Katri Kauppinen

Towards better information security with UX practices

A Systematic Literature Review

School of Technology and Innovation
Master's thesis in Information Systems
Information Systems

Vaasa 2023

UNIVERSITY OF VAASA
School of Technology and Innovation
Author: Katri Kauppinen
Title of the Thesis: Towards better information security with UX practices : A Systematic Literature Review
Degree: Master of Science in Economics and Business Administration
Programme: Information Systems
Supervisor: Tero Vartiainen
Year: 2023 **Pages:** 73

ABSTRACT:
When the risk of information security breach is rising higher, companies are trying to find ways to take better care of information security. There have been implications of making information security on the expense of user experience and vice versa. It'd be important to get people to understand that both information security and user experience are everyone's responsibility. This work attempts to find ways to combine information security and user experience theories and practices in a way which could make better and safer user experiences possible. This work is taking look at the subject on metalevel, and aim is to bring better understanding of possibilities in improving information security and user experience in collaboration with each other.

A systematic literature review was conducted to meet the goals set. Literature was retrieved from two different databases in January 2023. The research time range consisted of studies published during Covid-19 pandemic meaning January 2020 – January 2023. Material was evaluated on the relativity basis on both information security and user experiences studies. The material selection proceeded on first evaluating the article titles and abstracts also leaving out studies published out of the set time range. Secondly the introductions and conclusions and on the final round the studies were evaluated as whole and the most relevant 21 articles were chosen as primary studies.

The combination of information security and user experience has not been studied for long as it seems to have been studied for about past 20 years. Also based on the number of articles related it seems that the interest towards the subject has risen as the number of published articles annually has increased from about dozen to tens and during recent years even over 100 articles a year.

Synthesis was done based on the chosen primary articles. Plenty of different user experience actions were found to improve information security, as information security actions mostly either decreased usability or were mentioned not to decrease user experience. Only focusing development to security features users valued was considered to improve user experience.

The most important findings were, that organizations are providing different kinds of information security training, but plenty of adjustments can be made to make the training more effective. Interactivity, providing modest amount of visual effects, providing examples with more thorough feedback about signs of fraudulent actions, and including little bit of gamification increased the effects and therefore also the value of the training.

The research managed to show value in cooperation between information security and user experience experts and providing information regarding recent changes in the post-pandemic world.

KEYWORDS: information security, user experience, data security, privacy

VAASAN YLIOPISTO
Tekniikan ja innovaatiojohtamisen akateeminen yksikkö
Tekijä: Katri Kauppinen
Tutkielman nimi: Towards better information security with UX practices : A Systematic Literature Review
Tutkinto: Kauppatieteiden maisteri
Oppiaine: Tietojärjestelmätiede
Työn ohjaaja: Tero Vartiainen
Valmistumisvuosi: 2023 **Sivumäärä:** 73

TIIVISTELMÄ:
Aikana, jona tietoturvallisuus poikkeamien riski kasvaa korkeammalle, yritykset yrittävät löytää keinoja vastata tietoturvallisuudesta paremmin. Aiemmin on esiintynyt näkemyksiä tietoturvallisuuden toteuttamisesta käyttäjäkokemuksen kustannuksella ja toisin päin. Olisi tärkeää saada ihmiset ymmärtämään, että sekä tietoturvallisuus että käyttäjäkokemus ovat kaikkien toimijoiden vastuulla. Tämä tutkimus tarkastelee aihetta metatasolla tarkoituksena tuoda lisää ymmärrystä mahdollisuuksista parantaa tietoturvallisuutta ja käyttäjäkokemusta yhteistyössä toistensa kanssa.

Vastauksia haettiin systemaattisella kirjallisuuskatsauksella. Hyödynnetty aineisto noudettiin kahdesta eri tietolähteestä tammikuussa 2023. Tutkimukseen valittiin mukaan aineistoja, jotka oli julkaistu Covid-19 pandemian aikana tammikuussa 2020 – tammikuussa 2023. Aineistoa arvioitiin tutkimusten esittämän liitännäisyyden perusteella koskien tietoturvallisuutta ja käyttäjäkokemusta ja näiden vaikutusta toisiinsa. Aineiston valinta eteni ensin rajaamalla aikarajoituksen ulkopuolelle jäävät tutkimukset pois ja arvioimalla artikkeleiden otsikoita ja tiivistelmiä, sitten johdantoa ja lopputuloksia, ja tämän jälkeen vielä mukana olleet tutkimukset luettiin kokonaan, jolloin lopulta tutkimukseen valikoitui 21 artikkelia.

Tietoturvallisuutta ja käyttäjäkokemusta yhdessä on tutkittu vasta viimeiset 20 vuotta. Mielenkiinto tutkimukseen on kuitenkin yhteisöllä herännyt, sillä viime vuosina vuosittain julkaistujen artikkelien määrä on noussut noin tusinasta artikkeleita kymmeniin ja viime vuosina jopa yli sataan artikkeliin vuodessa.

Synteesi perustui valittuihin primaaritutkimuksiin. Tuloksissa korostui käyttäjäkokemukseen liittyvät toimet, jotka auttoivat parantamaan tietoturvallisuutta. Tietoturvallisuuden toimien osalta toimet lähinnä joko heikensivät käytettävyyttä tai niistä mainittiin, ettei toimet heikentäneet käyttäjäkokemusta. Ainoa käyttäjäkokemusta parantava asia oli tuotekehityksen keskittäminen tietoturvaominaisuuksiin, joita käyttäjät pitävät tärkeinä.

Tutkimuksen tärkeimmät tulokset olivat, että organisaatiot tarjoavat monenlaista tietoturvallisuuskoulutusta, mutta koulutuksen tehokkuuteen voidaan vaikuttaa useammillakin toimilla. Tehokkuutta saatiin parannettua interaktiivisuudella, rajaamalla visuaalisten efektien määrää, sisällyttämällä vähän pelillisiä piirteitä, nostamalla esille esimerkkejä ja sisällyttämällä niihin mukaan tarkempia palautteita ja sisällyttämällä tietoa potentiaalisen tietoturvapoikkeaman merkeistä.

Tutkimus onnistui osoittamaan, millaista arvoa on mahdollista tuottaa yhdistämällä tietoturvallisuuden ja käyttäjäkokemuksen asiantuntemusta. Lisäksi pystyttiin tarjoamaan tietoa liittyen viimeaikaisiin muutoksiin Covid-19 pandemian jälkeisessä maailmassa.

AVAINSANAT: tietoturva, käyttäjäkokemus, yksityisyys

Contents

Pictures

Tables

Abbreviations

CS	Cyber security
Infosec	Information security
UX	User experience

1 Introduction

Nielsen Norman Group's expertise is user experience and behind the company there are well renowned user expertise gurus Don Norman and Jakob Nielsen. According to Nielsen (2004) users shouldn't be obligated to take responsibility of information security (infosec) and training users about information security is not answer to information security issues though people were still considered as the weakest information security link. Verizon creates annually a data breach report and the report for 2021 included 80 000 cases where the data had been compromised and more than 5 000 cases where the data had ended to an unauthorized party (Verizon, 2021). The 2021 report was analysed by Drew Robb (2021) and he stated that according to the report 85% of the cases where data was compromised had included a human element.

So, when considering the user experience (UX) side there seems to be views where information security is created on expense of user experience. Or as Nielsen stated (2004), educating users is not working for computer security is considered too complicated and cyber criminals too devious. Nielsen included also view of having "the burden on the wrong shoulders" and these information security solutions making human adapting to the ways computers work instead of the other way around. And because of this burden the users are more reluctant to try new things and it prevents people from understanding the technologies full potential.

But even almost 20 years later we can see same issues on both sides. Weakest link is till human, and even though users are educated, these compromises and disclosures of data still occur. When discussing about this matter with person from Amazon Web Services (AWS) (2022) they stated that information security is built from many pieces eventually including every person and therefore it is important that everyone knows how to take care of their information security. The ways criminals trick people change and so it was mentioned also, how important it would be to have it as continuous process to keep everyone well educated on informed regarding the latest trends.

1.1 Objectives

The objective of this research is to investigate the possibilities to combine information security and user experience to find common ground between these two completely different views. The end results give metalevel information on both fields for even in early stage it can be seen that these matters affect each other.

This research will answer questions about:

How can user experience affect information security?

How can information security affect user experience?

If user experience is taken into consideration in information security point of view users could better adapt more secure ways. It is not beneficial for neither points of view if users are too scared to use technology and if UX takes infosec into consideration, there could be even possibilities to have better experiences for users when users can trust the tools and services better.

1.2 Methods

This research first focuses on the base about what is user experience and what is information security according to literature and theories on the field. In great relation to infosec is also privacy and disclosing personal information, so also that subject is covered. After presenting the UX, infosec and privacy theory, the systematic literature review method will be presented. Research follows the guidelines for systematic literature review for information systems studies. The process will be introduced in detail and later the data and results are presented. In the end the results will be discussed.

2 User experience

By Nick Babich (2020) UX is about how people interact with different kinds of products. He uses light switch as an example and the user experience would be human turning the lights on when needing more light in the dark. According to him the users are evaluating their experience by value the product provides, functioning of the product, how the product is to use and if the product is pleasant to use.

2.1 History of UX

According to Interaction Design Foundation (2022) in 1970s Xerox introduced first personal computer and it also had first graphical user interface and companies such as Windows and Apple followed with their own solutions. That had led to questions 'How should people interact with computers?' and 'How can we make that interaction as intuitive as when we interact with other humans?'. And from there came term human computer interaction (HCI).

From the Interaction Design Foundation (2022) the timeline is drawn by explaining that at first people working with HCI were mostly from fields like cognitive psychology and computer science and they had mostly focused on how to make interaction with computers as intuitive as possible. Later it was understood that to be able to create more intuitive computers they would require more understanding of matters such as motion graphics, storytelling, and linguistics. In the 1990s the term turned from HCI to interaction design and nowadays it is called user experience design.

2.2 Guideline examples and legislation

Humans are biased for example by their experiences, goals or emotional states and it is important to take that into account when designing products and services for it needs to be considered what developers want the user to pay attention to (Johnson, 2020). There

are guidelines based on how human perception works and by following them developers can create products and services more fit for human use.

2.2.1 EU web accessibility

In European Union member countries organizations need to follow the Web Accessibility Directive since December 2016. The directive provides better access to websites and mobile apps for public services for people with disabilities. (European Commission, 2022.)

The European Commission (2022) is working on building an European "Union of equality". The directive requires websites and applications to meet certain technical accessibility standards for public sector organizations. (European Commission, 2022.)

> *'The Directive requires : an accessibility statement for each website and mobile app, a feedback mechanism so users can flag accessibility problems or request information published in a non-accessible content, regular monitoring of public sector websites and apps by Member States, and reporting on the results.' (European Commission, 2022, The Web Accessibility Directive section, para. 5.)*

The European Union member countries make the decisions about penalties for not following the directives by themselves and therefore the penalties vary. But if not following the directive, organization would be breaking EU law. And member countries are required to monitor the public sector services to follow the directive and report outcomes to European Commission. (SiteImprove, 2022.)

2.2.2 Five principles of visual design in UX

Nielsen Norman Group is company focusing on UX research and consulting and is founded by UX experts Don Norman and Jakob Nielsen (2022). Kelley Gordon (2020) is digital design lead from Nielsen Norman Group and has provided five principles of visual

design in UX. She considers these principles important for they increase usability, provoke emotions and delight, and they strengthen brand perception.

First is **scale** meaning in proper use most important elements in the design should be bigger than the less important ones for big elements are more likely to be noticed. Though they also mention that visually pleasing design uses less than 3 different sizes. Second is **visual hierarchy** which means guiding users' eye on the page to different elements in order of the importance. Visual hierarchy can be affected for example by variations in scale, value, colour, spacing, placement. (Gordon, 2020.)

Thid comes **balance** which means '*a satisfying arrangement or proportion of design elements'*. Balance occurs when there is equal distribution of visual elements on both sides of an imaginary axis cutting the middle of the screen. The axis is usually vertical but it may be horizontal. Also the area taken by the element matters, not just the amount of elements. No one area is supposed to draw users eye so that it makes it impossible for users to see other areas. Balance can be: symmetrical, asymmetrical or radial relation to axis. They mention asymmetry being dynamic and engaging creating sense of energy and movement. Symmetry is mentioned being quiet and static and radial balance is told to always lead the eye to the centre of the interface.

In Gordon's list on place four is **contrast** which means coordination of effects differentiating elements from each other to create understanding for example that these elements belong in different categories or have different functions or otherwise behave differently. Contrast can be used for example by size or colour differences to tell user the elements are different. As an example, they use delete-function shown as red. Sometimes contrast can be used by decreasing text contrast to its background to reduce value of parts that are not so important, but it comes with cost of reducing legibility and making the text more inaccessible.

Last one in Gordon's (2020) list is **gestalt principles** which are established by gestalt psychologists. Principles provide information about our way to experience the matters as whole instead of separate individual elements. These principles provide information on how humans make sense of complex images which consist of multiple elements by subconsciously arranging the parts of the images into an organized system which creates a whole instead of interpreting them as different elements. There are multiple principles, as example similarity, continuation, closure, proximity, common region, figure/ground, and symmetry and order. Proximity is especially considered important in UX as elements visually closer to each other are somehow related.

2.2.3 Gamification

Gamification is about inserting game type mechanics into something nongame instances such as websites, online discussion boards, different kinds of learning management systems. The aim with these mechanisms is to increase the interactivity and user engagement. These matters can be found useful in either individuals consisting of consumers, employees, or partners. (BI Worldwide, 2023.)

Game mechanics can be described as sets of rules and rewards which appear on a digital platform. The rewards and rules may include points, levels, missions, badges, and progress for example. Gamification is a way to motivate and enhance individuals' behaviour to achieve set goals. (BI Worldwide, 2023).

It is suggested that gamified learning may ease cognitive overload. Cognitive overload happens, when studying in immersive manner and individual is no longer able to process all the incoming new information. Overall clear objectives for learning, having the content in smaller batches and including simple navigation help with cognitive overload. Gamification helps in a manner that user is not able to skip levels in between until they have studied the previous batch and achieved the requirements set. The set requirements support setting clear objectives for levels and users can go back to material if needed. (Subramanian, 2022.)

Some critics is presented towards gamification. For example, it is said that gamifying may distract individuals from the actual task for example from learning and makes individuals to rather focus on playing as just winning rewards (Growth Engineering, 2021). Garima Gupta (2022) has presented other cons towards gamification as it is expensive to develop, it won't take long until the game will look outdated which will make users to suspect the information might be outdated and truly creating game that is not just masked as quiz takes time and creativity. As pros of gamification Gupta presented note that gamified learning system provides instant feedback for learners, alongside with increasing motivation and engagement.

2.2.4 Trust

Regarding UX design and trust, trust is defined as user's confidence in or reliance on some quality or attribute of the design. Trust is usually built on previous experiences, it is complex and it tends to be subjective. Other people are also more trusting than the others. (Geddes, 2023.)

Trustworthiness is built on ability, goodwill and integrity. Instead of just paying money, in online services users are also expected to provide personal information which can be considered as an act of faith. The matters considering disclosing of personal information are presented more in depth later. (Geddes, 2023.)

Geddes (2023) presents three different points about how to gain users' trust. First is about creating familiarity as "using commonly known facts to show users you're credible". Second is about presenting frequently asked questions and last is about offering the users' only products and services related to their needs without up-selling.

3 Information security

Steve Watkins (2018) presents information security through example of handling money. Usually, person does not want other people spending their money which would then mean **restricting acces**s to these funds. Second thing is that you want to be able to spend your money when you like so this is concerning about **availability** of the funds. Last point is about certainty of understanding and knowing that when receiving money, you receive real money instead of fake money so last part is about **integrity**. The example used money, but information and data are individuals' and organisations' important assets, and information security includes all these three: restricting access to necessary information, availability, and integrity of information.

According to Watkins (2018) organizations then have policies, processes and working arrangements built around these matters and from these parts is constructed information security management system (ISMS). Taking care of confidentiality, availability, and integrity are important for every individual, company, and public actor. Regarding information security all acts related to information need to be secured, as an example: storage, handling, moving, and processing.

3.1 Cyber security

Cyber security includes technological and practical actions to secure digital systems and data (Patterson, 2022). Cyber security can be divided into 5 different types of security measures: critical infrastructure, application, network, cloud, and Internet of Things (IoT) security (CompTIA, 2023).

The Cyber Security and Infrastructure Security Agency has also described cyber security as "art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information" (2023, What is cybersecurity? section, para. 1). According to the Agency the way to

improving cyber security starts by gaining understanding about the possible risks. Overall risks related to infosec including cyber security are presented later on.

3.2 Regulation and standards

Organizations based in European Union need to consider General Data Protection Regulation (GDPR). In short GDPR is to set protect people's personal data which is information with which combined a person may be identified. The mentioned information can be name, address, ID car or passport number, income, cultural profile, IP address and information regarding person's health. GDPR states, what data and when it can be processed. As an example, person's ethnic origin, sexual orientation or political opinions are not allowed data points to be processed. GDPR gives people right to access their personal data, require corrections and removal of their data. GDPR also provides instructions how organizations need to work if data breaches including personal data occurs. If GDPR practices are not followed organizations may even be fined for it. (Your Europe, 2022.)

Many sectors have regulations about having some form of information security management. As an example, regarding banking sector in European Union there is also Payment Services Directive (PSD 2) which for example requires organizations to utilize strong customer authentication as in multi-factor authentication (MFA). This is to prevent unauthorized use of customer credentials. Also, if organization operating in the field is not following these regulations, they may be fined for it. (Finnish Financial Supervisory Authority, 2019.)

According to IT Governance Ltd (2022) ISO 27001 is global standard for information management which helps organisations to protect their data. It includes policies, procedures, processes, and systems to manage infosec risks. There are plenty of companies providing companies consulting services related to getting the ISO 27001 certification for organizations. According to Alliantist Ltd (2022) the key requirements of the certifications are following: "Understanding the organisation and its context, understanding the needs and expectations of interested parties, determining the scope of the ISMS, ISMS,

leadership and commitment, information security policy, organizational roles, responsibilities and authorities, actions to address risks and opportunities, information security objectives and planning to achieve them, resources, competence, awareness, communication, documented information, operational planning and control, infosec risk assessment, infosec risk treatment, monitoring, measurement, analysis and evaluation, internal audit, management review, nonconformity and corrective action, continual improvement".

3.3 Motivating factors for organizations

Companies are considering their stakeholders and customers' requirements and the companies' own needs to stay competitive when setting their objectives for ISMS but public sector also needs to consider the responsibility of becoming effective and efficient as possible in order to present proper usage of public funds. Also staff always expects their information to be handled appropriately for they expect their right also to privacy be respected. (Watkins, S. 2018.)

3.3.1 Information security risks

Luke Irwin (2020) has listed 10 top risks for companies to consider in their ISMS. These risks are summarized in Table 1. List starts with **social engineering** which is about manipulating people into performing actions or sharing confidential information for malicious purposes. This then continuous to **disclosure of passwords** which can be done for example via so called phishing emails.

Hacking is about gaining unauthorized access. Michael Marino (2022) has written article about most hacked passwords around the world in 2022. The most hacked password in the United States in 2022 was "password", in Germany it was "123456" and in Russia it was "qwerty". Password ending to a person with evil intentions risks the organizations confidential data.

Irwin (2020) continues their list then with **unauthorised access to the network** which may occur for example by a system weakness which allows malicious person to plant some sort of malware to system. Then comes **maintenance error** whereas an example other customer's bank information was shown to the user logging in S banks system (Laine et al. 2019).

There are also risks for **electrical outage** (Irwin, 2020) which will shut off servers and prevent employees from doing their job. Relating to this there are also **infrastructural damage** and **malfunctioning equipment**. Someone might vandalize properties or computer just breaks which happens from time to time. **Destruction of records** also might make important data unavailable.

Ninth on the Irwin's (2020) list is **theft** meaning someone stealing your information. The information may be physical or digital. Last one on the list is **weather events** not meaning just catastrophes but also snowstorm breaking power lines making this also related to electrical outages.

Table 1. Top 10 information security risks (Irwin, 2020).

Risk	Description
Social engineering	Manipulating people into performing actions or sharing confidential information for malicious purposes.
Disclosure of passwords	Passwords ending to unauthorized people for example via phishing emails.
Unauthorized access to the network	Unauthorized person accessing the network which allows attacker to plant malware to system.

Maintenance error	Error caused by development causing some issue in access restrictions, information availability, or information integrity.
Electrical outage	For example, shutting off servers.
Infrastructural damage	Something physical damage caused by vandalizing property or sabotaging systems.
Malfunctioning equipment	Equipment malfunction before the end of planned life cycle.
Destruction of records	Paper files may be damaged or digital files for example be corrupted.
Theft	Stealing either physical or digital information.
Weather events	Issues with not just earthquakes or hurricanes but also possibly snowstorm affecting power lines or people unable reaching office.

Non-harmful but oftentimes considered annoying are **ham emails**. Ham emails are resembling spam emails but as spam is directed to addresses that have not signed up for marketing emails, ham is marketing emails users have signed up for. At times it is done directly when for example installing new software and when accepting the terms of use there is next to it some checkbox stating “Yes, I want information about updates etc”. Or at times it is done indirectly as the checkbox for signing up the marketing emails is ticked already and not to sign user would need to remove the tick. (Dreamer, 2013.)

3.3.2 Information security opportunities

Plenty of companies have lot to lose if their information security is not in order. Mikko Hyppönen from F-Secure said in webinar (2022) that everyone is equally in danger when they are online in the Internet no matter what their physical location on the Globe is even though offline safety can be considered to be on different levels in different countries. This has then provided opportunities for companies who are focusing in information security and for example focusing on detecting new kinds of malware hackers are creating. Such companies are Avast and F-Secure.

Because remembering all different kinds of passwords is so difficult and to make things harder for hackers it is recommended that people should keep changing their passwords in active manner and passwords should not be too easy to guess as presented earlier, they are hard to remember. Also sharing passwords in safe manner is at times difficult for if they are written on paper and paper is lost there may be risk of unauthorized data breach. So some companies have been building these kind of password vaults called password managers which work as service or software on your computer or in cloud services where you can store your passwords and fetch them as the passwords are needed. Of if you are sharing some account in your team, you may share the password via this same service to your whole team so no post its nor papers are needed.

Such services are provided for example by LastPass. But these are not completely safe as LastPass got security incident where at least part of their development environment's source code and technical information got stolen. Later on LastPass also said that they had some unauthorized party using this stolen information and gaining access to some part of their customers' information. They ensure that the customers' stored passwords were safely encrypted time will show how safely the passwords were encrypted after all. (Toubba, K. 2022.)

Encryption changes the form of the password, so it isn't stored in readable form and therefore not so easily abused by hackers. Computers can test different kinds of simple

word lists or try to calculate the encryption but if the encryption and the password is strong enough it takes so long time to try get the password correct the hacker might give up and try to find another target. (Okta, 2022.)

3.4 Incidents in media

Finnish psychotherapy centre Vastaamo had an infosec breach on March 2019 and they reported breach in September 2020 to Data Protection Ombudsman. GDPR regulations require the reporting of personal data breaches needs to be done in 72 hours. According to the Deputy Data Protection Ombudsman the data had not been appropriately protected and imposed a fine worth 608 000 Euros. (European Data Protection Board, 2021.)

17th of January in 2022 happened a breach in Crypto.com service, where attackers were able to bypass two-factor authentication (2FA) and make transactions to raise cryptocurrencies from the accounts. Crypto.com had risk monitoring systems which had detected unauthorized activities and for this reason they reacted fast and suspended withdrawals and required all customers to use 2FA. Crypto.com reassured that any customers didn't lose any money in this attack, but it still cost the company millions of dollars. (Crypto.com, 2022.)

Lapsus$ group informed on March 20th, 2022, that they had breached Microsoft services. Two days later Microsoft gave their statement regarding the matter which mentioned only one account getting hacked for their security systems had been working and stopped the attackers before the attackers could get their hand on more Microsoft accounts. (Microsoft, 2022.)

4 Privacy

Privacy may have multiple meanings depending a bit on the context. “Data privacy means empowering your users to make their own decisions about who can process their data and for what purpose” (Proton Technologies AG, 2023, para. 2). Other meanings for privacy may mean anonymity, the decisions about handling your personal information or confidentiality (Spacey, 2019).

Person breaking their barriers of privacy is called **disclosure of personal information**. It is about giving personal information to another person or organization for them to use (Information and Privacy Commissioner of Ontario, 2023). There is also related term called **privacy paradox** which is described as users claiming to be interested and concerned about their privacy but still not doing much in order to protect their personal data (Barth, et.al., 2017).

Issues related to this matter may be called oversharing. Matters called oversharing for example in social media may be as continuously sharing with whom you are spending time with, sharing intimate details about relationships, friendships, family members and personal life issues, sharing location information on posts, sharing pictures of your outfits or sharing work-related information. Information shared especially about your routines and locations make person vulnerable for they are exposed to criminals in both digital and real world. (Velasquez, 2022.)

4.1 Social engineering

Regarding the issues in the digital world, oversharing may provide opportunities for cybercriminals to for example social engineering which has been earlier mentioned as high information security risk (Velasquez, 2022). Kaspersky’s (2023) definition for social engineering is manipulation which is exploiting human errors in order to gain private information, access or other valuables. Cybercriminal wants to get the user to act for their

bidding and the possible useful user actions towards the criminal would be data exposure, spreading of malware infections or providing accesses to restricted systems.

Picture 1. Enablers of social engineering and five common attack methods Kaspersky, 2023.

Picture 1 is presenting summary of the following enablers and attach methods for social engineering. Two factors which make social engineering victims essentially vulnerable are for the attacker creating feeling of **urgency** and **trust** with the victim. Users may be more likely to compromise information security compliance when the matter is presented as a great issue which would need to be assessed immediately. Trust is essential factor for social engineering attack, as attacker is impersonating as trustworthy, reliable

individual or organization which could be confided with certain information or access or whose email attachments and links should be trusted. (Kaspersky, 2023.)

According to Verizon (2022) occurrence of “mispresentation” tactics (which includes social engineering) has grown 15 times higher during the Covid-19 pandemic. Here is presented a few common social engineering attack types.

Phishing is about attacker presenting themselves as some trusted organization or person to gain users’ trust and user to act on their bidding. Different types of phishing methods include for example spam fishing without personalization regarding the victim and is aimed to multiple users at once. Whereas spear fishing uses personalized information to gain the trust of the aimed individuals. Extension to this method is called whaling where the targets are targets of higher value such as CEOs or other upper management persons, celebrities or higher government officials. (Kaspersky, 2023).

Baiting is about luring user with for example some free or exclusive offer to click email attachment infecting user’s device with malware. **DNS spoofing** is manipulating user to be routed to malicious websites though entering legitimate URL. This redirection will continue to exist until the erroneous routing data is cleared from systems. (Kaspersky, 2023.)

Physical breach is about attacker showing up in-person to some (usually) enterprise premises with restricted physical access and imposing themselves for example as some reliable used vendor to gain access to restricted areas. **Tailgating** is about someone following an authorized person inside area that is restricted to for example organization’s personnel only. (Kaspersky, 2023.)

4.2 Online flaming and bullying

Oversharing personal information may also at times lead to **cyberbullying**. It means using digital technologies for spreading lies or posting embarrassing material on websites

or social media. The material posted online may be hurtful, abusive and threatening and it may be public or private like direct messages, images or videos. It may also be impersonating and again sending hurtful messages on their behalf. (Unicef, 2023.)

The bullying may affect victims mentally, emotionally, and physically. The ways to protect oneself from cyberbullying is about being careful about material you share online or at times remove applications or stop using some services where users are at risk. Some services offer privacy settings where users can decide on visibility of the material they share. (Unicef, 2023.)

Bullying may also include **online flaming**. Often times the aim with flaming is to provoke an argument on some sort of social media, messaging forums or chat rooms. The flaming behaviour often includes posting hurtful messages and may use irritated and offensive language in a way to provoke another person to join the argument. (Nixon, et.al, 2009).

5 Research Method

The aim of systematic literature review (SLR) is to find plenty of already existing and relevant research regarding specified research question by using defined methods. These methods are used to bring up well-grounded findings based on the different chosen papers (Griffith University, 2022).

This research is conducted by following guidelines provided by Barbara Kitchenham and Stuart Charters (2007) who have based their guidelines to guidelines written be medical researches but Kitchenham and Charters have adapted theirs to fit software engineering fields' needs. Their guidelines provide information about review's phases of planning, conducting and reporting. Even though the phases seem to be in chronological order the matters related to these phases may be revised and adjusted as the process gets further.

The guidelines (Kitchenham et al, 2007) is using term **primary study**, which means a study "investigating a specific research question" (p. 6). This written SLR is considered **secondary study** which reviews all the chosen and found primary studies, which are somehow relevant for this review to find answers to research questions' answers.

5.1 Planning

According to Kitchenham and Charter (2007) the planning phase includes stages of identification of the need, commissioning, specifying the research questions, developing protocol and evaluation. They mention commissioning not to be mandatory if there is no commercial background on the research and evaluation may be left out if it is so decided by the review's stakeholders.

As of need and background, there are individual researches for example trying out different actions from system side affecting users actions with different types of products and services and then there are different types of information security related researches focusing for example one single application. Since previously presented conflict

between Nielsen's (2004) and Amazon Web Service expert's (2022) comments some sort of middle ground between these matters should be found and SLR could provide answers.

The search was done to two databases Scopus and Science Direct and to gather great amount of relevant primary researches for the review some individual researches from Google Scholar were included. The primary researches are limited by free accessibility to students of University of Vaasa since there are no financial contributors and limited resources. Review focuses on studies written in English and studies in other languages are excluded. After the search the results are presented in Excel spreadsheet.

Since there is no commercial background, there won't be commissioning for this review. The research questions are "How can user experience affect information security?" and "How can information security affect user experience?". By answering these questions, it may also partially answer about which infosec matters or actions don't affect or have only little effect on UX and the other way around. So, these questions are assessing the effect which is one of the question types presented by Kitchenham and Charter (2007).

According to Kitchenham and Charter (2007) the medical guidelines guide to consider the effectiveness of treatment and they mention for example population affected by the intervention, alternative interventions, and outcomes to compare interventions. In this review the population will be the software product or service user. The intervention is either infosec or UX action. The outcomes are related to either increased or lowered infosec levels and reliability, preventing or exposing infosec risks occurring or as increased or lowered user satisfaction from UX part. Table 2 summarizes these matters and is also presenting structure for the research questions.

Table 2. Research question structure.

Population	Software product or service users
Intervention	Information security or user experience related action

Comparison	For example previous experiences with information security features or information security trainings
Outcomes	Better or worse information security and user satisfaction levels

Kitchenham and Charter (2007) recommend having put up inclusion and exclusion criteria when developing protocol. Review includes all openly sourced studies without limitations in time fitting the search terms and providing answers to search questions. Informal material is excluded from the review.

As following the Kitchenham and Charter (2007) guidelines, the data collected will include article title, year when published, authors, source in example journal name, research question, research method and summary. The data is included in spreadsheet and is ordered alphabetically by the authors. Answers to the research questions and trends related to subject are then looked from the chosen primary studies.

5.2 Conducting

Kitchenham and Charter's (2007) guidelines include in the conducting phase: identification of research, selecting studies, quality assessment of studies, extracting and monitoring data and data synthesis. As part of the identification of research is the generating of search strategy. It includes preliminary searches and trial searches for example for assessing the volume of potentially relevant studies.

Primary search terms are "User experience" and "Information security". Search string is "User experience" AND "Information security". According to Kitchenham and Charter (2007) at times the search can't be just done from digital libraries and instead reference list of relevant primary studies and review articles should be looked, journals, research registers and the Internet. Though this disposes us to publication bias as positive results are more likely published than negative results.

As the guidelines state (Charter et al, 2007) the full studies are needed and will need to be fully reviewed. The search needs to be documented thoroughly in order for be open about the search and give thorough image for the reader. The search should be documented as it occurs and if something is changed it needs to be noted and reasoned. Study selection criteria should follow what is decided in planning phase, although the definition may be adjusted during the process. In software engineering the abstracts are considered too poor to rely on when selecting primary studies and instead also conclusions should be reviewed. Students should consider re-evaluating a random sample from chosen primary studies to check consistency of selection criteria used.

As an example, the guideline (Charter et al, 2007) provides example checklist for quantitative studies. It puts focus on for example the study's aim, design, research questions, if the study answers to research questions, population etc. It is also divided to parts such as design, conduct and conclusions. The example checklist for qualitative studies is a lot shorter and it starts by assessing how credible and important the study findings are when considering if the study should be included in primary studies. The quality as a tool can be used either when setting the study inclusion and exclusion criteria and in data analysis and synthesis.

Data also needs to be gathered and stored as planned (Charter et al, 2007). Data synthesis is about gathering and recapping the results of the primary studies included in review. With narrative synthesis the extracted data regarding the table 2 matters (population, intervention, comparison, and outcomes) should be gathered in a manner with which the data can be more easily compared and structured to highlight similarities and differences between the outcomes. This way the consistencies and inconsistencies may be shown.

This search was conducted in January 2023 and Table 3 presents the database search results. The dates differ a bit for after searching Scopus there came realization that this search ought to focus on recent events. There has been some debate about information

security during Covid-19 pandemic, and since the world started to truly shut down on 2020 forcing people to stay at home, this search is limited to sources published since 2020. But when doing search to Science Direct it was considered the actual pandemic starting during 2019 but it was later on figured out that it was year 2020 when the whole world actually started to shut down and the results of world shutting down because of Covid-19 would show more in the research later than 2019. It would've saved some time and effort to consider these matters in planning, but even though the first phase of quality assessment also older researches, they were left out in the 2nd phase.

Table 3. The search results in January 2023.

Database	Total amount	Date
Scopus	62	2006–2023
Science Direct	349	2019–2023

5.3 Quality assessment

Systematic literature review includes study quality assessment. Kitchenham and Charter (2007) explain that there is no agreed definition for study qualities, though Cochrane Reviewers' Handbook is suggesting that quality is related to matters minimizing bias and maximizing internal and external validity. Studies are gone through in 3 phases with inclusion/exclusion criteria and idea is that with quality assessment phases the resulting studies show less bias and increase the validity.

Inclusion/exclusion criteria for this research is presented in Table 4. The search string was presented earlier but here we have included more detailed information regarding the time when the paper's publication date and contents. There were plenty of recently published papers including some new technical advancements improving infosec somehow but if the effects of this technical advancements was not studied in the view of UX then the paper would be left out. The paper may have been able to present how the technical artefact may have made some infosec action more efficient and then the

writers may have said that since their finding is making process more efficient it would be obvious that it would increase user satisfaction but oftentimes the user satisfaction was not measured so there was no way of saying if this artefact had affected the user satisfaction.

Table 4. Inclusion/exclusion criteria.

Criteria	**Decision**
Predefined keywords exist in the paper	Inclusion
The paper is published in peer-reviewed scientific source	Inclusion
Paper is written in English	Inclusion
Paper is published during or after 2020	Inclusion
Studies presenting infosec action and show UX result	Inclusion
Studies presenting UX action and show infosec result	Inclusion
Duplicated search documents	Excluded
Papers not accessible, or not ready as peer reviewed or published	Excluded

This part of the study included three phases going through the previously selected studies and Table 5 is presenting summary of the phases. Only abstract and titles were supposed to be taken into consideration in the first phase, but because the inclusion criteria related to publication date range was adjusted after study selection, the publication date was also checked in this phase. After going through all these phases, 21 studies entered to data extraction phase.

Table 5. Results of the quality assessment phases.

Phase	Phase 1	Phase 2	Phase 3
Evaluated by	Publication date, title and abstract	Introduction and conclusions	Whole study
Number of studies evaluated	411	66	38

Number of excluded studies	345	28	17

5.4 Reporting

After the quality assessment there is data extraction phase. Table 6 is presenting the elements considered in the data extraction process. As it was presented earlier, it was considered exclusive factor if there was not clear tested and presented evidence of the effects of the action it was also included in the data extraction elements.

Table 6. Data extraction elements.

ID	Attribute	Description
A1	Title	Title of the study
A2	Authors	All authors of the study
A3	Publication year	Year when the study was published
A4	Journal	Journal in which the study was published
A6	Method	Method used
A7	Type	Empirical or theoretical
A8	Data collection method	How the data for empirical research was collected
A9	Actions	What kind of actions taken
A10	Effects	Reported or not, positive or negative or no effects

After the data extraction, the included studies and their data is summarised by synthesis. This research uses qualitative methods to build descriptive synthesis.

The last phase of Kitchenham and Charter's (2007) guideline's is reporting, and it includes specifying dissemination mechanisms, and editing and evaluation of the report. Evaluation may be left out if so is decided by the stakeholders. This review is to be shared in the university of Vaasa's digital publication archive Osuva. The report is to follow university of Vaasa's guidelines provided for Master's thesis. The report is to be evaluated by the guiding professor.

6 Results with Synthesis

Studies included in this review answer to presented research questions. They either consider more technical infosec actions and their effects on UX or more human behaviour related actions and their effects on infosec. Chapter 6 presents the results gathered from the studies and synthesis is built on data that was gathered from the included studies. The results are further discussed on chapter 7.

As presented earlier, the included studies are from 2020 to January 2023. Included studies have four studies from 2020, nine studies from 2021, seven studies from 2022 and one study from 2023. Table 7 is presenting the amounts of studies from each journals. As nine included studies was from Computers & Security and the whole amount of included studies was 21, the included studies from Computers & Science cover about 40% share of the included studies.

Table 7. Amount of included studies from different journals.

Number of papers	Journals' names
8	Computers & Security
2	Computers in Human Behavior, Information & Management, Journal of Information Security and Applications
1	AIS Transactions on Replication Research, Decision Support Systems, Electronic Commerce Research and Applications, European Journal of Information Systems, Patterns, Systems & Software, Telematics and Informatics

As technology is evolving with accelerating speed, there is coming more and more research related to these matters, as also cyber criminals are becoming more and more devious and it's clear that attacks involving social engineering has been rising. To fight against the cyber criminals, it is more important to find ways for users to protect

themselves, services, data etc against these efforts. Table 8 provides overview of the included studies. It could be seen that though information security consists of different matters such as physical security and network security, the included primary studies focused a bit more on cyber security and users disclosing personal information.

Table 8. An overview of the included primary studies.

ID	Reference	Focus
PS1	Aggarwal, et al., 2023	Finding effective ways to train people to detect phishing emails
PS2	Furnell, 2022	Presenting how websites guide user making good choices with password selection
PS3	Tejay & Mohammed, 2022	How infosec culture related matters effect on following infosec policies
PS4	Lancelot Miltgen , Liu & Xia, 2022	How privacy feedback and choice affect disclosure of private information
PS5	Ahmad, et al., 2022	Providing information about users' information security awareness related to mobile health apps
PS6	Fest, Wagner & Wieringa, 2022	Studying how legal and ethical frameworks influence the daily data science practices in two cases: public sector data

		professionals at municipalities and the Netherlands Police
PS7	Chang, Lee & Wong, 2022	The motivation and mechanisms for social network site users to protect the privacy of their peers and ensuring online security
PS8	Carte, Luu & Philip, 2022	Bringing understanding of individuals interests in securing their home network from cyber attacks
PS9	Aydin, Boyaci & Gûven, 2021	Finding ways to adjust users' password selection behaviour to decrease the passwords' predictability and increase security
PS10	Johnston, Singh & Yang, 2021	Finding out more information about the motivation of home users and organizational users to protect important information
PS11	Chen, Kim & Rao, 2021	How SNS users' perceived risk is changed by perceptions of the duality of potential cyber attacks and privacy breaches
PS12	Parish, Salehi-Abari & Thorpe, 2021	Studying presentation effect as if with gradually revealed images users can be

		guided to create better PassPoints-style graphical passwords
PS13	Faily, Henriksen-Bulmer & Pilton, 2021	Bringing more information about users' expectations regarding privacy and extending study to bring light to matters that cause change in users' privacy related behaviour
PS14	Dolezel & McLeod, 2021	Testing hypothesis of users giving up on security compliance because of believing breaches occurring is inevitable
PS15	Petrykina, Schwartz-Chassidim & Toch, 2021	Experimenting gamified interactive security system which rewards users for their online security behaviour
PS16	Akil, et al., 2021	Overview analysis of key cyber security takes to consider in future development of cyber security
PS17	Xiao, 2021	Focuses on gap between technology affordance and users' requirements in relation to mobile security
PS18	Dembinsky, Meyer & Raviv, 2020	Studying the outcomes of alerting about possibly

		risky choices vs. blocking the risky choices
PS19	Dincelli & Chengalur-Smith, 2020	Trying out visual and text based cyber security training methods to see their effectiveness
PS20	Bhana & Flowerday, 2020	Studying the effectiveness of authentication including passphrases and keystroke dynamics
PS21	Trang & Weiger, 2020	Studying the possibility of users disclosing more info and risking privacy because of gamification

Table 9 gives overview of the methods used in included primary studies. All the studies included were empirical for in the inclusion/exclusion criteria it was stated that there would need to be also tested and presented outcomes, so this setting didn't have any space for purely theoretical studies in this review.

Table 9. Data regarding the included primary studies.

ID	Year	Research method	Data collection method
PS1	2023	Experiment	Recruiting participants who got training and questionnaires from which it could be seen how well they had detected the phishing emails
PS2	2022	Experiment	Checking out websites every 3-4 years since 2007 about how websites guide and support with password selection

PS3	2022	Semi-structured interviews and survey	25 semi-structured interviews with cyber security experts and then then web based survey with 473 participants in Southeast USA from multiple companies
PS4	2022	Experiment	Lab experiment testing application where privacy feedback and choice were manipulated
PS5	2022	Case study	Study was conducted with two mobile health app providers in Saudi Arabia surveying 101 end-users
PS6	2022	Case study	Data was gathered by observing participants' work practice and meetings, and other times in court hearings or public documents over a 4-year time frame 2017-2021
PS7	2022	Survey	Gathered 740 questionnaire responses from social networking site users
PS8	2022	Survey	Surveyed 503 working professionals
PS9	2021	Statistical analysis	The breached data is shared in Internet and for this study the data was searched from Google and 8 different data sources were used
PS10	2021	Survey	They surveyed more than 300 organizational users who didn't have password management software installed
PS11	2021	Survey	Surveying existing Facebook users
PS12	2021	Experiment	They had 3 sessions over 8 days where users created graphical password and logged in with it several times over the 8 days period. Users also filled questionnaire and exit survey.
PS13	2021	Focus groups, interviews,	First they had focus groups, interviews and surveys to come up with proper extension for websites in order to experiment training and guiding users regarding privacy matters

		surveys, experiments	
PS14	2021	Survey	Online survey with 1-7 Likert scale gaining 134 responses
PS15	2021	Experiment	94 participants experimented with Security-Robot solution
PS16	2021	Interview	Interviewed European stakeholders from sectors considered critical (such as open banking, medical data exchange and smart cities)
PS17	2021	Survey	245 survey responses were received online from 92 developers and 153 smartphone users
PS18	2020	Experiment	They had 80 participants (48 women and 36 men) try out solution which would either warn about risky downloads or block them
PS19	2020	Experiment	1718 employees surveyed after they had been trained with either visual or text-based cyber security training method
PS20	2020	Experiment	At first, they experimented with a login assessment to collect data on user authentication and secondly, they had expert review for validating their findings
PS21	2020	Survey and Experiment	Two complementary studies where in first study they surveyed 491 people who had used some gamified apps and in second study they experimented with their own gamified app with 458 participants

Since descriptive synthesis is applied in this review, the sensitivity analysis is rather subjective (Charter et al, 2007). In this view it is therefore considered what kind of studies are included and what poor quality studies would do to this review. And in this relation, it is considered causing a clear effect that the study selection criteria didn't provide any space for theoretical views. And since studies for example improving infosec but not

presenting effects on UX were left out, this fact helps considering the return of the investment as in infosec and UX relation. As if the effect of the infosec is so great and improving UX then it might be worth it, but if it for example improves infosec and the considered UX gets worse then it still might need to be reconsidered or it might get even more expensive to kind of market the development and get users to follow the development.

There were plenty of studies left out that didn't provide any details regarding their infosec actions effects on UX. This still doesn't mean that researchers didn't consider this point but at this point it means that this view was not presented in their papers. So, there is possibility that some good quality studies were also left out and probably instead of just leaning on the paper it would've been better to at least in the last quality assessment round include part of contacting researchers asking if this view was considered and if they would have some data related to UX view.

6.1 Information security technology related actions

Infosec tech related actions were mostly about passwords. Table 10 is presenting overview of the actions, which included for example what kind of passwords websites accept when registering (Furnell, 2022) and forcing users to change their password selection patterns (Aydin, et al., 2021).

Table 10. List of information security technologies related actions.

ID	Actions
PS2	Plenty of infosec education has been given and plenty of lists of most used passwords but websites are not doing much to guide users to use better passwords
PS9	By forcing users to change their password selection patterns and behaviours they can improve their information security a lot

PS12	Users were guided towards making better graphical password selection by gradually revealing different kinds of images and it improved the security of the passwords without decreasing the usability
PS18	Blocking unsecure events was more effective than warnings, and researchers were worried about blocking leading to increased reliance to system but there was no evidence supporting. Though from UX point blocking may have been experienced as a negative outcome
PS20	Making users try out passphrases instead of passwords. Participants had overall more errors and problems with passwords than passphrases. Equal amount of memory and typing failures.

Furnell (2022) has pointed out fact that often users are blamed for making poor choices regarding their passwords for digital services but service providers are not blamed for allowing those poor choices and not guiding users to do any better. This paper from Furnell was fifth in the series of studies which have been conducted every 3-4 years since 2007 and it's point has been to take a look on how websites are guiding users making better choices.

Findings of this study (Furnell, 2022) point that all the websites included in study have now added length restriction but even though there are dictionaries existing providing information about the most common and poor passwords, there were only three websites including this restriction in their registration forms. Furnell has presented that this decision has been made to protect UX and to get users into the service. But he also states that to make services more secure, more of these websites are already using or guiding users to use two-factor or multifactor authentication and more websites are to follow to improve the security of their services this way.

Study PS9 pointed that when users have longer passwords they chose a more secure passwords by using more comprehensive character set adding more complexity to their passwords. When users had longer passwords they tend to more often combine special

characters, upper and lower case characters and numbers. With longer passwords usually the amount of lower case characters increased and about 90% of the users chose upper case letter for the first character of their passwords making the password cracking 36 times faster. The study result showed that users come up with these password selection patterns and behaviour and therefore even good password policies won't work if services are not from time to time forcing their users to also change these password selection patterns. (Aydin et al, 2021.)

In PS 21 it was tested how users would perform in logging in with passphrases instead of passwords. Passphrases are considered more secure as they are usually harder to crack. With this study it was shown that overall users had more issues with passwords than passphrases, but especially the error occurrence because of memory or typing failure was equal when comparing logging with passwords and logging with passphrase. (Bhana & Floweday, 2020.)

Especially mobile devices and other devices with touch screen may have PassPoint-type graphical passwords. It was then studied that users were shown pictures on the background while making these PassPoint-type graphical passwords and it was shown in the study that if the image was revealed gradually users tended to then choose more secure passwords. Though also the chosen image affected the user choices and some images caused users to make more poor choices security wise, but some images improved the security and overall, this kind of feature did not affect the usability. (Parish, et al. 2021.)

The previous method nudged and guided users in their graphical password selection, and then there was study warning about risky choices when users would be downloading something on their computers and in other cases they would block completely the risky download actions. The study presents security events which mean that users would attempt to download some malicious items, and user got risk percent information of how high risk there was downloading the item, and system didn't block downloading the item

or system notified user of the risk, but user still decided to proceed with the downloading. (Dembinsky, et al., 2020.)

In the results it was then presented that simply blocking all risky events was more effective for preventing security events from occurring comparing to the warnings. Though users were not pleased with the blocking and experienced it rather as a rather negative outcome. Overall, these features got researchers worried if the features would get users to rely too much on the solution but the study didn't show any results supporting this theory. (Dembinsky, et al., 2020.)

6.2 User experience related actions

Since the social engineering as an infosec attack method has risen, in the reviewed articles there were plenty of actions related to cyber security training. Some focused on some other specific method like phishing emails but there were lots of considering different training frameworks or adding gamification and interactivity and personalization in the training.

Other recognized phenomenon was studies focusing on attitudes towards infosec from a bit different points of views. Presented views include organizational users and home users but as organizational users may be considered protecting information belonging to other people or to their organization, from home user point of view was also considered social network sites (SNS) and their responsibilities towards their peers.

Table 11 is providing overview of the infosec UX related actions where these previously mentioned phenomena may be seen. These matters are presented more thoroughly further in the next subchapters.

Table 11. List of user experience related actions.

PS1	Training to recognise phishing attempts and providing feedback on phishing email recognition.
PS3	Linking core infosec values and goals with professional codes may improve infosec behaviour. Cohesiveness, professional code, information security awareness and informal work practices have significant influence on infosec culture and infosec culture has positive effect on infosec success perception.
PS4	Given choice to read privacy feedback and when reading it also being more motivated and making more conscious privacy decisions.
PS5	Providing users with chances to peer guidance and training from the provider may increase users' trust.
PS6	Pushing legal and ethical frameworks for these public sector professionals didn't get these presented matters into work practices because not having enough time and capacity for it.
PS7	The whole idea of SNS is to get users to share information and commit to site and this study is showing that users consider peer pressure effective, and users consider the consequences of disclosure of peers information so high as this triggers trust issues and reputation damage.
PS8	Line between home and workplace is getting blurred because of remote work and it could be seen that in workplaces the good practices had large impact, but the home network security has no such practices and normative way of working causing shortcomings in security measures.
PS10	Supporting the feeling of autonomy and sense of accountability caused also concern of embarrassment and loss of respect and goodwill among the colleagues if organizational users were to fall in some infosec breach but home users had accountability only for themselves.
PS11	Getting the feel of consumers not having liability of falling into fraudulent actions for they are not expecting future losses and rarely suffer personal losses as for an example, banks are securing the purchases.

PS13	Extension to train and guide users regarding privacy matters and explaining how websites gained their data.
PS14	Personal negative feelings and distrust towards security and the feeling of already losing personal information cause giving up on infosec policies causing more breaches. If people feel capable for protecting information, they are not so easily giving up on security policies.
PS15	Adding probabilistic warnings with gamification to downloading actions had positive effect towards more secure behaviour.
PS16	Presenting common challenges, requirements and technologies for future that have come up in interviews risen as an example from lack of understanding and lack of cyber security culture.
PS17	Providing more information on users' and developers' views and their differences on different mobile security features.
PS19	Users liked the visual based training best, but it seemed that in short term the text-based training provided clearly better results and in longer term only slightly better results.

It may be considered an action to make a decision about not doing something for example, not providing training or capacity as in resourcing time or specialists to focus on some specific matters regarding infosec. And this kind of actions also have effects and consequences regarding the stakeholders also affecting the future requirements. In a study there had been interviewed European stakeholders from critical fields including Open Banking, Supply Chain, Privacy-preserving Identity Management, Security Incident Reporting, Maritime Transport, Medical Data Exchange and Smart Cities. (Akil, et al., 2021.)

For example regarding the Maritime Transport there had been identified lack of understanding infosec matters and lack of cyber security culture. Lack of CS culture was recognized also on common levels, as were considered: ”building trust, privacy and identity management, secure and useable authentication, resilience, threats

identification and fraud detection, capacity building that includes the development of a cybersecurity culture, and the establishment of standards and certification frameworks" (Akil, et al., 2021, p. 13). The future requirements of the field as solutions to these challenges were: ", training, cybersecurity awareness campaigns, certified projects, widening the use of standard tools and technologies, resilient systems, security and privacy by design, and a secure and privacy-friendly environment where data are exchanged, and information is shared in volumes much larger than today". (Akil, et al., 2021.)

In PS3 they had made finds related to the infosec culture. According to the study, linking the core infosec values and goals with professional codes may effectively improve infosec behaviour. As in for example support following infosec policies better and overall making more secure decisions. Regarding the infosec culture it would be most rewarding to identify the high-risk sub-groups and focus on the training and culture building for those sub-groups. (Mohammed & Tejay, 2022.)

6.2.1 Training and interference with information security behaviour

In study PS1 it was found out that training helped users to recognize phishing emails, but with greater frequency of phishing emails in training, users tended to make more false alarms. Especially when the phishing email was very similar to ham. To tackle the issue of this response bias, they tried providing users with more detailed feedback regarding the signs of possible phishing. It was more effective in training and got users to recognize the actual phishing emails better. As training is considered effective in a fight against phishing, it should be taken into account, that frequency of phishing emails during training impacts the response bias getting users making false alarms, and type of feedback impacts the users' discrimination abilities. (Aggarwal, et al., 2023.)

Study PS5 presented results for surveyed mobile health apps' end-users and found out ways to improve users' information security awareness. They pointed out that all the infosec technology like encryption is not considered enough as users may still risk it all by poor password choice. That is why they suggested that the app providers should also

take part in educating their users or include some methods in their service which would enhance the users' understanding of infosec. (Ahmad, et al., 2022.)

They had come up with two different groups of end-users where first one consisted of users self-educating and another group of users needing support from app providers. From the survey responses they found out, that users self-educating themselves were interested in the app's functionalities and learnt about the app's infosec features by exploring the app. The methods to support other end-users were for example raising security awareness via social media, have more content related to infosec from app providers and some users rely to guidance from peer-groups. (Ahmad, et al., 2022.)

PS13 presented a solution (Paradox) as developed network browser extension for Google Chrome to bring transparency to different websites privacy policies and tracking methods as a bigger goal to raise awareness on privacy. The solution provided information for users about for example it's findings on website tracking and possible privacy violations. (Faily, et al., 2021.)

Before taking part in experimenting with Paradox the study only one participant had some concerns about their privacy and other participants hadn't really considered it. Some participants had just relied on websites to follow different privacy laws and use their data responsibly. When seeing the results about what data websites gathered from participants, they were not happy and often their expectations in relation to privacy were not met by websites. When learning about their data shared or sold to third parties by websites, the participants having more technical background were more familiar with it and also more accepting whereas participants with non-technical backgrounds were more concerned of this practice. (Faily, et al., 2021.)

Paradox had helped the study participants to become more privacy aware and all participants were willing to develop "a better privacy mindset". Researchers also mentioned the solution to inadvertently encouraging participants to openly discuss about their

privacy expectations and findings related to privacy even outside the research. The latter fact would be helpful in spreading the privacy awareness and affecting person's privacy behaviour. (Faily, et al., 2021.)

Primary study PS20 tested visual based material and text-based material in information security training. They investigated for example changes in users' attitudes, online self-disclosure of personal information, memorability, and user experience. Text-based training improved the changes in users' behavioural attitudes also affecting in positive manner disclosing of personal information. Though users found visual based training more memorable, and they overall liked it better. It was pointed out that interactivity is important no matter if the training is based on visual or text material. Though with the visual based training there is risk of cognitive overload as the visual effects may draw the attention from the actual message. (Chengalur-Smith & Dincinelli, 2020.)

6.2.2 Gamification and privacy of user and their peers

Security-Robot is created by Petrykina, Schwartz-Chassidim and Toch (2021) and their solution is a gamified interactive security system which rewards users for secure online behaviour. Their results are showing that the interactive gamified experience offered by Security-Robot succeeded to reduce the amount of downloaded malware without reducing productivity.

Though gamification has also it's dark side as Trang and Weiger (2020) found out, that gamification also increases disclosure of private information. They said, that gamification uses psychological pull to trigger users' willingness to provide personal info and with cognitive absorption as users are more concentrated to the task to fulfil and forgetting to pay attention to their privacy.

Study PS4 tested effects of providing users feedback regarding their privacy and disclosing personal information. They invented web shop with three different purchase

scenarios, where in one they didn't provide any feedback, in another they requested users to click "feedback"-button to check our their privacy feedback and in the third case they provided users with the "feedback"-button but didn't guide user to click it and users had option to pass this by clicking another button next to it and proceeding with the purchase process. (Lancelot Miltgen, Liu, Xia, 2022.)

This study presented, that the organizations provide some privacy statements before users disclosing their information, but these statements are often skipped as they are considered long or lacking meaningful choices for users. This causes that users don't know how their data is handled after disclosure. So the privacy feedback provided by research provided information about three matter: categories of personal data collected and processed, why this specific data processing is necessary, and if the data will be delivered further to third parties. (Lancelot Miltgen, Liu, Xia, 2022.)

The study found that providing the privacy feedback, and with it justifying the means behind data usage for users, grows users' trust for the service and users become more inclined towards disclosing their personal information. Privacy feedback also worked as educating users regarding their privacy and helped them to make more secure decisions regarding information disclosure. And as some of the study participants got to choose if they'd like to read the privacy feedback or not, most of the study participants chose to read the privacy feedback, which should encourage more service providers to provide this kind of privacy feedback with their service. (Lancelot Miltgen, Liu, Xia, 2022.)

The whole idea of social networking sites (SNS) is to get users to share (or disclose) their personal information and commit to the site. Primary study PS7 provided information of users' motivation to protect their peers' personal information via questionnaire. The study showed that users' relied heavily on peer pressure as they also considered the consequences of disclosing peers' information so high. Disclosing peers' information was considered to cause trust issues and reputational damage for the users acting against social norms. (Chang, et al, 2022.)

6.2.3 Organizational users versus home users and reasons behind behaviour

Fest, Wagner, and Wieringa (2022) studied the fulfilment of legal and ethical frameworks by data professionals in public organizations and Netherlands Police. Their findings presented that the organizations were not fulfilling the requirements these legal and ethical frameworks presented and there was a wide gap between the daily practices and the frameworks.

The reasons were for example that the workers simply didn't have enough time and resources for it. Other reasons coming up were that the there was gap between the decision making information provided by frameworks and the actual decision making done in daily work. "Data professionals struggle with the translation of ethical and legal frameworks to their daily practice". To cope with this issue they have tried to create tools to help with practicalities, but for example some study participant presented, that the tool still took too much time to use and therefore they would not continue to use it after trying it out. This all is causing that public organizations' data professionals need to base their practices on their own education and experiences rather than on some organization wide policies. (Fest, et al. 2022.)

PS8 focused on individuals' interests in securing their home network from cyber attacks. The study presented that as the amount of remote work is rising, the line between home and workplace is getting blurred. The workplaces having good infosec practices had large impact on their employees' infosec behaviour, but remote (or home) work securities have no such practices. Because of lacking the normative way of working causes shortcomings for remote workers network security. (Carte, et al., 2022.)

Though matters' differed comparing when the person in question was considered as home users or organizational users. As organizational users were found to have greater sense of accountability. Organizational users were for example more concerned of embarrassment, loss of respect and goodwill among their colleagues. Infosec culture and

collective nature gave impression of efficacy. When comparing home users to organizational users, home users were considered to have accountability only for themselves. (Carte, et al., 2021.)

In relation PS11 found that SNS users weren't worrying too much about cyber attacks or privacy breaches. They had surveyed existing Facebook users and came to conclusions that one great reason was that users didn't consider much liability. As banks keep for example securing credit card purchases or come in aid in case of identity theft or credit card information theft paying back the purchases or lost money in full, affected the users' thinking of not seeing themselves as liable. (Chen, et al, 2021.)

Dolezel and McLeod (2021) tested hypothesis of users believing that infosec breach occurring is inevitable would cause users to give up on security compliance. They had tested this hypothesis via survey, and the results showed that if user had personal negative feelings and distrust towards security and the feeling of already losing personal information caused giving up on infosec policies which then again would be causing more infosec breaches. Then again to counter this, if users have the feeling of being capable for protecting information, they would not be so easily giving up on security policies as they would want to avoid negative consequences.

6.3 Users' views versus developers' views on information security features

Some of the selected primary studies recognized a gap between users' and developers' views regarding provided infosec features. Xiao (2021) surveyed developers and smartphone users to find more information on possible gap between technology capabilities and users' requirements regarding mobile security. As an example, it was found out that users evaluated the quality of wi-fi security features higher than developers and fraud and harassment prevention features were rated lower by users than developers.

The study presented also considered how important the security features were considered by the respondents. Developers thought the most important features to be network and traffic management, cache and garbage clean up and wi-fi security. Users were also divided to subgroup by gender and the study was also able to point differences between the genders. Male users considered more important features to be system restoration and rescue, and banking and payment security. Female users found data back up feature to be more important than others. (Xiao, 2021.)

The study had taken account into views regarding 14 different mobile security features and eventually it was also considered, how well satisfied users were regarding the features and how well the level of satisfaction was also meeting the level of importance. Regarding features fraud and harassment prevention, network and traffic management, malware prevention, cache and garbage clean up, scanning virus and trojans, and mobile phone anti-theft the users seemed to be pleased with the features as well as considering them important. Meaning development has been doing good job with almost half of the studied features. (Xiao, 2021.)

The following features needed more work for them as users considered them important but were not satisfied with the features: URL and QR code security, app permission management, and system restoration and rescue. Even though female users had considered data back up feature important, overall view from the female and male users' view showed that it wasn't considered that important as was also with app encryption and lock feature. Users are not satisfied with the features but as they are not considered important it might not be worth it to push development to put in more effort to these two features. The fourth and last part points "possible overkill" including battery management, and banking and payment security, as users are satisfied with them but still are not valuing them so high. Though Xiao (2021) has also made notion that it might be good idea to raise the security awareness of these features by training.

In relation to matter, a previously presented study regarding the mobile health apps (PS5) also pointed out that developers who practice secure software development life cycle for creating mobile health apps often just assume that app they delivered is secure. Though often times the end-users may have difficulties understanding the security features of the application, may be deceived by cyber criminals and because of deception end up leaking private information, or at times may be misled by applications permissions and because of the misleading end up disclosing data which is classified. (Ahmad, et al. 2022.)

They continued by stating that the development teams focus on implementing the security mechanisms such as encryption and authentication, and privacy policies, for making the mobile health app secure. And developers assume that the end-users have already sufficient knowledge about how to utilize the security features they have implemented. But the results of their study pointed out that "developing secure apps or adopting state-of-the-art security practices" may not be enough if the end-users' security awareness is not at a proper level. The awareness reaches to knowledge, attitude, ability to identify threats and to adopt security aware practices. (Ahmad, et al. 2022.)

6.4 Consistency

It could be seen from the data that the data presented by selected primary studies was mostly consistent with each other. Often times they were complementing each other's results bringing more knowledge of the overall relation between UX and infosec.

As regarding to gamification (PS15), it could be presented that gamification was useful in learning and raising awareness of infosec practices helping users to make more secure choices. But it was also presented, that gamification had its downfalls (PS21) by putting users focus on just fulfilling the tasks instead of paying attention to the message or the getting users' to risk disclosing personal information without consideration of security.

There were multiple studies showing results regarding the infosec culture and peer pressure. As in considering lack of infosec culture to be issue (PS16), and how peer guidance is considered truly helpful and increasing trust for the service (PS5), and how the organizational users attempt to follow security practices partly because of being concerned of losing respect and goodwill among their colleagues (PS10). Or bringing personal negative feelings towards infosec to workplace may cause issues in infosec culture at the workplace (PS14).

Regarding the users' and developers' views towards infosec features, it was stated that it might not be enough to apply security features, and instead raising the awareness of security features by training and guidance is also something that should be considered (PS5 & PS17). And it was also presented, that affecting user's infosec behaviour and affecting users' attitudes towards infosec, could be done by training and guidance (PS13).

7 Discussion

This review is separating results into two different categories considering the type of action taken. If the action is closer to design or behaviour or human factor than technical infosec actions, it is considered UX action and presenting some effect on infosec. If the action is more technical then it is considered as infosec action presenting some effect on UX.

Table 12 presents summary of the studied UX actions and their effects on infosec. Training and guidance are important factors in improving infosec behaviour and culture, but training not including too much visual effects and being interactive is more effective. Example cases with more in depth information regarding the signs of phishing or fraudulent actions are also enhancing the effect.

Gamification may be used alongside with training but as too many visual effects may cause cognitive overflow and draw focus from the actual message it is not as effective in training. But as supportive method it is effective if for example via gamification users are provided information of possibly risky choices and rewarding users for more secure manners. But users ought to be informed not to stick to gamified services too much as also gamification may cause users to just focus on the given tasks and to forget the actually proper privacy behaviour and end up disclosing too much personal information.

Considering for example trust factor in UX design and providing users information about how their data is handled, guides users to consider their privacy and aides service providers in gaining trust. Providers promoting infosec discussion and culture are also supporting the trust generation and privacy and security awareness.

Insurances for infosec breaches are decreasing the infosec behaviour as users are not considering themselves liable of the consequences of their actions. But infosec culture between peers in work communities are also in home users provided positive signs in more infosec behaviour when both users considered themselves accountable for other

people than just to themselves. As in both cases users were worried of the consequences they would face from their peers. But if home users consider to be accountable just for themselves, they are not worrying the infosec matters as much as organizational users. Infosec developers have already created well-functioning and security increasing mobile security features users are not valuing that high. Training and guidance regarding these features would raise awareness and increase usage of these features also increasing security.

These findings show that taking UX actions have plenty of opportunities to affect infosec and have possibilities to improve infosec greatly. The value of infosec has been high for years but nowadays people are understanding better the value of data and privacy. With UX users can be guided towards more secure practices helping them to keep their data and privacy safe.

Table 12. How can UX affect infosec?

No	Action	Effect	Notable
UX1	Guidance and training	Improvement	Including too much visual effects may cause cognitive overload and to make the training more effective it ought to be interactive. Also providing tips with example cases about how to identify fraudulent attempts or a bit more in depth information how users' data is gathered raises awareness.
UX2	Promoting infosec discussion and culture	Improvement	Providing peers possibilities for discussion and encouraging infosec discussion helps in raising infosec awareness and more secure behaviour.
UX3	Providing privacy feedback	Improvement	Raising users' awareness and trust towards service provider if they explain, what data is gathered, why and it is somehow handed to 3rd party.

UX4	Providing insurances for infosec events (breaches)	Decrease	Users are considered not to consider themselves liable when for example banks come in aid paying the money some fraudster has stolen in credit card information theft.
UX5	Gamification	Both	May be useful together with training to provide information for example possible risky actions and get users to act in more secure manner. Though gamification may draw focus from the actual message and may also get users to focus on given task forgetting infosec and disclose personal info just to get task done.
UX6	Providing user training and marketing to mobile security features	Improvement	It gives users information in these security features encouraging using them and, in that way, encouraging more secure behaviour.

Table 13 presents summary of the infosec actions and how the actions affect UX. This review managed to present the views regarding infosec actions affecting UX as mostly either decreasing factors or studies mentioning just some action not decreasing usability and that is why they are presented as neutral with question mark. This result reflects the outcome of saying that information security is done by the cost of user experience as all of these actions were improving infosec and ought to be actions for service providers to consider. Only one infosec action is presented to improve UX.

Users are not satisfied with limitations such as blocking their actions. Also blocking non-secure passwords affects usability negative manner. Forcing password selection change pattern change is also related to this as if there were some systems being able to tell that the users' password is too closely like previous passwords and blocking the selection, then blocking the users password choice would be also seen as negative effect on UX. If this would be done instead via guidance and suggestions with for example priming

techniques such as providing user with different kinds of images for building their password, it might not affect usability. And this same is about changing passwords to passphrases, if passwords would be blocked it would have negative impact but if users would be one way or another encouraged towards selecting passphrases, it would not decrease usability and would still increase security a lot.

The only found infosec action to show positive effect on UX was to develop mobile security features users consider important but users were not satisfied with. Xiao (2021) presented the mobile security features users were not satisfied with but considered important to be URL and QR code security, app permission management, and system restoration and rescue.

Table 13. How can infosec affect UX?

No	Action	Effect	Notable
IS1	Limitations	Decrease	For example, blocking users' attempts to download risky items or choosing poor passwords are considered to decrease user satisfaction. Though it has been proven, that this kind of limitations increase security. Guidance regarding this matter provided better results in user satisfaction but as a method it was not as secure.
IS2	Priming techniques in password creation	Neutral?	Providing image to give user more inspiration for better password selection aided in creating more secure passwords and it was mentioned not to decrease usability.
IS3	Forcing password selection pattern change	Decrease	Users tend to stick to patterns making them vulnerable in case same users' passwords are leaked from multiple sources even though they were to use different passwords, as

			because of the selection pattern the cyber criminals would be able to figure out other services' passwords easier.
IS4	Changing passwords to passphrase	Neutral?	If users are blocked from selecting password, it would decrease usability but getting users to change from passwords to passphrases would increase infosec and would not decrease usability.
IS5	Focus development to mobile security features users consider important	Improvement	Figuring out features users find important but are not satisfied with would improve user satisfaction.

7.1 Recommendations

First recommendation to **practitioners** includes multiple points in infosec trainings. Training is proven to be effective to effect infosec behaviour and therefore infosec actions, but it works better when the training is effective. To make training effective it needs efforts towards interactivity to get users commitment and interest. Having modest amount of visual stimuli helps avoiding cognitive overload and with well explained examples regarding signs of possible fraudulent actions helps users to take theories into practice. Also adding some security-robot feature providing more information about risky choices and rewarding for secure behaviour would support learning after the training and would also help in taking the infosec practices discussed as part of their daily lives.

Second recommendation is about changing passwords to passphrases. Even though it might not be good idea or possible to force the change with tech, it would be highly recommendable to give users information about how the passphrase would make their

login credentials more secure instead of just giving the generic minimum requirements for the password. And maybe even providing users some inspiring images would help in shifting to passphrases and with changing pictures to also get users to change their password selection patterns.

More and more breaches are occurring year after year. And that is probably why users are more interested in mobile security features URL and QR code security, app permission management, and system restoration and rescue (Xiao, 2021). Users still find these features lacking, so mobile security practitioners ought to put more effort in these features to raise user satisfaction.

Last recommendation for practitioners is about gaining trust and support the users' infosec behaviour and culture and awareness for users to feel safe using the service. It was presented, that providing users information about what data is collected from them, reasoning why this is done and providing information openly if their data is going to be delivered to third parties. With this providing information about infosec features possible to use and supporting peer guidance and peers' infosec discussion supports building infosec culture among users which works well in raising awareness and promotes more secure behaviour.

Providing information regarding the already developed infosec features (UX6) fits well in the current context as current events have provided information of importance for this matter. A Finnish stock company Lemonsoft faced ransomware attack recently. The attacker had gained access to Lemosoft's server after gaining one of Lemonsoft's users' login credentials. The security could've been better if they had used VPN and 2FA authentication method, but the CEO of the company mentioned that their users have not shown much interest in using such features. If they would guide their users about the importance of these features, they might also be able to gain more billing for taking these features in use for their customers and increasing the security of their services.

With better security, they could have users trust and possible better user satisfaction towards the services. (Kolehmainen, 2023.)

Then here comes two recommendations for **researchers**. When studying new infosec technologies, frameworks, etc. there should be more usability testing and clear questions for users about how they feel about it. It would give better view on how users experience the features improvement on infosec and effect on UX. It would be great, if it could be defined more precisely in which ways users find it decreasing usability but would they for example still see increase in trust and if they were given choice, would they like to use it sometimes with some services or always or rarely or never.

Also, another recommendation would be to study more on different user groups and maybe sub groups' needs. As times and needs change there ought to be more studies about different levels of studies if infosec features are meeting requirements and expectations. As with Xiao's (2021) study it could be presented, which features users found lacking and this kind of information may provide opportunities for businesses to provide features meeting better users' needs.

7.2 Limitations and evaluation

The selection of the primary studies reflects writer's subjective choice. The subjectivity has been tried to limit with previously presented inclusion/exclusion criteria which was used to counter possible bias and errors. Also, the data extraction form was built to find relevant and good quality studies for the research.

One limitation was that some infosec actions related studies were excluded for not presenting effects on UX. Just because the effects were not mentioned in article, doesn't mean that the matters were not considered. To improve the quality of the study, the researchers should've been contacted regarding this matter.

The study is limited to studies published during Covid-19 pandemic meaning January 2020 – January 2023. Pandemic had a great effect on how world works today in regarding remote work and remote studies and companies offering more services online etc to limit the risks of the disease spreading and by limiting the study to this time range we are provided information up to date.

As pandemic changed the world and affected how people operate in their everyday lives, this study is fitting the current context reflecting recent changes. Though there has been plenty of studies in other sources and other studies done before Covid-19. Comparing to already existing research this study provides a snapshot on recent events instead of building bigger picture over decades of studies as both UX and infosec has been studied for decades before somewhat recently occurred Covid-19 pandemic.

8 References

Aggarwal, P., Gonzalez, C., Rajivan, P. & Singh, K. (2023, Jan 18). Cognitive elements of learning and discriminability in anti-phishing training. *Computers & Security, 127*. https://doi.org/10.1016/j.cose.2023.103105

Ahmad, A., Aljedaani, B., Babar, M.A. & Zahedi, M. (2022 Oct 20). End-users' knowledge and perception about security of clinical mobile health apps: A case study with two Saudi Arabian mHealth providers. *Journal of Systems and Software, 195*. https://doi.org/10.1016/j.jss.2022.111519

Akil, M., Alcaraz, C., Fernandez-Gago, C., Ferreira, A., Fischer-Hûbner, S., Islami, L., Lopez, J. & Markatos, E. (2021, Jun 30). Stakeholder perspectives and requirements on cybersecurity in Europe. *Journal of Information Security and Applications, 61*. https://doi.org/10.1016/j.jisa.2021.102916

Allaintist Ltd. (2022). *ISO 27001 Requirements.* https://www.isms.online/iso-27001/requirements/

Aydin, M. A., Boyaci, A. & Gûven, E. Y. (2021, Nov 30). A Novel Password Policy Focusing on Altering User Password Selection Habits: A Statistical Analysis on Breached Data. *Computers & Security, 113*. https://doi.org/10.1016/j.cose.2021.102560

Babich, N. (2020, Nov 24). *What You Should Know About User Experience Design.* https://xd.adobe.com/ideas/career-tips/what-is-ux-design/

Barth, S. de Jong, M. (2017, Nov). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics, 34*(7), 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

Bhana, B. & Flowerday, S. (2020, Jun 6). Passphrase and keystroke dynamics authentication: Usable security. *Computers & Security, 96*. https://doi.org/10.1016/j.cose.2020.101925

BI Worldwide. (2023). *What is gamification?* https://www.biworldwide.com/gamification/what-is-gamification/

Carte, T., Luu, T. & Philip, S. J. (2022, Nov 1). There's No place like home: Understanding users' intentions toward securing internet-of-things (IoT) smart home networks. *Computers in Human Behaviour, 139*. https://doi.org/10.1016/j.chb.2022.107551

Chang, H. H., Lee, H. C. & Wong, K. H. (2022, Jul 19). Peer privacy protection motivation and action on social networking sites: Privacy self-efficacy and information security as moderators. *Electronic Commerce Research and Applications, 54*. https://doi.org/10.1016/j.elerap.2022.101176

Charters, S. & Kitchenham, B. (2007, Jul 9). *Guidelines for performing Systematic Literature Reviews in Software Engineering.* https://www.researchgate.net/publication/302924724_Guidelines_for_performing_Systematic_Literature_Reviews_in_Software_Engineering

Chen, R., Kim, D. J. & Rao, H. R. (2021, May 20). A study of social networking site use from a three-pronged security and privacy threat assessment perspective. *Information & Management. 58*(5). https://doi.org/10.1016/j.im.2021.103486

Chengalur-Smith, I. & Dincelli, E. (2020, Aug 18). Choose your own training adventure: designing a gamified SETA artefact for improving information security and privacy through interactive storytelling. *European Journal of Information Systems, 29*(6). https://doi.org/10.1080/0960085X.2020.1797546

CompTIA. (2023). *What Is Cybersecurity?* https://www.comptia.org/content/articles/what-is-cybersecurity

Crypto.com. (2022, Jan 20). *Crypto.com Security Report & Next Steps.* https://crypto.com/product-news/crypto-com-security-report-next-steps

Cybersecurity & Infrastructure Security Agency. (2023). *What is Cybersecurity?* https://www.cisa.gov/news-events/news/what-cybersecurity

Dembinsky, O., Meyer, J. & Raviv, T. (2020, Jun 24). Alerting about possible risks vs. blocking risky choices: A quantitative model and its empirical evaluation. *Computer & Security, 97*. https://doi.org/10.1016/j.cose.2020.101944

Dreamer, F. (2013, Oct 3). *Ham v Spam: what's the difference?* Barracuda. https://blog.barracuda.com/2013/10/03/ham-v-spam-whats-the-difference/

Dolezel, D. & McLeod, A. (2021, Oct 30). Information security policy non-compliance: Can capitulation theory explain user behaviors? *Computers & Security, 122*. https://doi.org/10.1016/j.cose.2021.102526

European Commission. (2022, Jul 13). *Web Accessibility.* https://digital-strategy.ec.europa.eu/en/policies/web-accessibility

European Data Protection Board. (2021, Dec 5). *Administrative fine imposed on psychotherapy centre Vastaamo for data protection violations.* https://edpb.europa.eu/news/national-news/2022/administrative-fine-imposed-psychotherapy-centre-vastaamo-data-protection_en

Faily, S. Henriksen-Bulmer, J. & Pilton, C. (2021, Feb 24). Evaluating privacy - determining user privacy expectations on the web. *Computers & Security, 105*. https://doi.org/10.1016/j.cose.2021.102241

Fest, I., Wagner, B. & Wieringa, M. (2022, Oct 14). Paper vs. practice: How legal and ethical frameworks influence public sector data professionals in the Netherlands. *Patterns, 3*(10). https://doi.org/10.1016/j.patter.2022.100604

Finnish Financial Supervisory Authority. (2019, Feb 18). *PSD2.* https://www.finanssivalvonta.fi/en/regulation/regulatory-framework/psd2/

Furnell, S. (2022, Jun 5). Assessing website password practices – Unchanged after fifteen years? *Computers & Security, 120*. https://doi.org/10.1016/j.cose.2022.102790

Geddes, J. (2023, Jan). *Trust: Building the Bridge to Our Users.* Interaction Design Foundation. https://www.interaction-design.org/literature/article/trust-building-the-bridge-to-our-users

Gordon, K. (2020, Mar 1). *5 Principles of Visual Design in UX.* https://www.nngroup.com/articles/principles-visual-design/

Gupta, G. (2022 Mar 5). *Pros And Cons Of Gamification.* eLearning Industry. https://elearningindustry.com/pros-and-cons-of-gamification

Griffith University. (2022, Nov 1). *What is a systematic style literature review.* https://libraryguides.griffith.edu.au/systematic-literature-reviews-for-education

Growth Engineering. (2021, June 9). *Overcoming 10 common objections to gamification.* https://www.growthengineering.co.uk/overcoming-10-common-objections-to-gamification/

Hyppönen, M. (2022, Nov 29). *Mikko Hyppönen – hyvä ja paha Internet.* TEK – webinar. Recording was available for only 2 weeks.

Interaction Design Foundation. (2022). *User Experience (UX) Design.* https://www.interaction-design.org/literature/topics/ux-design

Irwin, L. (2020, Nov 11). *Top 10 risks to include in an information security risk assessment.* https://www.vigilantsoftware.co.uk/blog/top-10-risks-to-include-in-an-information-security-risk-assessment

IT Governance Ltd. (2022). *Key benefits of ISO 27001.* https://www.itgovernance.co.uk/iso27001-benefits

James, G. (2020, Mar 11). *The EU Web Accessibility Directive: Frequently asked questions. https://www.siteimprove.com/blog/the-eu-web-accessibility-directive-faq/*

Johnson, J. (2021). *Designing with the Mind in Mind (Third Edition).* Morgan Kaufmann. https://doi.org/10.1016/B978-0-12-818202-4.01001-1

Johnston, A. C., Singh, T. & Yang, N. (2020, Oct 8). A Replication Study of User Motivation in Protecting Information Security using Protection Motivation Theory and Self Determination Theory. *AIS Transactions on Replication Research, 6*.

Kaspersky. (2023). *What is Social Engineering?* https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering

Kolehmainen, A. (2023, Mar 31). *Lemonsoftiin kohdistetun kyberiskun tekotapa varmistui – yhtiö varautuu uuteen kiristysvaateeseen.* Tivi.

https://www.tivi.fi/uutiset/lemonsoftiin-kohdistetun-kyberiskun-tekotapa-varmistui-yhtio-varautuu-uuteen-kiristysvaateeseen/d9650aff-6f62-4ae3-94da-265eb21833b2

Laine, L. & Maukonen, R. (2019, Apr 8). *S-pankin mobiilisovelluksen häiriö on ohi – osa käyttäjistä näki toisen pankkiasiakkaan tietoja.* Helsingin sanomat. https://www.hs.fi/talous/art-2000006063680.html

Lancelot Miltgen, C., Liu B. & Xia, H. (2022 Jan 6). Disclosure decisions and the moderating effects of privacy feedback and choice. *Decision Support Systems, 155*. https://doi.org/10.1016/j.dss.2021.113717

Marino, M. (2022, Dec 1). *20 Most Hacked Passwords in 2022: Is Yours Here?* https://www.safetydetectives.com/blog/the-most-hacked-passwords-in-the-world/

Microsoft. (2022, Mar 22). *DEV-0537 criminal actor targeting organizations for data exfiltration and destruction.* https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/

Mimmit Koodaa x Amazon Web Services. (2022, March 23). Tietoturva AWS-pilvessä [Online webinar]. In Amazon Web Services, AWS Cloud Practitioner. https://mimmitkoodaa.ohjelmistoebusiness.fi/amazon-2022/

Mohammed, Z. A. & Tejay, G. P.S. (2022, Dec 30). Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. *Information & Management, 60*(3). https://doi.org/10.1016/j.im.2022.103751

Nielsen, J. (2004, October 24). *User Education Is Not the Answer to Security Problems.* Nielsen Norman Group. https://www.nngroup.com/articles/security-and-user-education/

Nielsen Norman Group. (2022). *About NN/g.* https://www.nngroup.com/about/

Nixon, J., Schoenholz, P. & Weitzenkamp, D. (2009, Jan). *Cyberbullying.* The Board of Regents of the University of Nebraska. https://extensionpublications.unl.edu/assets/pdf/g1903.pdf

Okta. (2022). *Password Encryption: How Do Password Encryption Methods Work?* https://www.okta.com/identity-101/password-encryption/

Parish, Z., Salehi-Abari, A. & Thorpe, J. (2021, Sep 17). A study on priming methods for graphical passwords. *Journal of Information Security and Applications, 62*. https://doi.org/10.1016/j.jisa.2021.102913

Patterson, N. (2022, Jul 21). *What is Cyber Security and Why is it Important?* Southern New Hampshire University. https://www.snhu.edu/about-us/newsroom/stem/what-is-cyber-security

Petrykina, Y. Schwartz.Chassidim, H. & Toch, E. (2021, May 29). *Computers & Security, 108.* https://doi.org/10.1016/j.cose.2021.102270

Proton Technologies AG. (2023). *Ai guide to GDPR data privacy requirements.* https://gdpr.eu/data-privacy/

Robb, D. (2021, June 15). *Data Breach Report Emphasizes Cybersecurity's Human Element.* SHRM. https://www.shrm.org/ResourcesAndTools/hr-topics/technology/pages/data-breach-report-emphasizes-cybersecurity-human-element.aspx?_ga=2.138668595.1427221803.1634564843-1773632542.1591208976

Spacey, J. (2019, June 7). *22 Examples of Privacy.* Simplicable. https://simplicable.com/society/privacy-examples

Subramanian, V. (2022, Dec). *Reducing cognitive overload through gamification.* Hornbill FX. https://www.hornbillfx.com/blog/reducing-cognitive-overload-through-gamification/

Trang, S. & Weigner, W. H. (2020, Nov 29). The perils of gamification: Does engaging with gamified services increase users' willingness to disclose personal information? *Computers in Human Behavior, 116*. https://doi.org/10.1016/j.chb.2020.106644

Toubba, K. (2022, Nov 30). *Notice of Recent Security Incident. https://blog.lastpass.com/2022/11/notice-of-recent-security-incident/*

Unicef. (2023). *Cyberbullying: What is it and how to stop it* https://www.unicef.org/end-violence/how-to-stop-cyberbullying

Velasquez, M. (2022, Dec 23). *How Oversharing on Social Media Affects Your Privacy.* Keeper Security Inc. https://www.keepersecurity.com/blog/2022/12/23/how-oversharing-on-social-media-affects-your-privacy/

Verizon. (2021*). 2021 Data Breach Investigations Report.* https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdfx

Watkins, S. (2018). *An Introduction to Information Security and ISO27001:2013: A Pocket Guide.* It Governance Publishing.

Xiao, Q. (2020, Nov 18). Understanding the asymmetric perceptions of smartphone security from security feature perspective: A comparative study. *Telematics and Informatics, 58*. https://doi.org/10.1016/j.tele.2020.101535

Your Europe. (2022). *Data protection under GDPR.* https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm

9 Appendices

Appendix 1. A list of the selected primary studies.

ID	Title	Year	Author(s)
PS1	Cognitive elements of learning and discriminability in anti-phishing training	2023	Kuldeep Singh, Palvi Aggarwal, Prashanth Rajivan, Cleotilde Gonzalez
PS2	Assessing website password practices – Unchanged after fifteen years?	2022	Steven Furnell
PS3	Cultivating Security Culture for Information Security Success: A Mixed-Methods Study Based on Anthropological Perspective	2022	Gurvirender P.S. Tejay, Zareef A. Mohammed
PS4	Disclosure decisions and the moderating effects of privacy feedback and choice	2022	Bailing Liu, Caroline Lancelot Miltgen, Huimin Xia
PS5	End-users' knowledge and perception about security of clinical mobile health apps: A case study with two Saudi Arabian mHealth providers	2022	Bakheet Aljedaani, Aakash Ahmad, Mansooreh Zahedi, M. Ali Babar
PS6	Paper vs. practice: How legal and ethical frameworks influence public sector data professionals in the Netherlands	2022	Isabelle Fest, Maranke Wieringa, Ben Wagner
PS7	Peer privacy protection motivation and action on social networking sites: Privacy self-efficacy and information security as moderators	2022	Hsin Hsin Chang, Kit Hong Wong, Ho Chin Lee

PS8	There's No place like home: Understanding users' intentions toward securing internet-of-things (IoT) smart home networks	2022	Sumesh J. Philip, Truong (Jack) Luu, Traci Carte
PS9	A Novel Password Policy Focusing on Altering User Password Selection Habits: A Statistical Analysis on Breached Data	2021	Ebu Yusuf Güven, Ali Boyaci, Muhammed Ali Aydin
PS10	A Replication Study of User Motivation in Protecting Information Security using Protection Motivation Theory and Self-Determination Theory	2021	Ning Yang, Tripti Singh, Allen C. Johnston
PS11	A study of social networking site use from a three-pronged security and privacy threat assessment perspective	2021	Rui Chen, Dan J. Kim, H. Raghav Rao
PS12	A study on priming methods for graphical passwords	2021	Zach Parish, Amirali Salehi-Abari, Julie Thorpe
PS13	Evaluating privacy - determining user privacy expectations on the web	2021	Callum Pilton, Shamal Faily, Jane Henriksen-Bulmer
PS14	Information security policy non-compliance: Can capitulation theory explain user behaviors?	2021	Alexander McLeod, Diane Dolezel
PS15	Modeling effective cybersecurity training frameworks: A delphi method-based study	2021	Nabin Chowdhury , Sokratis Katsikas, Vasileios Gkioulos
PS16	Nudging users towards online safety using gamified environments	2021	Yelena Petrykina, Hadas Schwartz-

			Chassidim, Eran Toch
PS17	Stakeholder perspectives and requirements on cybersecurity in Europe	2021	Simone Fischer-Hübner, Cristina Alcaraz, Afonso Ferreira, Carmen Fernandez-Gago, Javier Lopez, Evangelos Markatos, Lejla Islami, Mahdi Akil
PS18	Understanding the asymmetric perceptions of smartphone security from security feature perspective: A comparative study	2021	Quan Xiao
PS19	Alerting about possible risks vs. blocking risky choices: A quantitative model and its empirical evaluation	2020	Joachim Meyer, Omer Dembinsky, Tal Raviv
PS20	Choose your own training adventure: designing a gamified SETA artefact for improving information security and privacy through interactive storytelling	2020	Ersin Dincelli, InduShobha Chengalur-Smith
PS21	Passphrase and keystroke dynamics authentication: Usable security	2020	Bhaveer Bhana, Stephen Flowerday
PS22	The perils of gamification: Does engaging with gamified services increase users' willingness to disclose personal information?	2020	Simon Trang, Welf H. Weiger