Uppsala University
Department of Informatics and Media

“Cross Your Fingers and Hope You Don’t Get Hacked”:

A Qualitative Study on The Psychological Factors Behind Non-Compliance with Cybersecurity Recommendations

Rebecca Biese and Gabriél Österwall

Course:	Bachelor’s Degree Project
Level:	C
Semester:	HT-23
Date:	2024-01-19
Supervisor:	Steve McKeever

Abstract

Cybersecurity is one of the most important issues in today's digitalized society, with new technology and security policies constantly being developed. However, one of the largest challenges threatening cybersecurity is the human factor — an aspect that is often overlooked in cybersecurity research and development. Research shows a dissonance between security awareness and level of concern and security behaviours, finding that people are likely to disregard security recommendations and circumvent security measures at the expense of their own online safety. Prominent psychological theories on the topic largely examine the issue from a cognitive, affective, or behavioural perspective, while neglecting to consider a more integrative explanation. An exploratory qualitative study was conducted through interviews with students at Uppsala University in order to identify and analyse underlying psychological phenomena influencing and guiding user behaviours, perspectives and attitudes from a multi-dimensional angle. Three main themes were identified: resignation, naivety, and convenience. Analysis of these themes in relation to existing theories suggests a significant impact on security behaviour and attitudes, through complex mechanisms of interaction and contradiction.

Keywords:
Cybersecurity, Compliance, Security Fatigue, Optimism Bias, Cost-benefit Analysis

Table of Contents

1 Introduction

1.1 Background

In an age marked by relentless digital innovation, we are exposed daily to a huge amount of threats to our cybersecurity. A significant increase in cybercrime has followed this swift global shift towards digitalization (James, 2023). By 2022, the impact of this surge had affected approximately 422 million individuals, and estimates suggest that as many as 33 billion accounts are likely to be breached by the end of 2023 (James, 2023; Vojinovic, 2023). According to a report from Cybersecurity Ventures, the global economic cost of cybercrime is projected to reach an alarming eight trillion USD by the close of 2023 with an annual growth rate of 15 percent, ultimately reaching as much as 10.5 trillion USD by 2025 — more than triple the reported 3 trillion USD cost in 2015 (Sausalito, 2023). The 2023 Global Risks Report by The World Economic Forum identified widespread cybercrime and cyber insecurity among the top eight global risks, both in the short term and long term (World Economic Forum, 2023).

According to the International Telecommunications Union, an estimated 5.4 billion people — or 67% percent of the global population — were connected to the internet in 2023 (International Telecommunications Union, 2023). Following the digitalization of most of our societal and economical infrastructure, the ever-increasing threat of cybercrime has made comprehensive, effective and well-established security measures a priority (Jang-Jaccard & Nepal, 2014). As new, more sophisticated threats to cybersecurity emerge and develop, so too must cybersecurity research produce innovative and effective solutions to combat them.

One of the largest problems threatening IT security, however, and one significant enough to render many technological security measures useless, is the human factor (Hughes-Lartey et al., 2021; Spears & Barki, 2010). Research suggests that the average person rarely follows security advice despite extensive information on proper security behaviour being available (Tian et al., 2022). Despite regulations in many countries requiring organizations to send data breach notifications to affected users in the event of a data breach, research shows that few people take action and follow recommendations to change their passwords after such an event, despite users expressing worries about credential theft and privacy issues (Ponemon Institute, 2014; Zou et al., 2018, 2019). And in the case of well-established evidence-based guidelines for creating strong passwords, for example, studies on user behaviour reveal that these recommendations are rarely followed or do little to increase security (Stobert & Biddle, 2014; Wash et al., 2016).

The significant increase of cyberattacks and data breaches in recent years combined with overall poor security behaviours and a tendency to disregard security guidelines and recommendations poses a growing threat to individuals online (Zou et al., 2019). The long list of rules and demands placed on users combined with the ever-increasing amount of essential systems and personal information online creates unrealistic and unsustainable security expectations that the average user is incapable of meeting (Herley, 2009; Stobert & Biddle, 2014). In order to cope with these expectations, users create strategies to reduce the mental effort required, often resorting to risky security behaviours as a result.

As new threats arise, new guidelines and policies are implemented to help safeguard against them. The solution for lax security behaviours is often considered to be more rigorous security training and education to raise awareness of security threats. There is, however, a clear dissonance between data security concerns, training, and awareness, and the actions taken by users to mitigate risks and threats. Readily available security guidelines and recommendations, despite the substantial body of evidence-based research upon which they are based, are often overlooked or even ignored by users, not only prior to a security incident but even after being victimized.

When faced with the demands of an online society, it is evident that there comes a point at which people are incapable of meeting all of these requirements. Upon reaching that point, they instead turn to effort-saving strategies, loopholes and work-arounds in an effort to cope with the demands placed on them, effectively negating existing security measures and exposing themselves to more risk.

1.2 Problem Description and Discussion

This seemingly lax approach towards complying with security recommendations is not due to a lack of concern — studies show that high levels of concern are not an accurate predictor of online security behaviour (Tian et al., 2022; Barth et al., 2019). Nor does it stem from inadequate security awareness training — despite the widespread implementation of SETA (Security Education, Training and Awareness) programs in organizations, research provides limited evidence of their effectiveness (Stephanou & Dagada, 2008). While these programs do increase knowledge and awareness in participants, there is a lack of evidence showing a change in actual security behaviours.

It is clear that there is a dissonance between cybersecurity concerns and security behaviours that cannot adequately be explained through a focus on security policies and security training. Albrechtsen and Hovden (2009) describe a “digital divide” between security policy makers and the users who must navigate these policies, arguing that the cost of oftentimes overly complex and restrictive policies is borne by the users. Recent studies instead implicate underlying psychological factors that outweigh security concerns and impact security decisions to a larger degree (Choi et al., 2018). The most prominent theories include optimism bias: the belief that others are more likely to experience negative events than oneself; security fatigue: a sense of weariness, futility and lack of control over one’s online security borne from overwhelming demands; and cost-benefit analyses that weigh effort against anticipated gain (Beautement et al., 2008; Stanton et al., 2016; Weinstein, 1980).

These theories tend to focus on one dimension of human psychology; security fatigue encompasses the affective and emotional dimension, optimism bias refers primarily to cognitive biases, and cost-benefit analyses have a focus on behavioural aspects. The aspects described in these theories do not, however, necessarily exist as distinct phenomena separate from each other. When considered side by side, all three models overlap in many core aspects. Additionally, there are aspects between them that directly contradict each other, suggesting than one theory may be accounting for factors that are overlooked in another. These contradictions may provide meaningful insight into the human psyche and the factors governing irrational and unoptimal security behaviours.

Human behaviour with all its intricacies and contradictions is much too complex to be fully captured by one theory. An integrative, multi-dimensional synthesis of these psychological theories is necessary to provide a more nuanced and comprehensive understanding of the underlying phenomena influencing non-compliance with security policies and recommendations. This valuable perspective is conspicuously missing in current approaches to information security, and more tangible data on the psychological aspects may guide the design, development and enforcement of security policies, measures and training. Security policies that focus solely on security training, awareness, and the technical implementation of security measures are incomplete without consideration of the affective, behavioural and cognitive biases and factors underlying human action or inaction.

1.3 Research Question

The aim of this study is to gain a comprehensive understanding of the underlying psychological factors that guide perspectives, attitudes and behaviours students at Uppsala University have regarding recommendations and guidelines for cybersecurity. We aim to provide a deeper understanding of how these factors may interact with each other as well as modulate their respective effects through an integrative multi-dimensional analysis that examines the ways in which existing theories overlap as well as contradict each other.

To this end, our research question is:

What underlying cognitive, affective and behavioural factors determine an internet user's reaction to and compliance with cybersecurity recommendations and how do they interact?

1.4 Knowledge Contribution

The aim of this paper is to produce a descriptive qualitative contribution to the discussion surrounding security policies and recommendations in the form of a deeper understanding of underlying psychological factors that influence compliance. It focuses on inductively identifying themes derived from a thorough content analysis of interview responses gathered from students at Uppsala University.

During the global COVID-19 pandemic, large parts of higher education were moved online. Students along with faculty were more reliant on internet services than ever. This digitalization shows no signs of slowing in a post-pandemic world, nor does the threat cybercrime and as technological advancements are made in society, more and more critical infrastructure will exist primarily online. It is therefore crucial to examine the security behaviours of the individuals who will soon be at the forefront of this growing shift towards digitalization in the coming years. Furthermore, gaining a deeper understanding of how a more tech-savvy population approaches risk and compliance will also be important to future cybersecurity research. These factors make young adults and students a valuable resource of perspectives to further our knowledge and understanding of the topic at hand. The significance of these results for institutions responsible for developing and enforcing security policies and fighting cybercrime cannot be underestimated. As future generations continue to immerse themselves in technology, identifying significant factors surrounding their attitudes and behaviours will be instrumental in guiding future development of security policies and guidelines. Additionally, information on how students behave and perceive risk may be potentially both illuminating and disconcerting to Uppsala University and indeed universities in general.

While our study was based on responses from students at Uppsala University, there is little reason to suspect that students at other universities, both in Sweden and elsewhere, would have vastly different opinions. The questions included in the interviews did not concern risks and behaviours specific to students; therefore, we believe that the results of this study may be applicable for this age group on a broader scale outside of universities, as the threats and risks discussed are of equal importance to any young adult.

To summarize, we strongly believe that an understanding of how students perceive risks and respond to security recommendations and guidelines will be particularly useful for security departments and those responsible for the development of security policies both in universities and in other areas of society. Security policy makers will potentially benefit in the development process from considering further insights regarding human psychological factors that are commonly overlooked.

1.5 Scope

The primary focus of this study lies in the perception of cybersecurity risks and compliance with security recommendations in the average user. Aspects that are not examined as a part of this study include individual knowledge of cybersecurity. Studies show that individuals with a professional background in cybersecurity, either through work or studies, are likely to have different perspectives as compared to individuals without, and may suffer from security fatigue to a greater degree and exhibit more optimism bias (Barth et al., 2019). How prior technical knowledge may affect the influence of underlying psychological factors is a fascinating potential area of study. However, as our paper aims to gain a deeper understanding of the underlying psychological phenomena, we chose to eliminate advanced knowledge or experience as a potential individual factor that may affect our analysis. Therefore, none of the students participating in this study were enrolled in courses that specifically touched on IT security.

The sample group for this paper consists solely of students at Uppsala University — it does not include faculty members or other staff. While we have no reason to suspect that the responses gathered from students would differ from any other individual in this age range, we chose to include only students in this study for the sake of consistency, and to emphasize the importance of our findings for universities. This narrowed focus was chosen for several reasons.

There is research that suggests that age may be a significant determining factor for information security behaviours (Pattinson et al., 2015). A sample group consisting of university students at the undergraduate and graduate level effectively restricts the age range of participants, minimizing the chance of individual differences such as age to potentially skew results. The age range of participants is 20-27 years, which we believe is representative of the average age range of young adults.

Faculty members or other related staff were not considered due the potential difference in how security behaviours manifest in a professional setting as compared to personal use. Employees may have different motivations to follow security recommendations, either because it is stated in their job descriptions, or due to the involvement of sensitive information requiring a greater level of security. Furthermore, employees at Uppsala University are government employees, which provides them with different protections, whereas students are considered private actors, and are therefore not protected by the university in the event of a cybersecurity incident. This lack of protection could prove to be a substantial vulnerability for the university, should students exhibit significantly lacking security behaviours.

Our choice of theoretical frameworks to investigate consists of three well-established theories within the field of psychological aspects of cybersecurity. While many models exist for explaining risk perception and risk-taking behaviour as well as motivations to protect oneself against threats, these three theories specifically were chosen following a general, exploratory literature review. Other models may naturally be relevant for cybersecurity but our chosen frameworks have been directly implicated in several studies and are therefore deemed to be the most pertinent for our study. The vast majority of studies reviewed stayed within the boundaries of these three theories — while some used slightly differing terms, such as privacy fatigue instead of security fatigue, the underlying theories were the same. Our study therefore maintains a narrower focus on these frameworks rather than considering all possible explanation models that may exist.

2 Theoretical Foundation

2.1 Theoretical Background

In order to examine the perception participants have of the risks they are exposed to online, it is necessary to gain a basic understanding of what risks most commonly affect the average internet user. This section provides an overview of common cyber attacks, consumer responses to data breaches, as well as research on recommendations involving secure password management, the common risks individuals take, and the potential consequences of these threats.

2.1.1 Common Cyber Attacks

Cybercrime is an increasingly relevant issue not only for governments and organizations, but for anyone with an email address, online bank account or any potentially sensitive information online. Most internet users lack deeper knowledge of cybercrime, including its most common forms and methods, as well as how to best protect your information and devices from attacks (Khiralla, 2020). New forms of cybercrime emerge every year as criminals adjust their strategies and adapt to global and societal changes, such as the development of new technologies or major global events like the COVID-19 pandemic, which prompted a swift push towards digitalization and remote work (Khiralla, 2020**;** Deora & Chudasama, 2021).

Cybercrime refers to criminal activities committed using computers, networks and the internet. There are two general categories that define cybercrime as a whole; the first encompasses crimes that are more technically focused — so called 'cyber-dependent' or technical crimes — that can only exist within the limits of a hardware or software system. The second category, referred to as 'cyber-enabled' crimes, consists of crimes that are aided by or involve the use of technology or the internet, but where the technical aspects play a less significant role in the crime itself (Deora & Chudasama, 2021; Conway & Hadlington, 2021). It's worth mentioning that not every form of cybercrime, whether cyber-dependent or enabled, involves attacks on users, organizations or governments; for example, illegal streaming, downloading of software or purchasing of illegal goods all count as cybercrime but do not involve cyberattacks. These crimes, however, are not within the scope of this paper.

Phishing

Phishing attacks are a form of deception with the aim of tricking individuals into disclosing sensitive information, such as usernames, passwords and banking details (Choo, 2011). Perpetrators typically attempt to disguise themselves as trustworthy entities, attempting to lure people with fraudulent emails, messages, links and web pages. Phishing often involves a social engineering component that takes advantage of human naivety and emotion. Attackers may send messages that convey a sense of urgency in order to prompt immediate action from the victim, giving them less time to potentially grow suspicious. These messages may contain fraudulent links or attachments that lead to fake login pages or malicious software installations. Once victims provide their information, attackers can exploit it for identity theft, financial fraud, or unauthorized access to accounts.

Wi-Fi Eavesdropping

Wi-Fi eavesdropping, also referred to as an 'evil-twin' attack or a man-in-the-middle attack, involves the unauthorized interception and monitoring of wireless communication on unsecured Wi-Fi networks (Shrivastava et al., 2020). Through the use of specialized programs, cybercriminals are able to intercept the data being transmitted between connected devices and the Wi-Fi router. This form of cyberattack exploits the vulnerability of unencrypted Wi-Fi connections. Attackers may also set up their own unsecured public wi-fi hotspot and give it an inconspicuous name ("McDonalds Free Wifi", for example) in order to lure victims into connecting to their network, after which data transmitted may be easily intercepted. Data that may be captured includes login credentials, personal information and financial details. Users connected to unsecured public networks are particularly vulnerable to wi-fi eavesdropping attacks as these networks are typically found at public places such as restaurants, where anyone may gain access to the network without drawing suspicion.

Malware

Malware refers to malicious software, which encompasses a wide variety of software designed to steal data from or gain access to computer networks and servers (Choo, 2011). Various types of malware include ransomware, spyware, trojans, viruses, and worms. These types of attacks breach computer systems through system vulnerabilities, typically due to users being tricked into clicking on an unknown link or email attachment, which promptly installs the harmful software. Once deployed, malware can execute predefined actions, ranging from stealing sensitive information and monitoring user activity to damaging files, encrypting data for ransom, or providing the attackers with unauthorized access to the system.

Password Attacks

Password attacks are a common threat to cybersecurity that involve gaining unauthorized access to user accounts or computer systems by exploiting weaknesses in password security (Onaolapo et al., 2016). Attackers employ tactics such as brute-force attacks, where they systematically try numerous password combinations until the correct one is found, or dictionary attacks, in which precompiled lists of common words and phrases are applied in hopes that a match is found. Other techniques include credential stuffing, which involves attempting to use previously stolen usernames and passwords on multiple online platforms. The goal of password attacks is typically to gain unauthorized access to sensitive information, financial accounts, or other confidential data.

Third-Party Cookies

Third-party cookies can pose a significant threat to user privacy and cybersecurity as they are used to track users' online behavior across the internet (Marino, 2021). These cookies, often set by entities other than the website being visited, can be exploited for targeted advertising, user profiling and data monetization. Risks associated with third-party cookies include invasive tracking, where browsing habits are extensively monitored without users' consent or awareness. This tracking may be used to create detailed user profiles, raising concerns about potential exposure and misuse of personal information. Third-party cookies may compromise online anonymity as confidential, potentially identifying information may be spread to other websites and entities without the user's knowledge.

2.1.2 Consumer Response to Data Breaches

Data breaches are a growing concern — predictions estimate that 33 billion accounts will be breached before the end of 2023 (James, 2023; Vojinovic, 2023). As part of an effort to mitigate the consequences, legislation in large parts of the world requires affected users to be notified of data breaches. As of 2016, 47 states in the USA had passed legislation requiring companies to notify affected users of data breaches (Ablon et al., 2016). The EU General Data Protection Regulation (2016) requires the targets of a data breach to "communicate the personal data breach to the data subject without undue delay". According to a survey conducted in the US by Ablon et al. (2016), 43% of respondents (105 million Americans) recalled receiving a data breach notification in their lifetime.

However, research on consumer response in the wake of a data breach shows that a worryingly high number of recipients do not follow recommended security measures. Surveys conducted by Ablon et al. (2016) and the Ponemon Institute (2014) found that up to 32% of respondents ignored data breach notifications. Following the large-scale data breach targeting Equifax in 2017, a major U.S. credit bureau, less than 1% of customers froze their credit 10 days after the fact (Zou et al., 2018). While many victims of the Equifax breach reported increased concern, more than half took no protective measures whatsoever. The authors found that this widespread inaction was primarily influenced not by a lack of risk awareness, but by "costs associated with protective measures, optimism bias in estimating one's likelihood of victimization, and a general tendency towards delaying action until harm has occurred" (Zou et al., 2018).

Research has found that the design of breach notifications can have an effect on whether recipients take action. Zou et al. (2019) analyzed the efficacy of data breach notifications and found that many were subject to ambiguous language: "your data may have been compromised"; minimization: "we do not expect your data to be used", as well as general issues with clarity and readability. According to the authors, ambiguous claims minimizing the event increase optimism bias in users, who are less likely to believe they'll be personally affected. The study also found that users perceive the benefit of taking action to be too small compared to the required time and effort. Another similar study by Golla et al. (2018) found that data breach notifications, particularly regarding password breaches, raised concerns among users — however, less than a third of respondents indicated any intention to change their password.

2.1.3 Password Management

Passwords remain one of the most ubiquitous forms of security and authentication due to their ease of use (Wash et al., 2016; Lee et al., 2022). Being so widely implemented, however, also makes them one of the most high-profile targets — a study from 2017 found that an approximate 1.9 billion usernames and passwords were exposed through data breaches over the course of a year (Thomas et al., 2017). Thomas et al. estimated that 7-25% of these leaked credentials belonged to “high-value targets like Google accounts”. Another study showed that previously leaked credentials are often matched to identifiers like usernames, email addresses, and other known passwords by attackers to increase their chances of breaking into even more accounts in a cross-site attack (Das et al., 2014; Onaolapo et al., 2016). Onaolapo et al. showed that hackers who gain access to email accounts search for financial information and banking details which they can then use to turn a profit on their illegitimate activity.

Decades of research have gone into combating the inherent weaknesses of passwords. Guidelines aimed at users encourage long, randomized alphanumeric passwords not containing personal information such as birth dates or names; additionally, users are told not to write their passwords down, to use a unique password for each account, and to renew their passwords regularly (Herley, 2009; Wash et al., 2016). Websites are advised to implement security intervention mechanisms for users creating new accounts which include blocklists, password composition policies and strength meters to ensure that users choose strong passwords (Lee et al., 2022). New technologies such as password managers have been developed to enable users to have random and unique passwords for each account by storing these passwords and automatically applying them when logging in, eliminating the need for users to remember all their passwords themselves (Fagan et al., 2017).

Despite these advances in password technologies and policies, they remain vulnerable to attacks, largely due to insufficient password safety on the part of the user. Password reuse in particular is very prevalent; an estimated 43-51% of users re-use their passwords across multiple accounts, placing them at risk for cross-site password attacks (Das et al., 2014). While password managers exist to tackle this issue, studies show low adoption rates, suggesting that users instead resort to other methods to help them manage passwords, including re-use, writing passwords down, and creating weak passwords (Fagan et al., 2017).

2.2 Related Work

The information security industry overwhelmingly focuses on the technical dimension of security and often overlooks the human factor (Hughes-Lartey et al., 2021). Research over the past decade has attempted to expand the focus to include psychological perspectives. In order to form a thorough and nuanced understanding of some of the reasons as to why cybersecurity recommendations suffer from low compliance rates, we will present three different psychological theories exploring this phenomenon from different perspectives: (1) security fatigue, an affective approach; (2) optimism bias, a cognitive approach and lastly (3) cost-benefit analysis, a behavioural approach.

2.2.1 Security Fatigue

Fatigue is defined as a subjective sense of tiredness that often stems from an inability to meet high demands and expectations (Choi et al., 2018; Hardy et al., 1997). Failure to meet expectations leads to a sense of helplessness, futility and lack of control that in turn can affect motivation and effort levels. The term has been adopted in information security research to describe the affective weariness users experience as a result of the bombardment and subsequent hyper-awareness of security risks and recommendations (Choi et al., 2018; Stanton et al., 2016).

Security fatigue is a socio-emotional state of saturation, where a user becomes so inundated by the overwhelming amount of cybersecurity requirements, policies and reminders that they become resigned to security risks. When individuals reach this point, it often leads to less secure online behavior and reduced compliance with recommended security measures (Stanton et al., 2016; Cram et al., 2020). Choi et al. (2018) describe security fatigue as a state of emotional exhaustion and cynicism — in the face of the ever-increasing rates of cybercrime, users question what use there is in following security guidelines, since it is unlikely to prevent a motivated cybercriminal from achieving their goal.

Research shows that the complexity and sheer amount of privacy decisions a user must make and the perceived futility in adopting recommended measures leads to security fatigue, making users forego privacy protection behaviours (Choi et al., 2018; Stobert & Biddle, 2014). Faced with an unmanageable amount of security guidelines, recommendations and expectations, users resort to strategies that circumvent them in order to cope with high demands (Stobert & Biddle, 2014; Wash et al., 2016). These coping mechanisms ration mental effort and prioritize what users consider the most important aspects of online security. Stobert and Biddle identify a "mismatch between security expectations and user's abilities", indicative of a gap between user behaviour and design principles and implementation of security measures. Choi et al. (2018) similarly found that security fatigue has a stronger impact on the security decisions users make than the concerns they have over their online security and privacy — despite worries a user may have, the need to alleviate the mental load of overwhelming security recommendations outweighs those concerns and often leads to risky security behaviour.

2.2.2 Optimism Bias

The cognitive aspect of risk assessment has been the topic of research for several decades. Research conducted in the 80s found that individuals had a tendency to perceive themselves as less susceptible to negative incidents than others — shortly put, people believe it's more likely for something bad to happen to someone else than to themselves (Weinstein, 1980, 1989). This cognitive bias towards unrealistic optimism, or optimism bias, often skews judgement with regard to perceived vulnerability and can lead individuals to take more risks.

Optimism bias has proved to be among the most robust factors in research on risk judgement over the past few decades, emphasizing judgement of perceived vulnerability as a highly significant central aspect of risk perception (Cho et al., 2010). Research suggests several underlying mechanisms influencing this perception of vulnerability, among which are the illusion of control and psychological distance (Chapin, 2000; Cho et al., 2010). The illusion of control refers to a cognitive bias leading individuals to overestimate their ability to influence and control the outcome of events. Psychological distance, on the other hand, refers to the perceived closeness of potential events. Events that are judged to be distant, either temporally, spatially, or socially, are often perceived to be less probable or harmful.

More recent studies on the topic of information security have found that people are significantly influenced by optimism bias with regards to cybersecurity (Cho et al., 2010;

Hewitt & White, 2021). Cho et al. found that internet users displayed a strong optimistic bias, judging themselves to be at much lower risk of online privacy breaches than other users. Perceived controllability and prior experience were both significant factors; users with high perceived controllability and users for whom prior personal experiences were rare or otherwise lacking in significant consequences were more likely to exhibit optimism bias. Similarly, Hewitt and White noted that knowledge is a strong predictor of optimistic bias — individuals with more security education tended to be overconfident in their own ability to reliably recognize and protect themselves from threats, often leading them to take more risks.

The cognitive bias towards optimism that users portray when navigating cybersecurity often puts them at higher risk of malicious activity, and even more so when they consider themselves knowledgeable about the topic. This tendency towards unrealistically optimistic judgements has been implicated in a great deal of research into security behaviours and decisions, and is likely to continue being a significant factor.

2.2.3 Cost-Benefit Analysis

Lax attitudes towards security recommendations are often portrayed as irrational — after all, why would people choose not to safeguard themselves online given the tools and recommendations at their disposal? From a behavioural economics perspective, researchers argue that individuals calculate the perceived costs and benefits of security compliance resulting in some individuals reaching a limit where the costs outweigh the benefits, leading to the choice to disregard or circumvent recommendations (Beautement et al., 2008; Herley, 2009; Stanton et al., 2016).

Weak passwords are one such example — the large cost of creating unique, strong passwords for every new account does not justify what a user may stand to gain from it (Stanton et al., 2016; Herley, 2009). Herley argues that many of the rules imposed upon users when creating new passwords are arbitrary and only serve a purpose in specific circumstances, and many are rendered moot by certain attack vectors (Herley, 2009). Users are told never to write down passwords — but writing down passwords is only a risk if there's a chance that someone may gain access to the physical note. Targeting a notebook containing passwords that is stored in a user's home would be of little use for a hacker aiming to gain access to many online accounts — it is much more efficient to target online databases of user credentials. Similarly, changing passwords frequently is only useful if the account has been compromised — otherwise, it changes little at the moment of attack, and the user has instead expended a great deal of effort for no significant gain. People ultimately ignore "crushingly complex security advice that promises little and delivers less" (Herley, 2009).

Some recommendations have been shown to be counterproductive — the implementation of password composition rules encourages users to create passwords with predictable patterns that negate the security benefits (Lee et al., 2022; Ur et al., 2015). Ur et al. studied how users create passwords and found that the most common composition rules (must contain upper and lower case letters, digits, and special characters) lead users to create formulaic, easily guessed passwords rather than secure ones. When creating passwords for websites requiring at least one special character, for example, users tend to add an '!' on the end to satisfy the requirement.

Researchers argue that password composition policies promote misconceptions about password strength; claiming that a strong password should contain letters, digits, and special characters leads users to erroneously conclude that any password containing letters, digits, and special characters is, by definition, strong (Ur et al., 2015). While this may momentarily hinder standard dictionary attacks, Chou et al. (2013) showed that by implementing machine learning algorithms trained on a test set of passwords following the most common patterns, the amount of passwords cracked increased by 250%. Since users don't have a choice in following password composition policies (as websites often won't allow passwords that do not fulfill requirements), they instead resort to effort-saving strategies such as creating formulaic passwords and re-using them across several accounts.

3 Design

3.1 Research Strategy

This paper implemented a qualitative interview as an approach to answer the research question. Qualitative data includes all non-numeric data, such as images, audio or text, and is the main type of data generated by ethnography, observational studies and interviews (Oates, 2006). The choice of an interview study as our research approach is motivated by our goal of gaining a deeper understanding of the topics discussed in this paper, namely the underlying cognitive, affective and behavioural factors that determine a user's reaction to and compliance with security recommendations and how these factors interact.

Consequently, the most fitting characterization of this study is an interpretivist approach. Unlike positivist studies, interpretivist-based research, as exemplified in this paper, does not aim to prove or disprove any hypotheses (Hsieh & Shannon, 2005; Oates, 2006). The interpretivist approach instead focuses on identifying, exploring and explaining various factors within a specific social setting and how they interact. It seeks to comprehend how people perceive their world, emphasizing the meanings and values people assign to phenomena. This closely aligns with the goal of our study, as our aim was to examine attitudes, perspectives and habits in our participants. Although frameworks and theories from previous studies were used to guide our line of questioning and inform our analysis, our primary goal was to identify underlying themes and factors and their interactions based solely on interview responses rather than attempting to validate previous theories. We had no hypotheses and approached this goal with the intention to explore these perspectives. The interpretivist approach is therefore judged to be an appropriate paradigm (Hsieh & Shannon, 2005; Oates, 2006).

3.2 Data Collection

Qualitative data was gathered in the form of interview responses. Interviews are a readily accepted method of gathering qualitative data within the fields of Information Systems and Psychology, and are useful for gaining a deeper understanding of perspectives and opinions which may otherwise be difficult to infer from quantitative data (Oates, 2006; Blaxter et al., 2006).

There are three general types of interviews: structured, semi-structured and unstructured (Weiss, 1995). Structured interviews utilize a uniform and predetermined set of questions, identical for each participant. These types of interviews are more similar to surveys or questionnaires in the sense that the participant and interviewer don't engage in more conversation other than to ask, clarify or answer questions, where answers typically entail a yes, no or short response (Oates, 2006; Weiss, 1995). While these interviews have their areas of application, their strict nature risks limiting spontaneous thoughts and in-depth reasonings from participants. The opposite of these are unstructured interviews, which are more similar to a regular conversation and instead focus on particular topics rather than prearranged sets of questions, allowing the participant to freely express themselves and elaborate more on their responses (Oates, 2006).

While the latter option aligns more with the approach of this study it wouldn't make an appropriate choice for two main reasons: some degree of structure was necessary in the form of pre-defined questions in order to ensure coverage of all topics and themes as well as to keep the interviews within a reasonable time frame. To this end we instead opted for semi-structured interviews, which embody the characteristics of both structured and unstructured interviews. The choice of semi-structured interviews for this study is motivated by the method being particularly useful in exploratory studies as it allows participants the freedom to express themselves and elaborate on their responses more in-depth (Oates, 2006; Weiss, 1995). While pre-defined questions help to guide the topics of discussion and enable comparison with other interview responses, space and flexibility is also allowed to give researchers opportunity to ask follow-up questions based on participant responses. It also gives participants the opportunity to raise topics the interviewer otherwise might have overlooked, without interfering with the overall list of themes and questions.

A semi-structured interview study was chosen over other common forms of qualitative data collection methods after consideration of which aspects best support our goals. Ethnographic studies typically involve immersive engagement by the researchers with a particular cultural or societal group, with the aim to gain an understanding of cultural norms, attitudes and behaviours (Bryman, 2018). Researchers may observe and participate in group activities and conduct interviews with members of said group in order to gain a deeper understanding of these cultural aspects. While cultural norms could potentially be considered a factor in determining risk perception and behaviour, the aim of this paper is to gain an understanding on a broader level rather than focusing on a distinct socio-cultural group, to which end ethnography is not a relevant method. Further, observational studies where researchers do not interact with participants but rather gather information on their behaviours through observation are not relevant for this topic, as we aim to gain an understanding of participants' thoughts and attitudes — factors that are difficult to discern purely based off behaviour (Oates, 2006).

3.2.1 Interview Guide

To aid in the interview process, an interview guide (see Appendix A) was contructed that covers the main themes and questions, based on the interview framework defined by Kallio et. al (2016). This guide served two purposes — prior to conducting the interviews, we used the guide during training sessions amongst ourselves to ensure familiarity with the discussion topics as well as interviewer performance consistency. Then, for each interview, we used the guide as a framework to ensure that the main themes were covered and the same main questions asked, as well as to keep interviews within a reasonable time frame. The semi-structured nature of the interview allowed us to ask follow-up questions and probe participants' responses in order to encourage thoughtful consideration of the questions and topics.

The interview guide was structured around exploring behaviours and attitudes regarding common aspects of internet use and cybersecurity.

The first section concerned password management. Given that password re-use is one of the most prevalent forms of security non-compliance, we believed this line of questioning would be highly relevant to our topic. General questions about habits included questions about whether participants used password managers and whether they re-used passwords. Based on participant responses, we probed deeper into the reasoning for their habits and choices, as well as attitudes towards password composition criteria and recommendations for secure password management. Questions about password management were based on similar earlier studies (Das et al., 2014; Fagan et al., 2017; Stobert & Biddle, 2014; Ur et al., 2015; Wash et al., 2016).

Next, participants were asked about their familiarity with data breaches — if they were not familiar with the term, a short description was given in order to ensure a baseline level of understanding. Questions here were based on previous interview studies that examined consumer responses in the aftermath of a data breach conducted by Ablon et al. (2016) and Zou et al. (2018). Participants were asked if they had any personal experience with data breaches, and prompted to describe the incident, how it may have affected their behaviour, as well as their level of concern for potential data breaches.

The next section encompassed the broader topic of risky online behaviours and security recommendations. Participants were asked to give examples of risky behaviours in order to gauge their awareness of various risks. Based on their responses, additional examples were provided and potential consequences discussed. By ensuring that all participants were given the same examples of risky behaviours, we could be more confident that participants had a similar understanding of risks. Examples included visiting potentially suspicious websites, downloading unknown files, connecting to public wi-fi networks, clicking on unknown links in emails and messages, accepting third-party cookies, and re-using passwords. This list of examples was created based on the most common cybersecurity risks described in section *2.1 Theoretical Background*. Participants were then asked whether they could identify these risky behaviours in themselves, opening up the discussion to their thoughts about security recommendations, their own vulnerability to risk, and their behaviours online.

Lastly, we asked participants whether they considered the internet to be a riskier place now when compared to before. This was an open-ended question intended to encourage participants to share more of their thoughts, attitudes and perspectives that may not have been encompassed by previous questions.

3.2.2 Selection

Participants were selected through a convenience sample, based on their availability and willingness to participate in our study. A convenience sample does have some limitations: due to the nature of the sampling method, there is a risk that the sample group is not representative of the general population. In order to mitigate this, we attempted to recruit participants from a wide variety of academic fields, at both undergraduate and graduate levels. We also aimed for a relatively balanced distribution of men and women, as well as an age range that covers young adults as a target demographic.

Initially, participants were sought out through personal contacts and their acquaintances on social media platforms such as Facebook and LinkedIn. Six participants from different departments and programs were secured through these networks. These participants were interviewed over the online communication platform Zoom. The remaining five participants were approached in person at various campuses throughout Uppsala University, where on-site interviews were conducted. We introduced ourselves and the subject area of the paper to the participants, and also gave them an estimated duration for the interview. Those that agreed to participate were then informed of their rights, which are described in section *3.5 Ethical Considerations*. A demographic description of the participants can be seen below in *Table 1*.

Participant ID	Gender	Age	Education
1	Female	20	Media and Communication
2	Female	22	Media and Communication
3	Female	22	Media and Communication
4	Male	25	Psychology
5	Male	25	Psychology
6	Female	26	Biology, Ecology
7	Female	27	Physiotherapy
8	Male	24	Business and Economics
9	Male	23	Business and Economics
10	Male	21	Nursing
11	Female	22	Nursing

Table 1. Participants

3.3 Data Analysis

Qualitative content analysis is a widely accepted research method, considered useful for its flexibility in analyzing text data and the opportunity it provides for deeper exploration and understanding of human experiences and perspectives (Cavanagh, 1997; Erlingsson & Brysiewicz, 2017; Hsieh & Shannon, 2005). Although different approaches to content analysis exist, the general application involves the analysis of text in any form with the aim to classify and categorize underlying themes and meaning in the text (Hsieh & Shannon, 2005). This allows for more efficient interpretation of and comparison between different sources of text data.

Erlingsson and Brysiewicz (2017) describe content analysis as a multi-step process, systematically transforming large amounts of text into concise and organized summaries of key take-aways through identification and classification of meaningful themes. The steps involve dividing and condensing the text into increasingly smaller parts using codes and categories. Approaches to content analysis differ primarily in the choice of codes and categories used.

Conventional content analysis, also called inductive category development, is an approach commonly implemented in qualitative studies (Hsieh & Shannon, 2005; Mayring, 2000). This approach is useful in many cases where a limited amount of research literature on the topic exists. Instead of categorizing content according to predefined codes and categories based on prior research, categories are derived from the text itself based on the topics that arise, allowing for a more organic and exploratory analysis of the text (Hsieh & Shannon, 2005).

The directed or deductive approach to content analysis, in contrast, derives codes and categories from an existent knowledge base, using previous theories and research to guide and focus the research question with the goal of expanding upon or validating said theories (Hsieh & Shannon, 2005; Oates, 2006). This could be considered applicable in this study as previous research does exist on the topic — security fatigue, optimism bias and cost-benefit analysis are fairly prominent theories regarding underlying factors of non-compliance.

The aim of our study, however, is not to simply validate these pre-existing theories, but rather to investigate potentially overlapping aspects of non-compliance as well as how they interact. Hence the decision was made to opt for an inductive approach to allow for the flexibility to form our own categories based on the recurring themes in our responses, instead of restricting our analysis to predefined categories.

3.4 Implementation

Interviews were conducted either in Swedish or English and audio-recorded. The first step was to transcribe, translate and format the responses into a structure suitable for further analysis, as is standard for qualitative interview data (Erlingsson & Brysiewicz, 2017; Weiss, 1995). Both Erlingsson and Brysiewicz (2017) as well as Hsieh and Shannon (2005) recommend reading through the raw text data several times as the first step in content analysis. This helps researchers to gain an intuitive, overarching understanding of the topics and themes that arise, forming a preliminary idea of which categories may be relevant.

Erlingsson and Brysiewicz (2017) recommend separating text data into separate sentences or “meaning units”. These meaning units are then condensed into their core message in order to simplify the analysis process. Examples of this process are given in *Table 2*, with two meaning units taken from two different interviews conducted in this study.

Meaning Unit	**Condensation**
“Yeah, I guess I think that no one would want my accounts.”	No one wants my accounts
“I have a few different versions but I definitely re-use them [passwords], it’s just easier to remember.”	I re-use passwords because it’s easier

Table 2. Examples of Meaning Units and Condensations

Not every meaning unit found in the raw text data was subject to condensation; some responses involved clarification, repetition or other irrelevant information, and were therefore excluded from further processing. Next, a code capturing the core essence of each meaning unit was applied and subsequently categorized, as shown in *Table 3*. This process allows for a higher level of abstraction to be achieved, which reflects what Erlingsson and Brysiewicz (2017) refer to as the latent meaning of the text. Condensation, coding and categorization of each interview was initially carried out by both researchers individually, in order to enhance interrater reliability before defining overarching themes.

Overarching Themes		
Theme Convenience		
Condensed Meaning Unit	**Code**	**Category**
I re-use passwords because it's easier	Password re-use, ease	Effort-saving Strategies
Theme Naivety		
Condensed Meaning Unit	**Code**	**Category**
No one wants my accounts	Insignificant personal data	Insignificance

Table 3. Coding and Categorization Process

3.5 Quality Assessment

As for any research approach, there are quality concerns regarding our chosen methods and implementations that need to be evaluated and addressed. Usually, these evaluations are carried out with criteria such as *objectivity*, *reliability*, *internal validity (credibility)* and *external validity (generalizability)* – these are, however, rooted in the positivist paradigm and quantitative research. When evaluating qualitative interpretivist research, utilizing criteria based on positivism is not appropriate (Oates, 2006; Treharne & Riggs, 2015).

Objectivity refers to the notion that research should remain uninfluenced by the personal values and biases of the researcher. The interpretivist paradigm, instead, asserts that some degree of bias is unavoidable (Oates, 2006; Weiss, 1995). Interpretivist research instead evaluates *confirmability* and *dependability*, which examines whether the findings in the study can be derived from the gathered data as well as how well each process in the study is documented to support this, both of which can be assessed by research auditing (Oates, 2006; Treharne & Riggs, 2015). Regarding confirmability, we firmly believe that the findings of this paper have been formulated from a fair interpretation of the results, and can be traced back to the initial steps taken in gathering data. We chose not to disclose full transcripts of our interviews due to the potentially sensitive nature of the information disclosed by participants, which may potentially hinder an external quality assessment. However, we are confident that each stage of our research process from initial literature review to data acquisition and processing and subsequent presentation of results and analysis is thoroughly documented and motivated throughout the paper.

Regarding the *credibility* criteria, it can be compared to what positivistic research refers to as internal validity. Validity in positivist studies is concerned with the extent to which findings are accurate and correctly measured, emphasizing the importance of evaluating whether the researcher is justified in their claims and whether the findings "match reality" (Oates, 2006). Interpretivism, on the other hand, does not agree with the idea of one uniform and objective reality (Treharne & Riggs, 2015). It instead highlights the notion of several constructed realities, thus rendering any ultimate benchmark to compare any findings to meaningless. Interpretivist research is therefore more concerned with the concept of credibility. Credibility assesses whether the study correctly and extensively identifies and motivates the relevant topics of the inquiry, in order to assess how credible the findings are. For this study, extensive literature review was carried out in order to accurately identify the main themes that were included in the interviews. Prior to the interviews, we ensured that the participants were well informed of the aim of the study to promote relevant and thoughtful discussions, as well as informed them of their rights. For the analysis of the gathered responses, researcher triangulation was implemented in order to compare the results before presentation. Thus, we believe that our findings are credible.

Finally, there is the criteria of *transferability*, which in positivist studies corresponds to generalization or external validity. External validity is concerned with the degree to which the findings in positivist quantitative research are generalizable to other people, settings or times, and is largely dependent on the size and representativity of the sample and the validity of the research method. Interpretivism, on the other hand, accepts the differences and uniqueness of individuals and contextual factors (i.e. social constructs), resulting in a low likelihood of identical results being produced. However, this does not imply the absence of generalizations entirely in qualitative studies; applicability of findings in other contexts remains an important aspect of qualitative research. Evaluating applicability or transferability is therefore more reliant on the researcher presenting adequately detailed descriptions in order for readers and other stakeholders to judge whether findings from the study may be relevant in other problem areas and contexts (Oates, 2006; Treharne & Riggs, 2015).

3.6 Ethical Considerations

Since this study entails gathering data with interviews, various established ethical guidelines have been considered to ensure that the study complies with good research ethics. These include the right to not participate in the study, the right to withdraw from the study, the right to give informed consent, the right to anonymity and the right to confidentiality (Oates, 2006; Weiss, 1995).

The right to not participate entails not forcing or coercing any individual or organization intto participating in your research (Oates, 2006; Weiss, 1995). The right to withdraw expands on the right not to participate, by allowing participants to withdraw from the study at any time without consequences, which also includes parts of the study, such as declining to answer certain questions. The right to give informed consent means that the participant´s consent is only given after they have been made aware of the nature of the research, meaning any prior agreement infringes on their rights. The information required for this includes: the purpose of the research; the researchers' names, details and any sponsoring organization; what the involvement entails, i.e. an interview, questionnaire etc.; whether any payment or expenses are involved; and how the data will be used. The right to anonymity means that participants have the right to have their name and location protected, either by remaining undisclosed or by being given a pseudonym. Finally, the right to confidentiality specifies that the obtained data, or any findings derived from it, must be kept confidential upon request.

Prior to each interview, we ensured that every participant was fully briefed on the study's purpose, subject area and anticipated duration of the interview. Upon obtaining their agreement to participate, we expressed gratitude for their involvement and provided a more comprehensive overview of the study's nature and the interview process. Participants were explicitly informed of their right to withdraw at any point or decline specific questions, with the assurance that their information could be removed retroactively upon request. Additionally, participants were notified that the interview would be audio-recorded for subsequent transcription, but would only be used for the purpose of this study. Finally, they were assured of complete anonymity throughout the entire process.

4 Results and Analysis

4.1 Presentation of Results

Content analysis of the interviews conducted revealed a number of responses that we condensed and categorized according to recurring patterns and topics. We ultimately identified three themes that encompass the underlying sentiments and factors that were discussed with regards to non-compliance: resignation, naivety and convenience.

4.1.1 Resignation

One of the strongest themes present throughout our interviews was the resignation displayed in participants' attitudes towards potential security threats. While participants unanimously agreed on the importance of cybersecurity and the relevance of security recommendations, there was a pervasive sense of defeatism regarding their own ability to successfully guard themselves against cyberattacks. Despite most participants making at least some attempts to protect themselves, they felt that their safety online was ultimately out of their hands.

Several respondents expressed a sense of helplessness regarding the likelihood of being victimized by a cyberattack, citing the advanced skill of cybercriminals and the futility of attempting to prevent it. One participant believed that it "didn't matter" what password she used — a skilled hacker would have been able to access her accounts regardless. They were resigned to their own powerlessness when faced with the threat of cyberattacks.

"You're like pretty vulnerable today, and there's many people who are good with computers... so if someone wanted to, they would've gotten in anyway." - Participant 8

"It feels like hackers and stuff, they can get in anyway, so it doesn't matter what password I have." - Participant 10

When asked to consider a potential scenario in which participants were victims of a data breach, responses suggested a general sense of helplessness and futility. Participants felt that there was little one could do in the aftermath of such a situation in which the damage had already been done. One participant described the scenario as "miserable", and suggested that the emotional toll might be debilitating to the point where no action would be taken. Overall, participants indicated that they wouldn't know what to do in such a situation, beyond basic measures such as changing passwords, or in the case of unused accounts, deleting the account entirely.

"Yeah, change my password I guess. There's not even that much you can do, the information is already out there, so I guess you just change the information that can be changed." - Participant 4

*"It just feels like such a miserable situation. It must be super dark, like getting debts and then having to prove that you didn't take any loans... so no, I don't think I would've done anything special, I would've just felt like s**t." - Participant 5*

“Panic. ... I would have to ask my parents, like ask my dad what he would do because I have no idea what I would do.” - Participant 6

Many participants considered the risk of being exposed to cybercrime to be a matter of luck. They unanimously agreed that following security recommendations made them safer online, but also expressed a belief that security measures could only go so far — while they may be worth the effort in a general sense, they are also unlikely to deter a motivated hacker, and all it would take to be victimized is for a hacker to choose to target you.

“I mean I for example also had my life of streaming online ... and I had the luck to not get anything. ... I think it's just luck, or bad luck, you could do it all perfectly and still get a hacker in your wi-fi and that's that.“ - Participant 6

“It only requires someone to want to do it, for it to happen, or that you're unlucky.” - Participant 7

In addition to resignation, responses gave the impression that participants had a sense of acceptance towards risks. Participant 4 felt like there would always be something more that could be done in order to protect oneself. He further described feeling that despite having taken steps to improve his own security, these efforts were often left seeming inadequate by constant reminders of cybersecurity threats from social media and news outlets. Participant 5 likened an overly cautious attitude to preparing yourself for the possibility of being robbed every time you go outside, calling it an unsustainable way to live. Instead, participants seemed to accept their own inaction, stating that if something were to happen to them despite being warned, it was through no fault but their own.

“It just feels like you could always be doing something better — use a different browser, use something other than Google that doesn't collect as much of your data.” - Participant 4

“If someone hacks me then it's just my own fault, I got all the warnings. But ignored them anyway.” - Participant 3

“It's like me going around and thinking about getting robbed every time I go outside and making sure I put things in hidden pockets; you can't live like that.” - Participant 5

The responses gathered from participants suggest a paradoxical relationship between awareness of and regard for security recommendations and the overall sense of resignation towards security threats. Essentially all participants agreed that recommendations were necessary and useful, but still indicated a tendency to disregard these recommendations. They exhibited a resigned, defeatist attitude towards cybersecurity risks, often expressing a lack of energy and motivation to fully follow recommendations. Participant 7 suggested this being due to a lack of inner motivation — simply being told what not to do does not sufficiently promote more secure behaviour.

“All in all I think the information and recommendations you get are good, and it would be good to have the energy to follow them, and for that maybe you need inner motivation, that they would maybe talk even more about what risks there

> *are and what the danger is, as long as they just say 'don't do this' maybe you don't really have the energy." - Participant 7*

4.1.2 Naivety

The theme of naivety relates more strongly to how participants perceived themselves as potential targets of cybercrime. One part of the interview asked participants to think of examples of risky online behaviours. Based on their response, additional examples were given and some of the potential consequences briefly discussed. The majority of examples that were brought up involved visiting potentially suspicious websites, downloading unknown files, connecting to public wi-fi networks, clicking on unknown links in emails and messages, accepting third-party cookies, and re-using passwords. This was intended to prime the participants to consider the threats associated with internet use from a personal perspective. Participants were then asked whether they personally were guilty of any of these behaviours. While essentially all participants admitted to behaving in a risky way online, most did not believe that this caused them to be more at risk for cyberattacks.

Most were aware of the riskiness of their behaviours, but many felt that their information would hold no value for a hacker. They considered themselves and their information insignificant — as one participant phrased it, they're just "one in the crowd".

> *"I have this thought that I'm just a small girl in Sweden, that no one has any use for my account." - Participant 1*

> *"Yeah sometimes you connect to public wi-fi, especially when you're abroad. Then you might feel... or no, I don't reflect on the risks of it really, and like what interest would they have in seeing my address?" - Participant 8*

While the majority of participants were aware of shortcomings in their security, they also indicated no real inclination to act upon these shortcomings. Since they believed their information to have no real value, they generally did not see the need to increase their security. Consequences of cybercrime on the individual level felt harmless, insignificant, and intangible in a way that made it difficult to take the risks seriously. In cases where participants had experienced being victimized, the events ultimately led to no lasting consequences. Participants recalled receiving emails notifying them of data breaches where they were informed that no action needed to be taken, after which they didn't spare the incident any more thought. When asked whether the incident made them more wary of data breaches, the majority of participants responded negatively.

> *"I've experienced like that people on Instagram or something get hacked and you get some weird message but then they've gotten their accounts back, so it ended up fine, but you see that it happens, that it's normal." - Participant 2*

Participant 1 described an incident where she had accidentally clicked on a link sent by a phishing scammer through FaceBook Messenger, leading to the same message being sent to many of her contacts through her FaceBook account. She described the response from her friends as immediately skeptical towards the veracity of the message, and said many made jokes at her expense suggesting she was dumb for having clicked the link in the first place —

something everyone knows not to do. In this case, the incident had no harmful consequences beyond embarrassment.

> *"Nothing happened, it was just like that they spread this link but it feels like everyone knows that you shouldn't click it. Everyone just thought I was really dumb." - Participant 1*

Participants did exhibit some degree of awareness over their overly optimistic perceptions of potential risks — they were generally aware that they were being idealistic and overconfident and taking their safety for granted, but as evidenced by their other responses, this awareness wasn't sufficient to actively change their behaviours. Participant 3, for example, referred to herself as naive with regards to the value of her information.

> *"I guess it's important to have strong passwords, but I'm pretty naive, like what would anyone do with my information?" - Participant 3*

As most participants hadn't directly been exposed to cybercrime, and those that had reported no directly negative consequences, most maintained a generally optimistic outlook. Since nothing had happened so far, participants seemed inclined to believe it unlikely that something would happen in the future. As such, many participants seemed to have a somewhat idealistic attitude towards cyber threats and their severity, and lacked a sense of urgency regarding consequences.

> *"You're pretty idealistic, you think oh, it can't happen to me, up until it does happen. I've been fine in all my 22 years, it hasn't happened yet." - Participant 3*

> *"How you handle your safety on the internet is very, very important I think — but it's also easy to take it for granted, and I know that I've taken it very much for granted." - Participant 5*

One participant described a sense of overconfidence born from a belief in one's own ability to discern what is and isn't safe online. When asked about which social groups were most at risk, the same participant also indicated that he believed himself to be less at risk when compared to the older generation, due to his familiarity with and ability to identify scams and potential threats. This overconfidence seemed to contribute to an illusion of control, fostering the belief that being able to identify a threat lessens the severity of the risks you expose yourself to and renders you more able to control the outcome potential incidents.

> *"Sometimes maybe you're overconfident in yourself, that you think that you have a better handle on what happens and doesn't happen and can determine what things on the internet are to a larger degree." - Participant 4*

Participants' assessment of the level of risk to themselves and their own ability to control that risk suggests a sense of unrealistically naive optimism that does not reflect the actual level of risk. This seemed to be strengthened by a lack of personal experiences that caused significant harm and the intangibility of potential consequences. Additionally, their attitudes were influenced by their own judgement of the importance of their information and accounts, ultimately deeming them of no value to a hacker and therefore not vulnerable to threats.

4.1.3 Convenience

Another recurring theme concerning compliance with security recommendations was a tendency for convenience and immediate gratification to outweigh security concerns. Convenience featured most prominently in how participants responded to security measures and recommendations in their internet use. This was discussed in connection to the various examples of risky behaviours and security recommendations described in *4.1.2 Naivety*.

When participants were asked if they generally tried to follow security recommendations, all answered affirmatively — with some caveats. While most made efforts to keep security recommendations in mind and maintain good "internet hygiene", they also admitted that they were likely to fall into what they themselves identified as "risky behaviour": visiting potentially unsafe websites in order to stream films or find information, accepting all third-party cookies because it was quicker than rejecting them, and connecting to public wi-fi networks. These behaviours often arose from inconvenience or a desire for immediate gratification. One participant described this behaviour as greediness.

> *"Laziness or stinginess I would think… that you want internet quickly or that you don't want to pay for a film or whatever it is. That's what it is really, greediness." - Participant 9*

> *"Most places let you pick 'accept only mandatory cookies', but on some there's something to click and then you have to click to reject each one, and I don't have the energy for that every time… if you're in a hurry or just want to find something quickly it's just immediately like, what's the fastest way to get rid of it." - Participant 7*

> *"But it's like… you really want to have internet, then it's difficult not to connect to the restaurant's wi-fi. And sometimes you can't 'reject all' cookies either, so then it gets difficult [to follow recommendations]." - Participant 8*

Perhaps the most prevalent example of ignoring security recommendations for the sake of convenience concerned the re-use of passwords. When asked whether they re-used passwords across several accounts, 10 of our 11 participants responded affirmatively. The one participant who did not re-use passwords explained that he creates new passwords for every account, but instead stores them all in a note on his phone so as to remember them.

There were a few common strategies regarding password re-use. Several respondents had 2-3 different passwords that they cycled between different accounts. Two respondents indicated that they chose which password to use depending on the "theme" of the account; all accounts that had to do with bookings, for example, used the same password. Most participants also indicated that they had one "main" password that they used as a base, which they then created variants of by adding a number, a special character, or a capital letter in order to have slightly "unique" passwords, and to fulfill password composition criteria where necessary.

The general sentiment towards re-using passwords seemed to suggest that participants were aware it wasn't safe — most said as much in their response — but ultimately chose to continue re-using passwords due to a desire for simplicity and convenience. The thought of having to remember a different password for every account felt overwhelmingly difficult, with most stating they wouldn't be able to remember more than a few passwords.

"It's really bad, I use the same password for everything and have done that since I was 6 years old." - Participant 1

"For me it's a habit I think. I mean because it's easy to keep track of, I know exactly what I need to write… So it's really because yeah, the convenience — not having to think so much and not forgetting. I can only keep track of 4-5 passwords in my head, and if it starts to go over that then it gets difficult."
- Participant 5

Despite the prevalence of password re-use, it is worth noting that several participants did indicate that they used a different password than their "standard" one for what they considered to be more important accounts, such as their email. Other, less important accounts more often used the same password. In this way, participants were able to have unique passwords for important accounts while still only needing to remember a few passwords overall.

When asked about password managers, some participants knew what they were and one participant actively used one, but the majority reported knowing little about what they entail and how they work. The general attitude revolved around password managers being too complicated, and most participants preferred to manage their passwords by themselves.

"Now and then I've thought about making it safer … but since I don't understand how [password managers] work, I don't dare trust them, and I'm too lazy to take care of it properly." - Participant 7

"I don't really know how they work, and then it's just been more convenient to keep track of my passwords myself." - Participant 10

"No, I usually decline them, they're too complicated." - Participant 2

When asked whether they regularly updated passwords, very few participants reported doing so. Many had used the same password for several years, in some cases for more than a decade. Several said that the only time they updated passwords was if they had forgotten a password and were forced to reset it. Some then made efforts to change passwords for other accounts to the same new password, while others did not bother update passwords for other accounts. Most indicated that having to change the passwords to all of their accounts would be extremely tedious, even though they were aware of the potential risks of not updating passwords.

"There was some article, like 'Sweden's most common passwords' and mine was number one and even then I didn't change it. It's such a pain to have to change it for all the accounts you have, so I just felt like 'ugh, it can stay.'"
- Participant 3

Some participants also expressed that they believed certain security recommendations to be superfluous. Several responses indicated a belief that writing down passwords wasn't inherently risky, provided the location it was stored in wasn't easily accessible. Other responses suggested that writing down a password without any other context, such as a username or which account it was used for, was still relatively safe as well as necessary for remembering passwords.

> *"I don't know… I mean yeah, I'm sure it's safer but I can't see any obvious advantage to changing my password all the time. Then writing down passwords, like I don't think that makes a huge difference if you do it on a post-it note on your desk." - Participant 11*

One participant expressed annoyance at certain security measures, finding them to be too limiting. This mostly referred to cases where the computer operating system required certain configurations and permissions to be changed before being allowed to download a file or install a program. Participant 6 felt that since these downloads were from official websites, the security measures in place were too strict, too disruptive and too difficult to disable.

> *"[My computer] only allows downloads of specific things, and if something is not in the list then it's a pain in the a** because you have to go to configurations and make it accept, like you're downloading something from an official website and the computer asks if you're sure. It's too much sometimes, it's too limited." - Participant 6*

Overall, the general impression was that participants were familiar with security recommendations and were able to identify potentially risky online behaviour. Generally speaking, attempts were made to follow these recommendations — until it became inconvenient or too time-consuming to do so. At that point, participants indicated that they were likely to ignore recommendations or circumvent safety measures in favour of achieving their goals. Many of the responses suggested that the participants actively used effort-saving strategies in order to minimize the load of security recommendations, selectively applying them in order to simplify their own online experience.

> *"[Recommendations] are there for a reason, so of course you should follow them… as far as you can." - Participant 8*

4.2 Analysis of Results

Resignation, Fatigue and Convenience

Previous studies on the topic of compliance with security recommendations identify security fatigue as a significant factor (Choi et al., 2018; Stanton et al., 2016). These studies describe a sense of resignation, futility and helplessness as core aspects, arguing that the constant barrage of recommendations, reminders, and security requirements lead to a state of emotional saturation and exhaustion. When faced with the overwhelming demands of modern cybersecurity, people tend to become resigned to the risks they face, and feel a sense of futility in effectively combating them. This is directly reflected in our results, which suggest that participants have developed resigned, defeatist attitudes towards their own safety online, and further shows that many consider themselves unable to adequately guard themselves against cybercrime.

Stanton et al. (2016) describe the pressure the average internet user is put under to constantly be "doing something" to improve their security, while simultaneously being unsure what that something is or what the consequences of inaction may be. One of our own participants similarly described feeling like there was always something he could be doing "better" with regards to his own security. Cybersecurity is with no doubt an unendingly complex and constantly evolving field. To the average user with no advanced knowledge of cybersecurity, the technicalities involved may feel overwhelming. Making security decisions may in turn feel beyond one's understanding and capabilities, leading to a defeatist attitude and a sense of helplessness. Being faced with these seemingly impossible decisions on a daily basis results in what Stanton et al. call "decision fatigue" — a pervasive sense of weariness and exhaustion caused by the need to constantly be alert and proactive, which ultimately manifests as resignation.

Aspects of security fatigue were also evident in the way that convenience took precedence over security concerns in our participants' behaviours. Despite overall acknowledging the importance and relevance of security recommendations, participants indicated that they were highly likely to willingly ignore recommendations and act in risky ways if it got them to their goal quicker. Some security recommendations were essentially ignored from the start; very few participants reported updating their passwords regularly, expressing weariness at the idea of needing to change the password to every account they had, and even more so at the idea of needing to do so at regular intervals. The effort required to firstly create a new password that fulfills password composition criteria, and secondly remember that password was more than the majority of participants were willing to expend. The inconvenience of following this recommendation clearly outweighed the concern that their passwords weren't very safe, echoing the paradoxical attitudes found in earlier research on security fatigue (Tian et al., 2022).

Although this strong preference for convenience and simplicity was called laziness by several participants, research would suggest that fatigue may be a more fitting explanation. What many people call laziness may not in fact be laziness, but rather the effect of a state of emotional exhaustion and fatigue which renders them incapable of expending the effort needed to adequately fulfill security demands.

Naive Overconfidence and Optimism Bias

Optimism bias as described by Weinstein (1980; 1989) is the tendency to perceive oneself as less likely to be exposed to negative incidents than others. This cognitive bias, as evidenced by more recent studies, also applies to cybersecurity (Cho et al., 2010; Hewitt & White, 2021).

Participants' responses indicated an overconfidence in the judgement of their own ability to protect themselves and control the outcome of risks they exposed themselves to. This naive overconfidence echoes many of the core aspects of optimism bias in risk perception. Earlier research emphasizes the significance of perceived controllability, prior experience, psychological distance and familiarity in optimism bias (Chapin, 2000; Cho et al., 2010). The way in which participants described potential risks suggested a relatively large psychological distance. Participants who expressed a belief that their personal information and accounts were of no value to a hacker effectively distanced themselves as potential targets, contributing to their optimism. This optimism was likely further strengthened by a general lack of experiences involving meaningful, lasting consequences, reinforcing their perceptions of potential cyberattacks as essentially harmless.

Another factor that may affect the risk perception of our sample group as well as their cohorts is the fact that their generation largely grew up surrounded by technology. The exposure to the internet from an early age is likely to have imbued them with a strong sense of familiarity. This in turn, as evidenced by previous research, can have a strengthening effect on optimism bias and particularly the illusion of control (Chapin, 2000; Cho et al., 2010). In the same way that an individual raised in a "dangerous" area may nonetheless feel safe on familiar streets, a generation raised with the internet may be less likely to perceive it as dangerous, and more likely to overestimate their control of risks and threats.

Our participants indicated that they were aware of the risks taken when connecting to public wi-fi networks or re-using passwords. However, as evidenced by the quotes in *4.1.2 Naivety*, many of our participants believed their information had no value, and considered it unworthy of a hacker's efforts. They judged the risk to themselves in terms of what use a hacker could have for their accounts or their information, and as most participants considered themselves and their information to be insignificant, they by extension also considered themselves to be at low risk for cybercrime.

While the naivety exhibited by the participants suggests a lack of concern for their own online security, other responses nonetheless indicate an awareness of different threats, if to somewhat varying degrees. After all, most participants had some sort of personal experience with or knowledge of cyberattacks. While this naivety may stem from a lack of knowledge concerning the potentially serious consequences of cybercrime, it is also possible that the tendency towards unrealistic optimism is in itself a coping mechanism.

Optimism Bias as a Coping Mechanism

Equating the value of one's information with one's own level of risk is an overly optimistic perspective that does not accurately reflect the wide variety of methods and goals in cybercrime that do not directly target personal data or access to accounts. This false equivalence may therefore stem from the need to find methods of coping with the anxiety elicited by security demands. In order to justify the choice to ignore security recommendations, people may convince themselves that certain security recommendations are not important, thereby alleviating their guilt. This rings especially true in a society where people do not have much choice in whether to use internet services, creating a need for alternate ways of coping. Research conducted by Tversky and Kahneman (1973) found that people suffering from fatigue more readily relied on cognitive biases and heuristics or mental shortcuts when making decisions. Hence while optimism bias is not necessarily caused by security fatigue, it is entirely possible that the emotional fatigue brought about by overwhelming security demands pushes people to rely more heavily on cognitive biases, potentially strengthening optimism bias.

This way of justifying cyber threats and risky behaviours may be an attempt to minimize the anxiety that would otherwise be pervasive in everyday life. Anxiety is in itself emotionally exhausting and ultimately unsustainable, and people may instead attempt to minimize the risks and justify their inaction, believing that their information is too insignificant to be targeted, or that any potential incidents would be relatively harmless. The alternative — going through life constantly plagued by security-induced anxiety — is not an alternative most are willing or able to cope with. As aptly stated by participant 4, “you can’t live like that”.

The Contradiction of Illusion of Control and Resignation

The illusion of control exhibited by participants seems to directly contradict the sense of helplessness, futility and resignation expressed when considering security threats and an individual’s ability to guard against them. While individuals may certainly be affected by perceived controllability and resignation to risk to varying degrees, our interviews clearly showed that both attitudes can exist within the same person.

The pervasiveness of cybersecurity threats in the digital age can lead to a normalization and possibly even an expectation of risk. Individuals may resign themselves to the idea that some level of risk is unavoidable in the online environment, while selectively focusing their efforts on specific aspects of their online activity they feel they can control in order to recoup some of their lost agency. It is difficult to say whether this illusion of control stems from a coping mechanism boosting confidence and optimism, or whether it is the result of a cost-benefit analysis that determines which aspects of risk are most beneficial and prudent to guard against. More likely, an explanation model may need to consider the interaction effects of both.

It is possible that an individual may choose to focus on familiar or noticeable aspects of security where they believe they have a higher level of control and influence, rather than putting effort into security measures that may be beyond their understanding or might not produce any tangible benefit. A lack of comprehensive knowledge of cybersecurity threats and the measures needed to protect oneself can also contribute to both overestimating one's control in certain areas and feeling resigned to risks in others.

The contradiction between these cognitive and affective factors suggests the existence of strongly influential underlying mechanisms which are yet to be explored on a deeper level, but that may be incredibly valuable for cybersecurity research and the development of security policies. This paradox emphasizes the importance of a multi-dimensional understanding of the human factors influencing compliance with security recommendations.

Saving Effort with Cost-Benefit Analyses

The theory behind security fatigue suggests that people simply do not have the mental or emotional capacity to care about every aspect of their online security, leading them to develop effort-saving strategies that help them manage the huge amount of demands placed on them (Stobert & Biddle, 2014; Wash et al., 2016). Strategies commonly involve prioritizing the distribution of their energy according to what is important and what is convenient.

These strategies are evident in the responses given by our participants, with password re-use being the most prevalent. While the majority of our participants re-used passwords, citing convenience as the primary motivation, some reported using different passwords for their most important accounts. This prioritization of accounts is in line with the results found by Stobert and Biddle (2014), which suggested that the primary concern for users is "rationing effort to best protect important accounts". Several of our participants also reported writing down their passwords, despite being aware of the supposed risk of doing so. To them, it was a necessary measure in order to remember their passwords, and they questioned how risky is actually was to keep a password written down by their desk at home, or to save it as a note on their phone with no other contextual information such as usernames or websites. To them, the perceived risk of writing down passwords was not significant enough to justify the effort needed to memorize them.

These effort-saving strategies can easily be compared to the cost-benefit perspective described by Herley (2009). Herley suggests that people choose which recommendations to follow based on an analysis of the costs versus the perceived benefits of expending effort — for example, while writing down passwords is often emphasized as an unsafe practice, Herley argues that many people see no real consequence of storing passwords at home, where it is unlikely that anyone would be able to access them.

A recurring sentiment in our participants was a feeling of laziness with regards to security recommendations and adopting new security measures. Participants often opted for the more convenient option when faced with security measures that were seen as tedious or annoying. Overly limiting security measures were seen as an inconvenience rather than as a beneficial function, which prompted users to circumvent them rather than heed their warnings. Although participants were aware of the potential riskiness of their behaviours, they readily abandoned efforts to follow recommendations when it stopped being convenient to do so.

Perception of Risk Now and Before

As a final question to conclude our interviews, we asked our participantsts whether they considered the internet to be riskier today when compared to before. Responses were mixed; most considered the current landscape to be riskier in some aspects, but safer in others. The main issues revolved around the fact that a great deal more sensitive personal information exists online and is in many cases a requirement in order to utilize digital services, such as banking, authentication, and medical journals. Participants generally regarded the internet during the 90s as a more "lawless" place, where opportunistic hackers could roam with little resistance. However, participants also noted that it was much less common for sensitive personal information to be available online. Nowadays, the general level of awareness and knowledge surrounding the internet and online hygiene is greater — so too, however, are the stakes. Most participants therefore agreed that existing on the internet today was more risky.

It is worth reiterating that the participants interviewed in this study were all between the ages of 20 and 27 — they would have been far too young during the 90s or early 2000s to fully experience the dangers of the early internet which was lacking in many internet security protocols that are ubiquitous today, such as TLS (Transport Layer Security) which encrypts data sent to and from web browsers, certificate authentication to indicate legitimate websites, and firewalls to prevent various attacks. Their perception of the internet as riskier today, however, still speaks to the anxiety and stress they experience that may be caused by the demands of cybersecurity. It is essentially impossible to exist in society without a significant digital footprint, especially as more services become digitized and the average number of accounts the average person has grows larger and larger. Keeping track of each of these accounts and the information they have access to and share is simply unfeasible. Individuals born into this system may feel trapped by it and unable to influence these circumstances, which may contribute to a sense of resignation and defeatism.

5 Conclusions

5.1 Discussion

The goal of this study was to explore non-compliance with security recommendations and the underlying psychological aspects and phenomena from affective, cognitive, and behavioural perspectives. With these results we hoped to illuminate connections, interactions and contradictions between existing psychological theories and provide a multi-dimensional overview of these underlying aspects. Therefore, our aim was not only to produce results that validate these established theories, but to gain a perspective that considers the ways in which these underlying psychological factors interact with and modulate the effects of each other in order to provide a more nuanced and comprehensive understanding of why people choose not to comply with security recommendations.

Throughout the process of literature review, data collection and analysis, it became clear that the aspects introduced as underlying factors for non-compliance based on previous research — security fatigue, optimism bias, and cost-benefit analysis — did not necessarily exist as distinctly separate phenomena. Our results indicate a significant amount of overlap and interaction between the three, with aspects of one perspective potentially modulating and influencing the effects of another. Individuals may, for example, turn to optimism bias as a coping mechanism in an effort to justify their behaviours and minimize the anxiety associated with knowingly disregarding security recommendations. Cost-benefit analyses may contribute to the adoption of effort-saving strategies that focus energy on the aspects of online security that are perceived as the most important, while security fatigue may instead push users towards what is most convenient.

The discussion surrounding the issue of non-compliance concerning security recommendations tends to focus on the technical aspects of security measures, and attempts to mitigate the problem often lead to even more recommendations being put in place. If these results say anything, it's that the psychological perspective is sorely lacking in this discussion — indeed, a vital part of any system or policy is the user herself, and any purported solution to the issue of non-compliance is incomplete if psychological determinants of behaviour aren't taken into consideration.

The paradoxical juxtaposition of an optimistic illusion of control and the sense of helplessness characterized by resignation and defeatism paints a worrying picture of how the current generation of young adults perceives risk and their own ability to make effective decisions regarding their own security. If these results are indicative of an emerging trend in cybersecurity, policy makers may soon have to contend with a growing population of people that overestimate their own ability to influence and control threats to their security, while simultaneously resign themselves to the inevitability of risk, foregoing security recommendations for the sake of convenience and instant gratification.

An individual suffering from security fatigue does not necessarily have the capacity to care about every aspect of their online security. They must therefore choose what to prioritize, analyzing the costs and benefits of their behaviour to form effort-saving strategies to help them cope. In this sense, cybersecurity becomes not a question of what matters, but a question of what matters most. As more and more critical societal services and infrastructure are affected by digitalization, this question becomes impossible to sufficiently answer. If these underlying psychological factors aren't taken into account when developing new security policies, it may give rise to a population that is too overwhelmed by the demands of cybersecurity to take any kind of decisive action at all.

5.2 Reflections and Future Research

The variety of risks that has been discussed in this study is quite extensive. This was in order to allow for a broader range of responses in the interviews, as to gain more insight into the phenomena from several angles. However, future studies in the subject could potentially benefit from narrowing the focus down to only one or two threats, in order to examine how to best mitigate them in a more practical sense.

Another suggestion for future studies would be to introduce advanced knowledge of IT and cybersecurity as an individual factor. Previous studies have found results that suggest level of knowledge to be a significant factor in security fatigue and optimism bias, and while our study aimed to gain an understanding of the average user with no IT-related background, participants with more substantial knowledge in IT and cybersecurity may provide unique insight into how the psychological factors discussed in this study are affected by this factor.

We believe that our chosen approach for this study is relevant and appropriate in allowing us to effectively investigate risk perception, compliance with security recommendations and the psychological phenomena that guide security decisions. As with any research study, however, there are limitations of this paper that are worth being critically examined. While attempts were made to include a representative sample of the student population at Uppsala University in terms of age and field of study, the limited number of participants naturally restricts the variance of these factors. Follow-up studies may benefit from gathering responses from a larger number of students from different departments in order to further validate the transferability of our results. Additionally, studies with participants from different age groups are likely to offer perspectives that may not have come to light in this study.

6 Bibliography

Ablon, L., Heaton, P., Lavery, D. C., & Romanosky, S. (2016). *Consumer attitudes toward data breach notifications and loss of personal information*. Rand Corporation.

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security*, *28*(6), 476-490.

Barth, S., de Jong, M. D., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and informatics*, *41*, 55-69.

Beautement, A., Sasse, M. A., & Wonham, M. (2008, September). The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 new security paradigms workshop* (pp. 47-58).

Blaxter, L., Hughes, C., Tight, M. (2006). How to research. Open University Press. ISBN: 978 0 335 21746 5 (pbk).

Bryman, A. (2018). Kvalitativ metod. *Samhällsvetenskapliga metoder*, *3*, 453-509.

Cavanagh, S. (1997). Content analysis: concepts, methods and applications. *Nurse researcher*, *4*(3), 5-16.

Chapin, J. R. (2000). Third-person perception and optimistic bias among urban minority at-risk youth. *Communication research*, *27*(1), 51-81.

Cho, H., Lee, J. S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, *26*(5), 987-995.

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42-51.

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & security*, *30*(8), 719-731.

Chou, H. C., Lee, H. C., Yu, H. J., Lai, F. P., Huang, K. H., & Hsueh, C. W. (2013). Password cracking based on learned patterns from disclosed passwords. *IJICIC*, *9*(2), 821-839.

Conway, G., & Hadlington, L. (2021). How do undergraduate students construct their view of cybercrime? Exploring definitions of cybercrime, perceptions of online risk and victimization. *Policing: A Journal of Policy and Practice*, *15*(1), 119-129.

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2021). When enough is enough: Investigating the antecedents and consequences of information security fatigue. *Information Systems Journal*, *31*(4), 521-549.

Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014, February). The tangled web of password reuse. In *NDSS* (Vol. 14, No. 2014, pp. 23-26).

Deora, R. S., & Chudasama, D. (2021). Brief study of cybercrime on an internet. *Journal of communication engineering & Systems*, *11*(1), 1-6.

Erlingsson, C., & Brysiewicz, P. (2017). A hands-on guide to doing content analysis. *African journal of emergency medicine*, *7*(3), 93-99.

EU General Data Protection Regulation (GDPR 2016/679, OJ 2016 L 119/1). European Parliament. https://gdpr-info.eu/

Fagan, M., Albayram, Y., Khan, M. M. H., & Buck, R. (2017). An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences*, *7*(1), 1-20.

The Global Risks Report 2023 (18th Edition). World Economic Forum. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

Golla, M., Wei, M., Hainline, J., Filipe, L., Dürmuth, M., Redmiles, E., & Ur, B. (2018, October). "What was that site doing with my Facebook password?" Designing Password-Reuse Notifications. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1549-1566).

Hardy, G. E., Shapiro, D. A., & Borrill, C. S. (1997). Fatigue in the workforce of National Health Service Trusts: levels of symptomatology and links with minor psychiatric disorder, demographic, occupational and work role factors. *Journal of psychosomatic research*, *43*(1), 83-92.

Herley, C. (2009, September). So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop* (pp. 133-144).

Hewitt, B., & White, G. L. (2022). Optimistic bias and exposure affect security incidents on home computer. *Journal of Computer Information Systems*, *62*(1), 50-60.

Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative health research*, *15*(9), 1277-1288.

Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*, *7*(3).

International Telecommunications Union. (n.d.) *Statistics.* Retreived January 3, 2023, from https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

James, N. 2023, August, 4th. 90+ Cyber Crime Statistics 2023: Cost, Industries & Trends. *Getastra*. https://www.getastra.com/blog/security-audit/cyber-crime-statistics/#2_Cyber_Crime_Statistics_By_Year.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of computer and system sciences*, *80*(5), 973-993.

Kallio, H., Pietilä, A.-M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. Journal of Advanced Nursing, 72(12), 2954–2965. https://doi.org/10.1111/jan.13031

Khiralla, F. A. M. (2020). Statistics of cybercrime from 2016 to the first half of 2020. *Int. J. Comput. Sci. Netw.*, *9*(5), 252-261.

Lee, K., Sjöberg, S., & Narayanan, A. (2022). Password policies of most top websites fail to follow best practices. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)* (pp. 561-580).

Marino, B. (2021). Privacy concerns and the prevalence of third-party tracking cookies on ARL library homepages. Reference Services Review, 49(2), 115–131. https://doi.org/10.1108/RSR-03-2021-0009

Mayring, P. (2004). Qualitative content analysis. *A companion to qualitative research*, *1*(2), 159-176.

Oates, J. (2006). Researching information systems and computing. London: SAGE Publications

Onaolapo, J., Mariconti, E., & Stringhini, G. (2016, November). What happens after you are pwnd: Understanding the use of leaked webmail credentials in the wild. In *Proceedings of the 2016 Internet Measurement Conference* (pp. 65-79).

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2015). Factors that influence information security behavior: An Australian web-based study. In Human Aspects of Information Security, Privacy, and Trust: Third International Conference, HAS 2015, Held as Part of HCI International 2015, Los Angeles, CA, USA, August 2-7, 2015. Proceedings 3 (pp. 231-241). Springer International Publishing.

Ponemon Institute. (2014). *The Aftermath of a Data Breach: Consumer Sentiment.* Ponemon Institute LLC. https://www.ponemon.org/news-updates/blog/security/the-aftermath-of-a-data-breach-consumer-sentiment.html

Sausalito, C., 2023, May, 24th. 2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics. *Cybersecurity Ventures*. https://cybersecurityventures.com/cybersecurity-almanac-2023/.

Shrivastava, P., Jamal, M. S., & Kataoka, K. (2020). EvilScout: Detection and Mitigation of Evil Twin Attack in SDN Enabled WiFi. IEEE eTransactions on Network and Service Management, 17(1), 89–102. https://doi.org/10.1109/TNSM.2020.2972774

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS quarterly*, 503-522.

Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security fatigue. *It Professional*, *18*(5), 26-32.

Stephanou, T., & Dagada, R. (2008, July). The Impact of Information Security Awareness Training on Information Security Behaviour: The Case for Further Research. In *ISSA* (pp. 1-21).

Stobert, E., & Biddle, R. (2014). The password life cycle: user behaviour in managing passwords. In *10th symposium on usable privacy and security (SOUPS 2014)* (pp. 243-255).

Tian, X., Chen, L., & Zhang, X. (2022). The role of privacy fatigue in privacy paradox: a psm and heterogeneity analysis. *Applied Sciences*, *12*(19), 9702.

Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., Markov, Y., Comanescu, O., Eranti, V., Moscicki, A., Margolis, D., Paxson, V., & Bursztein, E. (2017, October). Data breaches, phishing, or malware? Understanding the risks of stolen credentials. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security* (pp. 1421-1434).

Treharne, G. J., & Riggs, D. W. (2015). Ensuring quality in qualitative research. *Qualitative research in clinical and health psychology*, *2014*, 57-73.

Tversky, A., & Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability. *Cognitive psychology*, *5*(2), 207-232.

Ur, B., Noma, F., Bees, J., Segreti, S. M., Shay, R., Bauer, L., Christin, N., & Cranor, L. F. (2015). " I Added'!'at the End to Make It Secure": Observing Password Creation in the Lab. In *Eleventh symposium on usable privacy and security (SOUPS 2015)* (pp. 123-140).

Vojinovic, I. 2023, July, 14th. More Than 70 Cybercrime Statistics – A $6 Trillion Problem. *DataProt*. https://dataprot.net/statistics/cybercrime-statistics/.

Wash, R., Rader, E., Berman, R., & Wellmer, Z. (2016). Understanding password choices: How frequently entered passwords are re-used across websites. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)* (pp. 175-188).

Weinstein, N. D. (1980). Unrealistic optimism about future life events. *Journal of personality and social psychology*, *39*(5), 806.

Weinstein, N. D. (1989). Optimistic biases about personal risks. *Science*, *246*(4935), 1232-1233.

Weiss, R. S. (1995). *Learning from strangers: The art and method of qualitative interview studies*. Simon and Schuster.

Zou, Y., Danino, S., Sun, K., & Schaub, F. (2019, May). You ‘Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-14).

Zou, Y., Mhaidli, A. H., McCall, A., & Schaub, F. (2018). " I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)* (pp. 197-216).

7 Appendix

Appendix A: Interview Guide

Password Management

1) Do you use a password manager? Why or why not?
    - If you do, does it make you feel safer?
2) Do you re-use passwords across multiple accounts?
3) Can you think of any recommendations for strong passwords?
    - *Examples: upper and lower case letters, numbers, special characters, minimum length, not using personally meaningful words or phrases*
    - Do you tend to follow these recommendations?
    - Do you think following recommendations is worth it?
    - Do you find it difficult to create passwords that fulfill these criteria?
    - Do you think these criteria make your passwords stronger?
    - Do you think strong passwords make your accounts safer?
4) Do you ever write down your passwords?
5) Do you update your passwords regularly?
6) Do you think it's important to not write down passwords or update passwords?

Data Breaches

1) Do you know what a data breach involves?
2) Have any of your accounts ever been involved in a data breach?
    - *YES:*
        - Can you describe what happened?
        - Did you do anything in response to the data breach?
        - Did it make you more worried about potential data breaches?
        - Have you changed your behaviours online as a result?
    - *NO:*
        - Do you worry about potential data breaches?
        - Do you consider yourself to be at risk of a data breach?
        - Have you taken any steps to protect yourself from data breaches?
3) If a data breach occurred tomorrow, how would you react?
4) Are you concerned about identity theft?

Risky Behaviour and Security Guidelines

1) How would you characterize risky online behaviour? Can you give some examples?
    - *Examples: visiting suspicious websites, downloading unknown files, opening link in emails, connecting to public wi-fi networks, accepting third-party cookies*
    - Do you ever do any of these things?
2) Can you think of any guidelines or recommendations for cybersecurity?
    - Do you try to follow these recommendations?
    - Do you find security recommendations to be difficult or tedious to follow?

- Do you think following security recommendations makes you safer online?
- Do you think these security recommendations are always necessary?

3) How likely do you think you are to be exposed to negative consequences due to these behaviours?
4) Do you think these risks are exaggerated? Why?
5) Do you think it's more risky online now compared to before?