript that was followed in the usability evaluation. In addition to this, the table for test scenarios, table 6.2, and the procedure followed the table of test procedure, table 6.1.

Introduction:

"Welcome to this usability test! Before we begin we would like you to read through this document and sign it."

Present form of consent

"If you have any questions, do not hesitate to ask them."

After TP has signed form of consent:

"Now we can move on to our first survey, which will contain some short background questions."

Present pre-test survey

After TP has completed the pre-test survey:

"Next we will complete three different test stages together. I would like to remind you that this is not a test of your knowledge or abilities, but a test of the product, and I will once again encourage you to speak aloud while conducting the tests.

Albin will take notes during the test and as mentioned in the form of consent we will audio record your test session starting now."

Start audio recording

During the test scenarios:

Present the test scenarios according to the table and ask eventual questions.

Finishing part:

"Thanks for participating in this test!"

Stop audio recording

A.2.3 Pre-test survey

* = mandatory question

Introduction

Thanks for participating in this evaluation! Before completing this survey, please make sure that you have signed the *Form of consent*.

Questions

How old are you?*

Which gender do you identify as?*

- Woman
- Man
- Non binary
- Other...

My current occupation is: *

For example *Student Msc in Computer science* or *Employed within the IT sector*.

When was the last time you participated in an IT-security education?*

- Less than a year ago
- 1-2 years ago
- 3-5 years ago

A.2.4 SUS-survey

* = mandatory question

Introduction

Start with filling in which poster you have in front of you, then study the poster and answer the statements below.

Questions

Which poster do you have in front of you?*

- Poster 1
- Poster 2
- Poster 3
- Poster 4
- Poster 5

I think the poster is a good way to frequently remind the viewer about information.*

- | | | | | |
|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| 1 | 2 | 3 | 4 | 5 |
| <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Strongly
disagree | | | | Strongly agree |

I found the poster unnecessarily complex.*

- | | | | | |
|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| 1 | 2 | 3 | 4 | 5 |
| <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Strongly
disagree | | | | Strongly agree |

I thought the poster was easy to understand.*

- | | | | | |
|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| 1 | 2 | 3 | 4 | 5 |
| <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Strongly
disagree | | | | Strongly agree |

I think that I would need support to understand the poster.*

- | | | | | |
|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| 1 | 2 | 3 | 4 | 5 |
| <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Strongly
disagree | | | | Strongly agree |

I found the various parts of the poster worked together.*

1	2	3	4	5
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Strongly disagree				Strongly agree

I thought the poster contained inconsistencies.*

1	2	3	4	5
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Strongly disagree				Strongly agree

I would imagine that most people would find the poster easy to understand.*

1	2	3	4	5
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Strongly disagree				Strongly agree

I found it cumbersome to take part of the information contained on the poster.*

1	2	3	4	5
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Strongly disagree				Strongly agree

I felt confident that I understood the information on the poster.*

1	2	3	4	5
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Strongly disagree				Strongly agree

I needed to learn a lot of things to understand the information on the poster.*

1	2	3	4	5
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Strongly disagree				Strongly agree

Appendix B

Prototypes

Posters

Below are all the posters in a larger, more easy to view format.

B.1 Lo-fi



Figure B.1: Lo-fi poster 1

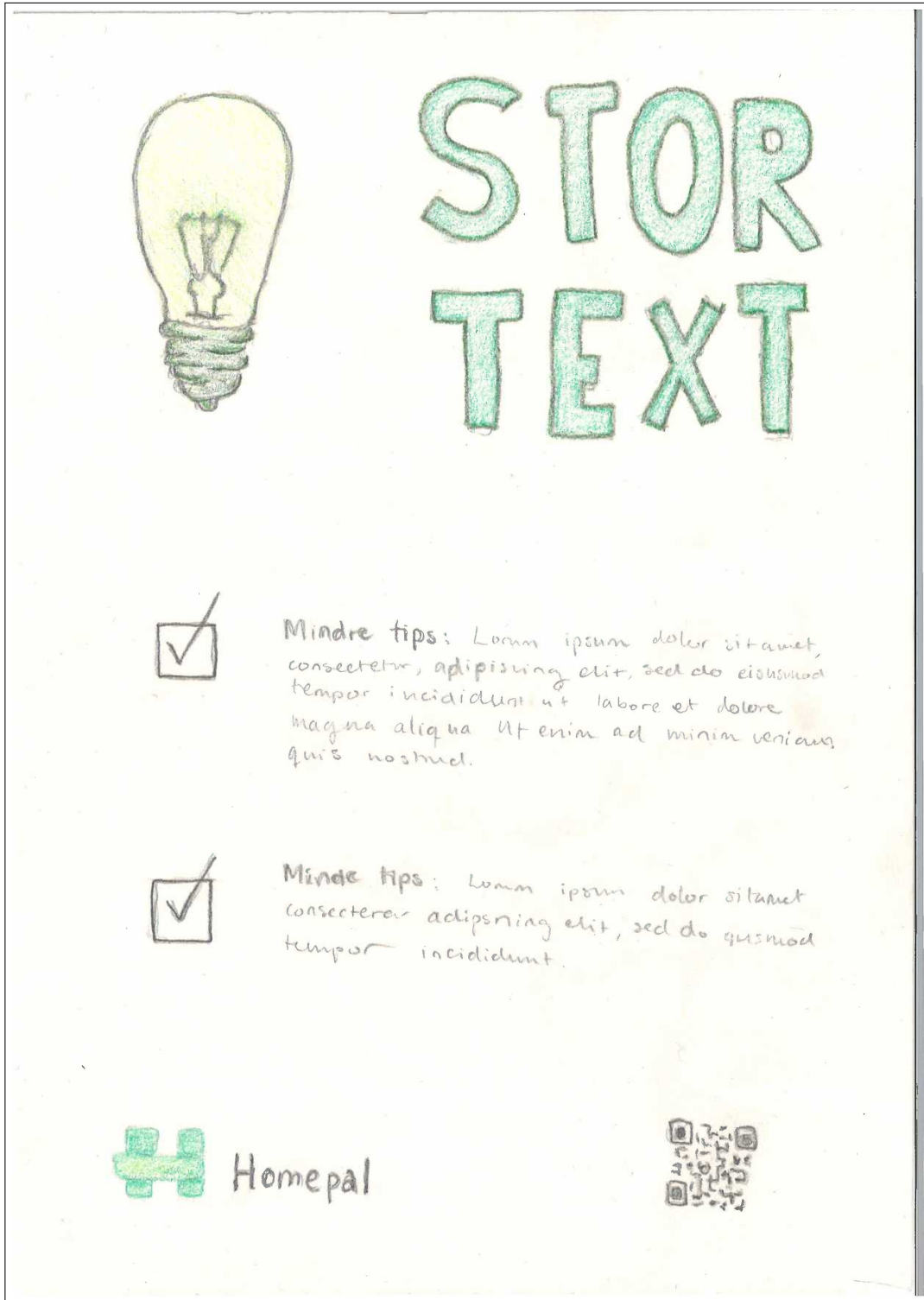


Figure B.2: Lo-fi poster 2

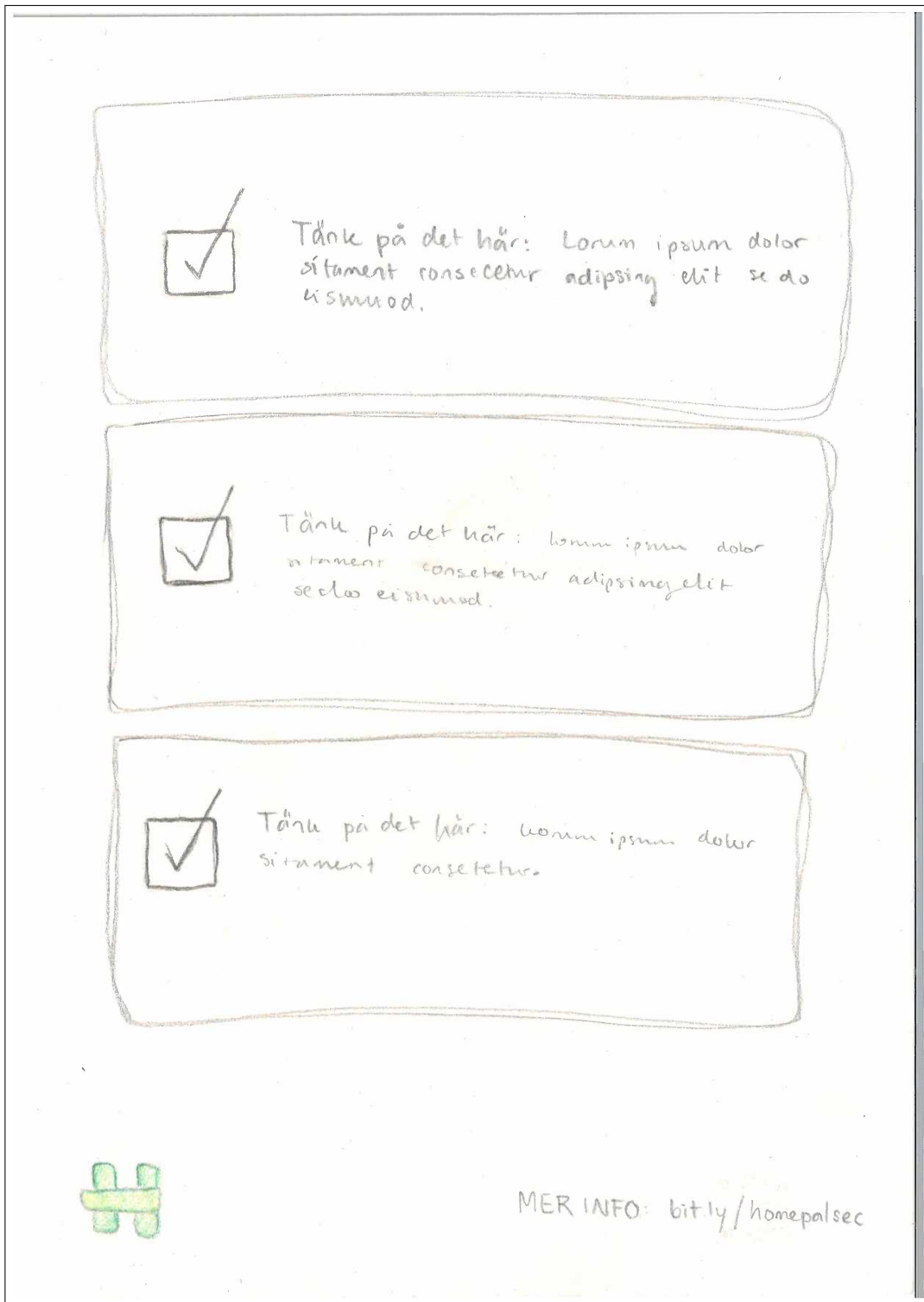


Figure B.3: Lo-fi poster 3

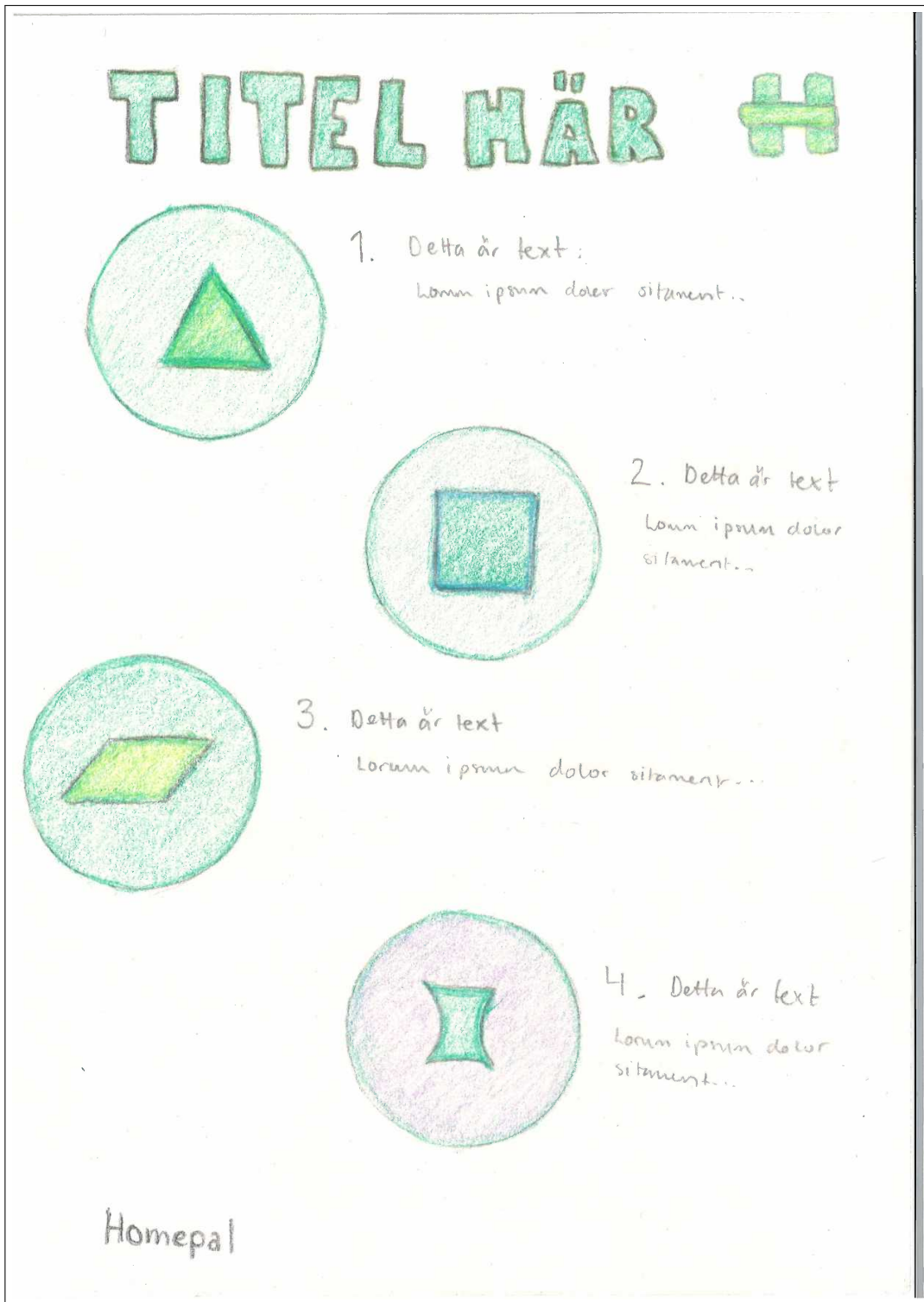


Figure B.4: Lo-fi poster 4

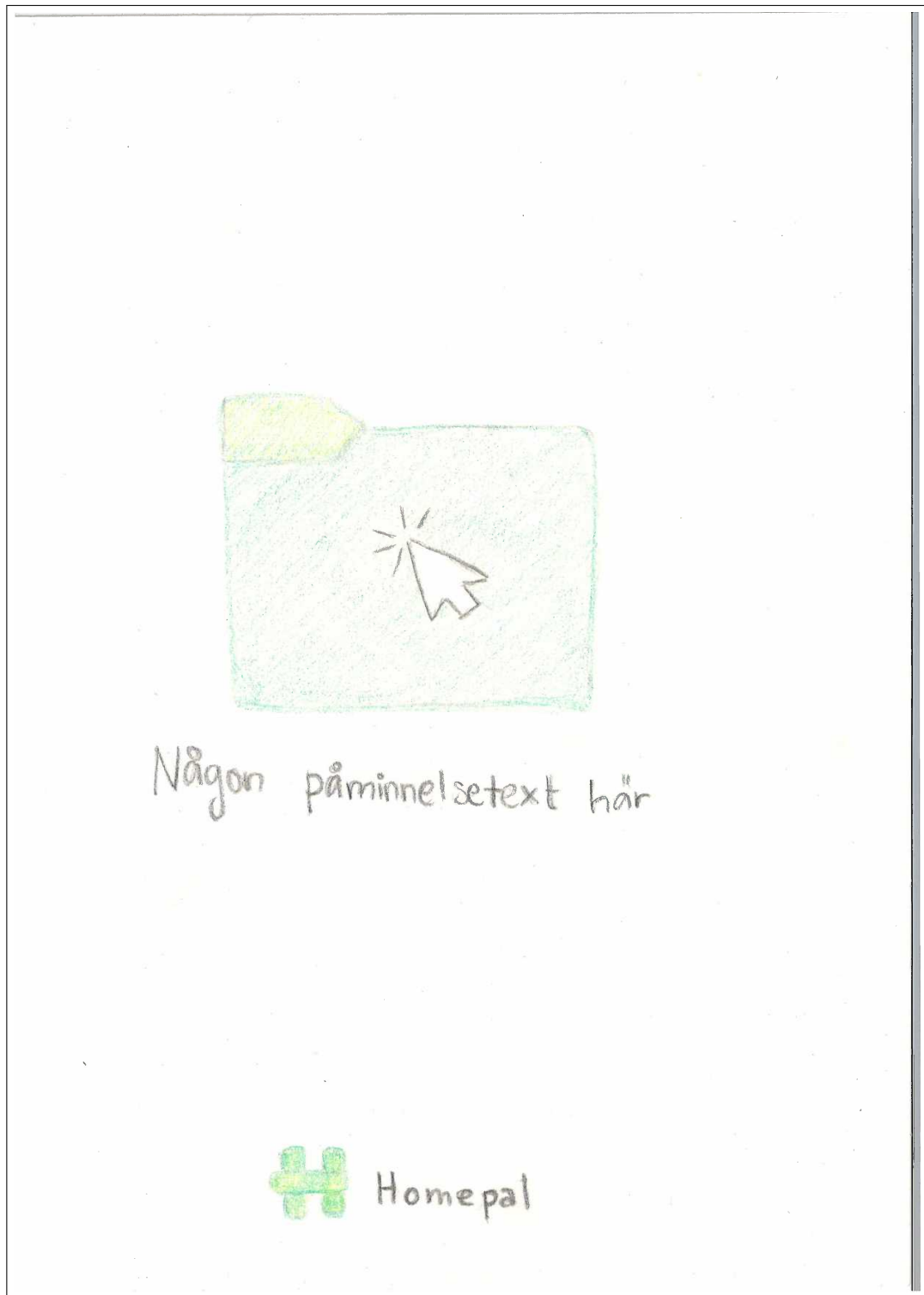


Figure B.5: Lo-fi poster 5

B.2 Hi-fi



Figure B.6: Hi-fi poster 1



The poster features a large green lightbulb icon on the left, with a person standing next to it. To the right, the words "PHISHING" are written in large, bold, black letters. Below this, a light green box contains two sections of text, each preceded by a green checkmark icon. At the bottom left is the Homepal logo, and at the bottom right is a QR code with the text "Mer info:" above it.

PHISHING

Klicka bara på kända länkar
Tänk på att vara försiktig med att klicka på länkar, bilagor eller ladda ned program som kommer via mejl, sms eller olika webbsidor särskilt när du inte känner till avsändaren.

Alla gör misstag! Är du anställd i en organisation och misstänker skadlig kod eller tror att du klickat på en olämplig länk ska du genast rapportera till din it-funktion.
Har du angett inloggningsuppgifter för att få åtkomst till information, ändra dem omedelbart.

 **Homepal**

Mer info: 

Figure B.7: Hi-fi poster 2

The poster is divided into three horizontal sections by a light green background that tapers from top to bottom. Each section contains an illustration and a text block.

Top section: An illustration of a woman in a green shirt and black pants standing next to a large white envelope with a green document icon inside. To the right, the text reads: "Granska mejlet noga innan du öppnar en bifogad fil eller klickar på en länk. Är meddelandet förväntat? Brukar avsändaren uttrycka sig på det här sättet?"

Middle section: An illustration of a man in a dark suit and a woman in a green shirt standing next to a large white laptop. The laptop screen shows a red warning triangle and a document icon. To the left, the text reads: "Var vaksam och klicka inte om meddelandet innehåller uppmaningar att till exempel lämna ifrån dig kort- eller kontonummer eller lösenord, ber dig ladda ner bilagor eller programvara eller uppmanar dig att agera snabbt."

Bottom section: An illustration of a woman in a green shirt and a man in a dark suit standing next to a large green shield with a white checkmark. To the right, the text reads: "Om du fattar misstankar bör du **verifiera avsändaren** via andra kanaler än de som anges i utskicket eller avstå från att öppna/klicka. Om du är anställd i en organisation ska du kontakta din it-funktion."

Bottom left: The Homepal logo, consisting of a green cross-like symbol followed by the word "Homepal" in a bold, black, sans-serif font.

Bottom right: A rounded rectangular box containing the text: "Mer info: bit.ly/homepalsecurity"

Figure B.8: Hi-fi poster 3

PHISHING



1
Granska mejlet. Är meddelandet förväntat?
Brukar avsändaren uttrycka sig på det här sättet?



2
Klicka inte om avsändaren ber dig om kort- eller kontonummer eller lösenord, att ladda ner bilagor eller uppmanar dig att agera snabbt.



3
Vid misstankar, **verifiera avsändaren** via andra kanaler än utskicket, exempelvis din IT-funktion.



Homepal

Mer info:



Figure B.9: Hi-fi poster 4



Figure B.10: Hi-fi poster 5