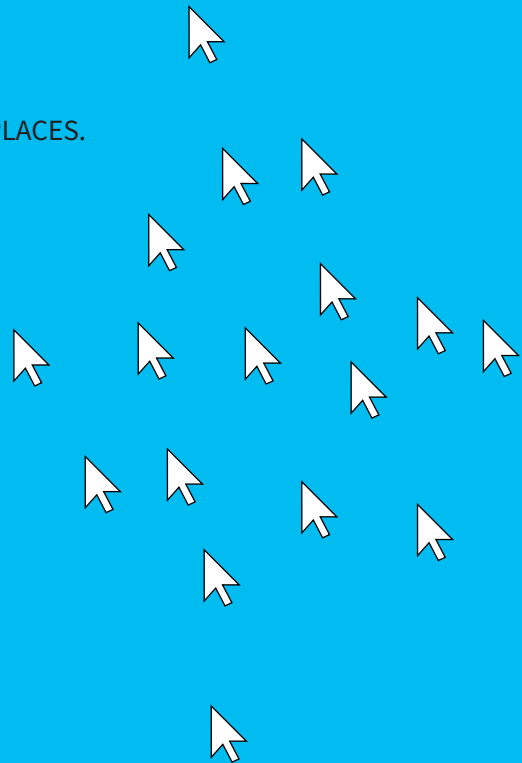


DIGITAL SECURITY CULTURE

INTERACTIVE LEARNING FOR NORWEGIAN WORKPLACES.



Diploma candidates:

Inés Andrea Høvring Delgado and Marte Wang Engen

Main supervisors:

Mosse Sjaastad and Einar Sneve Martinussen

Secondary supervisor:

Natalia Agudelo

Master's thesis in Interaction design
The Oslo School of Architecture and Design
Fall 2018

Abstract

A secure digital environment is influenced by the systems we use and the people who interacts with it. Although media frequently reminds us of the emerging digital threats, we tend to skip even basic precautions to protect our digital property.

This project explores the human and cultural aspect of digital security in Norwegian workplaces, and how interactive learning can support employees in making good risk assessments. Through simulated game scenarios employees increase their knowledge and train their ability to identify the risks in digital space. Our aim is to make employees aware of how their digital behaviour affects security within a business and why they should take responsibility.

CONTENT

00. Introduction

- 03 Abstract
- 06 Excecutive summary
- 09 Personal Motivation

01. Frame

- 12 Relevance
- 14 Actors and Initiatives
- 16 Need for competence boost
- 18 Scoping the project
- 20 Working with Culture
- 24 Target group
- 28 How employees are exploited

02. Research

- 34 The experts
- 38 Evaluating digital security culture
- 40 Focus area
- 41 Digital security drill
- 42 How to build a security culture
- 44 Gaining user insight
- 50 Analysis

03. Define

- 54 The human factor
- 64 Need for designers
- 65 Different culture=different challenges
- 66 Bad systems

04. Explore

- 70 Brainstorming and Ideation
- 74 Choosing direction

05. Develop

- 78 Existing learning tools
- 82 Requirements
- 84 Learning goals
- 85 Interactive learning
- 86 Concept directions

06. Deliver

- 96 Design proposal
- 98 Main pages
- 112 Design elements
- 114 Features
- 123 Further explorations
- 124 Flowchart
- 126 User testing
- 130 Visual Identity
- 132 Service onboarding
- 134 Service journey

07. Conclude

- 138 Reflections

EXECUTIVE SUMMARY

Context

Every day, billions of people around the world use the internet to share ideas, trade with one another and keep in touch with family, friends and colleagues. The digital transformation influence our daily lives, creating opportunities we can barely imagine. At the same time, it brings new challenges where our privacy and identity becomes more vulnerable. 'Cybercrime' is on a rise, costing the Norwegian society an average 19 billion NOK yearly (Malmedal and Røslie, 2016).

Contribution

Data breaches are not solely caused by limitations of technical solutions, they are often results of 'mistakes' caused by human factors or by bad user experiences. This interaction design diploma explores digital security from a human centered approach where it aims to encourage users to take control over their digital property.

Design proposal

Our final design proposal is an interactive learning program on digital security for employees in Norway. The purpose is to teach the users about why digital security is important, and to train their ability to do risk assessments in digital space. This is done through a scenario game where the user is exposed to various security challenges and where he or she makes choices to progress.

The solution provides a learning experience that differs from existing solutions in several ways: By adapting content to the employees working sector, by introducing scenarios, and by breaking with the stereotypical tone of voice and aesthetics of the cybersecurity industry. With this diploma we hope to put digital security on the agenda and inspire designers to play a bigger role within the field.

Process

Throughout the different phases of our project we have applied various techniques and methods. In order to get a holistic view on digital security culture, we sought expertise from the fields of ICT security, psychology, design, and sales. Their knowledge and experiences together with user insight from employees, helped us gain a deeper understanding of digital security challenges within a workplace. Their input was important throughout the whole design process and built the foundation for our design proposal.

How to read the report

The report is structured as separate design phases in order to make the process easy to follow for you as reader. In reality the phases have overlapped and has been far from the linear process.

00. Introduction



PERSONAL MOTIVATION

Design contribution

For us the diploma was an unique opportunity to acquire new knowledge and develop our skills as interaction designers. As we had limited previous knowledge about the topic of 'cyber security', we asked ourselves: which role can interaction designers play within this field? Our profession works with digital solutions and we were curious about the security aspects of it.

Male dominated field

Within cybersecurity women represents only 20% of the industry (Sausalito, 2018). The lack of diversity motivated us even more to work with the topic.

01. Frame

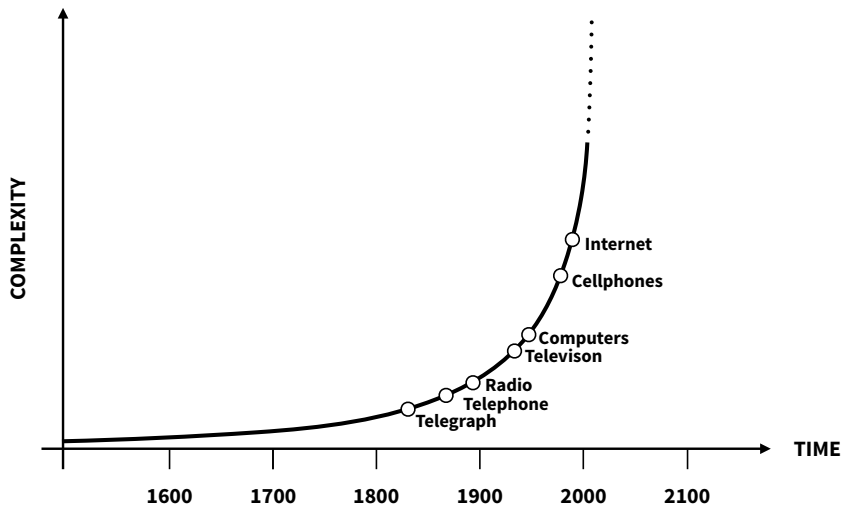
In this first chapter we will present the frame of our project and explain why it is relevant for the Norwegian society. We will then introduce our chosen target group and context.

The methods we used:

- Desktop research
- Zip analysis
- Expert interviews
- Personas

RELEVANCE

The growth in technology has accelerated the last 100 years. Norway is one of the most digitised societies in the world, making us an attractive goal for digital crime. To follow the rapid change we need to understand the threat landscape and how to stay secure in digital space.



GRAPH: <https://www.webolutions.com/denver-executives-seek-stay-ahead-curve/>

“A prerequisite for good digitization is that it must happen within a framework where the ICT security is maintained in all sectors and at all levels.”

Prime Minister Erna Solberg, March 2018

The Norwegian society

The digitised society has made social functions, services, production and infrastructure easier to control, while the ability to execute routines manually are vanishing. As a result, society has become more reliant on the the digital services to function normally and there is a growing need to ensure the security of our digital property (Malmedal and Røslie, 2016).

New national strategy for ICT security

In march, The Norwegian government presented a new national strategy for ICT security as they are promoting the use of digital solutions in both public and private companies. According to the Prime Minister Erna Solberg, digitisation provides great opportunities for both efficiency, competitiveness and, not least, the creation of new jobs. However it also leads to a change in society's risk image demanding that ICT security must be taken care of in all sectors and in every aspect (Solberg, 2018).

As society is becoming reliant on digital services we believe that designers should participate more in the work of ensuring digital security.

ACTORS AND INITIATIVES

These are the actors that has been relevant to our project. We met up with NorSIS, NSM and CLTRe who gave us valuable input in the research phaze, they will be mentioned later on in the report.

The government

The government are making efforts to **strengthen ICT security** in both **public** and **private sectors** to meet the digital security challenges. (Regjeringen, 2017).

NSM

The National Security Authority

NSM has a **mission to detect, alert and assist** in incidents **handling attacks against socially important functions**.

NSR

The Norwegian Business and Industry Security Council

NSR is an organization whose **purpose** is to **prevent crime against industries**. They deliver the Norwegian computer crime and **data breach survey** (Mørketallsundersøkelsen) as well as arranging courses and seminars.

NorSIS

The Norwegian Center for Information Security

NorSIS is part of the government's overall commitment to information security in Norway. They aim to **ensure** that **information security** is a **natural part of everyday life** for both **public** and **private businesses**. NorSIS functions as a **knowledge sharer** with the intention of creating awareness, influence attitudes and change security behavior in Norway's population.

CLTRe

CLTRe is a private company that **delivers a toolkit used to measure security culture**. It offers a software that provides deep insights of the human factor in a business.

The Norwegian National Security Authority (NSM) conducted an e-mail attack against a Norwegian government in April, 2018.



9 out of 10 employees clicked the link



5 out of ten activated the simulated malware



3 out of 10 specified their login credentials

NEED FOR A COMPETENCE BOOST

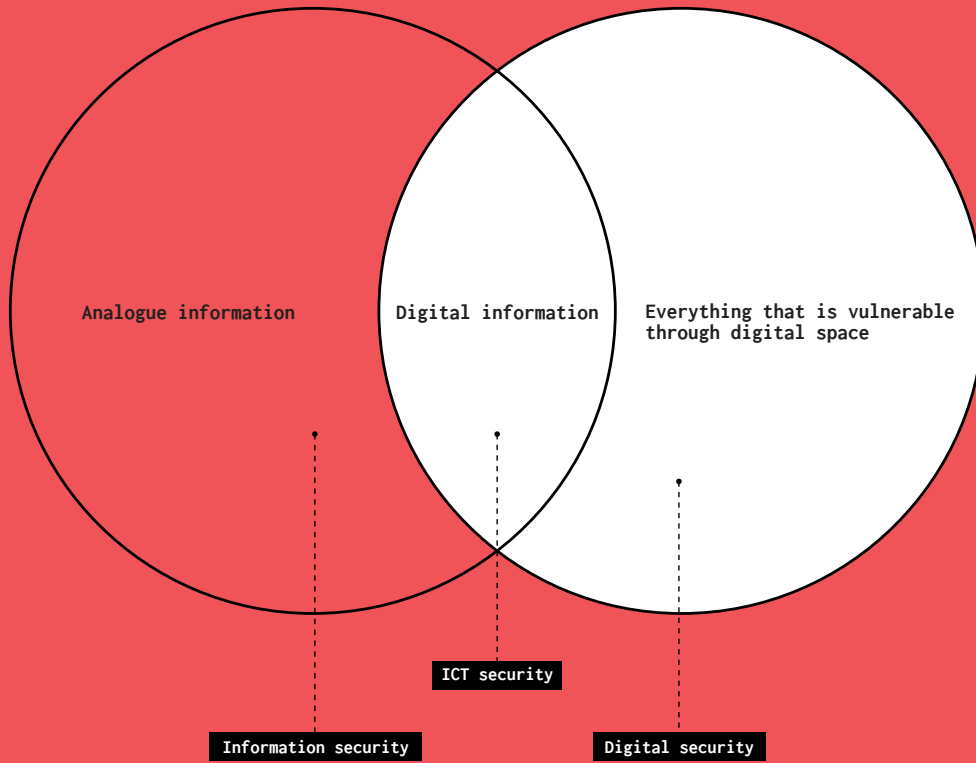
In april 2018, NSM conducted an e-mail 'attack' against a Norwegian government administration and was designed to capture the employees attention. The result of the attack was that nine out of ten employees clicked the link while half of them activated the simulated malware. In addition to this three out of ten employees specified their login credentials (Nielsen and Strøm, 2018).

The test gave us an indication on how uncomplicated attacks can be an easy way to access information and systems. We wanted to investigate how employees are used as an entry point.

"Seemingly small events and 'banal' details can trigger large, serious security-threatening events"

The Norwegian National Security Authority, 2018

01. Framing



SCOPING THE PROJECT

Terminology

Our project focuses on the field of cybersecurity which is about protecting computers, networks, programs and data from unauthorized access or attacks (Solms and Niekerk, 2013).

People often mix the terms Cybersecurity, ICT (Information and Communication technology) security and Information security although they do not refer to the the same definition. Information security has to do with securing both analogue and digital information, ICT security refers to information that is vulnerable through digital space and Cybersecurity is everything that is vulnerable through digital space (Solms and Niekerk, 2013).

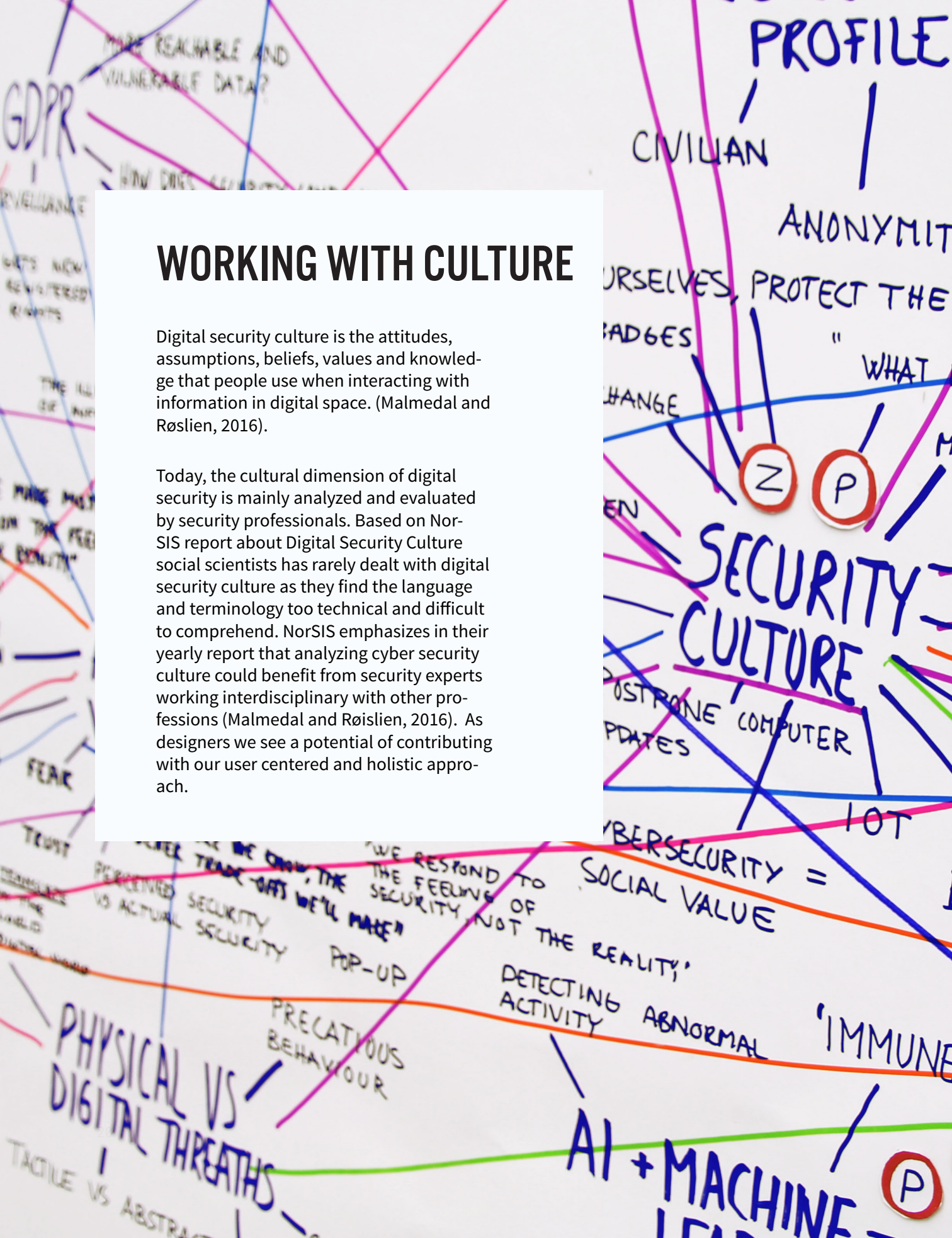
Rephrasing the term

Cyber is a word that is broadly used to explain various computer and internet related concepts. But what does it really mean? In our project we have chosen to rename the term 'cybersecurity' to 'digital security' as it is more descriptive for the time we live in and more understandable for people.

WORKING WITH CULTURE

Digital security culture is the attitudes, assumptions, beliefs, values and knowledge that people use when interacting with information in digital space. (Malmedal and Røslie, 2016).

Today, the cultural dimension of digital security is mainly analyzed and evaluated by security professionals. Based on NorSIS report about Digital Security Culture social scientists has rarely dealt with digital security culture as they find the language and terminology too technical and difficult to comprehend. NorSIS emphasizes in their yearly report that analyzing cyber security culture could benefit from security experts working interdisciplinary with other professions (Malmedal and Røslie, 2016). As designers we see a potential of contributing with our user centered and holistic approach.



What makes a digital security culture?

In this project we met NorSIS and CLTRe who translates these factors into ‘cultural dimensions’ that are used to describe digital security culture. Norsis’ and CLTRe security dimensions have been important for us in order to address key challenges within digital security.

NorSIS:

Community
Leadership and control
Trust
Risk perception
Optimism for technology
Competence
Interest
Interest

(Malmedal and Røslie, 2016).

CLTRe:

Norms
Compliance
Responsibility
Communication
Cognition
Attitudes
Behaviour

(Roer and Dr. Petric, 2017).

Reducing to four key dimension

To frame our project we prioritized four key dimensions. These were selected by listing down the risky behaviour we addressed in our research phase and by connecting them to NorSIS and CLTRe dimensions. We found that behaviour patterns, competence, trust, and risk perception were the most relevant dimensions that established a base for our further design work.

Risk perception

Interpretation of risk associated with online activities, and whether the user take responsibility for the security.

Behaviour patterns

What users do in digital space which has direct or indirect impact on digital security culture.

Trust

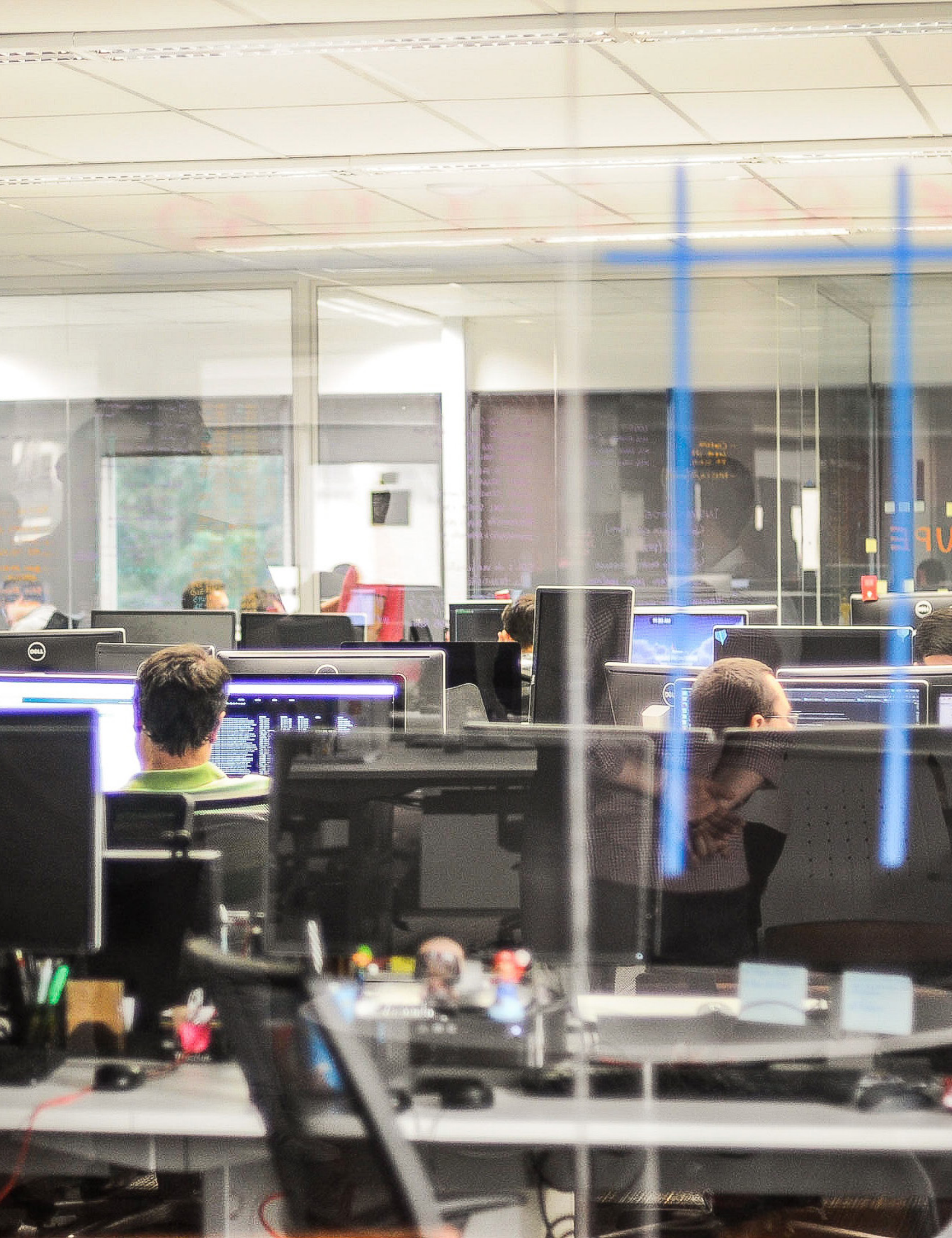
In which degree people have trust in digital services and people in digital space.

Competence

How aware people are of the digital security risks and how much they know about security related issues.

Project statement:

HOW CAN DESIGN IMPROVE DIGITAL SECURITY CULTURE?



TARGET GROUP

Norwegian workplaces

A workplace houses people from different cultures, genders, and age groups that shapes the company culture where security behaviour and habits are established. The workplace provides us with a natural structure where security measures can be introduced to people.

Employees

Our target group are employees working in Norway who are active users of technology and frequently communicate through e-mail. They are especially vulnerable to digital crime as they process sensitive information such as social security numbers, health data, banking details or internal business secrets. This information is important to safeguard as it can lead to big consequences for both the company and their clients if they end up in the hands of people with bad intentions.

Personas

A workplace consists of different people with various demographics, and they all affect the security within a company. NorSIS told us that there are differences in level of competence about technology and digital security within a company, and between companies. With this in mind, we decided to look closer at people's attitudes and behavioural patterns to understand who we are designing for. This created a base for our further ideation and concept development. We based the personas on insights from design probes, expert interviews, as well as reports and statistics from NSM, CLTRe and NorSIS.



Applying key dimensions

To understand who we are designing for we used the four key dimensions to create personas. The dimensions to the right highlights their characteristics.

Paranoid Pia

Is part of the older generation, has little experience with technology and is afraid to make mistakes in contact with digital space. Paranoid Pia is a loyal employee who follow rules to the point.

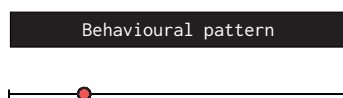
Competence





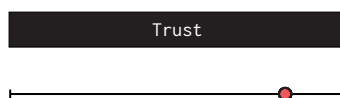
Millennial Mia

Is part of the younger generation, has great confidence in using technology and often experience security measures as a hurdle. Millennial Mia is a frequent user of social media and shares information uncritically.



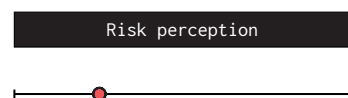
Naive Nils

Has a high trust in people and have a tendency to be naive when meeting cynical powers in digital space. Naive Nils is very service minded and has little interest in technology.



Confident Claus

Is tired of revisiting digital security issues and does not care much about the pleas from the IT department. Confident Claus is comfortable with using technology, and might overestimate his risk assessment abilities.



HOW EMPLOYEES ARE EXPLOITED

According to the The European Union Agency for Network and Information Security, 74% of the digital threats entered a system through an e-mail attachment or link in 2017. Threats as these are referred to as 'Phishing' attacks and they aim to infect systems with malware or manipulate users to share sensitive information that can be exploited. (ENISA, 2017).

What is Phishing?

Phishing attacks are often used as an entry point for infecting systems with malware such as ransomware, banking trojans and backdoors. Although companies usually filter out phishing emails with help from technology, the attackers constantly change their tactics, making detection more difficult (NSM, 2018).

Phishing attacks often succeed because they use a technique called 'social engineering' where they target people and exploit their human characteristics to gain access to resources.

Social Engineering

Social engineering is a technique with an unfriendly purpose used to manipulate the recipient into sharing sensitive information. By using this method criminals exploit human trust and pressure, persuade, flatter, seduce, reward or lure employees to expose their business values (NSM, 2018).

CEO scam

The consequences of social engineering can be serious as the employees are used for accessing information. NSM warns against these type attacks, particularly director fraud where the scammer pretends to be from management and asks them to pay a bill or transfer money to an account overseas (NSM, 2018).

The consequences

By clicking a link or opening an attachment in a phishing email, the victim's computer can be infected with harmful software known as 'malware'. The intention with malware is to gain access or cause damage to a computer or network. There are many types of malwares. The most common one is the 'Trojan Horse' which is a software that disguises itself as a legitimate tool and tricks the user into installing it. Once installed, hackers can potentially access all information including logins and passwords details, banking details, files and system information. In other cases the attachment or link in the phishing email causes the user to get 'Ransomware'. This malware locks the users computer until they pay a ransom to unlock it. The payment is often delivered in bitcoin or other cryptocurrencies. Hospitals, school districts, state and local governments, law enforcement agencies, small businesses, large businesses have all been victims of ransomware (Palmer, 2018).



Who are the criminals

When googling 'cyber criminal' or 'hackers' as they often are referred to, google will give you image results of a man wearing a black hoodie sitting in front of his computer while executing cyber crime. This image of a cyber criminal does not entirely tell the true story. The practice has become far more organized and sophisticated than what google present to us. In reality modern cybercrime is large-scaled and can be compared to corporate businesses, that are often more organized that the security experts who works to stop them. They have organizational structures with defined roles just like a regular company (Badrick, 2018).

02. Research

In this part we present you information about digital security culture that has been relevant to our project. We then take you through methods and techniques used to gain user insight, followed by analysis and summary of our findings.

The methods we used:

- Desktop research
- Expert interviews
- Design probes
- Memes & comics

THE EXPERTS

In order to get knowledge about digital security and the challenges people face, we talked to experts working within the field of information security, IT, and Psychology. This was valuable in order to get reflections and different perspectives on the topic of digital security culture.



Tonje, NorSIS

Tonje works as supervisor in NorSIS and has a background as product developer and project manager. She is occupied with creating good user experiences and believes that bad experiences is due to bad solutions and not the people using them.

“There is no such thing as a good or bad security culture. A health worker has other challenges than an software developer, thus security measures must be tailored.”



Roar Thon, NSM

Roar Thon is the Vice President for the Security Culture in NSM. He is a known speaker and travels around the country to raise awareness towards the topic of digital security. In his talks he aims to make people understand how what we do in digital space has consequences in our own lives. To make these risks understandable he use situations from physical life to explain digital ones.

“We call it cybercrime, but it’s not something you can avoid by the sole use technology. It’s about awareness and processes, where the human plays an important role.”



Anette Rimereit, Skill

Anette works with sales in an IT consultancy company called Skill where she focuses on microsoft technology. Her aim is to identify what is relevant for each business considering all the distractions and opportunities that technology brings. Cybersecurity is a part of the services that Skill delivers.

“If security affects the employees too much, they will find ways to go around the systems.”



Mona Halland, Mindshift

Mona works with business development and user experience in 'Mindshift'. She has a masters degree in Psychology from NTNU and 15 years of experience working with user focused processes and service design. She's a specialist in organizational psychology, process management and change management. Mona is committed and genuinely interested in the interaction between people, the environment, and technology.

"You don't smell fire, or experience digital security the way you do in real life. Because of this, we tend to relax, and become careless to our online actions."



Kai Roer, Cltre

Kai is an author, lecturer and consultant on information security. He is the co-founder and CEO of the CLTRe Toolkit. The Toolkit is used to measure security culture, which is a requirement for all businesses after the GDPR regulation is initiated in may. The software gives a company a security score based on a 5 min survey done by each employee.

"In order to change digital security culture you need to start measuring it to evaluate if the preventative initiatives has had any effect."



Frode, Head of IT at AHO

Frode is the head of IT at AHO and is responsible for information security. He defines the routines for how to deal with safety and writes an annual report where he analyses the risks, vulnerabilities and suggest initiatives for the upcoming year.

"It's important that everyone takes responsibility for their own digital security."

EVALUATING DIGITAL SECURITY CULTURE

In Norway, digital security culture is evaluated by the use of surveys, and false e-mail phishing attacks within businesses. We have met with two actors - 'Norsis' and 'CLTRe', with different aims and views on how to approach cyber security culture evaluation.

Evaluating security on a national level

NorSIS argues that security culture is a collection of behaviour, values and attitude that cannot be reduced to a score. As Tonje told us during an interview, "There no such thing as a bad security culture".

Measuring security within a business

CLTRe on the other hand, argues that security measurements are insignificant if we cannot evaluate the effectiveness of them. Their business is based on a software that can reduce a companies security culture to a single score based on a short survey handed to the employees. In that way they can find areas where the business needs to improve their security skills (Roer and Dr. Petric, 2017).

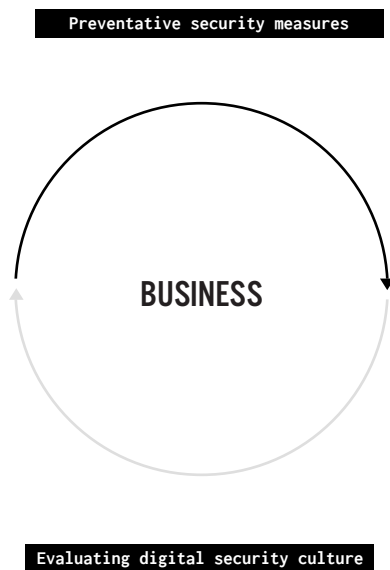
GDPR

In May 2018, the General Data Protection Regulation (GDPR) is initiated. In the new regulation, all businesses are required to evaluate the effectiveness of technical and organization measures (Roer and Dr. Petric, 2017).

“...implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk...and a **process for regularly testing, assessing and evaluating the effectiveness** of technical and **organisational measures for ensuring the security** of the processing.”

EU GDPR Article 32

FOCUS AREA



Focus on preventative measures

As explained , there are several ways of evaluating digital security. However, as interaction designers we think our human centered approach, methods and skillsets are most needed in developing preventative security measures rather than tools for evaluation.

“Employees usually don’t get any digital security training.”

Anette Rimmereit, Skill

DIGITAL SECURITY DRILL

During our research phase, we looked at security solution for different problem spans. We wanted to see if there were any resemblances or differences between the activities, and if we could translate some of the initiatives to the context of digital security.

In conversation with Anette who is an IT consultant, we were informed that digital security training is given a low priority and that employees usually don't get any training on the topic. This was confirmed by our probes as very few of the participant had received any course on digital security.

Firedrills

In comparison, all businesses in Norway are required to conduct firedrills at least once a year. During a drill an alarm is set of and everyone has to evacuate the building. The purpose of fire drills is to ensure that everyone knows the evacuation plan in case of an emergency. We wonder why this kind of activity hasn't been applied for digital security when a data breach is just as likely of occurring as a fire emergency? Based on this insights we saw the potential of executing digital security drills equivalent to a safety drill.



HOW TO BUILD A SECURITY CULTURE

As we do not have experience with working with culture change, we sought advice from experts within psychology and design that had experience with changing organisation cultures. Their insights created the foundation for one of the design proposals in the concept development.

Group conformity (Kai Roer)

Told us that it is quite easy to change peoples habits by using psychological mechanisms. He pulled out an psychological experiment called 'The Stanford prison experiment' as an example of how **group conformity is a very efficient mechanism for changing individual behaviour in a group**. This mechanism refers to situations where people adapt their behaviour to what they perceive as the group norm. In the Stanford prison experiment these norms were established by the participants who took leadership in the groups.

Role model (Stein Helgar)

Stein Helgar design lead for critical systems in Halogen emphasized the importance of having a role model in the organization when there is a need for a cultural change. He called this role model a 'champion'. **It is a person within the organisation that has credibility and that other employees admires, and wants to be like.**

Let the employees decide (Mona Halland)

Mona Halland is a psychologist and designer from Mindshift. In her experience, **letting users decide the measures themselves** is important when changing organisational culture. That gives them ownership and a feeling of responsibility for their organisation. In mindshift they arrange workshops for the users to help them define concrete tasks and ways to achieve them.

GAINING USER INSIGHTS

One of our early findings was that accessing users were hard as the companies we approached were afraid of getting labeled for having bad security. Instead they sent us to security departments and ICT experts that could talk on behalf of the the company.

We then changed our tactics and approached our users in a different way, sending out design probes to people from different professions and various demographics. By using this method, we could communicate directly with the end user.

Companies we approached were afraid of getting labeled as having a bad security culture.

Design Probes

The goal with the probe was to gain insight on how the users meet digital security in the workplace, and address potential security challenges. The probe had to be simple as it was suppose to be done during working hours.

The probe was delivered to users by email. Altogether we received replies from 10 people from different working sectors, genders and age groups. They worked within banking, IT consultancy, social services, project management, and health care.

We asked them the following:

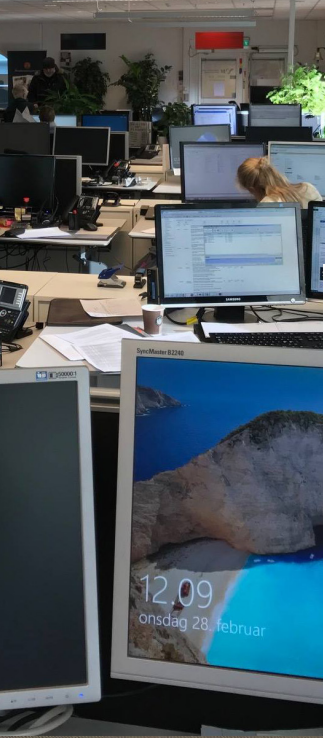
- What type of data they handle at work
- Where they are when handling sensitive information
- Which channel they used to send or receive the information
- If they have had security training at work.

“I’m very scared of getting my computer infested or stolen.”

Female (64), Project management

“Unsynchronised password updates means that I have to change 7-10 passwords all the time.”

Male (33), Economy



Male (33) - Banking

Type of data: Passports, and ID papers

Platform: Scanner, computer

Context: Always in the office

Female (27) - Banking

Type of data: Personal - and economic data

Platform: E-mail, computer, smartphone

Context: In the office, and sometimes on public transport and on my way to meetings.

Female (27) - The government

Type of data: business secrets, and sensitive information that is withheld the public

Context: The office

Platform: E-mail, word-document, phone calls.

Female (64) - Project manager

Type of data: Personal data, bank information, business results

Context: Home office

Platform: Email, sms, paper mail

Female (27) - Social worker

Type of data: Personal data, ID

Context: the office

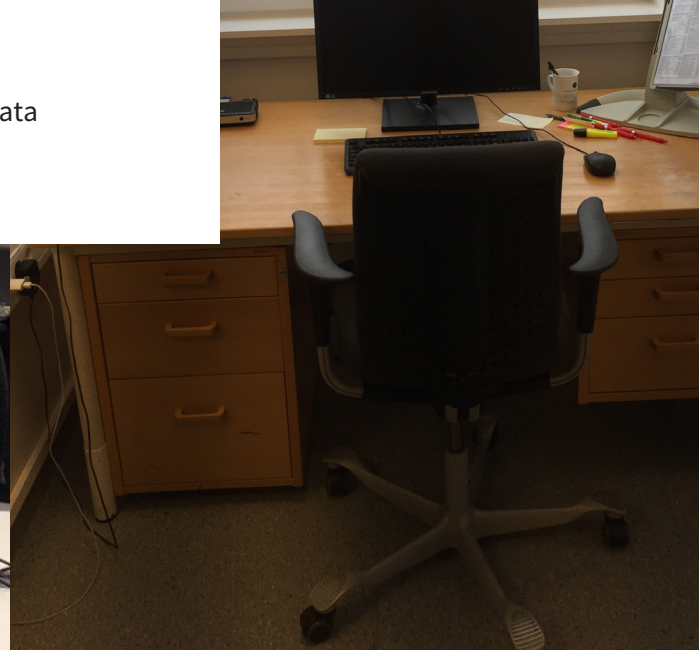
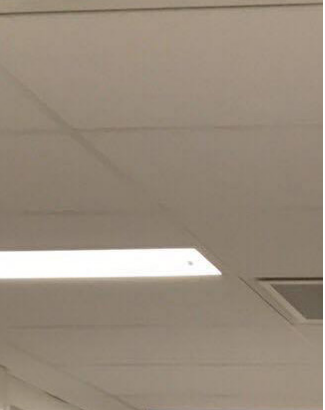
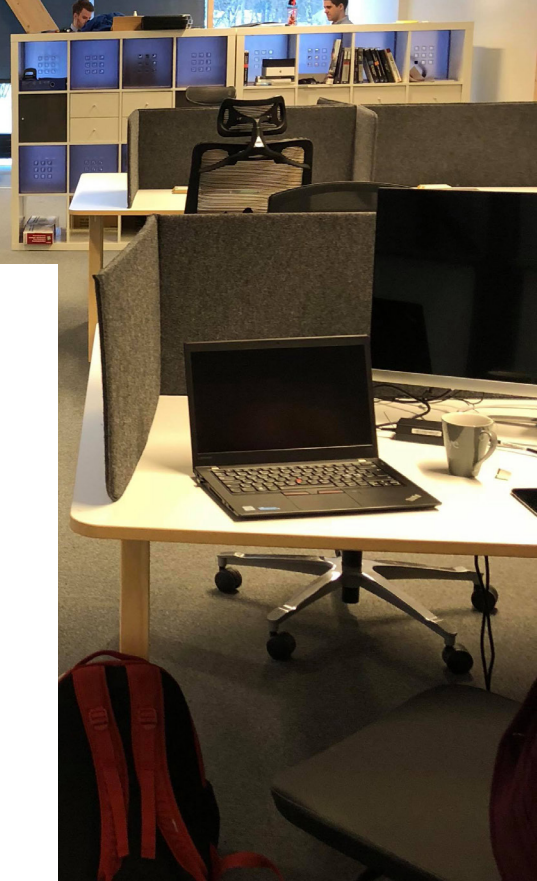
Platform: email, phone

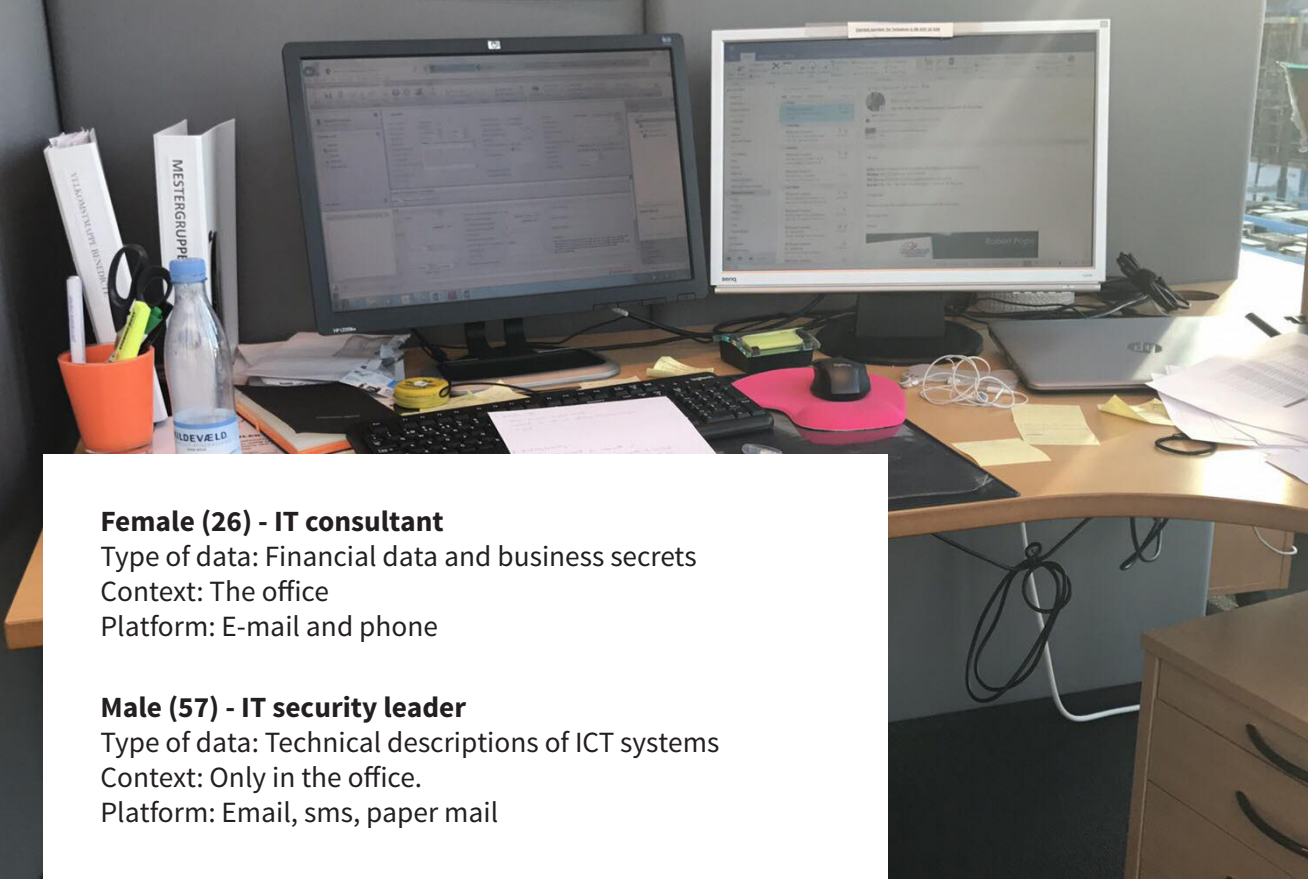
Male (33) - Doctor

Type of data: Health data, personal data

Context: In the office

Platform: DIPS





Female (26) - IT consultant

Type of data: Financial data and business secrets

Context: The office

Platform: E-mail and phone

Male (57) - IT security leader

Type of data: Technical descriptions of ICT systems

Context: Only in the office.

Platform: Email, sms, paper mail

Female (27) - Consultant working with social services

Type of data: Client information, personal data,

Context: Open office landscape

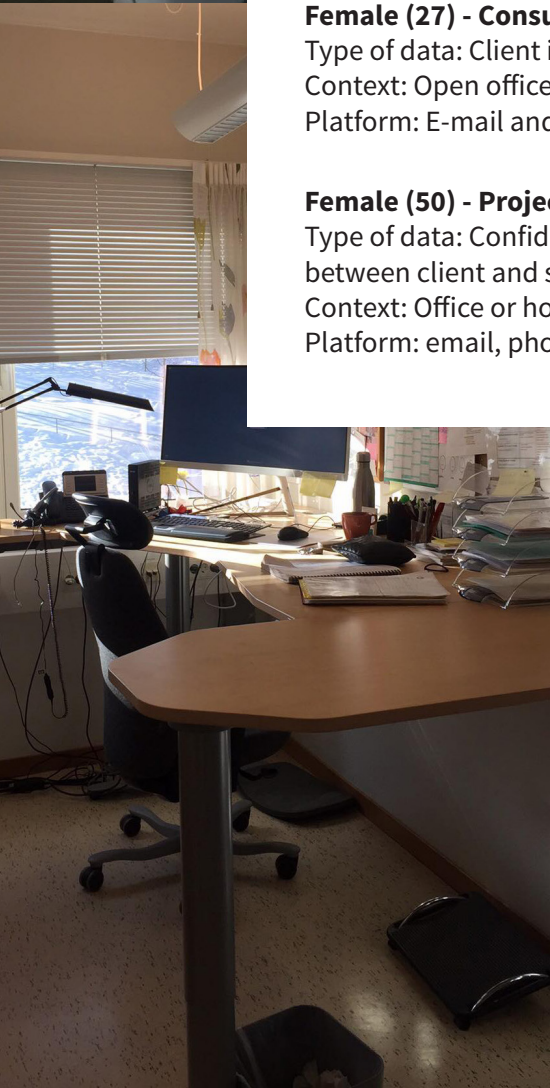
Platform: E-mail and intranet

Female (50) - Project manager

Type of data: Confidential business information, information between client and supplier.

Context: Office or home

Platform: email, phone call



“IT consultants never experience friction with technology.”

Female (26), IT consultant

“We have internal tests where we receive fake phishing e-mails.”

Female (50), Project manager

Findings

We found that the employees handle different types of data that varies in sensitivity. In banking and health, there were strict routines on how to handle sensitive data.

A challenge that several of the participant had, was email and password related. This confirmed findings from our research phase.

We also found that only a few of the participants had security training at work.

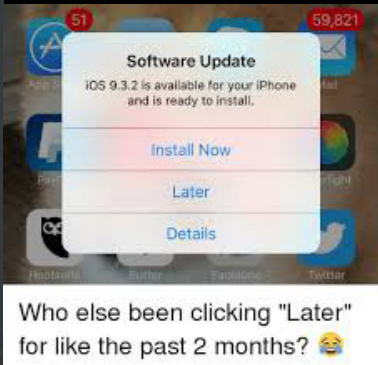
It is important to note that a small probe like this is not representative for whole sectors.

Memes and cartoons

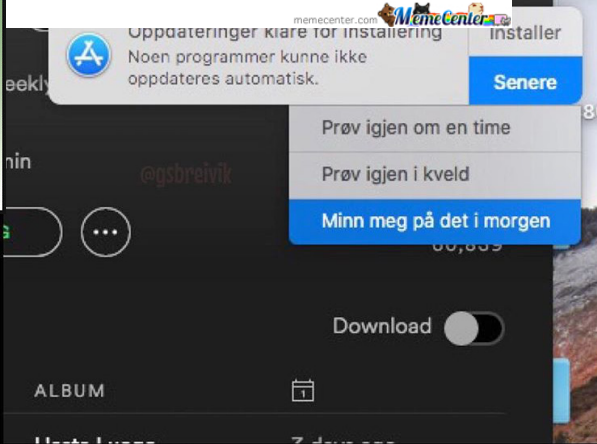
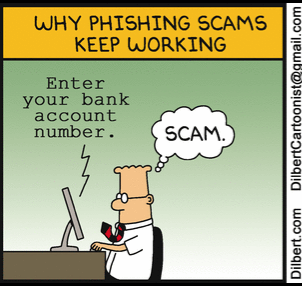
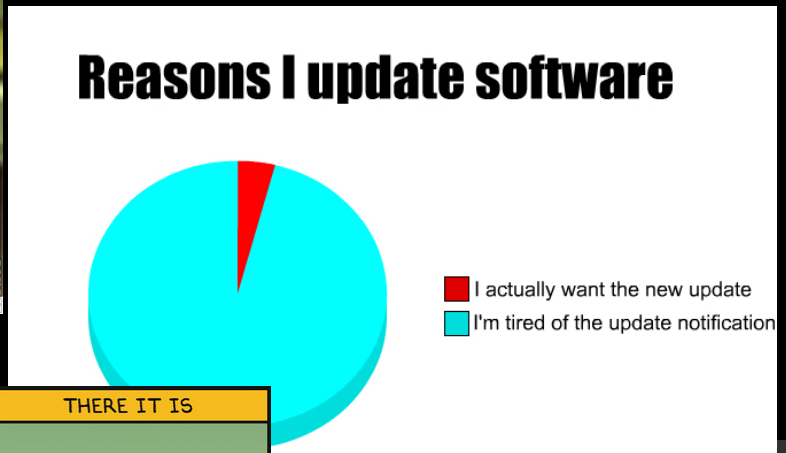
In our search for user- and cultural insight on digital security in workplaces, we took a dive into social media where we found plenty of comics and memes about the theme. Memes are looked at as cartoonish jokes shared across social media and are a way for people to share relatable experiences, and make us laugh. Today they are part of the way we communicate digitally. (Watercutter and Ellis, 2018).

Reflections

Memes and cartoons were good alternatives to identify frustrating user experiences in contact with digital security. We categorized the collected material and found user challenges related to passwords, software updates, phishing scams, and 2 factor identification.



Who else been clicking "Later" for like the past 2 months? 😂





ANALYSIS

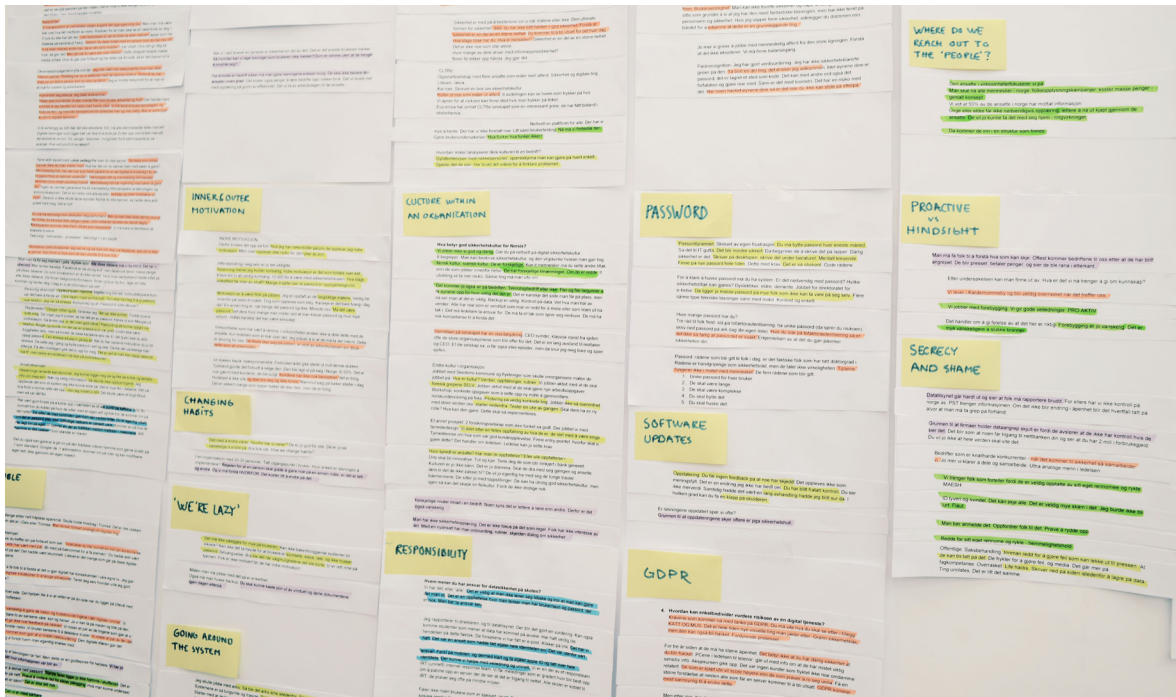
The goal with analysing the research was to address needs and challenges within the field of digital security .

We started the analysis by printing out transcripts from expert interviews. We highlighted interesting statements with a separate colour for each person and clustered the information by problem areas. We then connected our findings from probes, comics and memes to the problem areas and defined four key insights.

We named them:

- 'The human factor'
- 'Need for designers'
- 'Bad systems'
- 'Different cultures =different challenges'

In next chapter we will go in depth of these insights.



03. Define

In this chapter we will present our key insight from the previous chapters.

THE HUMAN FACTOR

Risk perception

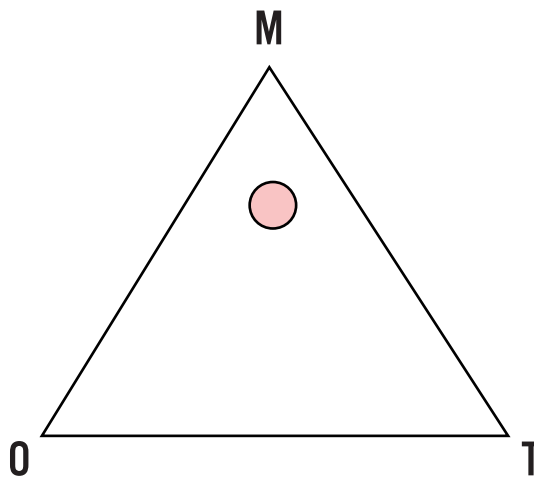
Security is both a feeling and a reality. You can feel secure even though you're not, and you can be secure even though you don't feel it. In digital space people do not see or hear those who do them harm and this makes it harder to identify risky behaviour. We tend to feel invisible in digital space and think «Why would anyone bother to target me?». However, we are just as likely of being victims of digital crime as getting our wallet stolen in real life (Schneider, 2015).

'Cyber Fatigue'

Cyber Fatigue is a feeling of being overwhelmed by and tired of cyber security warnings and, advice on how to stay safe. This leads us skipping basic precautions even though media, and IT departments advice us to do them. Examples of measures we skip are passwords updates, backups, and software updates. (Forno, 2017).

“ Consumers’ actions revealed a dangerous disconnect: despite a steady stream of cybercrime sprees reported by media, too many people appear to feel invincible and skip taking even basic precautions to protect themselves. ”

Nick Shaw, Norton’s general manager for EMEA (Hern, 2018).



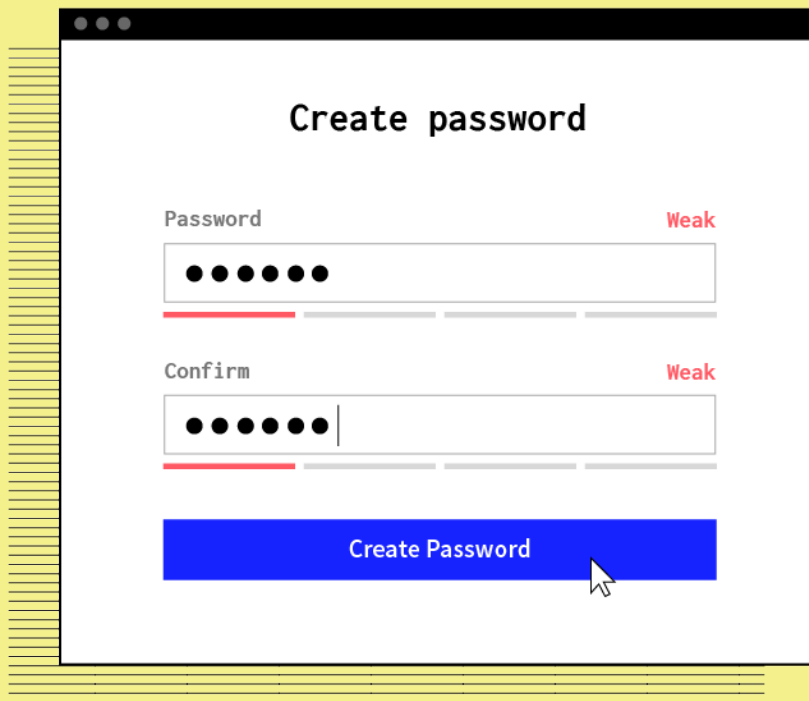
MTO analysis

(the interaction between Man, Technology and Organisation)

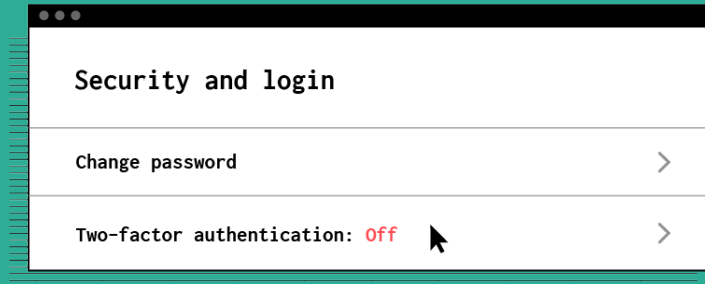
To detect abnormalities and protect ourselves against the digital threats we need technical security systems. However it’s also important to work on a human and organisational level as the security is influenced by both the environment and the individual who interacts with the systems. We have positioned our project towards the human where we take the possibilities, constraints and needs into account when dealing with cybersecurity.

Behaviour patterns

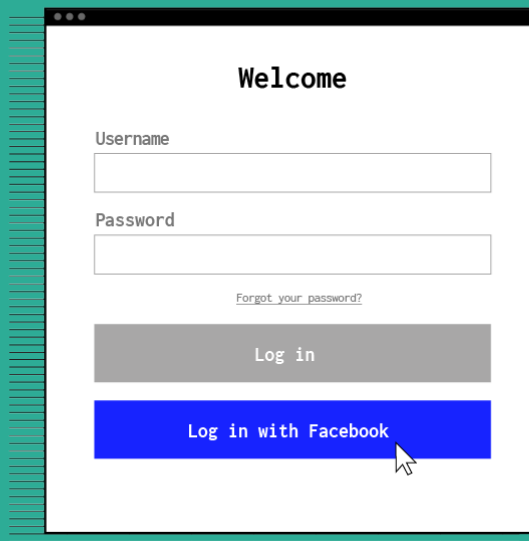
Creating weak passwords



Not using two-factor-authentication when possible

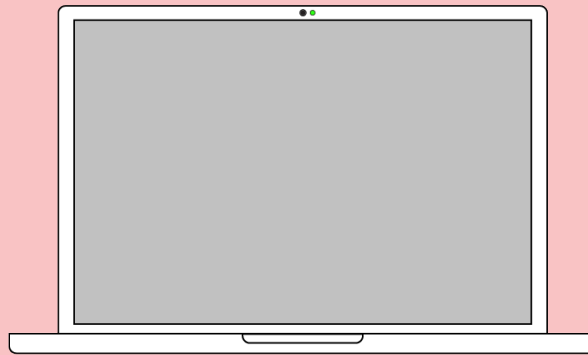


Connecting accounts to facebook



03. Key insights: The human factor

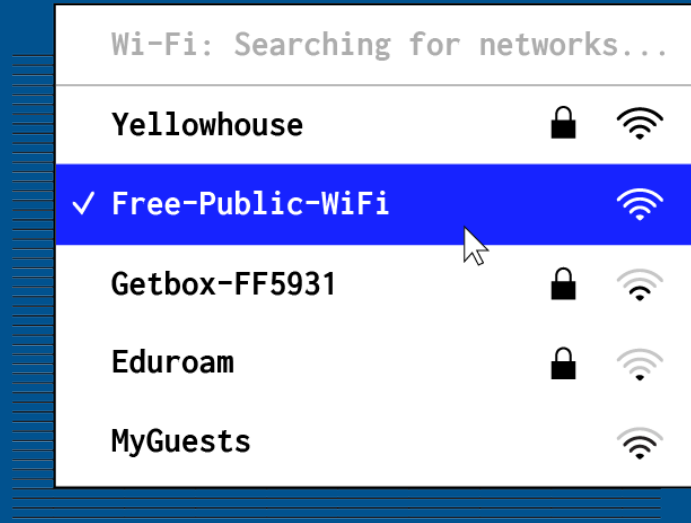
Not covering your camera lens



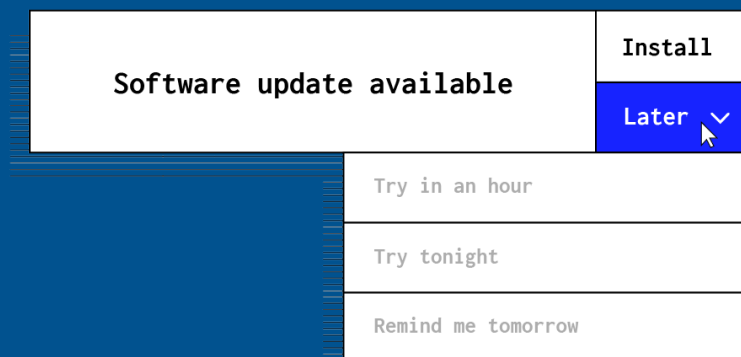
Expose yourself to 'shoulder surfing'



Using public WiFi for work

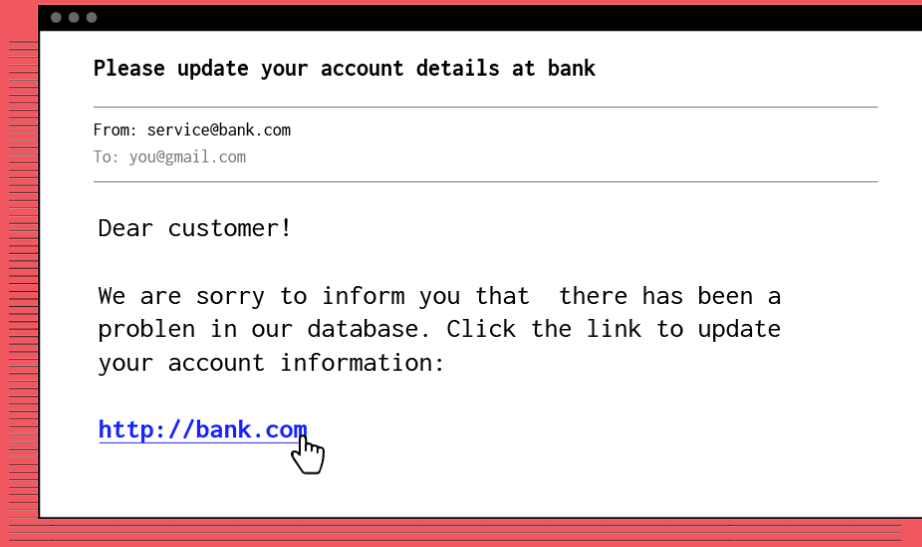


Postponing software updates



03. Key insights: Behaviour patterns

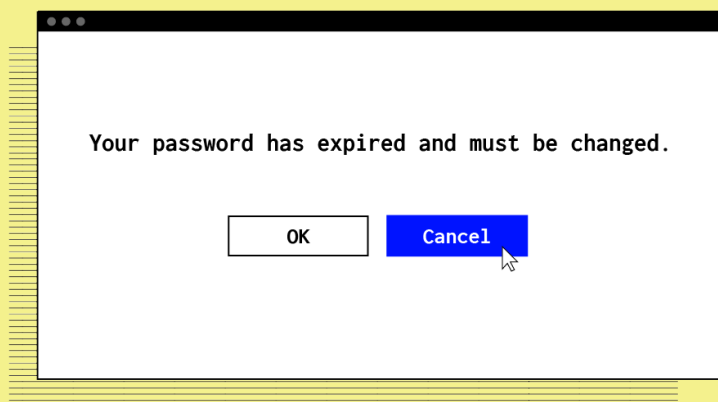
Trusting all senders



Using the same weak password for several accounts

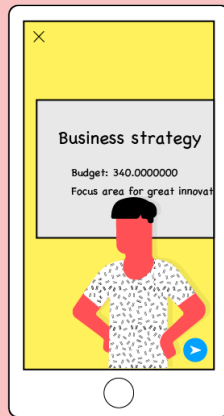


Avoiding password updates

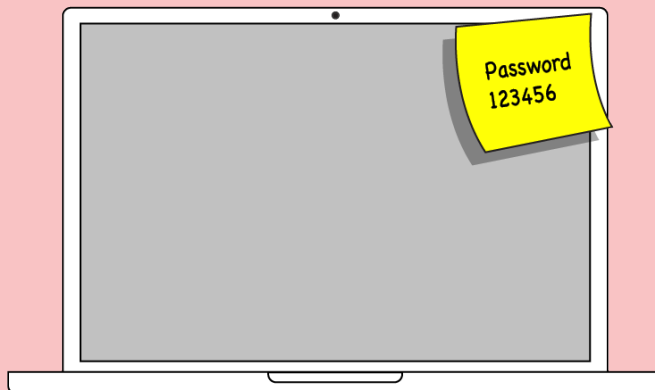


03. Key insights: Behaviour patterns

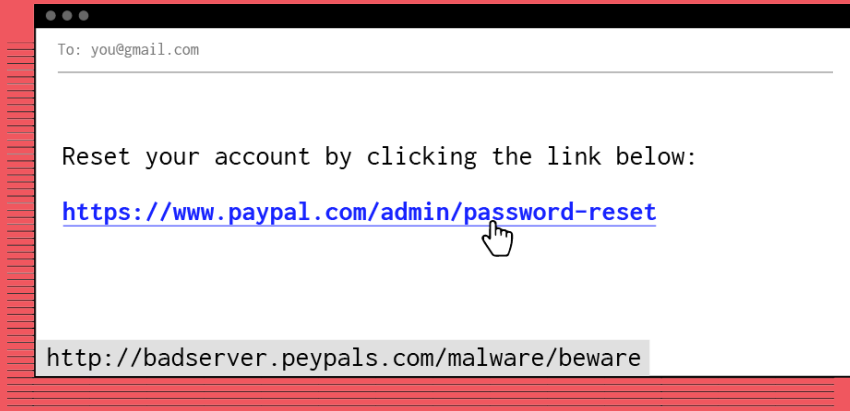
Snapchatting business secrets



Keeping password-notes next to the computer



Not checking links



Avoiding security warnings



NEED FOR DESIGNERS

IT dominated field

In Norsis' report about digital security culture they argue that communication about digital security is too technical and specialized for people working within ICT rather than the general public. This leads to people losing interest about the subject as its too hard to comprehend (Malmedal and Røslie, 2016). As designers working with the topic, we have experienced this aspect ourselves as we constantly have dealt with new and foreign terms. Norsis argues that this aspect describes why social scientists so rarely have dealt with cyber security culture (Malmedal and Røslie, 2016).

“ Cybersecurity solutions and initiatives are colored by the IT and engineer industry. It would be valuable with input from designers who has a human centered approach. ”

Tonje, Norsis

DIFFERENT CULTURES = DIFFERENT CHALLENGES

Early in the project we learned that every company has its unique culture. They consist of people who process sector specific data, and interacts with different systems. The size of the company also influence the culture. According to Roar Thon, CEO scams are often more successful in large companies as there is usually a distance between the employees and the CEO. In smaller companies it is possible for an employee to validate a suspect email as they can ask the CEO in person. As a result of cultural differences between sectors and companies, the security challenges also differs.

“Security is part of a larger picture -
it's not something that stands alone.”

Roar Thon, NSM

BAD SYSTEMS

“ The balance between security and usability is difficult, but not impossible. What is certain is that social and technical security must be seen in conjunction for overall safety to improve. ”

Mona Helland, Mindshift

UX and security friction

The more we are in touch with technology the less patient we are with friction: the frustrating aspects of interactions that slow users down when they attempt to complete an action. While some sources of friction are necessary to ensure security and privacy many others are unnecessary and needlessly frustrate users (Mastercard, 2017). That's why we often have a tendency to take 'shortcuts' in digital space skipping important security measures such as software updates and strong passwords.

As of now designers are often included at the end of the process, where they peel off a lot of the security measures developed by security engineers. This results in better user experience, but on the expense of the security. Other times, engineers develop secure solutions that are on the expense of user experience.

04. Explore

In the previous chapter, we presented our key insights. In this chapter we explore how we can design for these findings.

BRAINSTORMING AND IDEATION

Throughout the project we wrote down and visualized our ideas that we gathered on an 'ideation wall'. Every second week we met with fellow interaction design students where we amongst other things arranged workshops for gathering new thoughts and inspiration. This was very useful in order to get a fresh input and avoid getting stuck in a rut. We also used different brainstorming methods where our key findings worked as a base for the ideas. Our ideas had a broad span; From password games, social activities, competition between employees, to awareness campaigns and installations. When the wall of ideas started to fill up we organized the sketches by themes and found three main areas with design potential.

Design opportunities

After organizing our ideation wall we found three interesting areas with several design opportunities.

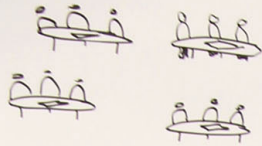
These were:

- 'Social structures'
- 'Education'
- 'Balancing security and usability'.

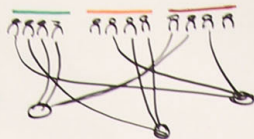
"Group mentality is important in order to change behaviour. We adapt quickly to group norms"

Kai Roer

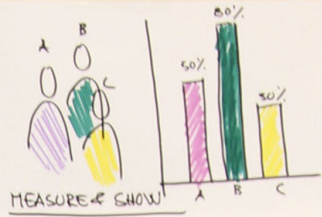
MONTHLY TOURNAMENT



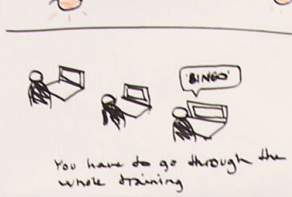
REARRANGE WORKSPACE EVERY MONTH



SECURITY THEATRE



ONCE A MONTH: SECURITY TRAINING

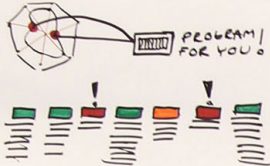


THE IDOL

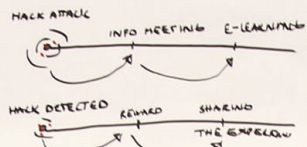
MOTIVATE THE WEAK

JEG VIL HA ARNE I TILBÆTT

SECURITY ANSVARLIG



EVERYTIME THERE'S A HACK ATTACK OR AN AVERSION...



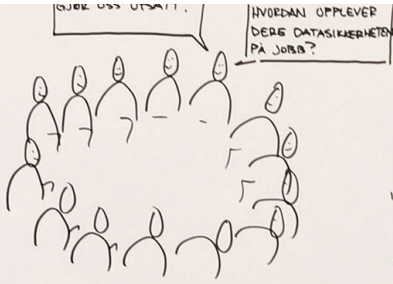
PREVENT ACCESS

WHAT? WHO YOU



1. Social structures
 This direction explores how group dynamics can motivate employees to improve their security hygiene. Many of our experts mentioned how effectively group dynamics could affect human behaviour. So how could we design for it? Some of our ideas were rearranging the workplace every month, gamification for social comparison, and positive punishments.

HOW CAN WE DO THE SAME WITH CYBER - SECURITY?

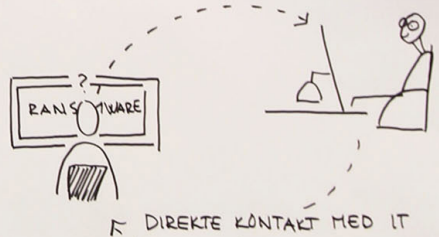


FRONTFIGUR "CHAMPION"

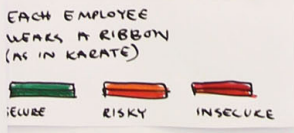
SAMARBEID KONKURRANSE

"HEI, JEG FÅR IKKE TILGANG PÅ PCN MIN. HVA BETYR RANSOMVARE?"

IT SUPPORT

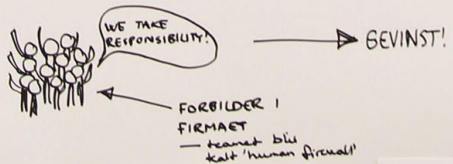


"DA TRØR JES DU HAR BLITT HALVET. VI ER PÅ SAKEN"



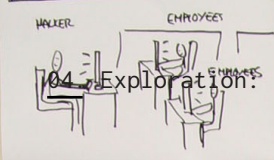
... whole hacking...

HUMAN FIREWALL + CRYPTOCURRENCY

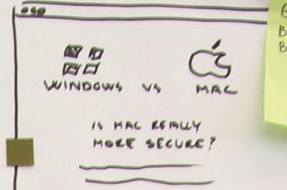
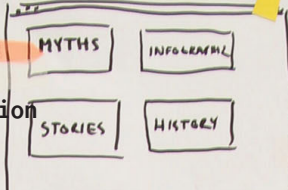


BONUS You get bitcoins as an award BE A HUMAN FIREWALL!

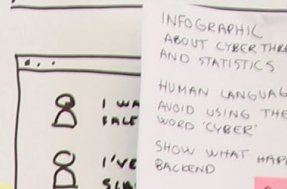
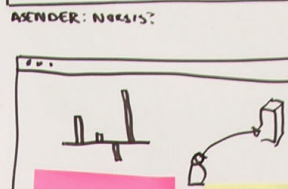
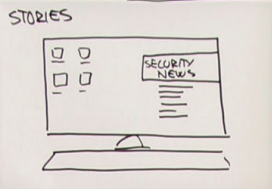
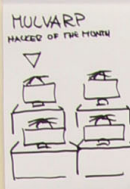
HACKER EDUCATION



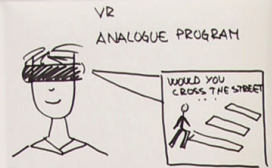
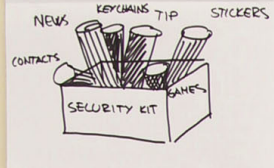
SIMULATE



GOOD SITUATED, BUT CAN IT BE EVEN BETTER? SCORED!
YOUTUBE VS. YAHOO?



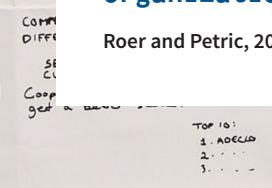
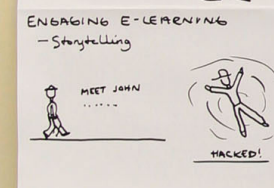
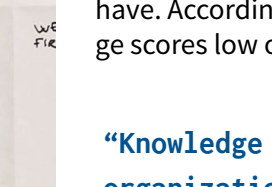
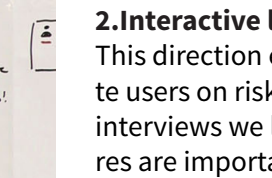
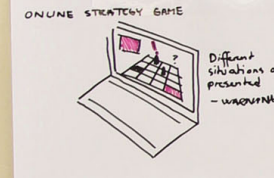
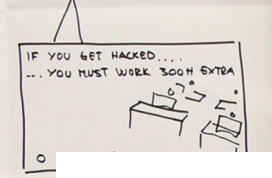
INFOGRAPHIC ABOUT CYBER THEAT AND STATISTICS
HUMAN LANGUAGE AVOID USING THE WORD 'CYBER'
SHOW WHAT HAPPENS BEHIND
PODCAST
"I've been hacked"
- Telling stories
- Inform people
- If it can happen to me, it can happen to you!



TAILORMADE SECURITY MEASURES



SCREENSAVER
SCREEN IN THE VISUALIZE OFFICE HACK ACTIVITY (INTERNET)

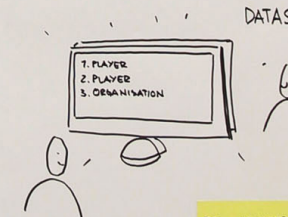
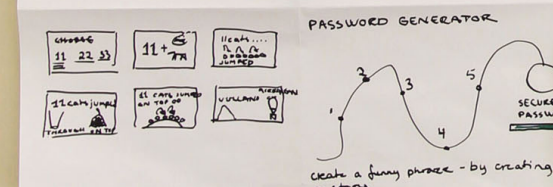


2. Interactive learning

This direction explores how we can use interaction design to educate users on risks associated with their online activities. In our expert interviews we learned that many people do not know why basic measures are important for security, or what consequences their actions may have. According to studies conducted by CLTR, organizations in average scores low on the dimension 'knowledge'.

"Knowledge and awareness of security issues in the organizations studied is on average very weak"

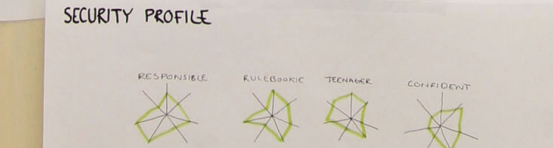
Roer and Petric, 2017



SPREAD A FRIENDLY RANDOMNESS APP THAT 'STEALS YOUR DATA' UNTIL YOU PROMISE TO UPDATE YOUR SETTINGS



BRANNISIKKERHET
SECRET THIEF
HMS BEGLER
RISIKKURDERING
BRANNKUNNS - E
MEDARBEIDERSAMTALE

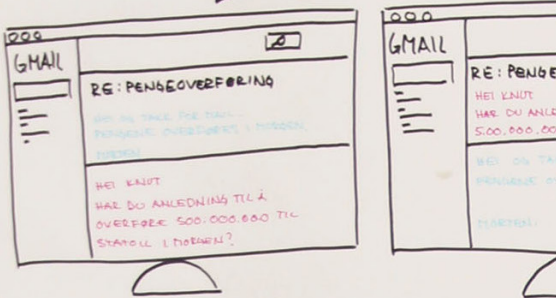


3. Balancing security and usability

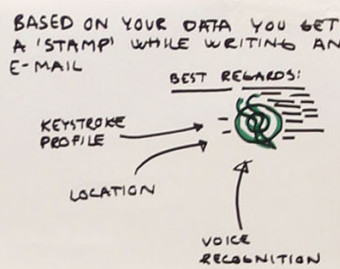
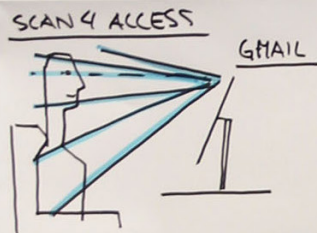
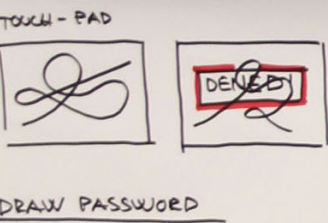
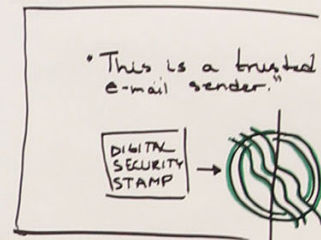
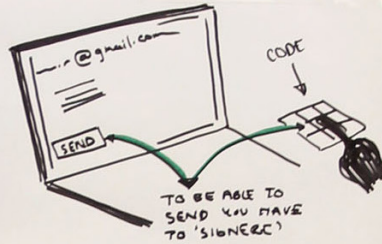
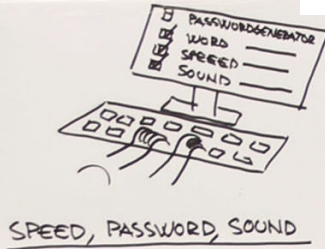
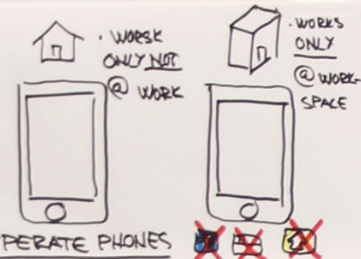
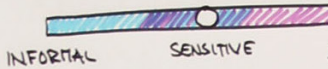
In this direction we wanted to explore how we could design secure solutions without affecting the user experience.

Research showed us that security measures is a hassle for users. For instance, the ideal password has to be as long as possible, contain different symbols, and be different for every account. They also have to be changed every month. The human brain is simply not taken in consideration as most of us are not able to remember such random codes. To add an extra layer of security to your account the two-step authentication is a good alternative. However it adds friction when logging in to a service. Based on these insights we sketched out different ways of making secure logins more human friendly.

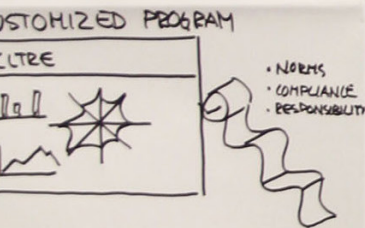
SIGNATUR MAIL



- FARGEKODE
- IKON
- "VANNMERKE"
- TOUCH ID
- KRYPTERING



WRITE YOUR NAME: KAI USER
.... generating profile
- YOU LIVE HERE - [map icon]
• You've complained to referees
times.
• Based on your img-collage of
LOOKS LIKE YOU LOVE YOU
DOGS!
• RISK LEVEL: 97% [grid icon]



BASED ON THIS DATA, THIS IS YOUR PERSONALITY

Caring animal lover who isn't afraid to complain when I look deep into your green eyes I realize that you have glasses.

CHOOSING DIRECTION: EDUCATION

For choosing a design direction we took three factors into account. Those were level of impact, relevance, and personal motivation. The final direction we chose was Education.

Why we chose education

One of our main findings in this project is how important role employees play on security in a company. At the end of the day, the humans are vulnerable links who criminals exploit to gain access to the business resources. As Roar Thon put it “Digital crime is about humans manipulating other humans using technology as a tool”. Thus it is important to teach people how to do risk assessments in digital space. In this direction we saw plenty of possibilities and great potential for using- and developing our skills sets as interaction designers.

Why we did not select the others

The “Social Structures” direction was an interesting alternative, but we felt that it required more knowledge about organisation culture and change management than we could offer. We didn’t see as many opportunities for interaction design with this direction, and since that was one of our motivations for this diploma we chose to not go for this one.

The last direction “Balancing security and usability” was clearly an interaction design go-to direction. However, we realized that working with login usability required a technical skill set from a security engineer to be realistic. As we do not acquire this, we had to let it go.

Rephrased project statement:

**HOW CAN WE DESIGN AN
INTERACTIVE LEARNING
PLATFORM THAT SUPPORT
EMPLOYEES IN DOING RISK
ASSESSMENTS AT WORK?**

05. Develop

In this phase we will go through the concept development that is based on our chosen direction 'interactive education'.

Methods:

- State of the art
- Targeted sketching
- Prototyping
- User testing
- Iterations

EXISTING LEARNING TOOLS

We have looked into examples of educational tools for digital security to get an overview on how the market educates employees about digital security challenges.



Databehandlerens plikter under avtalen

Databehandleravtalen viser hvordan databehandleren skal hjelpe den behandlingsansvarlige i forhold som gjelder informasjonssikkerhet, avviksrapportering, konsekvensanalyser osv.

Viktige instruksjoner vil tyvsnisk være å

En vanlig situasjon: Ett selskap samler inn data, et annet analyserer dem.

Hva om noe går galt på veien, slik at vi bryter loven og de registrertes rettigheter? Hvem har ansvaret?

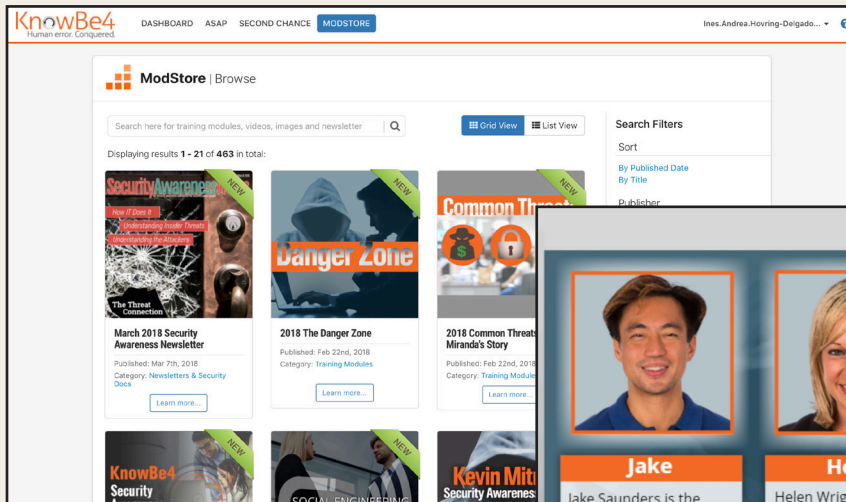
Bruk noen minutter på å lære mer om databehandleravtalen.

Start leksjon



Junglemap

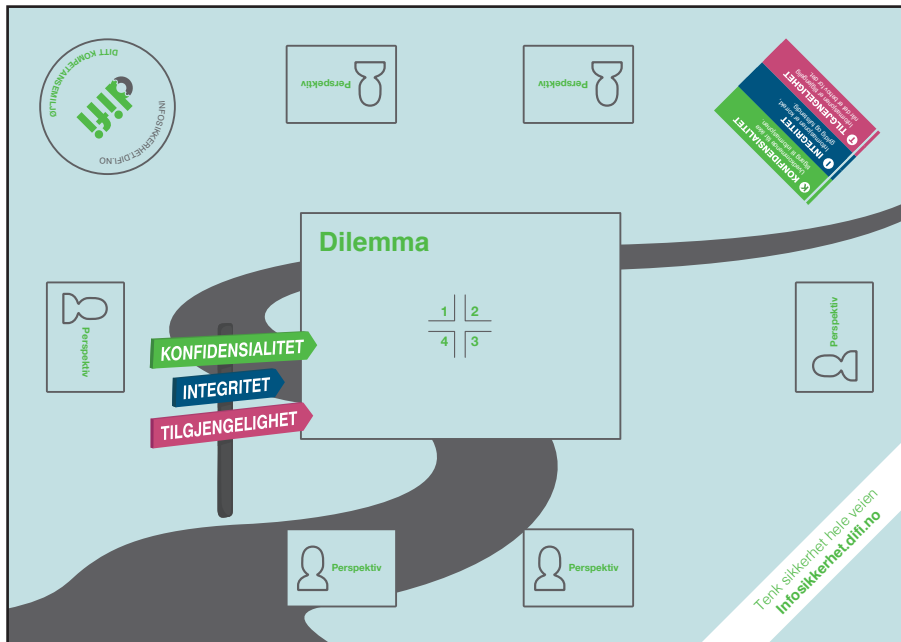
Junglemap is an e-learning tool that is widely used and every security expert we have talked to during the diploma mentioned this tool. It is adaptive in the way it offers a template where text, media and questions can be added and it is then sent out to employees in a company. We tested this tool, and experienced it as little engaging as we became passive recipients, swiping through slides with snippets of text and pictures. In our opinion the Junglemap-format doesn't exploit the full potential of a digital platform where it provides little interactivity.



KnowBe4

KnowBe4 is an IT security company with the world's largest library of security awareness training content. They aim to help employees understand the mechanisms of spam, phishing, malware, ransomware and social engineering. We requested a demo of this program and were presented with a library of 463 different training programs. This felt like an information overload as all the programs were presented at the same level.

05. Concept development: Existing learning tools

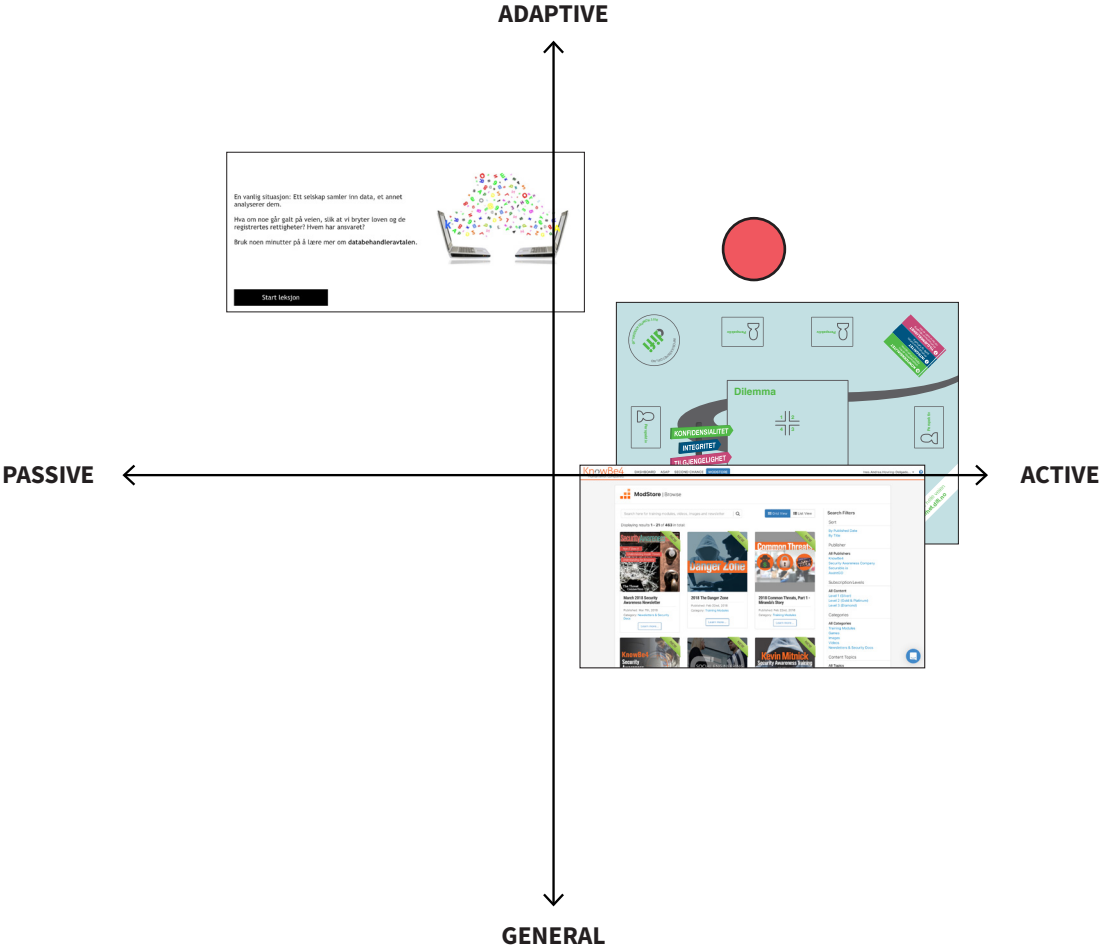


Dilemma tool

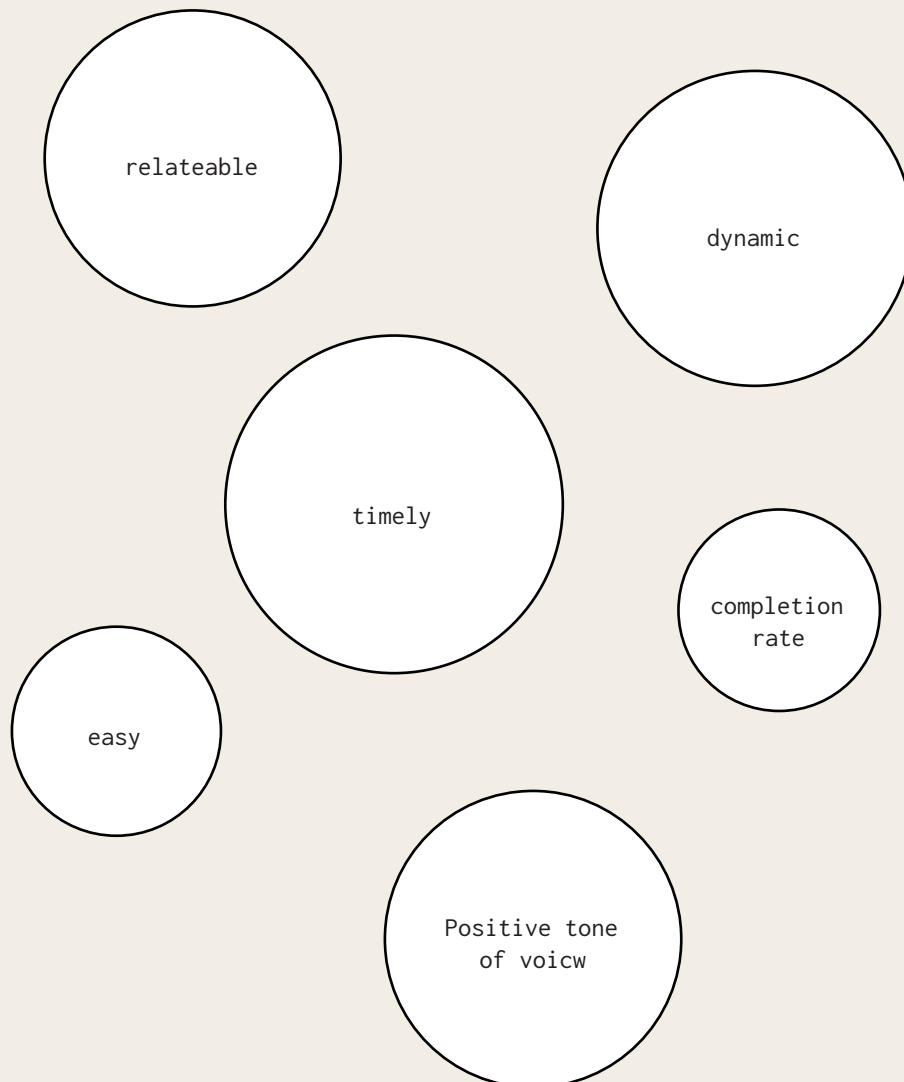
Difi also has some learning programs teaching the public sector about digital security related issues. One example of this is the dilemma tool: CEOs are presented with different scenarios where they discuss how different personas would react to the issues they face. We like how this tool forces the users to take part actively in the learning, however, we think it's important that it's a tool available for every employee in the business.

Positioning

We sorted the examples in a graph that position them by adaptivity, and in which degree the user is active or passive in the learning process. This was useful for us in order to make a statement on where we wanted position our learning program (red dot).



REQUIREMENTS



Timely

If businesses are to invest in the interactive learning program, it cannot take too much of the employees valuable working hours. Employees are more likely to learn and engage in the program if it's not too time consuming.

“Security is looked at as something ‘in addition’ to work, therefore it’s important that it doesn’t interrupt the employees.”

Anette Rimmereit

Relatable

Based on the insight that different sectors has different challenges ---- We aim to make the employee feel that their workplace is reflected in the learning platform, and that they recognize the challenges that it address.

Dynamic

Our interactive learning program should have content that can easily be adapted to different sectors in order to make it relatable for different workplaces. It is also important to be able to update the content as the digital threat landscape is in constant change.

Completion rate

By incorporating a completion rate in our interactive learning program the employees can pause and continue as they wish. This also provides the security administration with an overview of how many employees has completed the program.

Easy

The learning platform must be easy to navigate through as it's supposed to be used by people from different age groups and understanding of technology.

Positive tone of voice

It is important to use a tone of voice that is motivating rather than fearful.

LEARNING GOALS

Based on all insight from research, we defined a set of learning goals that aims to cover the main challenges for our users. Due to the time limit of this project we did targeted sketching and prototyping, choosing a few of them for our concept development.

Those are:

- What is sensitive data
- **Software update**
- Backup
- **Phishing**
- **Ransomware**
- CEO fraud
- **Social Engineering**
- ID theft
- E-mail guidelines
- How a password is hacked
- How to create a safe password
- Why you should vary passwords
- 2FA authentication
- How to safety check a website
- Social media guidelines
- USB stick
- Travel guidelines

INTERACTIVE LEARNING

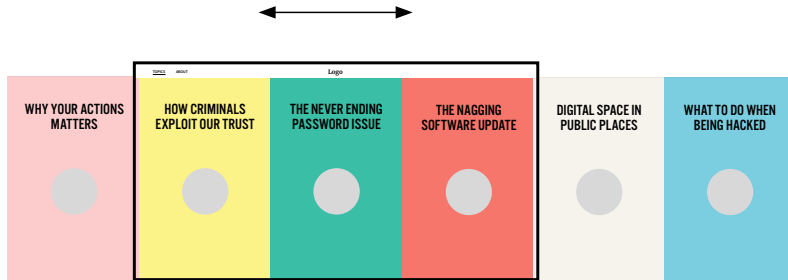
Structure and dynamics

Compared to a book where the content remains in the same structure from beginning to end, a digital platform has the potential to vary the content and structure in multiple ways. The order of the content can be determined, or it can be dynamic and change according to the users actions. A digital platform has the advantage of using different types of mediums such as text, film, animations, games, and so on. In our concept development we have explored different ways of presenting our content and learning goals by the use of different structures and medias.

CONCEPT DIRECTIONS

Information presented through different mediums

In this direction we categorized the learning goals into chapters where we sketched out both linear and non-linear ways of navigating through the material. In order to make the content dynamic we explored how different media could present the different topics. This was done by the use of visualized statistics, questions/myths, exercises and parallax scrolling. We quickly realized that this format didn't function as a learning tool as the users became passive recipients of the content.



Getting software updates always seems to happen at the most inappropriate times. Which makes us postpone it, postpone it and postpone it over and over again.

Software update available

It is easy to skip software updates because they can take up a few minutes of our valuable time, and may not seem that important.

I've got to send this email

This action keeps the door open for hackers to access your private information

As quickly as software providers find ways to fix exploitable holes in their software, hackers have found new ones. It's a never-ending game of cat and mouse that software companies are caught up in with cyber criminals in order to protect their consumers.

The main reason anyone has for downloading and installing the latest update is to stay protected from security threats. Older software and operating systems have the same bugs and exploitable holes in their code that allow hackers and cyber criminals to get up and go. This is made even more serious by the fact that all of these exploitable entry points have generally been made public after the release of updates.

More recently, WannaCry and ransomware style malware have been hitting personal and company documents hostage until a payment has been received. Making sure you update operating systems and update software can help to mitigate the risk you'll face from these kinds of threats.

< >

44%

It is a long established fact that a reader will be distracted by the readable content of a page when looking at its layout. The point of using Lorem Ipsum is that it has a more-or-less normal distribution of letters, as opposed to using 'Content here, content here' making it look like readable English. Many desktop publishing packages and web page editors now use Lorem Ipsum as their default model text, and a search for 'lorem ipsum' will uncover many web sites still in their infancy.

As irritating as they are, software updates are important, and we should each getting in the habit of following through on those notifications.

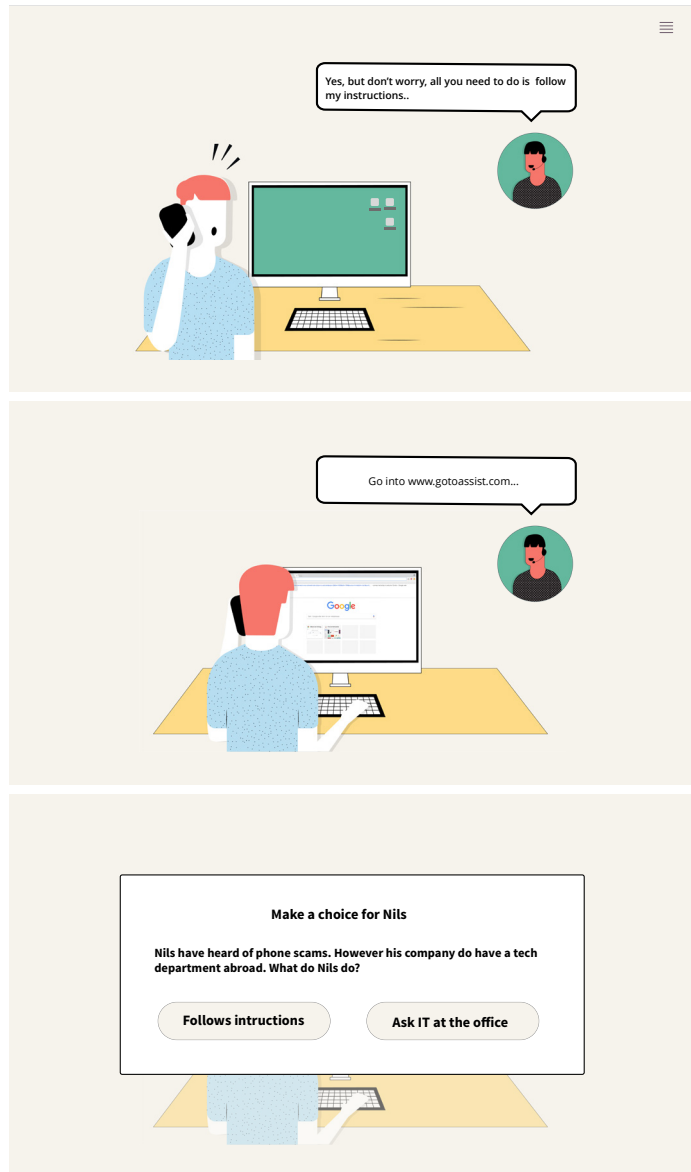
I've got to send this email

I've got to send this email

Four grey circles are arranged horizontally below the text.

Storytelling and dialogue

To capture the users attention and make them active in the learning process we explored the potential of visual storytelling. We found inspiration from cartoons and tested how multiple choices or dialogue trees could create non-linear stories. After sketching out two stories we realized that the flow became static and it was too obvious for the user which alternative was the right one. The direction also had limited options for adapting content.



On a regular basis something really annoying happens...



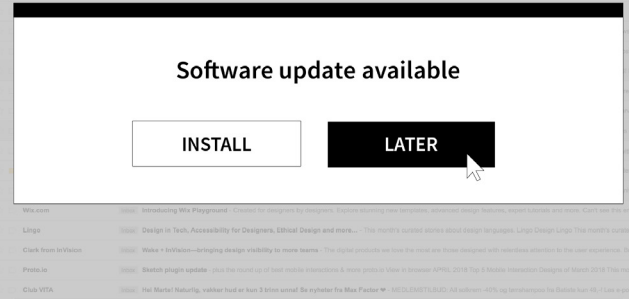
Something that disturbs you at the most inappropriate times...



Which makes you postpone it...



...and postpone it over and over again



And it doesn't stop with the nagging

April 02



Don't forget to software update!

Tuesday 03



Still we choose to postpone it...



This action makes you vulnerable for a criminal act called RANSOMWARE

Friday 06

HELP NINA

WTF just happened?!



Ransomware

Nina just got a ransomware. This means that all her data is encrypted

Pay Contact IT



Ransomware

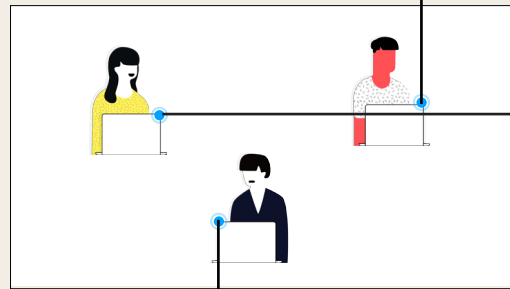
Ransomware that is a type of malware that threatens to publish or destroy the victim's data by blocking the access to it unless a ransom is paid. The payment is often executed by the use of cryptocurrency. The malware is spread by e-mail, pop-ups on websites, or like in this case by weaknesses in a software.

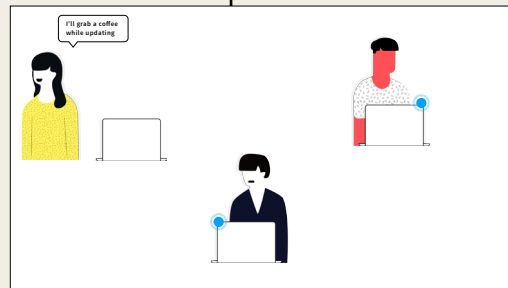
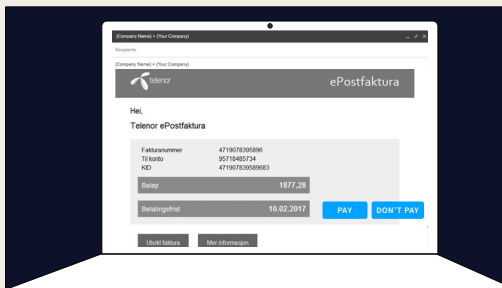
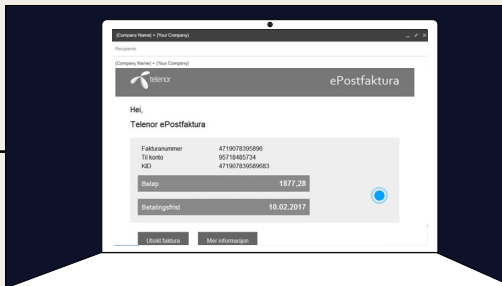
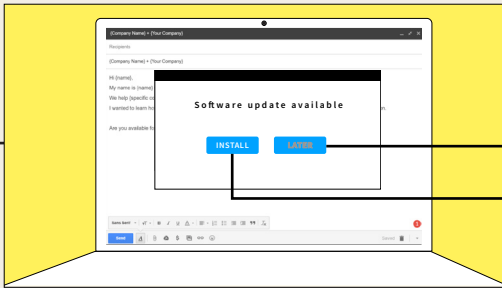
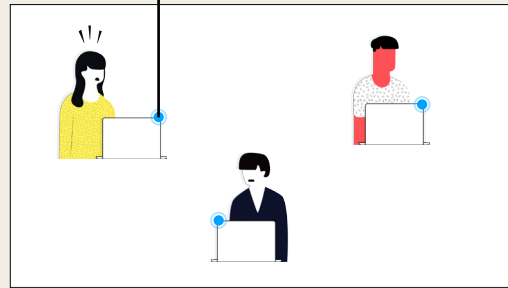
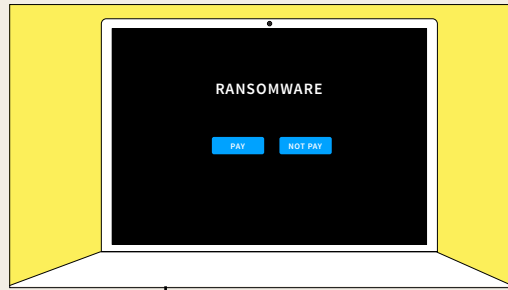
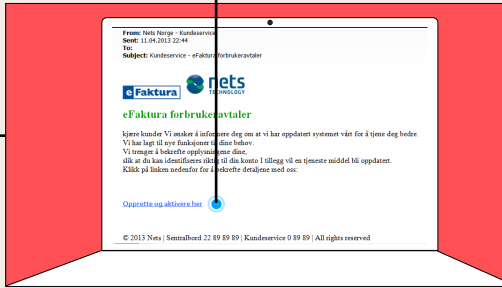
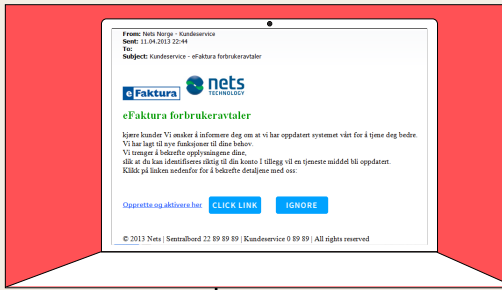


Simulation game

With this concept we aimed to involve the user throughout the whole program and make them experience how digital threats might approach them.

In this concept we wanted to give the user a 'realistic' experience of how their behaviour affects security. The user is presented with scenarios from the workplace and can change view from third to first perspective. He or she is served everyday tasks that influence the digital security.





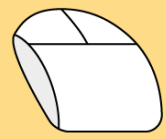
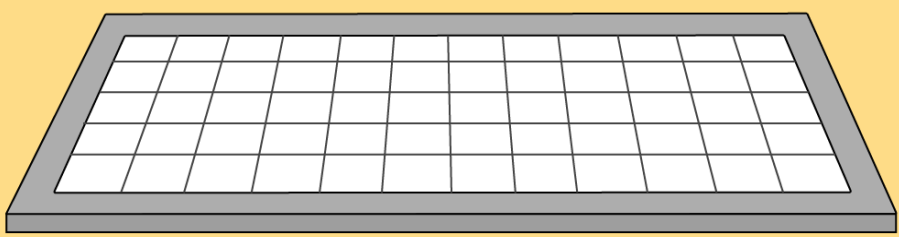
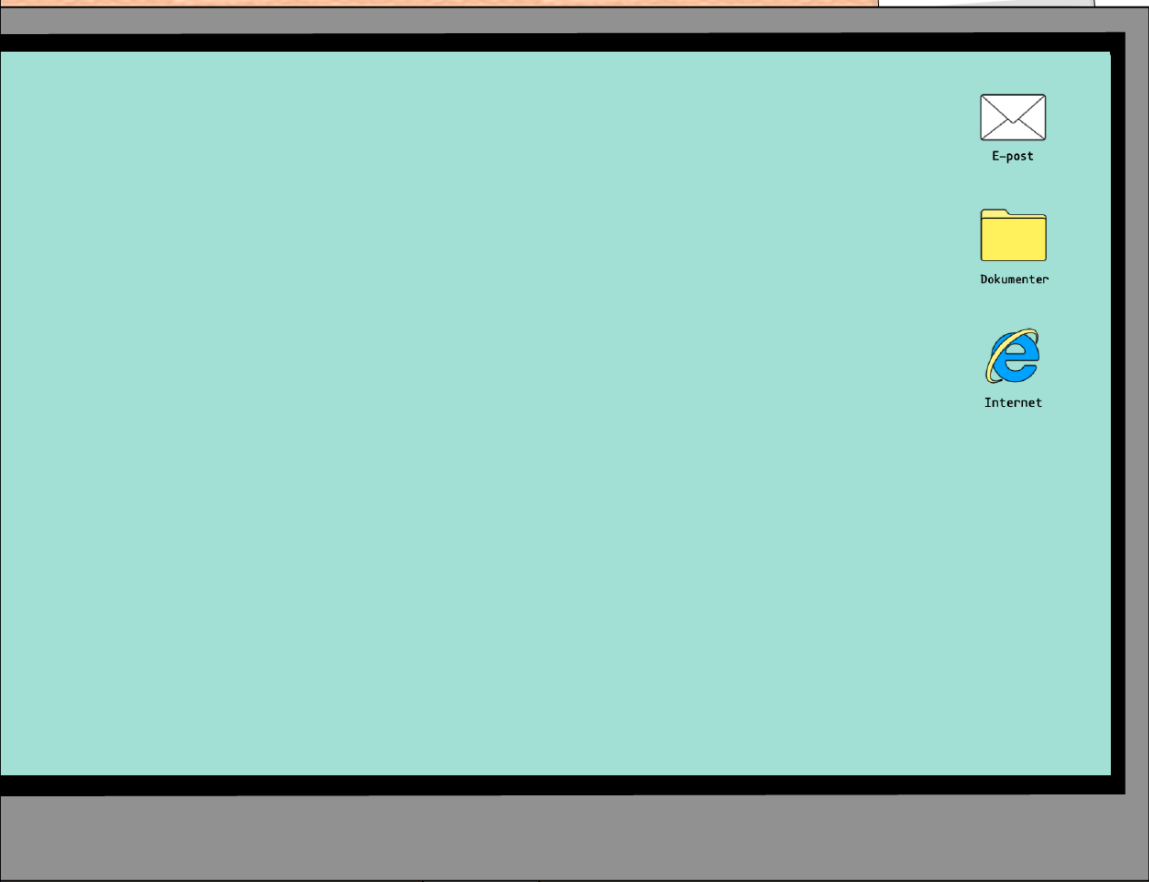
Choosing concept: simulation game

Through user tests with people at school we discovered that the simulation game offered the most engaging learning experience among the three directions. However changing viewpoints was a bit confusing. We chose to explore the first person perspective further as the user seemed to reflect more around the possible choices they faced. It also had the potential to adapt and change the content easily.

After choosing this direction we sketched out different tasks that could be included in the program, before creating a clickable prototype for user testing with our target group.

The first prototype

Before testing on the actual users, we tested on other students at AHO. We soon realized that the aesthetics were too similar a real desktop, as some students got insecure if the events happening on screen were real or fake. As one of our requirements was to not scare people, we chose to stylize the visual expression so that it couldn't be mistaken for being real.



06. Delivery

In this section we will present our design proposal and explain why exists, what it offers and how it works.

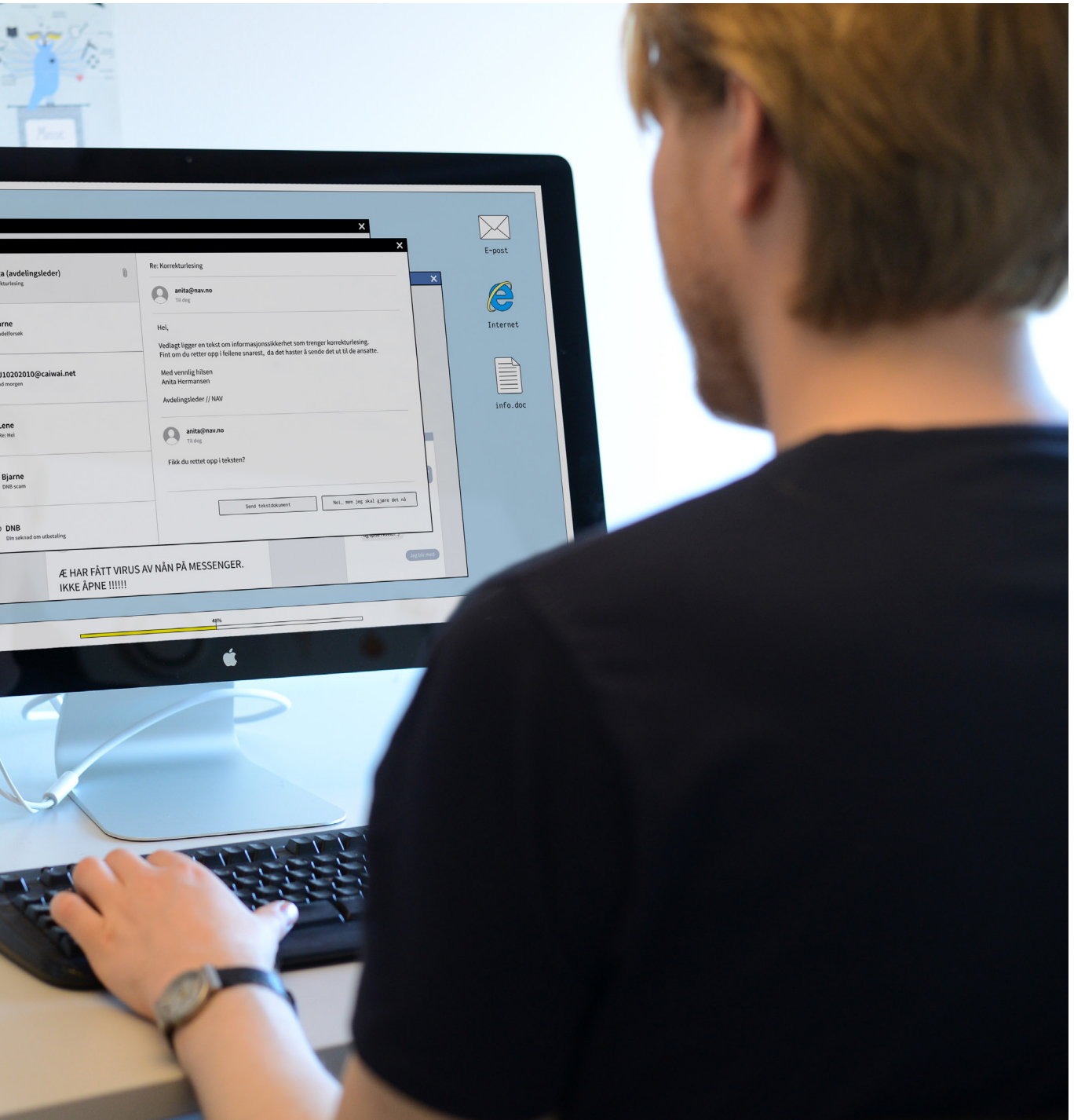
DESIGN PROPOSAL

Interactive learning program

The purpose with the solution is to inform users about digital security and train employees on how to do risk assessments in digital space.

This is done through interactive scenarios where the user is exposed to various security challenges that he or she has to act upon. Throughout the story, the user is guided and given feedback on the decisions that the user has made. In this way the user learns how to detect criminal attempts, and what security measures he or she should do in order to protect valuable information at work. The advantage of this program is that the user can learn through trial and errors in a safe environment.





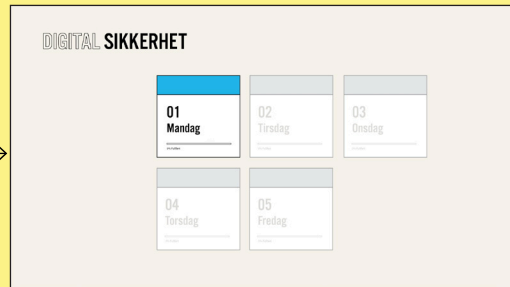
MAIN PAGES

This page explains the main structure of the e-course.

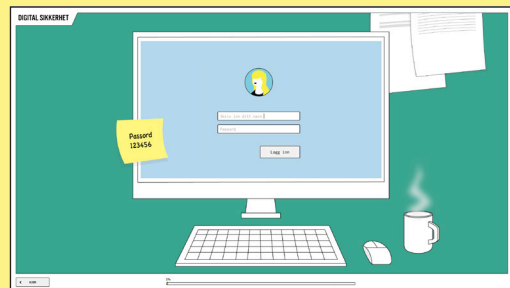
A: Introduction part



01. Prologue
Course introduction

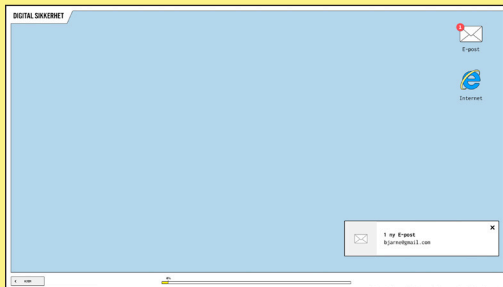


02. Home page
Course- and progress overview

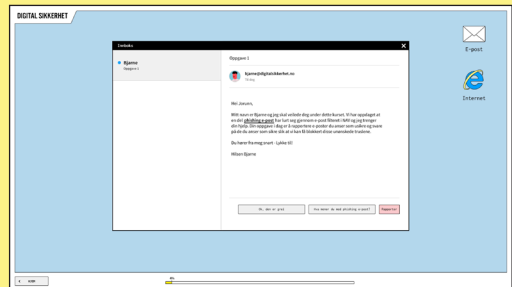


03. Log-in:
Starting point of the course

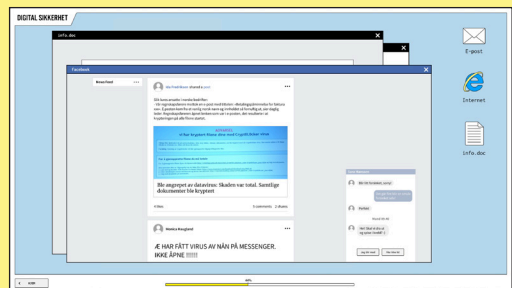
B: Course part



01. Landing page: Desktop
Main navigation



02. Main page: E-mail
Task provider



03. Sub page: Internet
Various content

A01: Prologue

Course introduction

In this sequence, the employee meets 'Bjarne the mentor' who introduces the course and explains why digital security is important.

Som ansatt i NAV behan
informasjon som er vi

du skal
beholde
den
sensitive
data
du
skal
beholde
den
sensitive
data
du
skal
beholde
den
sensitive
data

Name of workplace is included in the introduction.

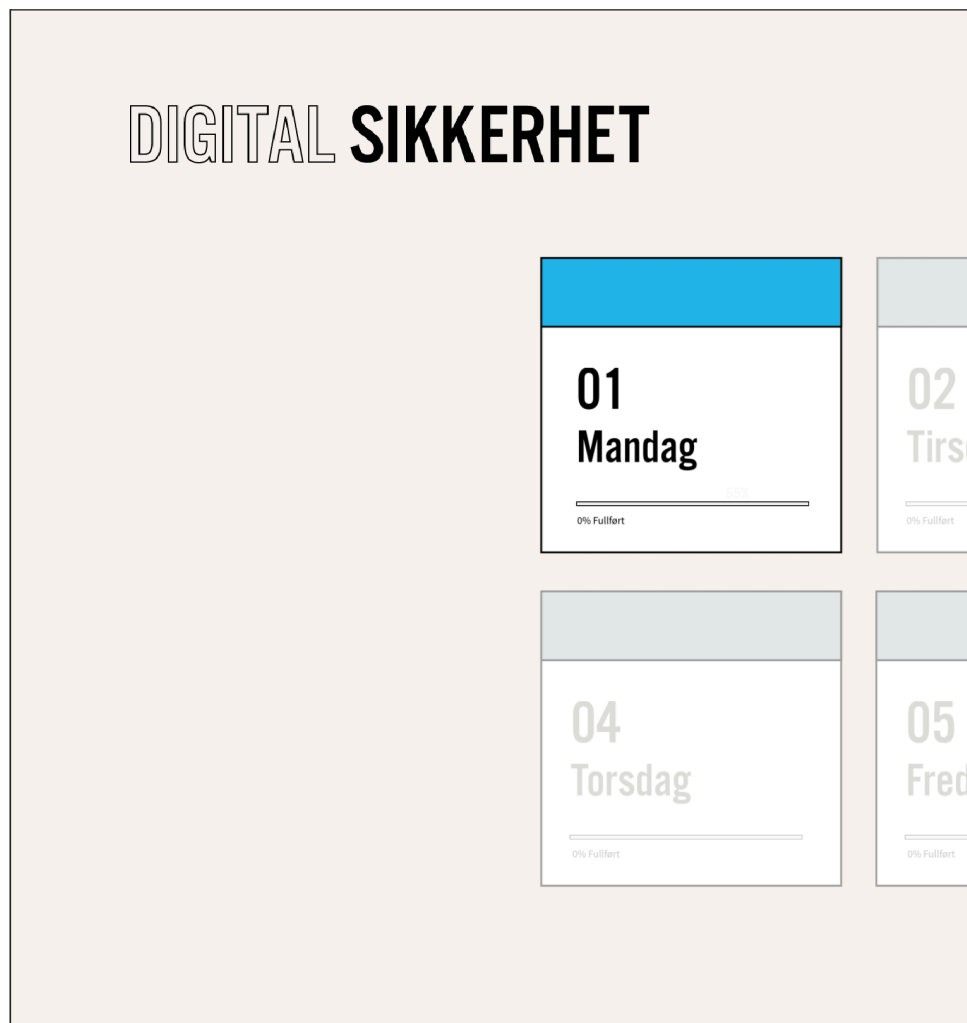
Information about sensitive data relevant to sector.

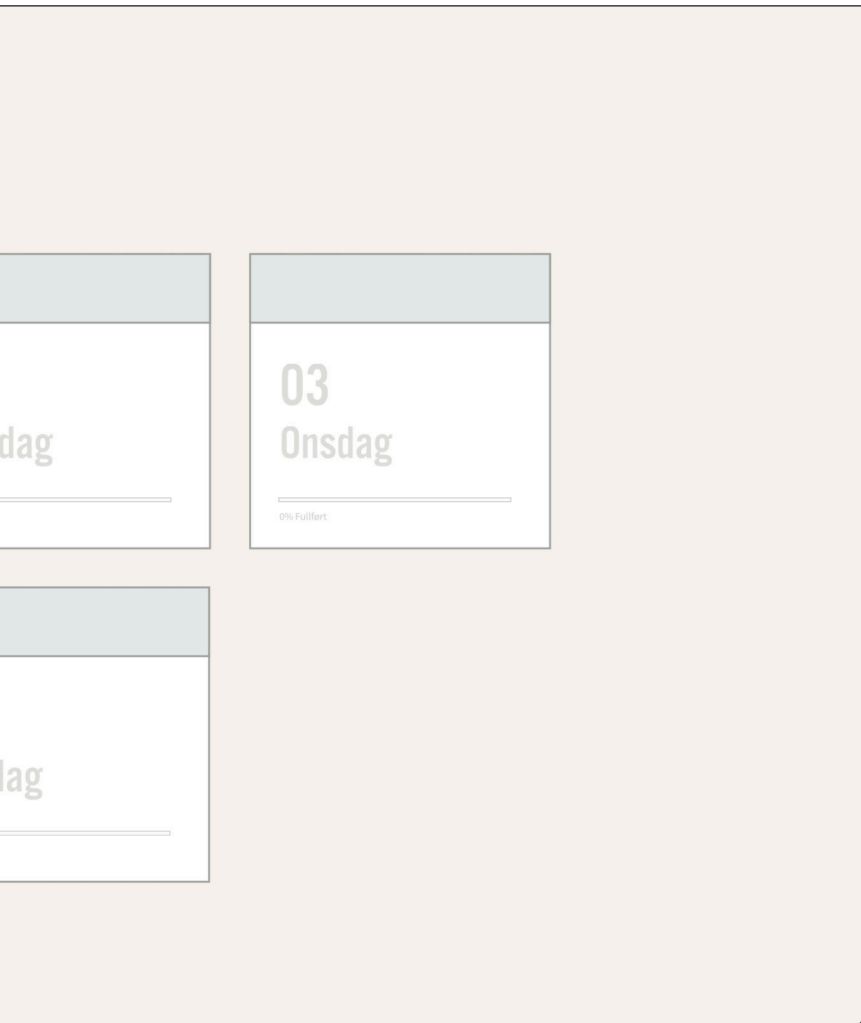
Bjarne explains the purpose of the course.

A02: Home page

Course- and progress overview

The program consists of six courses that covers different learning goals.

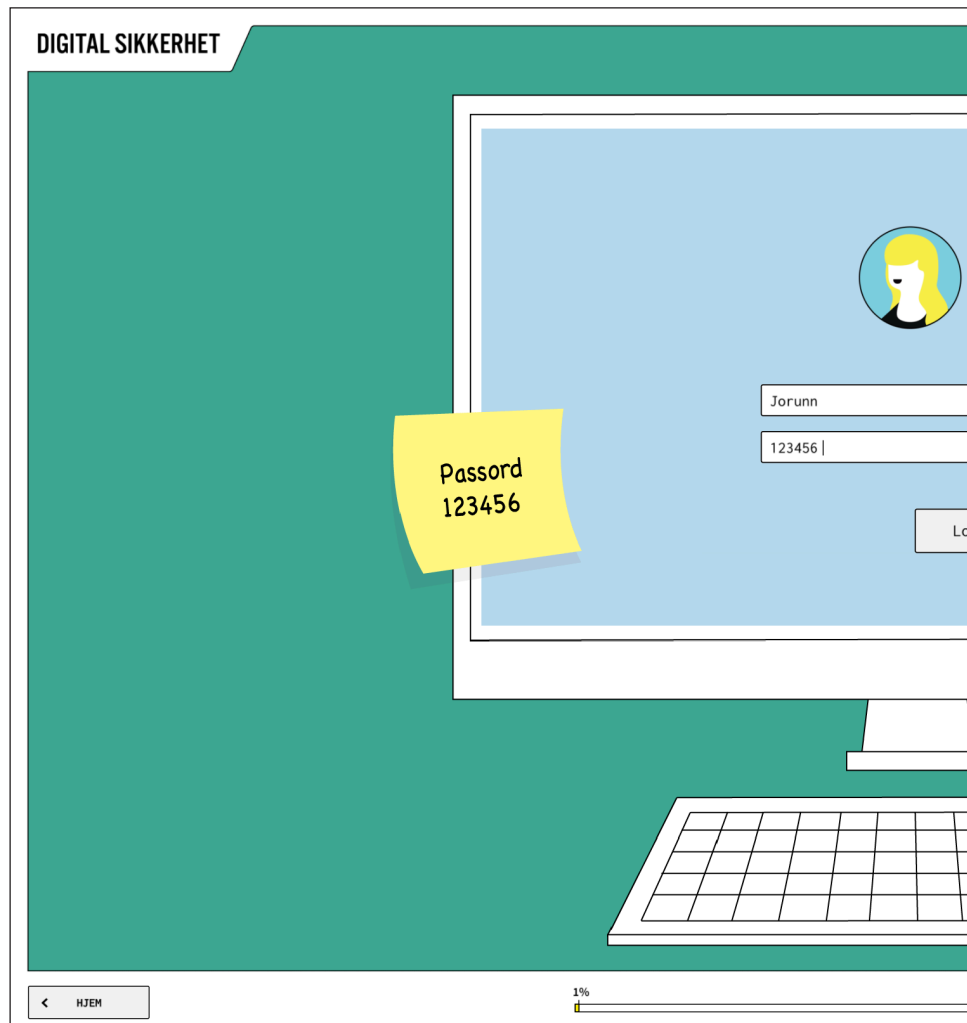


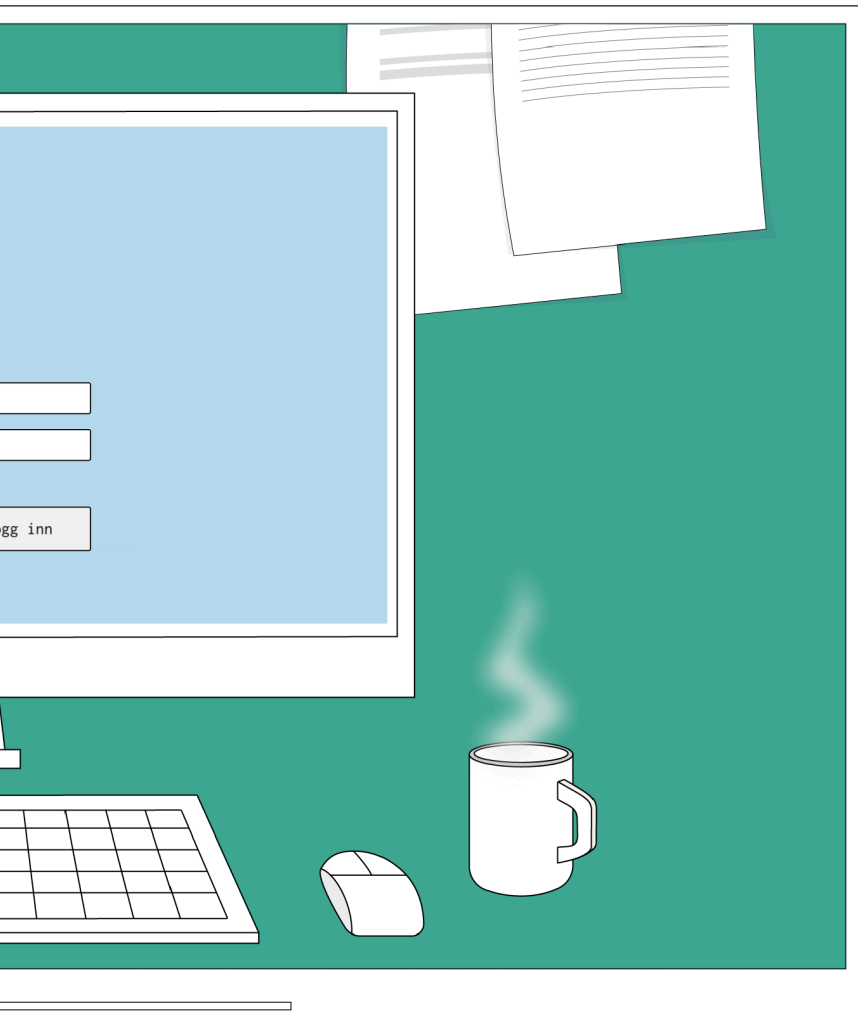


A03: Login

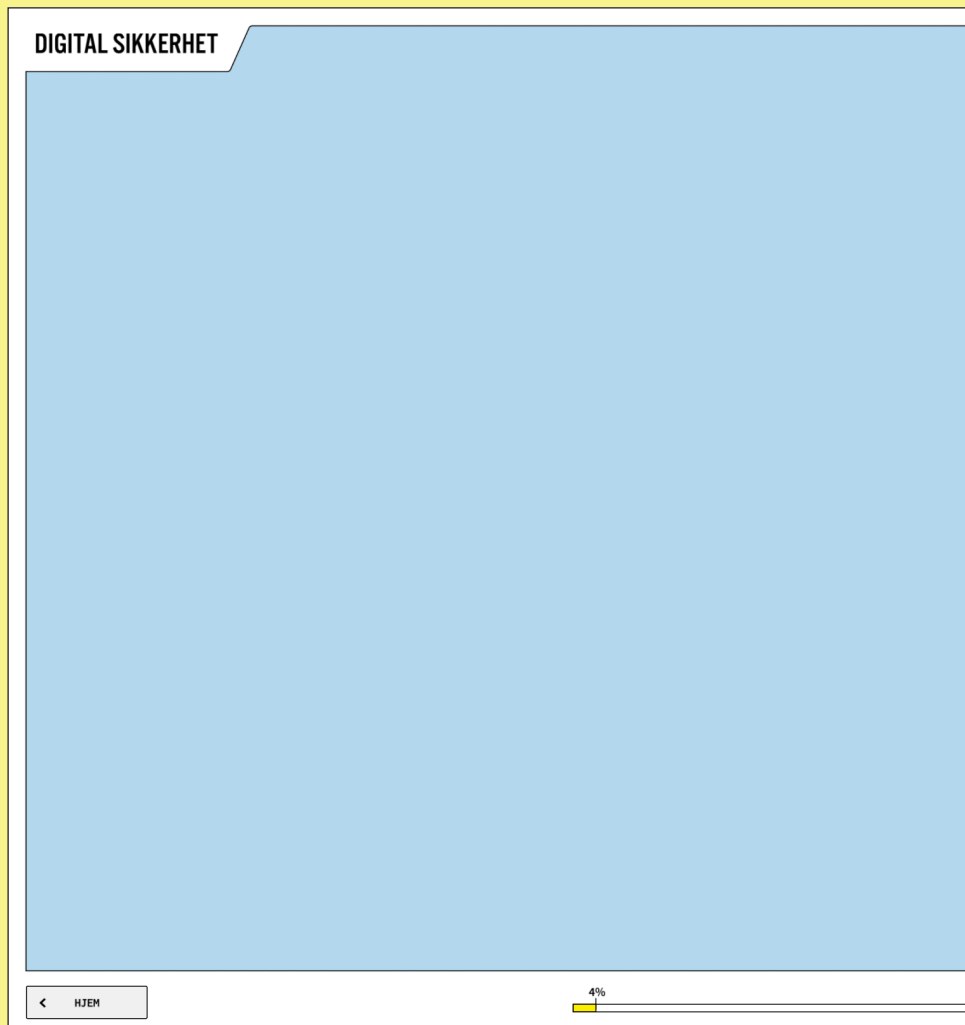
Starting point of the course

A workplace is introduced and the user enters their name and a password that is written on a post-it.





06. Deliver: **Main pages**



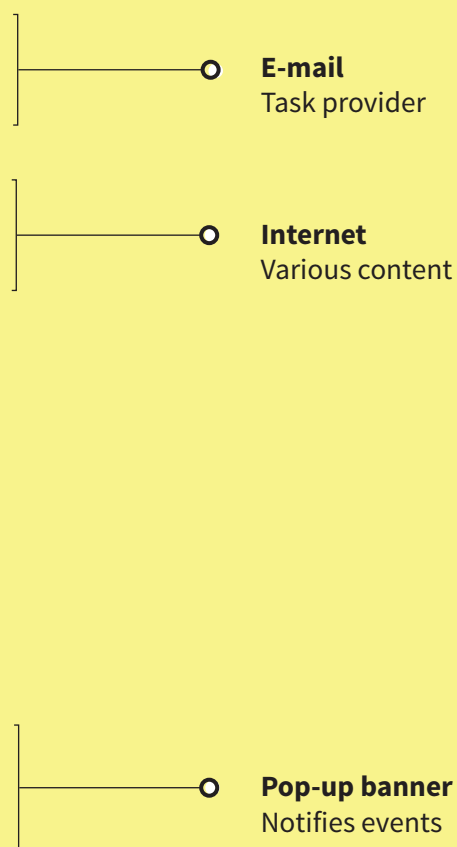
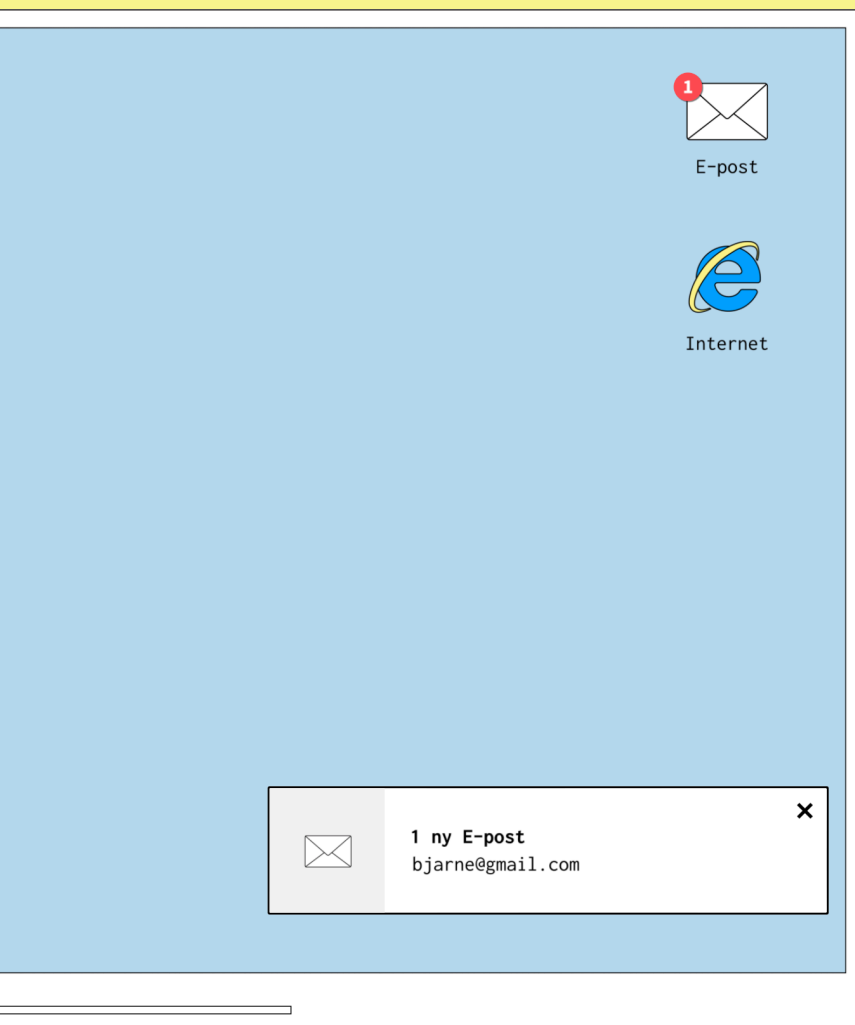
Home button
Takes you back to
Home page

Progress bar
Shows progress

B01: Landing page

Main navigation

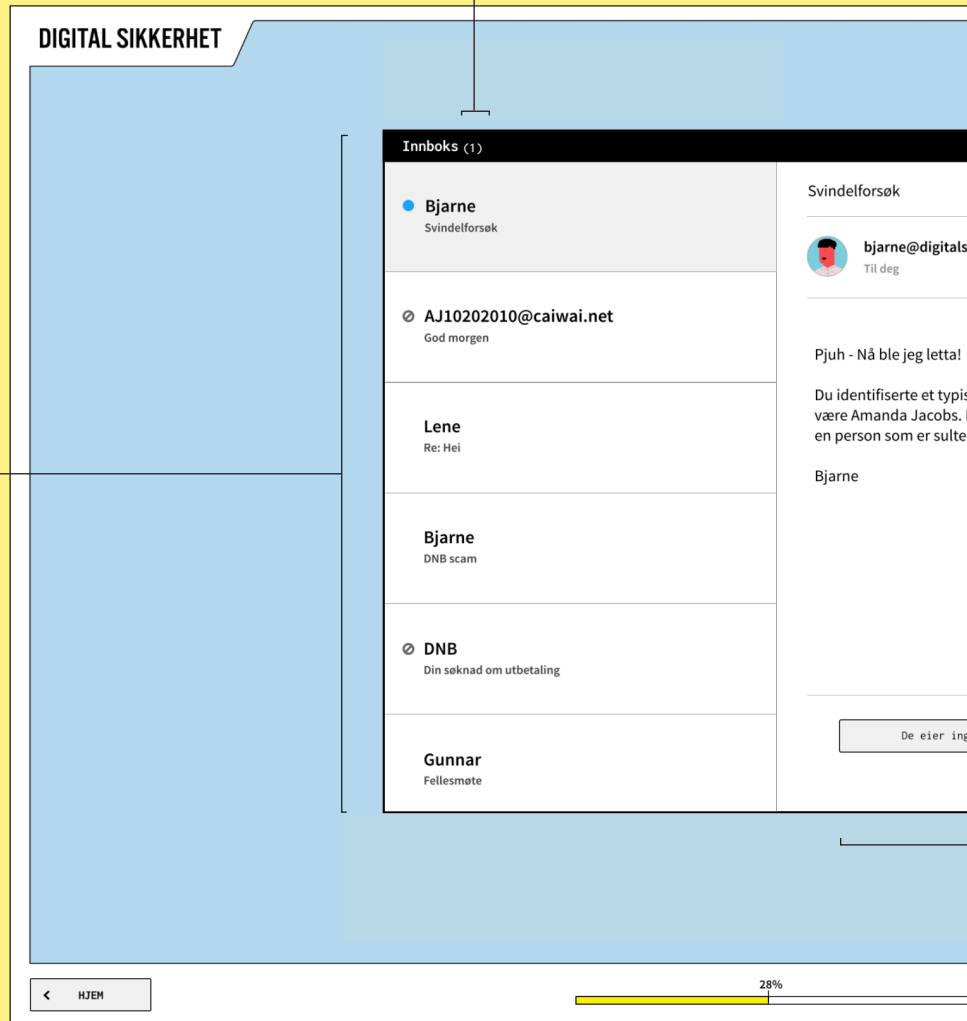
The user has the option to interact with the 'e-mail'- or 'internet' page and can at any time go back to the homepage.



06. Deliver: Main pages

○ **Unread Emails**
Visualized by number

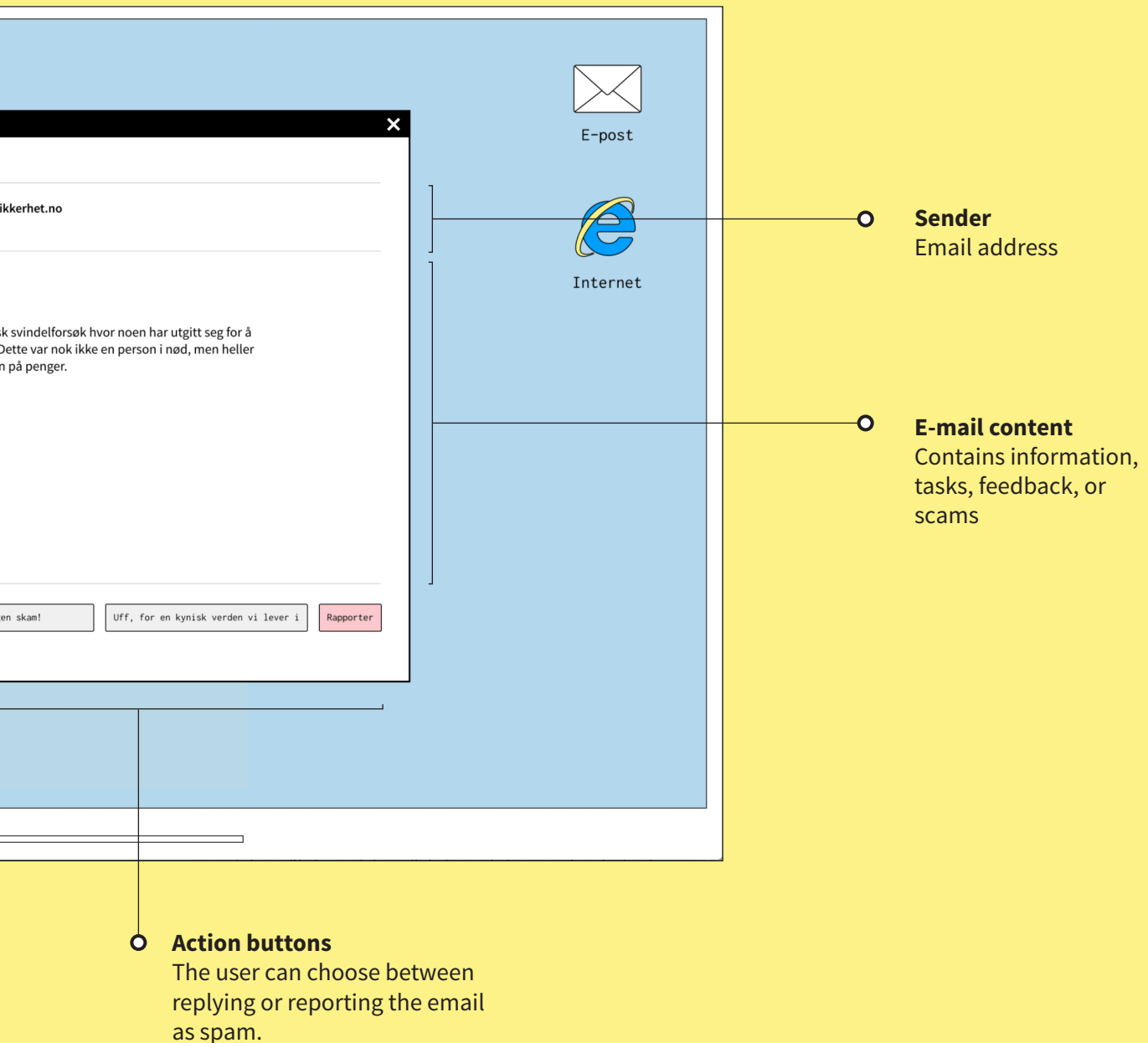
Recieved E-mails ○
From Bjarne, the CEO,
coworkers and scammers.



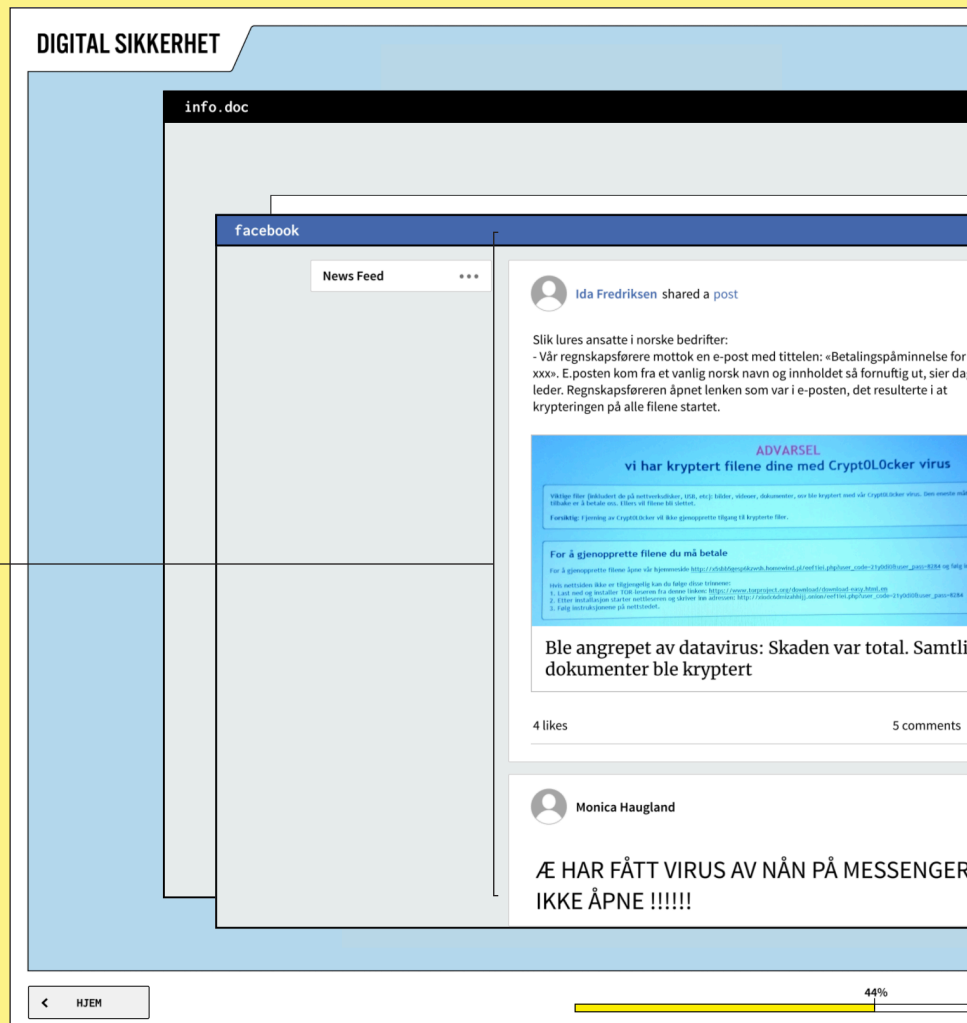
B02: E-mail

Task provider

The e-mail provides tasks and information where the user has to make decisions in order to progress. The e-mails varies in content and be everything from advices from Bjarne, tasks from the boss, gossip from colleagues and phishing e-mails from scammers.



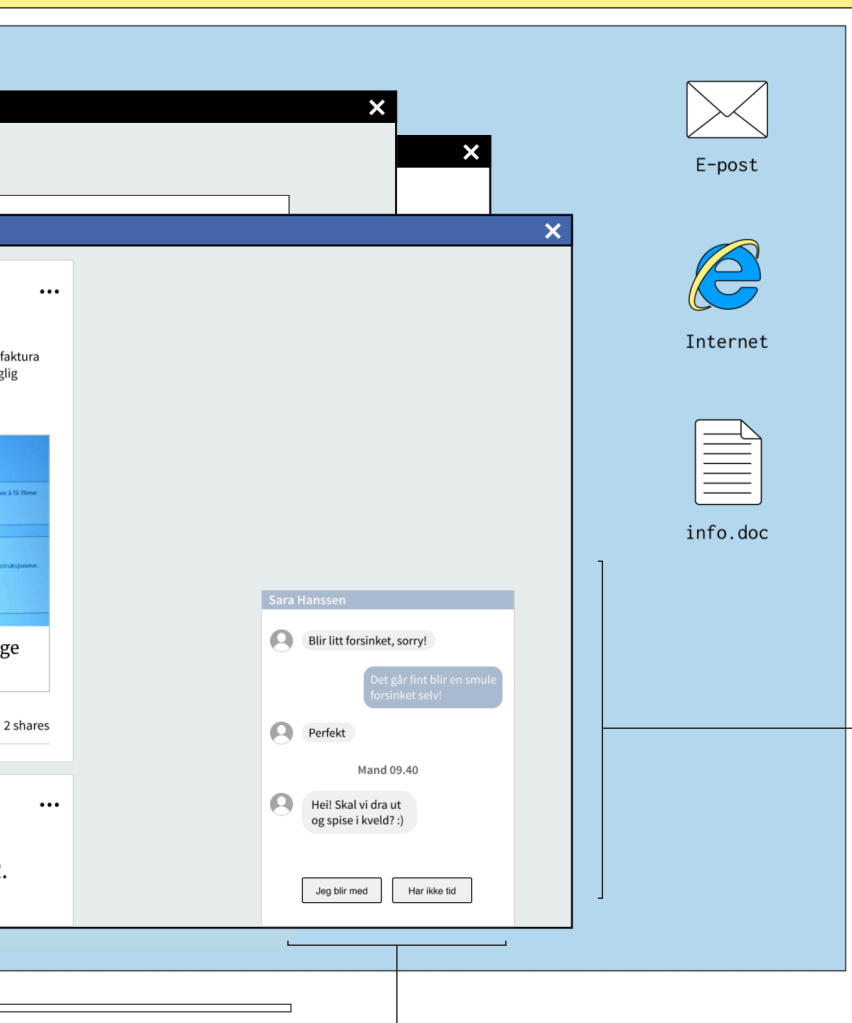
Adaptable content
The news feed covers
Digital security matters



B03: Internet

Various content

The Internet page can serve several purposes: in our prototype the user is distracted by notifications from facebook which he/she can choose to act upon.



New message
The user receives chat messages

Dialogue buttons
The user can choose between two replies.

DESIGN ELEMENTS

Notifications

As a workplace consists of people with different background, age group, and interest for technology, it is important that the navigation is easy to understand. We have used conventions such as colours and symbols to catch the users attention, and to differentiate events from each other.



Red dot

Notifies new events

● Bjarne

Blue dot

Unread e-mails

Inbox (1)

Inbox (x)

Illustrates number of new emails



Banners

Notifies new events



Hovereffects, links and attachments

Some E-mails contains links, attachments or terms that the user can interact with.

Links

Mouseover links to verify the url

http://wb.hrtfh.com/img/DNB
Klikk for å følge linken

[sjekke detaljene av kontoen din](#)



Terms

Mouseover terms to get more information

Phishing er en metode kriminelle bruker for å lure mennesker til å gi fra seg sensitiv informasjon eller penger via Internett.

[phishing e-post](#)

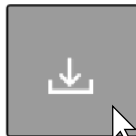


Attachments

Mousover attatchments and download if it's from a trusted sender



Last ned



Last ned

Dialogue buttons

The user has two dialogue options: a positive or a negative loaded reply. The third option is to report an email as spam. The choices you make will have an impact on how the story plays out.



FEATURES

Template model

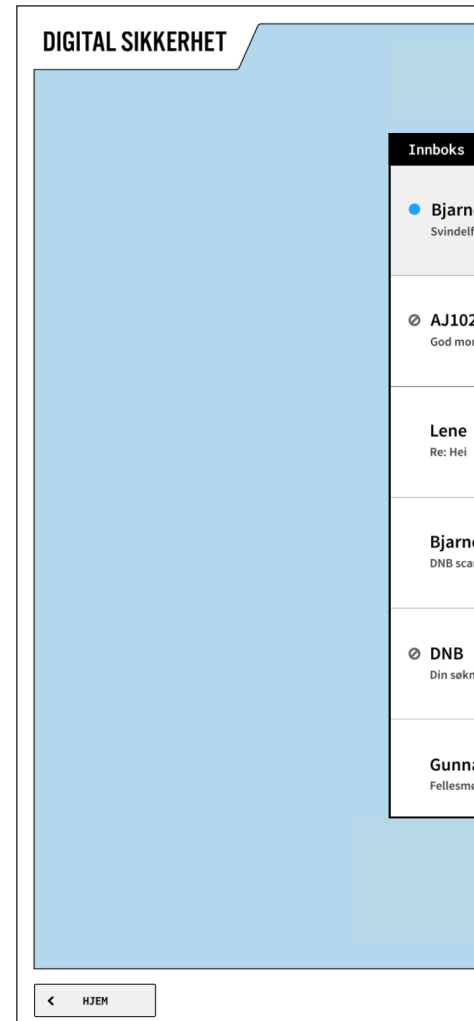
The learning program is based on a template model that has a permanent structure and adaptive content.

Updated on the risk image


Most content is text based, and easy to update. This enables the program to keep up with the changing threat landscape.

Relatable

The service adapts the content to working sectors and companies in order to make it more relatable for the users.



Svindelforsøk

 **bjarne@digitalsikkerhet.no**
Til deg

Pjuh - Nå ble jeg letta!

Du identifiserte et typisk svindelforsøk hvor noen har utgitt seg for å være Amanda Jacobs. Dette var nok ikke en person i nød, men heller en person som er sulten på penger.

Bjarne

De eier ingen skam! Uff, for en kynisk verden vi lever i Rapporter

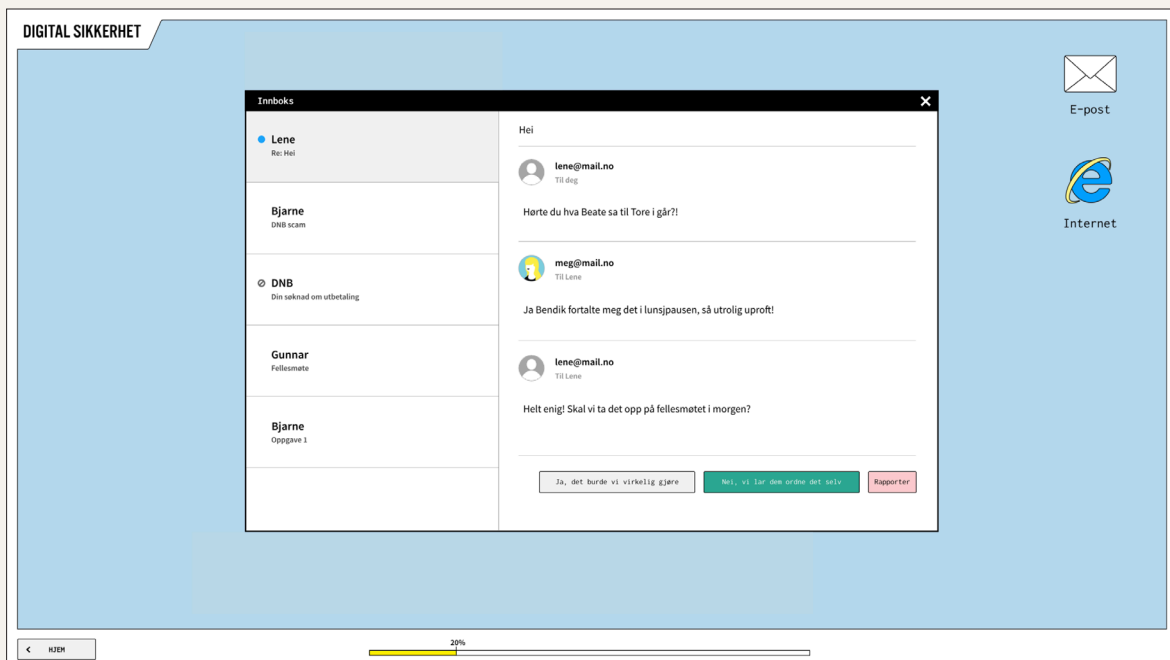
E-post

Internet

28%

Culture

We have implemented references from daily life in the workplace in order to make the learning program relatable for the user. The elements are based on user insight and validated through user testing.

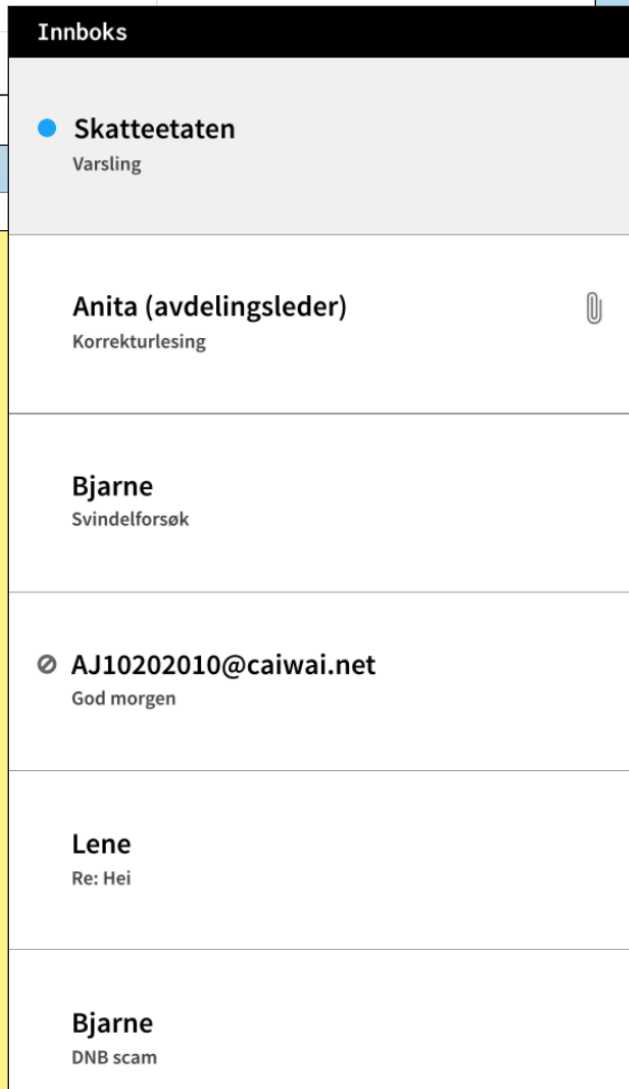
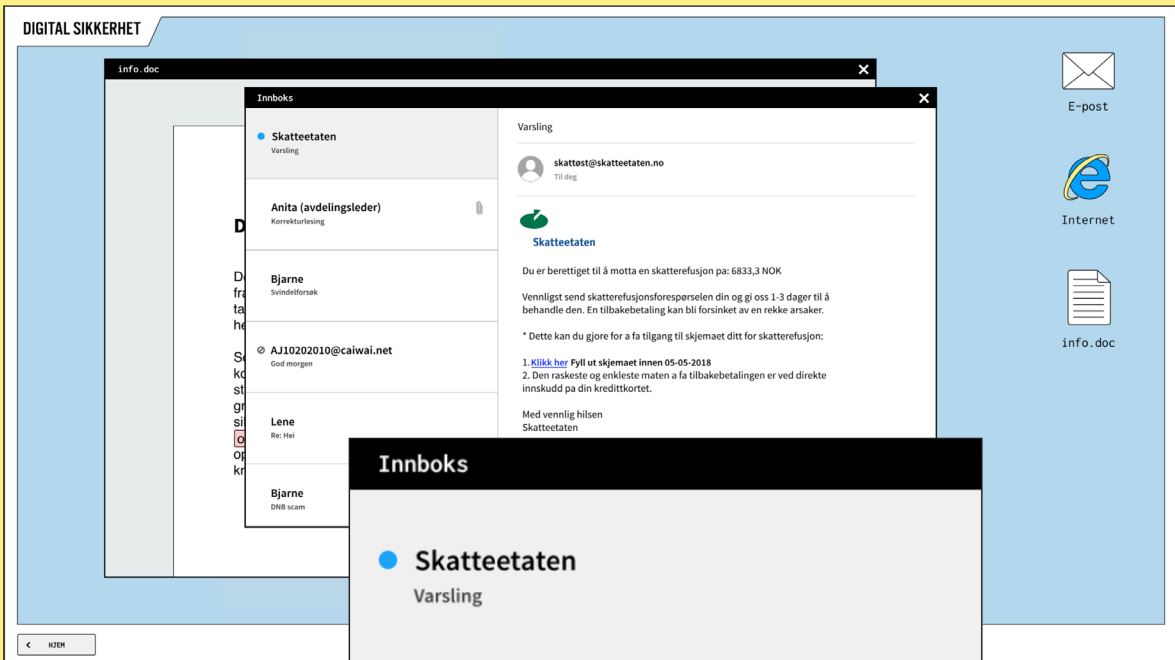


Personalization

A way of personalizing the story is to include the users name that is specified during the login phase. The sender refers to this name throughout the course where the user plays the 'role' as him/herself.



06. Deliver: Features



Storytelling through emails

The storytelling plays out through different characters that appears via emails. By telling the story through email we aimed to spark curiosity and motivate the user to complete the course.

- **Anita, the CEO**
The CEO provides the user with tasks, and gives feedback when the user has performed a bad security decision that affects the company. Through the CEO, the user is taught how an individual action can lead to bigger consequences.
- **Bjarne the storyteller**
Guides the user through the course and teach them how to do good risk assessments. Bjarne also gives instant feedback on the choices that has been made.
- **Scammers**
The phishing mails are based on actual scams that manipulate users to give them sensitive information. The goal is to teach the user how to identify real life fraud attempts.
- **Coworkers**
The coworkers send work related- and private emails and plays on cultural aspects from daily life at work: how they communicate, norms, and habits at the workplace.

Discrete learning

How can the learning program inform users about security measures without being preachy? The solution contains a feature we call 'discrete learning'. In the prototype they appear as facebook posts and work tasks from the CEO. The purpose is to implicitly inform the user about digital security matters, and by that avoid overwhelming the user with cyber security 'nag'.

Levels of learning

The feature also facilitates for different levels of learning. If the user find something very interesting, he or she can go in depth of the material and learn more about it.

Task from boss ▾

The user has to proofread a text that informs about digital security.



”Tell me more”

When you are introduced to a task by Bjarne, you have the option to get more information about the topic

Ok, den er grei

Hva mener du med phishing e-post?

Rapporter

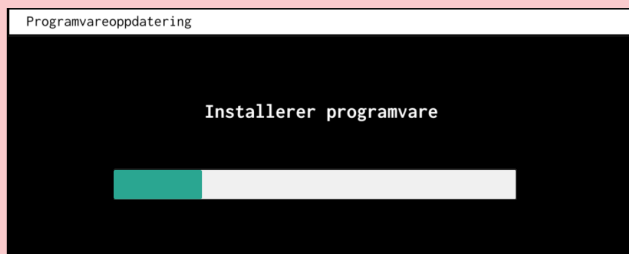
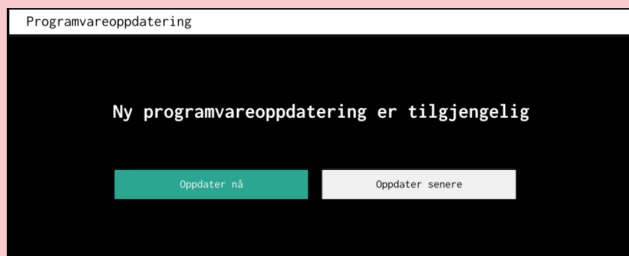
The screenshot shows a desktop environment with a taskbar on the right containing icons for E-post, Internet, and info.doc. A window titled "DIGITAL SIKKERHET" is open, displaying a Facebook post by Ida Fredriksen. The post text reads: "Slik lures ansatte i norske bedrifter: - Vår regnskapsfører mottok en e-post med tittelen: «Betalingspåminnelse for faktura xxx». E-posten kom fra et vanlig norsk navn og innholdet så fornuftig ut, sier daglig leder. Regnskapsføreren åpnet lenken som var i e-posten, det resulterte i at krypteringen på alle filene startet." Below the text is a blue warning banner: "ADVARSEL vi har kryptert filene dine med CryptOLocker virus". Under the banner, it says: "Ble angrepet av datavirus: Skaden var total. Samtlige dokumenter ble kryptert". The post has 4 likes, 5 comments, and 2 shares. Below the post is another post by Monica Haugland with the text: "Æ HAR FÅTT VIRUS AV NÅN PÅ MESSENGER. IKKE ÅPNE !!!!!".

Facebook posts >

The user can click to read more about the post in the news-feed.

'Distracting' elements

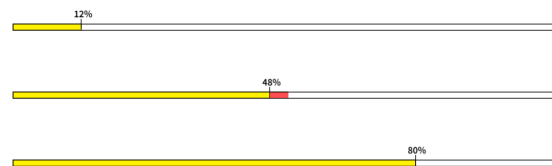
Through the course the user will be exposed to what we call 'distracting elements'. The purpose is to show how concentration, stress level and workflow can affect security. They appear as pop-ups for new emails, software update, and facebook notifications.



FURTHER EXPLORATION

Progress bar

The progress bar shows how much of the course is completed, and it adapts to the user's actions. If choosing all right actions, the user will finish the program faster. When choosing a wrong action, you will get a short term or long term consequence leading the progress bar to be reduced.



Digital security drill

During our research phase we realized that businesses have a written evacuation plan, and hold fire drills regularly. But what about holding a digital security drill?

We suggest that the companies who use our service establish a breach response plan that is practiced through a security drill routine once a year. The drill aims to improve the reaction time as the employees are trained on how to act and who to contact during such times.

IP Address

IP addresses contain information about which software- and browser you are using whilst conducting the course. It would be interesting to explore how this information could be used to make the experience even more user adapted. If you for instance use a windows computer and are browsing through Internet Explorer the interface could adapt accordingly.

FLOWCHART

The flow chart shows how the users actions affects the story line.

Actions

Click a link and enter account information: If the user clicks a phishing link and specify their account details, they will either get feedback from the CEO or Bjarne (consequences).

Download attachment from CEO: a task that you have to execute.

Reply

Replying scam: negative feedback

Replying Bjarne, colleague and CEO: positive feedback

Unless you ask for more information, you have two dialogue options which leads to the same point. The purpose with having the options is to involve the user. However if you reply to scams you'll have a detour.

Report

Reporting a scam: positive feedback and information on why this was the right choice.

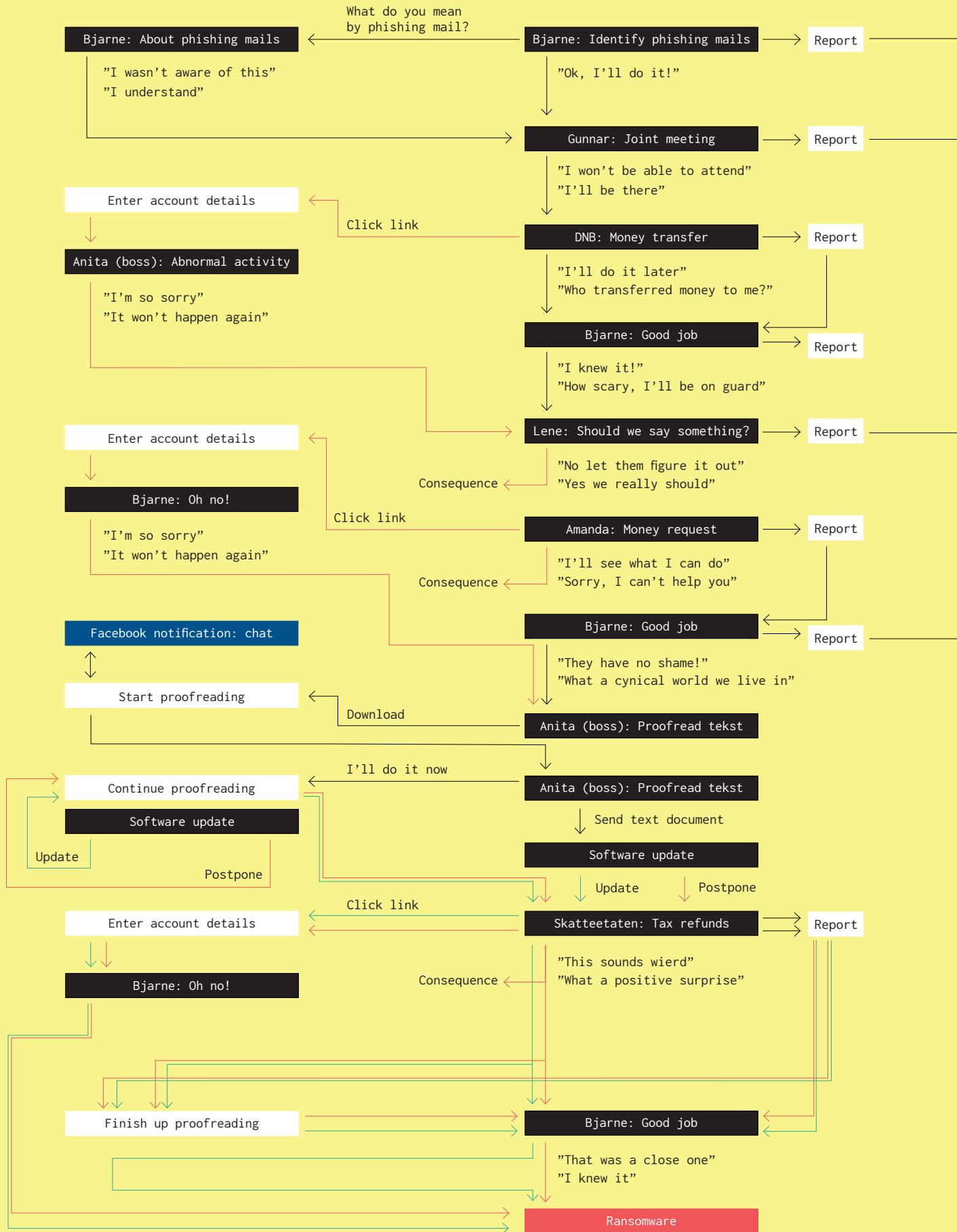
Reporting Bjarne, a colleague or the CEO: leads to various funny replies. These are not included in the flowchart, as we have chosen to focus on the main flow of the prototype for this delivery.

Long term and short term feedback

When acting upon a dialogue, task or distracting element, you will either receive an instant or long term feedback.

Short term: Instant feedbacks from Bjarne, telling you why you made a good or bad decision.

Long term feedback: For example a consequence of postponing a software update. In our prototype this happens when you postpone a software update. You will then receive ransomware later in the program.



USER TESTING

As our learning program aims to be relatable, the prototype was adapted to the working sector of our test participants. They were employees working with social services at NAV.

Our success criterias

- The users understand the structure
- The users understand the navigation
- The users relates to the content
- The content is understandable
- The tone of voice is friendly and empathic



First test

Participants:

Female (27), social services, NAV
Female (28), social services, NAV
Male (25), interaction design student,
previously worked at NorSIS)

Observation and feedback

In this test the participants conducted the course together.

- The users had fun
- The users cooperated and discussed with each other
- The users disagreed on some of the task
- The users understood how to navigate through the course
- The users had comments on the introduction text
- The users wondered who Bjarne was: Was he a scammer or was he a friend?
- Confusion around the report and dialogue button as they were presented on the same level. It also felt like clicking next as you only had the possibility to choose one answer or report the email
- Input on adding standard signature in mails.

“I believe that to change people’s security habits you need to train on it.”

Female (27)

First iteration

Separate the dialogue buttons and report buttons. From having one dialogue response, we decided to go for two. Our thought was to make the user reflect more upon the answers and avoid having a dialogue button that functioned as a next button.

We also changed Bjarne’s mail to bjarne@digitalsikkerhet.no to make him seem more trustworthy and not mistaken for a scam-email.

Added standard signature in mails

Second test

Participants:

Female (50), social services

Male (47), social services

Female (27), consultant, social service

Observation and feedback

In this test the participant conducted the course individually.

- The new dialogue buttons worked as we hoped as the participants spent time reading the information, and reflected upon which answer they should pick.
- Female (50) and the female (27) instantly postponed the software update when it appeared on the screen. One of them even thought it was actually happening on the computer.
- The female (27) was very secure in her actions. She knew what to look for to spot scam emails. However she failed in one of the tasks.
- The male (47) didn't know what phishing was, and wanted more information it
- Event invites for meeting was typical NAV 'style'
- The male user did not register events when multiple things happened on the screen at the same time
- The users still didn't trust Bjarne
- The user did not understand the scenario with the e-mail thread where the user was part of a conversation.



2nd Iteration

Bjarne is introduced in the intro part of the course. The user has the possibility to get more information if they want to by answering a mail from bjarne with "what is phishing?" To emphasize who is saying what a user profile picture is implemented in the e-mails.

"I've conducted several e-learning courses before, but I have a tendency to quickly flick through the content. I believe that this is a good solution as it's fun to interact with."

Female (50)



Evaluation of testing

We were happy to see that the participant enjoyed the sequence and that the level of difficulty was well balanced. We were surprised to see that most participants postponed the software update. This reflected the users habits and verifying the learning goal. It is important to note that user testing by observation can give biased responses as the user might act differently when they are being watched. However we got many valuable feedbacks and observations that we have accounted for in our final design.

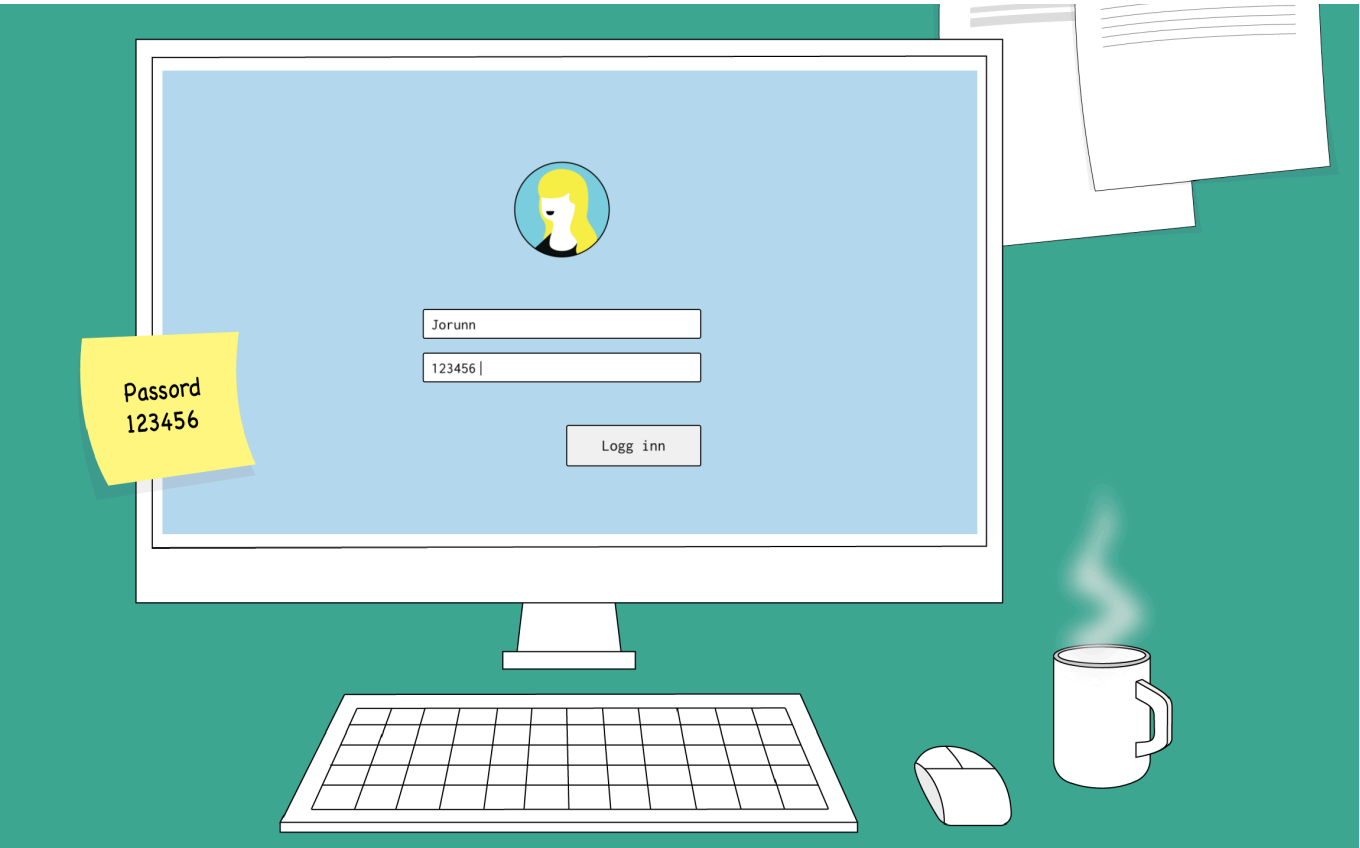
VISUAL IDENTITY

The cyber security industry is characterized by a high tech expression, with dark colours of black and blue. As our project is focused on people, we have decided to take distance to this expression, and take a different approach in the visual identity of the service.

Our service 'Digital Sikkerhet' aims to educate users on the threat landscape without playing on fear. This is done through the use of bright colours, and playful expression. The learning program has a flat, stylized design so that the user cannot mistake it for being real. With these design grips the service aims to provide the user a learning environment that appears safe, positive, and engaging.

Tone of voice

The service main audience are employees working in Norway, thus the main language is Norwegian. The tone of voice is coloured by the working culture where we combine both informal and formal language based on who you are communicating with. It's an overall friendly and down to earth tone in our prototype and we've worked on making the content relatable as well as keeping it short and concise.



Typography:

ALTERNATE GOTHIC NO3

Inconsolata

Colors:



ONBOARDING SERVICE

Understanding need

Company experience hack attempts

/

Media informs of increasing hacking events.

/

Company conducts a digital security culture evaluation.

Contacting Digital Security

Security responsible visits Digital Security website

Orders security package

Orders a package specific to working sector

Package

Company Recieves Material

Inviting employees to course



ed for

E-learning

Intranet

/

E-mail

/

Slack

SERVICE JOURNEY








Course Introduction

Meeting the service

Implementation

Conducting web course



Scenario	User receives course invitation from security department	Opens course website	User conducts web course Scenario 1. Scenario 2. Scenario 3.
Context	At the office	At the office	At the office / at home
Touchpoints	 Intranet/Email/Slack	  Intranet/Email/Slack Website	 Website
Platform	 Computer	 Computer	 Computer

Evaluation

Evaluating culture (GDPR Regulation)



Scenario 3.	Scenario 4.	Scenario 5.	User participates in security drill	Security culture evaluation
			Activity at work	At work
	 Website	 Group activity	 Survey/Test	
	 Computer	 Phone	 Computer	 Survey/Test

07. Conclusion

This section outlines our own reflections on our results and the project as a whole.

REFLECTIONS

We started the project with little previous knowledge about the field of cyber security and wondered where the project would lead us. What we initially thought was a technical and complex field soon turned out to be about the people, the culture they form and the digital environment that influence them. What astonished us was that serious data breaches in many cases starts with a simple click on a link where an attack could have been prevented if the user had been precautious.

A discovery we made throughout the project was that the cyber security business is hard to cooperate with due to business secrecy. We met with two potential partners with business models based on trade secrets. A prerequisite for collaboration was that we had to give away ownership to our work, before knowing the details of what companies did. As we wanted to have an open diploma, we decided to pave our own path.

Although we found that the cyber security industry is not solely about technology, it still seems to be coloured by IT and security professionals. Here we see a potential for designers to play an important role. By introducing a human centered approach we can contribute with secure and user friendly experiences in contact with digital systems, or as in our project, apply our communications skills for teaching and engaging people on how to do risk assessments in digital space. There are many ways designers can influence the cyber security field, and we have addressed some of them. With this diploma we aim to inspire other designers to participate in solving the challenges we are facing in the increasingly digitised society.

REFERENCES

Online articles

Hern, A (2018). Cybercrime. Retrieved January 24, 2018, from:
<https://www.theguardian.com/technology/2018/jan/23/cybercrime-130bn-stolen-consumers-2017-report-victims-phishing-ransomware-online-hacking>

Forno, R (2017). Overcoming 'cyber-fatigue' requires users to step up for security. Retrieved January 24, 2018, from:
<https://theconversation.com/overcoming-cyber-fatigue-requires-users-to-step-up-for-security-70621>

Solberg, E (2018). Nasjonal strategi for IKT-sikkerhet. Retrieved March 06, 2018, from:
<https://www.regjeringen.no/no/aktuelt/nasjonalt-strategi-for-ikt-sikkerhet/id2592996/>

Nielsen, H. S and Strøm, T. J (2018). Tre av ti oppga passordet da Nasjonal sikkerhetsmyndighet «angrep» offentlig virksomhet. Retrieved March 25, 2018, from:
<https://www.aftenposten.no/norge/i/L0ew0P/Tre-av-ti-oppga-passordet-da-Nasjonalt-sikkerhetsmyndighet-angrep-offentlig-virksomhet>

Soloms, R. V. and Niekerk J. V (2013). From information security to cyber security. Retrieved April 05, 2018, from:
http://www.profsandhu.com/cs5323_s18/Solms-Niekerk-2013.pdf

Watercutter, A. and Ellis E. G (2018). The wired guide to memes. Retrieved April 06, 2018, from:
<https://www.wired.com/story/guide-memes/>

Sausaluto, C (2018). Women Represent 20 Percent Of The Global Cybersecurity Workforce In 2018. Retrieved May 03, 2018, from:
<https://cybersecurityventures.com/women-in-cybersecurity/>

Palmer, D (2018). What is malware? Retrieved May 03, 2018, from:
<https://www.zdnet.com/article/what-is-malware-everything-you-need-to-know-about-viruses-trojans-and-malicious-software/>

Badrick, C (2018). How Organized Cybercrime Works. Retrieved April 29, from: <http://www.turn-keytechnologies.com/blog/network-solutions/how-organized-cybercrime-work>

Schneier, B (2015). What Does It Take To Feel Secure? Retrieved April 29, from: https://www.schneier.com/news/archives/2015/04/what_does_it_take_to.html

Online publications

The Norwegian Business and Industry Security Council - NSR (2016). Norwegian computer crime and data breach survey 2016. Retrieved January 24, 2018, from: https://www.nsr-org.no/getfile.php/Bilder/M%C3%B8ketallsunders%C3%B8kelsen/morketallsundersokelsen_2016_eng.pdf

The Fletcher School at Tufts University, in partnership with Mastercard (2017). Digital Evolution Index 2017. Retrieved February 08, 2018, from: https://newsroom.mastercard.com/wp-content/uploads/2017/07/Mastercard_DigitalTrust_PD-FPrint_FINAL_AG.pdf

Malmedal, B. and Røislien, H. E (2016). The Norwegian Cyber Security Culture. Retrieved March 7, 2018, from: <https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf>

The Norwegian National Security Authority - NSM (2018). Risiko 2018. Retrieved March 7, 2018, from: https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2018_web.pdf

Roer, K., Dr. Petric, G, Indepth insights into the human factor (2017). Retrieved March 7, 2018, from: <https://app.hubspot.com/presentations/2826562/view/5425421?accessId=438567>

European Union Agency for Network and Information Security - ENISA (2017). Retrieved April 3, from: <https://www.enisa.europa.eu/publications/info-notes/phishing-on-the-rise>

