Emilia Kariuki

UNDERTANDING COOKIE CONSENT: HABITS AND PERCEPTIONS ACROSS INFORMATION TECHNOLOGY BACKGROUNDS AND LEVELS OF SECURITY AWARENESS

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

ABSTRACT

Kariuki, Emilia

Understanding cookie consent: habits and perceptions across information technology backgrounds and levels of security awareness
Jyväskylä: University of Jyväskylä, 2024, 68 pp.
Cyber Security, master's Thesis
Supervisor: Woods, Naomi

This thesis investigates the user consent habits and perceptions of website cookies across differing information technology backgrounds and levels of security awareness. The importance for the thesis derives from the increased focus on online security, with the increasing amount of internet usage by all demographics.

Website cookies are commonly defined as small files that websites use to track user activity and preferences. They can save data such as usernames, passwords and user preferences. Specific cookies are also used to identify specific users, thus making it possible to offer the user personalized advertisements and enhanced user experience.

Due to international laws such as the EU's General Data Protection Regulation (GDPR), websites are required to ask the user for permission for the use of optional cookies. This allows for research to inspect user consent habits as well as perceptions of the interaction.

The research consists of two main sections, literature review and an empirical section. In the literature review section prior research is used to form a basis for the empirical section. The empirical section consists of a quantitative case study which collects information about the user's consent habits and perception to website cookies across differing IT backgrounds and levels of security using an online survey tool.

Findings from this case study show a degree of consistency with the results from the literature review. The study suggests that security awareness significantly correlates with cookie consent habits, a higher level of security awareness correlating with declining cookies more often. Interestingly, the same significant correlation was not found between IT expertise and cookie consent habits. The literature review revealed that IT expertise does not necessarily correlate with higher levels of security actions, making the results logical in that context.

Additionally, the research identified significant differences in perceptions. The trend indicates that security awareness and IT expertise positively correlate with both positive and negative perceptions of website cookies.

Keywords: cookies, security awareness, online privacy

TIIVISTELMÄ

Kariuki, Emilia
Evästeiden suostumuksen ymmärtäminen: tavat ja käsitykset tietotekniikan taustoista ja tietoturvatietoisuuden tasoista riippuen
Jyväskylä: Jyväskylän yliopisto, 2024, 68 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Woods, Naomi

Tässä tutkielmassa selvitetään käyttäjien suostumustottumuksia ja näkemyksiä verkkosivuston evästeisiin liittyen, erilaisilla tietotekniikan taustoilla ja tietoturvatietoisuuden tasoilla. Tutkielman merkitys johtuu lisääntyneestä keskittymisestä verkkoturvallisuuteen, kun kaikki väestöryhmät käyttävät internetiä yhä enemmän.

Verkkosivuston evästeet määritellään yleensä pieniksi tiedostoiksi, joita verkkosivustot käyttävät käyttäjien toiminnan ja mieltymysten seuraamiseen. Ne voivat tallentaa tietoja, kuten käyttäjänimiä, salasanoja ja käyttäjäasetuksia. Erityisiä evästeitä käytetään myös tiettyjen käyttäjien tunnistamiseen, jolloin käyttäjälle voidaan tarjota henkilökohtaisia mainoksia ja parannettu käyttökokemus.

Kansainvälisistä laeista, kuten EU:n yleisestä tietosuoja-asetuksesta (GDPR), johtuen verkkosivustojen on pyydettävä käyttäjältä lupa valinnaisten evästeiden käyttöön. Tämä mahdollistaa tutkimuksen käyttäjien suostumustottumusten ja vuorovaikutusta koskeviin käsityksiin liittyen. Tutkimus koostuu kahdesta pääosasta, kirjallisuuskatsauksesta sekä empiirisestä tutkimuksesta. Kirjallisuuskatsaus osiossa, aiempaa tutkimusta käytetään empiirisen osion pohjana. Empiirinen osio koostuu kvantitatiivisesta tapaustutkimuksesta, jossa kerätään tietoa käyttäjän suostumustottumuksista ja käsityksistä verkkosivustojen evästeisiin liittyen erilaisilla IT-taustoilla ja turvallisuustasoilla verkkokyselytyökalun avulla.

Tämän tapaustutkimuksen tulokset osoittavat jonkinasteista yhdenmukaisuutta kirjallisuuskatsauksen tulosten kanssa. Tutkimus viittaa siihen, että tietoturvatietoisuus korreloi merkittävästi evästeiden suostumustottumusten kanssa, korkeampi turvallisuustietoisuuden taso korreloi evästeiden hylkäämisen kanssa. Mielenkiintoista on, että samaa merkittävää korrelaatiota ei havaittu IT-asiantuntemuksen ja evästeiden suostumustottumusten välillä. Kirjallisuuskatsaus paljasti, että IT-asiantuntemus ei välttämättä korreloi korkeamman tason tietoturvatoimien kanssa, joten tulokset ovat loogisia tässä yhteydessä. Lisäksi tutkimuksessa havaittiin merkittäviä eroja käsityksissä. Trendi osoittaa, että tietoturvatietoisuus ja IT-asiantuntemus korreloivat positiivisesti sekä positiivisten että negatiivisten käsitysten kanssa verkkosivuston evästeistä.

Asiasanat: evästeet, tietoturvatietoisuus, yksityisyys verkossa

FIGURES

TABLES

CONTENTS

1 INTRODUCTION

In the dynamic landscape of digital interactions, the use of website cookies has become an integral aspect of user experiences on the internet. Website cookies, small pieces of data stored on users' devices by websites, serve diverse purposes, ranging from enhancing personalization to targeting ads (Cahn, et al., 2016). As users traverse the online realm, they are routinely presented with cookie consent prompts, inviting them to make decisions that intertwine individual preferences, security awareness, and technological backgrounds. Originally conceived in 1994 to maintain state between servers and clients (Bortz et al., 2011), cookies have evolved to serve various functions, including targeted online advertising. As businesses strive to optimize their online presence, understanding how user backgrounds influence their choices regarding cookies becomes imperative.

1.1 Motivation and research problem

Research on users' opinions and behaviours about cookies on websites has grown over time, which is indicative of the increasing significance of digital privacy and security. Studies have been done on a variety of topics, such as how users respond to cookie disclaimers (Kulyk et al., 2018), how non-technical users feel about cookies (Ur et al., 2012), and general worries about the subject of tracking users online(Leon et al., 2013). But there's a notable knowledge gap about how different groups of people—that is, those with and without IT or computer backgrounds—manoeuvre through cookie consent.

While there have been studies that have explored user consent habits and perceptions of website cookies, the focus has predominantly been on non-IT users (Ur et al., 2012) or users in a general sense (Ha et al., 2006a; Habib et al., 2022; Kulyk et al., 2018). A notable absence exists in research specifically targeting individuals with a background in IT or computer-related fields. By narrowing the scope to include both IT and non-IT users, this research seeks to provide a more comprehensive understanding of the diverse factors influencing user choices in the realm of website cookies.

An existing study by Chanchary and Chiasson (2015) suggests a surprising trend: individuals with a computer background are more likely to consent to website cookies and the use of their information. In their study, they found that individuals with a technical background were significantly more willing to share their personal identification data and financial information, as well as computer related information compared to the group without a technical background. They discussed that their findings could be the result of people with computer-related degrees or work experience being more confident in their abilities to handle the risk of information leaking, thus being more willing to share data (Chanchary & Chiasson, 2015). It has also been found that providing information about website cookies does not necessarily correlate with increased cookie declining (Vásquez Duque, 2024).

By subjecting these claims to empirical investigation, the research aims to either validate or challenge these initial observations, contributing to the refinement of our understanding of user behavior in the digital space. By including both IT and non-IT users in the study, this research aims for a comprehensive understanding of factors influencing user choices in the digital space. It is important to examine security awareness across differing backgrounds and study their comparison, as a computer background does not automatically equate to a high level of security awareness. Additionally, an up to date look on user backgrounds affecting cookie consent decisions and perceptions is needed since previous research is nearly 10 years old at this point.

This study seeks to address this research gap by conducting a comprehensive exploration of user background and the possible relationship to behaviours regarding website cookies. It positions itself at the intersection of human-computer interaction, digital security, and user perceptions, with a particular focus on the influence of individual knowledge levels of information technology and security awareness on cookie consent decisions. As the digital ecosystem evolves, understanding these nuanced interactions becomes increasingly important, not only for academic discourse but also for practical applications that can provide information for web development, privacy policies, and digital security measures.

The motivation behind this thesis stems from the large presence of cookie banners encountered by internet users daily, coupled with a lack of comprehensive research on the specific topic of user backgrounds. As websites increasingly rely on cookies to gather data and personalize user interactions, understanding how individual characteristics, such as demographics, online behaviour, and privacy attitudes, influence users' choices regarding cookies are key. There is a noticeable gap in research regarding how different user backgrounds impact their preferences and behaviours in relation to cookies. This gap presents an opportunity to explore how factors such as technological proficiency influence users' awareness, understanding, and acceptance of cookies.

Beyond filling the gap in the current literature, there exists a genuine interest in comprehending how user backgrounds and security awareness intersect in the context of website cookies. The outcome of this research not only contributes to academic discourse but also holds practical implications for web developers, policymakers, and educators striving to create digital environments that align with user expectations and security best practices. The outcome of this research would be to ultimately encourage a safer, more user-centric digital environment as well as offer a deeper understanding of the factors shaping our online experiences. The research questions of the study are the following:

1. Does the level of IT knowledge influence website cookie consent habits?
2. Does increased security awareness influence website cookie consent habits?

The research questions will be answered by conducting an online survey to people with both IT and non-IT backgrounds, to gain insight about the website cookie consent habits of the two groups. The connection between IT expertise and security awareness will also be researched, as the effects of security awareness to cookie consent habits is one of the research questions. The results will contribute to existing research on user perceptions and behavioural habits when it comes to website cookies.

1.2 Literature review and thesis outline

In the first three chapters of the study, a literature review was conducted to gain insight about website cookies, user perceptions and consent habits towards them, as well as security awareness as a concept. Mainly online publications and literature were utilized, primarily searching from IEEE (Institute of Electrical and Electronics Engineers), the university of Jyväskylä's own online library JYKDOK, and web search engine for academic publications and literature Google Scholar. The research process predominantly utilized keywords such *website cookies, security awareness, online privacy, user perceptions and privacy calculus theory*.

In the fourth chapter of the study, the methods of the research will be presented. This will include the creation and execution of the survey, sample collection, as well as the participants of the survey are described.

The key results of the study will be presented in the fifth chapter. After this, there will be a chapter discussing the research, discussing the key findings in comparison to prior research in the field. The study's limitations will also be discussed. Finally, a summary is provided, where the implications for future research will also be examined.

2 WEBSITE COOKIES

This chapter gives an overview of website cookies – what they are, the history behind cookies, the legal and regulatory frameworks, studies of user perceptions on cookies as well as the privacy concerns around website cookies from the user's perspective. Since cookies can often consist of multiple networks, they can be a complex topic. However, for the sake of this research, the first section attempts to provide a general description of cookies. This thesis uses terms "web cookie(s)" and "cookie(s)" interchangeably. Other types of cookies like zombie, flash, and edible cookies are not in the scope of the term "cookie" in this study.

2.1 What are website cookies

Cookies are small files that websites use to track user activity and preferences (Greenberg & Long, 2003). This description is supported widely by various other research, Kristol (2001) writes that cookies are small pieces of information used to implement shopping applications, store login information, and track user journeys. Sit outlines that cookies can be used for various positive purposes, such as maintaining a shopping cart, but activities like tracking user behaviour for targeted advertising are more intrusive (Sit, 2001). So, cookies can be used for enabling functionalities and potentially improving user experience; however, they can also negative implications for the user and thus be a potential threat to user privacy (Kulyk et al., 2018). The most prominent benefits of cookies to the providers are things such as retargeting, personalization and analytics helping to optimize business strategies.

A range of cookies exist, each serving different purposes. Session cookies, stored temporarily on the server's hard drive, and persistent cookies, which remain on the client's computer, are two common types (Argerich, 2003). These are often used in web-based applications, with over two-thirds of sites deploying them (Tappenden, 2009). Session cookies can be used to for example hold items in an online stores shopping cart while the user is using the browser, whereas persistent cookies stay on the user's computer until deleted and can be stored by website providers or third parties (Kulyk et al., 2018). Third-party cookies, particularly persistent ones, are used for tracking and profiling user behaviour, with potential privacy risks (Ruohonen, 2017; González, 2018). Third-party cookies in particular, are prevalent and can aggregate information across multiple websites, raising privacy concerns (Cahn, 2016). Despite these concerns, cookies remain a popular and flexible tool for website authentication and personalization.

2.2 History

The history of cookies is rather short, them being around since the mid-90s, however there are still a few opinions as to when cookies became commonly used and known by the users. Kulyk et al. (2018) outline that cookies have been commonly used on websites ever since the year 1994, originally intended to provide a better user experience and additional functionality. Kristol (2001) however writer thinks that the cookie history truly dates to April 1995, when the technical community were only speculating the possibilities of e-commerce and most people had internet access only at home.

The original inventor of cookie, web programmer Lou Montulli (JENTIS, 2023), has shared that he intended cookies to improve customer experience while maintaining the user's privacy. Montulli outlines that tracking was never the intent of web cookies, quite the opposite as avoiding them being used for tracking purposes what the goal when starting out with the development. He first heard of cookies being used for tracking purposes in 1996 and was quite surprised since they had supposedly been designed to not being able to be used in user tracking (JENTIS, 2023). After their originally intended enhancing purposes, they have since been exploited for more commercial use like advertising and user tracking (Rasaii et al., 2023).

2.3 Legal and regulatory frameworks

This chapter focuses especially on the legal and regulatory frameworks on cookies in Europe since the study is conducted in Europe and on people living in Finland. In the European Union (EU), the use of website cookies is regulated by two primary legal frameworks: the General Data Protection Regulation (GDPR) and the ePrivacy Directive, also known as the Cookie Law or the Cookie Directive. In this chapter we will focus on these two frameworks.

2.3.1 GDPR

The GDPR as well as the Cookie Law aim to protect the privacy and personal data of individuals accessing websites within the EU. Under the GDPR, which became enforceable on May 25, 2018 (European Data Protection Supervisor, 2018), cookies that store personal data fall under its scope. The GDPR sets requirements for providers on collecting, storing and managing personal data of users in the EU (Your Europe, n.d.).

According to the European Parliament regulation 2016/679 (EUR-Lex, 2016), websites must obtain explicit consent from users before placing cookies that track or collect personal information. This consent must be freely given, specific, informed, and unambiguous. Consent mechanisms must involve clear affirmative actions from users, such as clicking an "Accept" button or adjusting cookie settings. Pre-checked boxes or implied consent are not considered valid forms of consent. The parliament also outlines that some cookies may be exempt from consent requirements if they are strictly necessary for the functioning of the website or if they meet certain criteria, such as anonymizing user data. However, for cookies that require consent, websites must provide users with options to manage their cookie preferences, including the ability to withdraw consent and delete cookies. This ensures that users have control over their personal data and can make informed decisions about cookie usage (EUR-Lex, 2016).

Since the regulation requires that users be informed in a clear, accessible manner about how their data will be used, which has not only increased transparency but has also led to a more cautious approach among users when granting consent. Nouwens et al. (2020) found that following the implementation of GDPR, user engagement with cookie consent interfaces increased, leading to a more informed user base. Users reported being more conscious of their data privacy, prompting them to scrutinize cookie policies more closely (Nouwens et al., 2020a). On the other hand, with the amount of websites people visit on the daily basis, and websites with poorly designed usability could cause privacy fatigue, and a “ok, whatever” type attitude in users (Habib et al., 2022).

2.3.2 ePrivacy Directive

The ePrivacy Directive 2009/136/EC complements the GDPR by specifically addressing the use of cookies and similar tracking technologies for tracking and storing information on users' devices. Enacted in 2009, the ePrivacy Directive aims to protect the privacy of individuals using electronic communications services, including websites and mobile apps. The first version of this directive was introduced in 2002 and has since been updated. It supplements and works alongside the General Data Protection Regulation (GDPR), which provides broader protections for personal data. Since 2013 the directive became mandatory and was in use in all European Union member states (Trevisan et al., 2019). The directive also includes non-European web providers with European users.

One of the key provisions of the ePrivacy Directive is the requirement for websites to inform users about the use of cookies and obtain their consent before placing non-essential cookies on their devices. That means that cookies that are essential for tasks such as authentication or maintaining user preferences are typically exempt from this requirement. The directive by the European Parliament (EUR-Lex, 2009) mandates that users must be provided with clear and comprehensive information about the purposes of the cookies and any third parties involved in their use. The directive outlines that this information must be easily accessible and presented in a manner that enables users to make informed choices about whether to accept or reject cookies. Furthermore, the ePrivacy Directive stipulates that user consent for cookie usage must be obtained through affirmative action, such as clicking an "Accept" button or adjusting cookie settings. Pre-checked boxes or passive consent (e.g., continuing to browse the site) are generally not considered valid forms of consent under the directive (EUR-Lex, 2009).

2.3.3 Noncompliance

Despite these regulations, a significant number of websites do not comply with the directive, as 49% of websites in their research did not respective the directive rules and were using cookies before consent from the user (Trevisan, 2019). Nouwens et al. on the other hand found that in Britain, a few years ago only 11,8% of websites met the European requirements (Nouwens et al., 2020b). Non-compliance with these regulations can result in fines imposed by data protection authorities in EU member states. Therefore, it's crucial for website operators to understand and comply with these laws to ensure that their use of cookies respects users' privacy rights and legal requirements in the EU.

2.4 Privacy concerns

Website cookies raise significant privacy concerns, particularly in relation to user profiling and data tracking (Aladeokin et al., 2017). While possibly improving user experience and providing additional functionality, a real threat to user privacy can be especially cookies used by third parties for data analysis (Kulyk et al., 2018). These concerns are further intensified by the prevalence of registration and cookies on the web, which are seen as potential invasions of privacy. Cookies can collect a wide range of information, including user agent, operating system, screen colours, and more. They are also used to track web and app activities, store unique identifiers, and record browsing history. Cahn (2016) further highlights the prevalence of third-party cookies and their potential to aggregate user information across websites. However, the use of cookies raises privacy concerns, as noted by Hormozi (2005), and is subject to legal regulations in the US and EU. The use of tracking technologies, including cookies, is also a source of privacy concerns, with the potential for intrusion upon privacy rights (Sipior et al., 2011).

According to research by Wheeler et al. (2022), users often express distrust toward websites with vague cookie policies, which has led to a general reluctance to consent to cookies. The study emphasized that this distrust could harm website engagement metrics, as users may abandon sites that fail to reassure them about their data security (Wheeler et al., 2022).

As discussed previously in this study, there can be several benefits and value in collected personal data for the website owners. There is also an evil side to interface design, made to steer people's behaviour in a certain direction. As discussed previously in this study, there can be several benefits and value in collected personal data for the website owners. It has been found that when coming across dark patterns in design, or a privacy unfriendly option, most agree to all consent requests (Graßl et al., 2021). There is research that support this claim, Bermejo Fernandez et al. (2021) found that nudging interfaces can greatly affect users cookie consent choices. It was also found that anything the user does not see at first glance when it comes to cookie banners, goes mostly unnoticed (Nouwens et al., 2020a). In the light of this research, it is clear that the design choices of website providers can greatly affect user's cookie consent choices. For example in the UK, it was found that over half of their top 10,000 websites do not provide a 'reject all' button, affecting user consent choices significantly (Nouwens et al., 2020a).

2.5 User perceptions and habits

Over the years, scholarly inquiry into user attitudes and behaviours concerning the online world has flourished, including online tracking, reflecting the growing importance of digital privacy and security. There are various studies of user perception and understanding about cookies from different perspectives. User perceptions have been inspected from the viewpoint of cookie disclaimers (Kulyk et al., 2018), awareness, user experience and brand trust (Jayakumar, 2021) as well as non-technical users (Ur et al., 2012). However, a notable gap exists in the understanding of how individuals with distinct backgrounds, specifically those with a computer-related or IT background versus those without, navigate the complex landscape of cookie consent.

Before the implementation of the current GDPR regulations of making cookie consent mandatory, in a study conducted in 2001 fewer than 1% of users rejected cookies in over a billion page views (WebSideStory, 2001). Since, by the regulations concerning website cookies, they have become more visible to the everyday user, and declining the use of cookies has become much easier since the mandatory implementation of GDPR. User perception of these risks is influenced by their knowledge and awareness of cookies, with many users expressing a need for more information about their uses and implications (Wheeler et al., 2022). Kulyk et al. (2018) supports this claim with their findings about users having the most concerns of the lack of transparency on how the collected data is used by the service provider. An American study found that users commonly have misconceptions about cookies and the effects of their consent choices (McDonald & Cranor, 2010). Other research supports this claim, as Ha et al. (2006) highlight that users may have misconceptions about cookie use, highlighting the need for increased awareness. It has been researched that the text of the cookie disclaimer does not have a significant influence on the user decision to either deny or consent, but rather their trust on the website itself (Kulyk et al., 2018). An opposing view has also been presented, as Ma & Birrell (2022) found that especially negative framing in wording is significantly effective at nudging user decisions.

Research by Jayakumar (2021) adds significant insight into the discussion on website cookie perceptions and behaviours. The study highlights the influence of various factors such as user awareness, intent, and trust on cookie acceptance and perception. Notably, the research emphasizes that while users may understand the risks associated with cookies, their decisions are often driven by situational factors, such as when quick access to a task completion is essential (Jayakumar, 2021). Users have been also found to be more inclined to accept cookies from websites they trust and visit frequently, however this is secondarily significant compared to the situational factors (Jayakumar, 2021). In addition, research has found that people are more likely to consent to website cookies with dark design like nudging (Borberg et al., 2022). It has also been studied that user perceived usefulness of programmatic advertising, has a negative influence on the concerns about the use of website cookies (Núnez-Barriopedro et al., 2022).

3 SECURITY AWARENESS AND IT EXPERTISE

In this chapter, the concept of expertise, especially in the information technology context is discussed. After this, security awareness online is discussed, looking into its definition and determining factors in modern society. Because of the subject of this research, when discussing security awareness, I will be focusing especially on behaviours by the average user, and not on organizational cultures where the term is also widely used.

3.1 Security awareness

In an era characterized by constant digital connectivity and data interchange, it is essential to emphasize the significance of security awareness. Being aware of and cautious about cyber dangers has become essential as people and businesses navigate an ever-more complicated technology landscape. For everyone who uses the internet, from the average user to the largest corporate organization, knowing and reducing security threats is a basic requirement for maintaining institutional integrity, protecting individual privacy, and maintaining public trust.

3.1.1 What is security awareness

Security awareness refers to the level of understanding, knowledge, and consciousness individuals possess regarding, potential information security risks, and best practices for mitigating them (Tsohou et al., 2010). It encompasses a range of cognitive, behavioural, and socio-cultural factors that influence individuals' ability to recognize, respond to, and prevent security incidents in the digital realm (Schipper, 2014). However, Hänsch & Benenson (2014) aimed to find a standardised description for awareness in the context of IT, and could not do so based on existing research. This means that the topic is not as simple to define or examine. However, at its core, security awareness empowers individuals to make informed decisions and adopt proactive measures to protect their digital assets and personal information from unauthorized access, exploitation, or compromise.

Security awareness is crucial for individuals, not just organizations, as it can help protect against cybercrime and ensure the confidentiality, integrity, and availability of information (Dahbur et al., 2017).

In today's hyper-connected and digitally driven world, the proliferation of cyber threats poses significant challenges to individuals, organizations, and society at large. From sophisticated cyber-attacks targeting critical infrastructure to pervasive data breaches compromising personal privacy, the stakes of cybersecurity get higher every year. Against this backdrop, security awareness emerges as a cornerstone of cyber resilience, offering a frontline defence against a multitude of cyber risks, ranging from phishing scams and malware infections to social engineering exploits (Flinn, 2004; Mallela & Jonnalagadda, 2018). Whether accessing online banking services, shopping on e-commerce platforms, or communicating via social media networks, individuals are constantly exposed to a variety of cyber threats that can undermine their digital security and privacy (Furnell, 2005). Despite the part internet plays in our everyday lives, many users still lack needed knowledge of possible internet threats as well as the needed knowledge to protects their devices (Zwilling et al., 2022).

3.1.2 Determinants of security awareness

In this chapter we examine the determining individual-, technological as well as socio-cultural factors of security awareness for individual users.

Educational attainment has been associated with greater knowledge and understanding of cybersecurity concepts and best practices. In addition, an individuals' knowledge and perceptions of cyber risks profoundly impact their security awareness and behavior (Zwilling et al., 2022). Those who possess a deeper understanding of common cyber threats, such as phishing scams, malware infections, and identity theft, are more likely to adopt proactive measures to protect themselves online (Kimpe et al., 2021). This is supported by various research, such as Fertig & Schutz outline that an important part of security awareness is users wanting to utilize their theoretical knowledge of information security into practise in real life (Fertig & Schütz, 2020). In addition Furnell in an early 2000's study found that just the lack of technical knowledge in general can make users more vulnerable to a variety of online scams and threats (Furnell, 2005). Moreover, individuals' risk perceptions, including their perceptions of vulnerability and severity of potential threats, influence their willingness to engage in security-enhancing behaviours (Furnell, Tsaganidi & Phippen,2008). Effective cybersecurity education and awareness programs can help bridge knowledge gaps and promote accurate risk perceptions among users (Khan et al., 2011), thereby enhancing their overall security awareness.

The design and usability of digital interfaces play a crucial role in shaping users' security awareness and behaviour. Intuitive user interfaces that prioritize simplicity, clarity, and accessibility can facilitate users' engagement with security features and encourage adherence to security best practices. Adams (2005) argues that users' cyber security behaviour online is often a result of poor security mechanisms and lack of knowledge, and advocate for a user-centred design approach.

An issue with the topic is also that the people designing the tools and websites are often quite tech savvy, so for them it can be hard to imagine themselves in the shoes of the average end-user (Furnell, 2005). Complex or confusing interfaces may impede users' understanding of security measures and deter them from taking proactive steps to protect their digital assets. Human-centered design principles can help optimize user interfaces to promote security awareness and empower users to make informed decisions about their digital security.

The availability and accessibility of security tools and resources can significantly influence individuals' levels of security awareness and preparedness. Access to user-friendly security software, such as antivirus programs, firewalls, and password managers, can empower individuals to protect themselves against common cyber threats. However, studies have shown that these mitigation tools are many times beneficial to the user, they do not totally mitigate security breaches (Furnell et al., 2006; Parsons et al., 2014) as the user themselves are still the biggest threat to their own cyber security (Bandi, 2016; Mittal, 2016). Similarly, access to educational resources, online tutorials, and cybersecurity training programs can enhance users' knowledge and skills in identifying and mitigating cyber risks.

Social networks and peer influence exert a powerful influence on individuals' security awareness and behaviours (Dincelli & Goel, 2015). Peer recommendations, social norms, and collective attitudes towards cybersecurity can shape individuals' perceptions of security risks and influence their adoption of security practices (Benjamin, 2017). Positive social reinforcement and peer support can encourage individuals to prioritize security and seek out information about best practices. Conversely, social pressures to conform to risky behaviours or disregard security measures may undermine individuals' security awareness and resilience. Building supportive social networks and fostering a culture of mutual accountability can strengthen individuals' commitment to cybersecurity and promote collective security awareness (Srivastava & Roychoudhury, 2021).

Cultural attitudes towards privacy and security vary widely across different societies and cultural contexts, influencing individuals' perceptions of digital risks and their willingness to adopt security measures (Li et al., 2017). Research indicates that cultural factors significantly influence information security awareness in various contexts. Kruger et al. (2011) found that cultural elements like mother tongue and area of upbringing impact security awareness levels. Similarly, Chen et al. (2008) observed differences in the effectiveness of situational awareness learning between American and Taiwanese users, highlighting the cultural influence on security education. Understanding cultural norms and values is essential for designing effective security awareness campaigns and tailoring messages to resonate with diverse audiences.

3.1.3 Website cookie awareness

Website cookie awareness in this thesis refers to users' understanding and knowledge of cookies and their privacy implications. Studies have shown that most users lack sufficient knowledge about cookies and their uses (Wheeler et al., 2022). This limited awareness can lead to privacy risks, especially with third-party cookies used for targeted advertising (Jayakumar, 2021). From a regulatory perspective insufficient user understanding can undermine the effectiveness of privacy laws and regulations such as the GDPR. While such legislations call for transparency and informed consent from users, the main objectives could be harder to achieve if users fail to engage critically towards cookie consent. The duality of cookies being both beneficial and potentially malicious creates challenges for proper cookie management (Ha et al., 2006). Research suggests that improving user awareness is crucial for addressing privacy concerns associated with cookies (Ha et al., 2006b).

Research indicates that website cookie knowledge among users is generally insufficient for informed consent (Smit et al., 2014; Wheeler et al., 2022). Factors affecting cookie knowledge include age, education level, and privacy concerns (Smit et al., 2014). Despite privacy concerns, especially among older and less-educated groups, most users do not read privacy statements (Smit et al., 2014). Legal knowledge about data collection has been shown to empower consumers, positively impacting their motivation to reject online data collection (Strycharz et al., 2021). Personalizing cookie banners based on users' privacy knowledge can lead to fewer accepted cookies and improved usability (Biselli et al., 2024). Strycharz et al. (2021) suggest that legal knowledge about data collection empowers users to reject cookies, while technical knowledge may lower threat perception. Both technical and legal information are required by GDPR for transparency (Strycharz et al., 2021). However, simply providing information may not be sufficient; reducing privacy concerns, especially among older and less-educated groups, is also important (Smit et al., 2014).

3.2 Expertise – what makes you an IT expert

Experts in various domains, including language learning and web searching, demonstrate distinct strategies and greater success compared to non-experts (Johnson, 2010; White et al., 2009). They employ different vocabularies, utilize resources more effectively, and approach tasks uniquely (White et al., 2009). Expertise generally extends beyond technical proficiency, in the medical field, it has been described as encompassing non-cognitive skills like effective patient communication and recognizing safety limits (Smith et al., 2006). In nephrology nursing, experts exhibit more comprehensive knowledge and broader practice focus compared to non-experts (Bonner, 2006). However, some argue for a postmodern approach where professionals, such as reference librarians, adopt a non-expert stance to enhance collaboration and user satisfaction (Stover, 2004). In web accessibility evaluation, expertise significantly impacts the quality of assessments. Expert evaluators spend less time, show higher confidence and productivity, and provide more effective and reliable judgments compared to non-experts (Yesilada et al., 2009). Expertise can have different qualifications when it comes to the field, however it can be found that experts are individuals with exceptional skill and knowledge in a specific field (Bartold, 2018; K. A. Ericsson et al., 2018).

The development of expertise involves deliberate practice, self-regulated learning, and is influenced by factors such as innate talent and social support (K. A. Ericsson et al., 2018). Research on expertise spans multiple fields, including medicine, finance, law, and computer science, utilizing methods such as observational analysis, log-based studies, and retrospective interviews to understand the characteristics and acquisition of expert knowledge and performance (Gobet, 2006; Smith et al., 2006; White et al., 2009). Becoming an expert requires deliberate practice, which involves pushing beyond one's comfort zone, analysing mistakes, and making corrections (K. A. Ericsson et al., 2018). According to the study called 'The making of an expert' by (A. Ericsson et al., 2007),this learning process can last over a decade and often requires guidance from an expert teacher. It is also outlined that expertise is always learnt, not something you are born with (A. Ericsson et al., 2007). This is also supported by other research in the field, expert performance is not automatic or effortless but involves conscious thought and reflection (Montero, 2016). Experts engage in thoughtful, effortful, and reflective actions, drawing on their deep understanding of their field. To acquire expertise from others, one can employ a systematic approach that includes extensive observation, practice, problem-solving partnerships, and gradually taking on responsibilities (Leonard et al., 2013). By combining deliberate practice, conscious engagement, and structured learning, individuals can develop the expertise in their respective fields.

Information technology expertise refers to the comprehensive knowledge, skills, and experience necessary to effectively navigate, manage, design, implement, and or innovate within the realm of digital systems and technological infrastructures. As a concept, IT expertise encompasses a knowledge of both foundational and specialized knowledge domains, including but not limited to programming, data analysis, network security, system architecture, and user experience design. Beyond technical proficiency, it can also involve an ability to integrate strategic thinking with problem-solving capabilities, to make informed decisions. In the process of becoming an expert in information technology, requirements from other fields can be adopted. For example in the study researching medical expertise, it was defined that expertise involves a balance of theoretical and practical knowledge, developed through reflection on experiences (Smith et al., 2006). In the context of information technology, this would most commonly mean studying the subject or working in the field gaining practical knowledge. Theoretical and practical knowledge in the subject of information technology van also be gained by self-learning methods, however in the context of this study that type of gained expertise would be quite difficult to measure in an online survey format.

Security awareness is another basis for the hypotheses of the study. Security awareness amongst information technology experts has been researched prior though the results have been somewhat conflicting. Bostan (2015) found out that a higher education level is associated with better security practices in using computers, the web, and email. In the research, a survey was conducted among 433 citizens from different layers of the society. Interestingly, the results indicated that education level has significant impact on all security issues included in the analysis regarding computer usage, web usage and e-mail usage. This research clearly provides results that provide us with a viewpoint that an increase in education level correlates with increase in better security awareness. Clarke et al. (2016) on the contrary found out that information technology knowledge does not necessarily equate to better online security practices. Clarke et al., (2016) noted that users often lack the required security knowledge despite being technology dependent. The research conducted a survey which suggests that whilst levels of security awareness are improving, there is still a significant gap between existing and required levels of information security knowledge and practice (Clarke et al., 2016). This can be seen as a contradicting result, that increased information technology knowledge does not equal to better security awareness. The research conducted by Clarke et al. (2016) outlines that the level of security awareness can be seen as an intricate role of information technology especially since users are currently being overwhelmed by the burden being placed upon them to remain secure. The range of technologies they use (60% using more than 3 devices), the widespread use of online services (89% using at least 5 IT services) highlight users are becoming or have become technology dependent but perhaps without being security savvy (Clarke et al., 2016). Knowledge transfer through cybersecurity education can positively affect information security practices, as demonstrated in a study on library employees (San Nicolas-Rocca & Burkhard, 2019). While education level has a significant impact on security awareness in ICT usage (Bostan, 2015), users often practice security at a basic level despite increasing awareness (Clarke et al., 2016).

Based on research done on expertise in the context of information technology, as well as security awareness, the following hypotheses are set:

> H1: There will be a significant difference in security awareness between IT experts and non-IT experts.
>
> H2: There will be a significant positive difference in cookie awareness between IT experts and non-IT experts.
>
> H3: There will be a significant positive correlation between security awareness and cookie awareness.

4 PRIVACY CALCULUS THEORY

Privacy calculus theory (PCT) is a framework used to understand individuals' decision-making process regarding personal information disclosure in various technological contexts. It posits that people weigh perceived benefits against perceived risks when deciding to share information or use a technology (Majumdar & Bose, 2016). In practise this means that individuals share data online if the perceived benefits are greater than the risks (Alwahaishi et al., 2023).

The privacy calculus theory has been adapted to various research contexts related to technology adoption and data disclosure. It has been applied to smart technologies in transportation, fitness, and medical treatment, revealing that privacy concerns and perceived benefits influence acceptance across different domains (Schomakers et al., 2022). The theory has also been extended to consider irrational factors and context sensitivity in online data disclosure decisions, highlighting the dominant role of habits (Fernandes & Pereira, 2021). In healthcare technology adoption, an extended privacy calculus model incorporating health condition emotion has been proposed to explain patients' acceptance behaviour (Rahman, 2019). Additionally, the theory has been used to investigate consumers' perceptions of personalized advertising on social networking sites, examining factors such as invasiveness, privacy control, and consumer innovativeness that influence behavioural intentions (Gironda & Korgaonkar, 2018). In addition PCT has been applied to emerging technologies like internet of things (IoT) (Majumdar & Bose, 2016), mobile banking (Njenga & Ndlovu, 2012), online learning (Jiang et al., 2022), and mobile location-based advertising (Gutierrez et al., 2019). Studies have found that benefit perception and trust positively influence willingness to use a technology, while risk perception has a negative effect (Jiang et al., 2022).

As the PCT outlines, people are more likely to disclose their personal information online when they perceive the benefits to be high and the costs to be low (Li, 2012). There have been multiple studies to confirm the theory in researching how perceived privacy risk affects users sharing personal information online negatively (Bhatia & Breaux, 2018; Torabi & Beznosov, 2013). As prior research and hypotheses suggest, expertise in IT, security awareness and cookie awareness all increase the perceived privacy risks in the context of website cookies. According to PCT, this would again lead to being more active in taking privacy measures online. Based on this supposition, the following hypotheses are set:

> H4: There will be a significant difference in website cookie consent between IT experts and non-IT experts.
>
> H5: There will be a negative correlation between security awareness and website cookie consent.
>
> H6a: There will be a significant difference in positive cookie perceptions between IT experts and non-IT experts.
>
> H6b: There will be a significant difference in negative cookie perceptions between IT experts and non-IT experts.
>
> H7a: There will be a negative correlation between security awareness and positive cookie perceptions.
>
> H7b: There will be a positive correlation between security awareness and negative cookie perceptions.

5 METHODOLOGY

The methods of the empiric research are introduced in this section. The topics covered are the creation and execution of the questionnaire, as well as the analysis method. In addition to this, the participants of the survey are described.

5.1 Participants

To achieve a rather even sampling of information technology professionals as well as non-professionals, the survey was shared in two Finnish information technology companies and social media. Participating in the survey was optional and anonymous, and there was no incentive for the participants to take part in the study.

The total number of responses was 80 (N=80). 58,9 % of the respondents are under 30 years old, and 22,5 % are between 30 and 39 years old, whereas over 40-year-olds include 18,7 % of the respondents (Table 1). Education level distribution shows that the majority of the respondents at 39,2 % have a master's level degree, 27,8 % have a bachelor's level degree, 20,3% have a polytechnic degree and 11,4 % have an upper secondary school or vocational level education (Table 1). Only one respondent reported to have a doctoral degree (1,3%), and no respondents reported of having a basic level education.

Table 1 Distribution of survey respondents

Gender	**Number of Participants**
Female	41 (51,3%)
Male	38 (47,5%)
Other	0 (0.0%)
Would not disclose	1 (1.2%)
Total	80
Age (years)	**Participants**

Under 20	0 (0,0%)
20 - 29	47 (58,8%)
30 - 39	18 (22,5%)
40 - 49	8 (10,0%)
50 – 59	7 (8,7%)
60 and older	0 (0,0%)
Total	80

Education level	**Participants**
Basic education	0 (0,0%)
Upper secondary school/vocational studies	9 (11,3%)
Polytechnic	16 (20,0%)
Bachelor's degree	22 (27,5%)
Master's degree	31 (38,8%)
Doctoral degree	1 (1,3%)
Would not disclose	1 (1,3%)
Total	80

The respondents were allocated into two groups based on if they have experience in the field of information technology or not. This was determined based on whether the attendees had either education, work experience or both in the field of information technology. Out of 80 responses 46 (57,5%) reported that they have work or study experience in the field of information technology whereas 34 (42,5%) reported that they do not have work or study experience in the field of information technology. When asked about the level of work experience of the attendees in the IT experience group, the most prominent categories were 2-4 years of work experience in the field at 32,6% and over 10 years of work experience at 23,9%. With these requirements, the IT expert group had 46 participants, whereas the non-IT expert group had 34 participants.

5.2 Measures

To address the research questions, the empirical study of this thesis was conducted utilizing quantitative methods. A structured online questionnaire was utilized to collect data, enabling the efficient gathering of measurable insights into participants’ attitudes and behaviours concerning cookie consent. Surveys can be a useful research tools that can gather data on demographics, histories, knowledge, behaviours, and attitudes (Passmore et al., 2002). Therefore, an online survey was used to get an accurate view into effects of user background into website cookie consent behaviour, by reaching a wide range of different people and backgrounds. The questionnaire was executed as an electronic survey, created with the online survey tool Webropol. The electronic survey was distributed with an online link, ensuring anonymity for the respondents.

A commonly used survey tool, the Likert scale, was used in the survey as it is familiar to many respondents and suits especially well in measuring constructs such as attitudes (Passmore et al., 2002). Based on previous research and the research questions, five different constructs were established for the survey.

The information technology section was designed to separate the participants into two groups, IT experts and non-IT experts, as well as gain an understanding of the level of knowledge participants have in the field of information technology. The participants were asked to state whether they have study or work experience in the IT field. If they reported to have work or study experience, two additional questions were visible to determine the level of education or work experience they have in the field. All participants were also asked to self-evaluate their level of expertise in the IT field.

The security awareness section of the survey is designed to get an understanding of the level of online security knowledge participants have. Each survey item is presented with five-point Likert scale ranging from never to always. The participants were asked to estimate how often they engage in the security measures stated in the survey items. The chosen statements are about reading privacy policies, deleting cookies from a web browser, activating the 'do not track' -option, refusing to give information to a website because it felt too personal and deciding not to use a website because the user was unsure how their personal information would be used.

The cookie awareness section of this study is designed to get a better understanding of participants' knowledge of website cookies. A five-point Likert scale is used to collect the answers, and in order to measure participants knowledge in the subject. The answer options range from strongly disagree to strongly agree, with the higher the answer correlating with stronger cookie awareness with each survey item. The participants are asked if they have a general idea what website cookies do, if they have a general idea of what kind of information is stored with website cookies, and if they feel like website cookies can benefit Internet users. These three survey items are combined into a single sum variable to represent the cookie awareness construct for further analysis.

The cookie perceptions section of the survey intends to measure participants insights, thoughts and feeling on the website cookies. The section consists of two five-point Likert scale questions where the participants answer two statements on the subject, and in addition there are three open answers question in order to understand the reasoning for participants perceptions better. There is no sum variable created for the construct, because of the nature of the questions.

The cookie consent habits section of the survey, was designed to understand how and why participants deal with website cookies in their everyday lives. This was done with two survey items. Firstly, a five-point Likert scale asking the participants to estimate how often they accept or decline website cookies. The answer options range from always decline to always accept. The second survey item is an open answer question where the participants can explain their previous answer further.

Table 2 includes each item for each of the four constructs, together with the source each item was adapted from. The survey (APPENDIX 1) consists of 22 questions, which were mandatory except the demographic questions and one open response regarding website cookie descriptions, to ensure there is no missing or incomplete data.

Table 2 Constructs and the survey items

Construct	**Survey items**	**Adapted from**	**Original question**
Information technology expertise	I have work or study experience in the IT field. (This could mean computer science, software development, web development or similar computer related fields.)	(Chanchary & Chiasson, 2015) -	
	I have work experience in computer science, software development, web development or similar computer-related fields.	-	
	I have study experience, a degree, or extensive training in computer science, software development, web development or similar computer-related fields.	-	

	How would you rate your level of expertise with computers/information technology.	-	
Security awareness	I decide not to use a website or purchase something online because I was unsure how my personal information would be used.	(Chanchary & Chiasson, 2015)	Decided not to use a website or not to purchase something online because you were not sure how your personal information would be used
	I read a website's privacy policy.	(Chanchary & Chiasson, 2015)	Read a website's privacy policy
	I delete cookies from my web browser.	(Chanchary & Chiasson, 2015)	Deleted cookies from your web browser
	I activate the "do not track" option in web browsers or use any tracking prevention tools.	(Chanchary & Chiasson, 2015)	Activated the" do not track" option in your web browser or installed tracking prevention tools
	I refuse to give information to a website because I feel it is too personal or unnecessary.	(Chanchary & Chiasson, 2015)	Refused to give information to a website because you felt it was too personal or unnecessary
Website cookie awareness	I feel like I have a general idea of what website cookies do.	-	
	I feel like I have a general idea of what kind of information is	-	

	stored/transmitted with website cookies.		
	I feel like website cookies can benefit internet users.	(Ur et al., 2012)	How do you think behavioral advertising can benefit Internet users?
Website cookie perceptions	I feel like there are positive aspects to website cookies.	-	
	I feel like there are negative aspects to website cookies.	(Ur et al., 2012)	Are there any negative aspects of behavioral advertising?
	How would you describe website cookies? Please use this space to respond freely about your thoughts and feelings about the subject. (You can use bullet points, individual words or sentences)	(Ur et al., 2012)	Overall, how do you feel about online behavioural advertising? Why?
Website cookie consent habits	How do you generally deal with website cookies?	-	
	What kind of factors affect you accepting/declining the use of website cookies? This could mean for example choosing one of the options because it's easier to choose, less harmful to you or just because you don't	-	

	really know what website cookies do. Also, for example the reasoning could be that you believe website cookies have a positive or negative impact on your user experience.		

The field background section aims to split the attendees into information technology professionals and non-information technology professionals. This is done by establishing weather or not the attendee has either work or study experience in the field of information technology. In establishing the level of information technology expertise, various options were given both in the level of work and study experience. A Likert scale was used to establish the attendee's own idea of their level on expertise in information technology. In this as well as the following sections, a traditional odd number of five response points was used in the Likert scale (Passmore et al., 2002).

The security awareness section describes five different statements regarding measures that based on prior research are considered to be signs of a security aware individual. The attendees were given a five-point Likert scale in between never and always, to express how often they partake in the measures referred to in the statements. Never was used to express the least frequent option, and always being the most frequent option.

The third construct, website cookie awareness, consists of 3 statements looking to gain insight on the attendee's knowledge on website cookies. A five-point Likert scale was used ranging from strongly disagree to strongly agree, the more positive answer indicating about a higher level of knowledge on the subject.

The fourth construct aims to understand attendee's website cookie perceptions, contains six statements aiming to establish the users' thoughts and views on website cookies. On two of the first statements in the website cookie perception section (Table 2), a five-point Likert scale was used ranging from strongly disagree to strongly agree. In addition to this, on the statements regarding the perceived positive and negative aspects of website cookies to users, open responses were included in order to gain a deeper insight into why attendees feel either positively or negatively about the aspects of website cookies.

The fifth and final section on website cookie consent habits, consists of one question utilizing a five-point Likert scale. The aim of this section is to understand the consent habits of attendees, on a scale of always decline being the sparsest option, and always accept being the most frequent option concerning the frequency of cookie consent. In addition, a mandatory open format question was added, to establish what kind of factors affect users making their consent decision.

A few examples of the possible answers were given maintaining a neutral wording, for the attendees to describe their reasoning for their habits freely.

For two of the constructs presented in Table 2, security awareness and website cookie awareness, an arithmetic mean was calculated. The validity of these constructs was deemed adequate (Table 2), after evaluating them using Cronbach's alpha. The level Cronbach's alpha value of the security awareness construct is found to be .600. This could be due to the number of questions, as it is known that scales of less than ten items generate lower Cronbach's alpha values (Robertson & Evans, 2020). In addition, a higher sample size ensures better statistical power to really detects effects. However as was acknowledged in the literature review of this study, there are multiple factors that affect users' security habits online. Since this was a short online study, there was no further input into why the participants answers on security awareness did not correlate with each other at an expected level. The possible reasonings of inconsistent answers are discussed in the limitations and future research chapter.

Table 3 Cronbach Alphas

Construct	***Cronbach's Alpha***	***N of Items***
Security Awareness	.621	5
Cookie Awareness	.748	3

5.3 Procedures

The ethics of the research were considered when creating the survey. Participants were provided with extensive information about the study, before consent. A research notification and privacy notice were provided before the survey, explaining for example the purpose and procedure of the research. In addition, a separate consent form was provided for the participants to read before answering any survey questions. Participant consent was obtained by submitting the survey, confirming consent to the research notification, privacy notice and consent form. All of the answers were gathered anonymously, with the use of an open link so that no emails were connected to the respondents at any point in the study. Participants had the right to withdraw their consent at any point of the research.

The participants were invited to take part in this study through personal communication channels, on private communication channels of two large IT firms in Finland and through social media on LinkedIn and Instagram. In the recruitment message, study purpose and participation requirements were shortly outlined. Participants did not have specific criteria in order to take part in this study, however in the recruitment message it was outlined that participants should be over 18 years of age. A brief introduction to the topic of website cookies was given at the beginning of the survey. This was done to ensure that each participant knew in what context website cookies were discussed in the survey. In the analysis section of the thesis the participants were divided into two groups, IT experts and non-experts, the questions were standardized across these two groups. Since the survey was conducted in an online survey tool all data collected was self-reported and data was recorded and stored in the Webropol online survey tool. There were no follow up activities post study, for example follow-up emails.

6 RESULTS

The data was analysed with IBM SPSS statistics software. This chapter presents the results of the survey, and how the two groups of IT experts (N = 46) and non-experts (N = 34) as well as different security awareness levels correlate with cookie awareness, cookie perceptions and cookie consent habits. The chapter is divided into four sections, based on the constructs used on the survey.

6.1 Security awareness

The security awareness construct consists of the five survey items described, that were combined to form a sum variable that represents the *security awareness* construct in analysis. An independent *t*-test was used to examine the difference between both groups. The analysis on the sum variable suggests there is a significant positive difference between security awareness in IT experts and non-experts (t = 2.865, df = 78, p = 0.005, two tailed), thus H1 is supported (Table 11).

These five survey items were combined into a single sum variable to represent the security awareness construct for further analysis.

When asked if participants have decided not to use a website or purchase something online because they were unsure how their personal information would be used, the majority of participants answered that they have rarely done that, with 41% experts 37% non-experts. The noticeable difference was that 28% of IT experts reported often decided not to use a website or purchase something online because they were unsure how their information would be used when in contrast only 9% of non-IT experts reported the same.

When asked about reading a website's privacy policy, the most popular answer in both groups, 45% of experts and 62% of non-experts, was that they have never read a website's privacy policy. 37% of experts and 29% non-experts reported that they rarely read a websites privacy policy. 9% of each group reported reading a website's privacy policy, whereas 9% of experts also reported that it was too often reading a website privacy policy when the correlating number for non-experts was 0.

When asked about deleting cookies from their web browsers, the most popular option for both groups were rarely deleting cookies from their web browser, this being chosen by 35% of non-experts and 30% of experts. The never, sometimes and always options followed similar distributions for both groups, however a noticeable difference was found at 28% of experts and in contrast only 9% of non-experts reported to often delete cookies from their web browser.

When asked about activating the do not track option on web browsers or installing tracking prevention tools the most popular choice for both groups was to often do one of these tracking prevention activities. 30% of experts and 35% of non-experts reported activating the do not track option often. 26% of non-experts and 13% of experts reported to a rarely activating the do not track option. A significant difference was found where 22% of experts reported to always taking these tracking prevention measures, whereas the correlating number for non-experts was 3%.

When asked about whether participants have refused to give information to a website because it felt too personal or unnecessary, significant differences between the groups were found. 32% of non-experts reported to rarely take these measures, when in contrast 11% of experts reported the same. 24% of experts reported to always refusing to give information to a website when it feels too personal, the correlating amount for non-experts being significantly less at 3%. The statements of IT experts (Table 1) and non-IT experts (Table 2) can be found in graphs below.

Table 4 Descriptive statistics of security awareness

Measure	*Group*	*N*	*Mean*	*Standard deviation*
Security awareness	Experts	46	2.87	0.66
	Non-experts	34	2.45	0.63

Figure 1 Security awareness statements IT experts

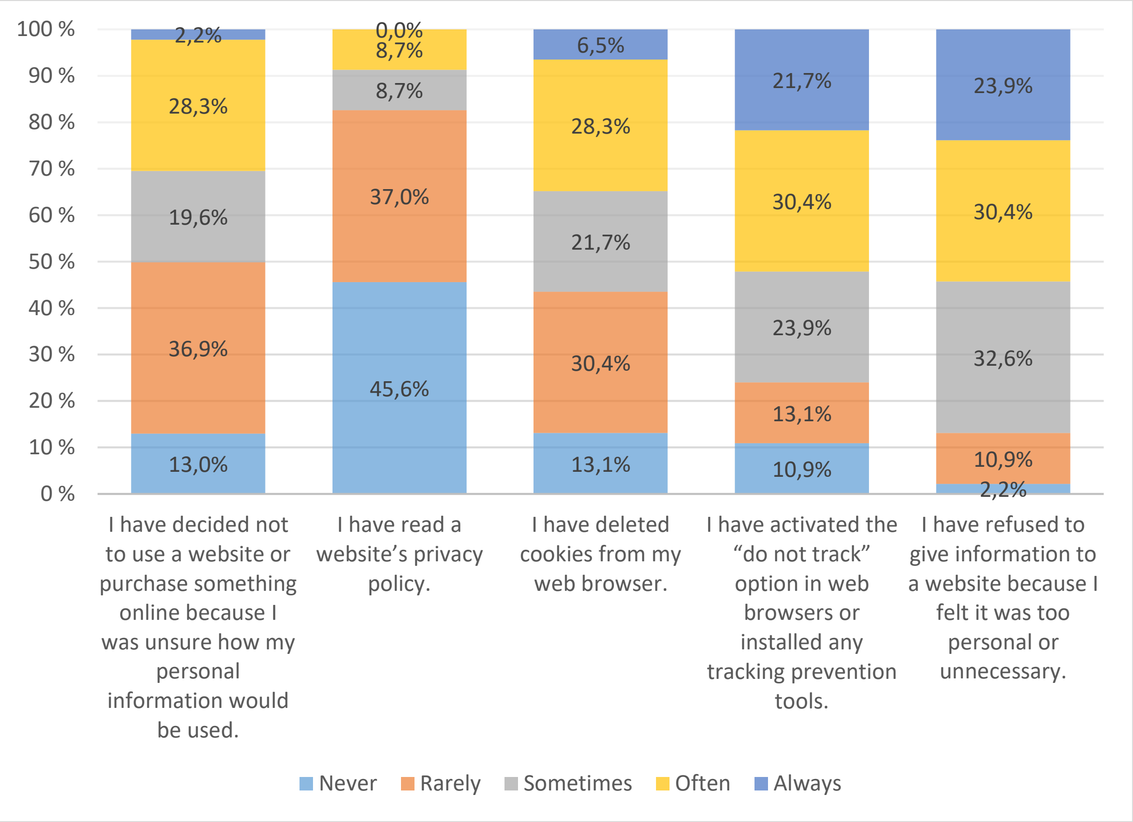
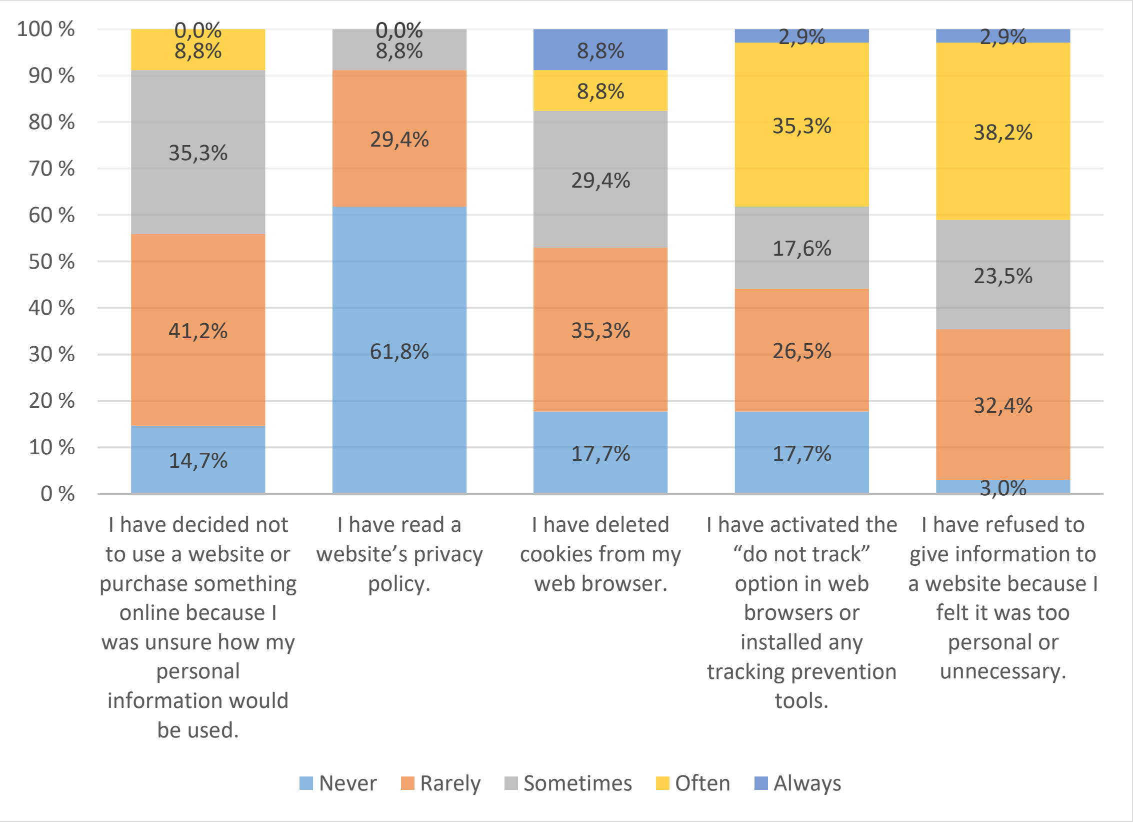


Figure 2 Security awareness statements non-IT experts



6.2 Cookie Awareness

When asked about general knowledge on website cookies there were significant differences between the two groups. Most IT experts reported to either agree with this statement 46%, or strongly agree with the statement 39%. In contrast, non-experts reported to agree 32%, agreed with 29%, and strongly disagreed with 18%. The corresponding numbers for experts with neither agreeing nor disagreeing, disagreeing, and strongly disagreeing were significantly less than the non-expert groups' answers.

When asked about knowledge on what kind of information is stored or transmitted with website cookies there were again significant differences between the two groups. Most IT experts stated to either agree 44%, or strongly agree 39%. Only 3% of non-experts stated to strongly agree with the statement.

When asked about whether the participants agree with the statements that website cookies can benefit internet users, generally the experts agreed with this statement more, with the most common answer from the experts being agree at 48%. In contrast 29% of the non-experts reported to agree with this statement. The most common answer for the non-experts was the neutral option on the five-point scale, neither agreeing nor disagreeing at 44%.

The cookie awareness construct consists of these three items, which were combined to form a sum variable that represents the *cookie awareness* construct in analysis. An independent samples Mann-Whitney U test was conducted, as the distribution of the cookie awareness variable was not normally distributed. there is a significant positive difference in cookie awareness between IT experts and non-experts (U = 294.000, N1=46, N2= 34, p = <0.001), hypotheses H2 is supported (Table 11).

To analyze the correlation between sum variables cookie awareness and security awareness, a Spearmans Rho was conducted to analyze the correlation between the two variables since both of the variables were not normally distributed. The analysis shows that there is not a significant positive correlation between security awareness and cookie awareness (rho = 0.158, p 0.081, one-tailed), thus H3 is not supported (Table 11).

Table 5 Descriptive statistics of cookie awareness

Measure	*Group*	*N*	*Mean*	*Standard deviation*
Cookie awareness	Experts	46	3.94	0.75
	Non-experts	34	2.92	0.88

6.3 Cookie consent habits

Out of the IT experts the majority 41% reported to usually decline website cookies, the correlation number for the non-experts being 23%. Out of the non-experts the majority reported to usually accept website cookies 35%, when 24% of the experts reported the same. These statistics are shown in Figure 3.

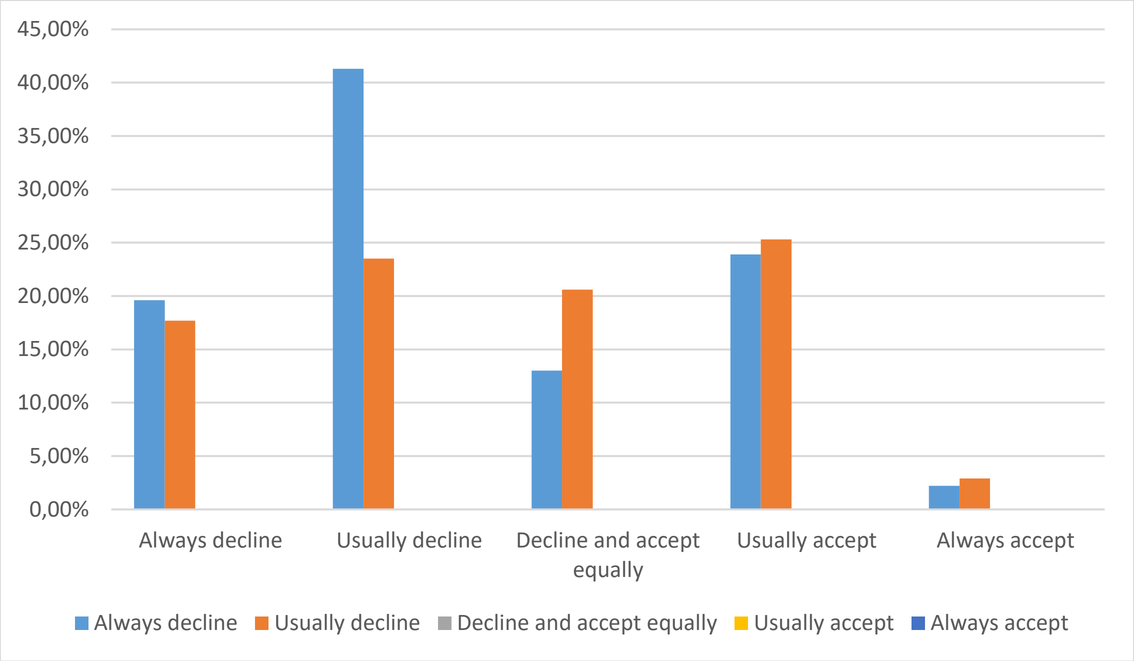
An independent samples Mann-Whitney U test was conducted, as the distribution of the cookie consent variable was not normally distributed. The analysis of the sum variable shows that there is not a significant difference in website cookie consent between IT experts and non-IT experts (U = 911.500, N1=46, N2=34, *p*= 0.191, two-tailed), thus hypotheses H4 is not supported (Table 11).

To analyze the correlation between sum variables cookie awareness and security awareness, a Spearmans Rho was conducted since both variables were not normally distributed. The analysis shows that there is a significant negative correlation between security awareness and website cookie consent (rho = -0.367, n=80, *p* = < 0,001, two-tailed), thus H5 is supported (Table 11).

Table 6 Descriptive statistics of cookie consent habits

Measure	*Group*	*N*	*Mean*	*Standard deviation*
Security awareness	Experts	46	2.47	1.10
	Non-experts	34	2.68	1.17

Figure 3 Cookie consent habits



6.4 Cookie perceptions

The first statement was whether the participants feel there are positive aspects to website cookies. Over half of the experts reported to agree or strongly agree with this statement at 67,4%, when the correlating number for non-experts was 35,3%. There is a significant difference found between the groups; experts agree with the statement more. In addition, 23,5% of non-experts reported to either disagree or strongly disagree with the statement, when only 4,4% of experts reported the same. 41,2% of non-experts reported to neither agreeing nor disagreeing with the statement, however compared only 28,2% of experts reported the same.

The second statement of the section was whether the participants feel like there are negative aspects to website cookies. Here the answers of the groups were slightly more evenly distributed compared to the previous statement, however the experts reported to agree with this statement more than the non-experts. The majority, 76,1% of experts reported to either agree or strongly agree with this statement. The majority of non-experts, 58,8%, also reported either agreeing or strongly agreeing with the statement. Non-experts reported to neither agreeing nor disagreeing with the statement more at 35,3%, whereas 21,7% of experts felt the same way. 5,9% of non-experts and 2,2% of experts reported to disagreeing or strongly disagreeing with the statement.

Due to the nature of the questions, a sum variable of the cookie perception construct could not be calculated like in the other constructs of this study. However, the analysis of the correlations of the two induvial survey items with IT expertise levels was very interesting. Therefor analysis on the positive and negative cookie perceptions was performed separately in order to see the difference in IT experts and non-IT experts as well as the correlation with security awareness. An independent test was used to analyze differences in both factors with IT experts and non- IT experts because the distribution of their population scores were normally distributed. A Pearson's R test was used to analyze the correlation between security awareness and both positive and negative factors.

6.4.1 Positive perceptions

A significant positive difference was found in positive cookie perceptions between IT experts and non-IT experts (*t* = 3.202, df = 78, *p* = 0.002, two-tailed). Thus, hypotheses 6a is supported (Table 11). This means that IT experts feel that there are positive aspects to website cookies more often than non-IT experts (Table 7).

Table 7 Descriptive statistics: positive cookie perceptions and IT expertise groups

Groups	Mean	Standard deviation	Significance
Experts	3.78	0.841	The correlation is statistically significant
Non-experts	3.15	0.925	

No significant negative correlation was found between security awareness and positive cookie perceptions (r = -0.018, n = 80, *p* = 0.874, two tailed). Thus, hypotheses 7a is not supported (Table 11). Security awareness had a correlation with positive cookie perceptions, however the correlation was not significant (Table 8).

Table 8 Descriptive statistics: security awareness and positive cookie perceptions

Factors	Mean	Standard deviation	Significance
Security awareness	2.70	0.679	The correlation is not statistically significant
Positive cookie perceptions	3.51	0.928	

6.4.2 Negative perceptions

No significant difference in cookie perceptions between IT experts and non-IT experts was found. (*t* = 1.744, df = 78, *p* = 0.084, two-tailed). Thus, hypotheses 6b is not supported (Table 11). IT experts had more negative perceptions about website cookies than non-IT experts, however the correlation was not significant (Table 9).

Table 9 Descriptive statistics: negative cookie perceptions and IT expertise groups

Groups	Mean	Standard deviation	Significance
Experts	4.02	0.774	The correlation is not statistically significant
Non-experts	3.71	0.836	

A significant correlation was found between security awareness and negative cookie perceptions (r = -0.319, n = 80, *p* = 0.004, two tailed). This means that security awareness significantly positively correlates with negative cookie perceptions (Table 10). Thus, hypotheses 7b is supported (Table 11).

Table 10 Descriptive statistics: security awareness and negative cookie perceptions

Factors	Mean	Standard deviation	Significance
Security awareness	2.70	0.679	The correlation is statistically significant
Negative cookie perceptions	3.89	0.811	

Table 11 Inferential statistics

Variables	*Hypothesis*	*Sig. /Supported*
Security awareness: IT expertise	H1: There will be a significant difference in security awareness between IT experts and non-IT experts.	*t* = 2.865, df = 78, *p* = 0.005, two tailed, Supported
Cookie awareness: IT expertise	H2: There will be a significant positive difference in cookie awareness between IT experts and non-IT experts.	U = 294.000, N1=46, N2= 34, *p* = <0.001, Supported
Cookie awareness/security awareness	H3: There will be a significant positive correlation between security awareness and cookie awareness.	rho = 0.158, *p* 0.081, one-tailed, Not supported
Cookie consent: IT expertise	H4: There will be a significant difference in website cookie consent between IT experts and non-IT experts.	U = 911.500, N1=46, N2=34, *p*= 0.191, two-tailed,

		Not supported
Cookie consent: security awareness	H5: There will be a negative correlation between security awareness and website cookie consent.	rho = -0.367, n=80, *p* = < 0,001, two-tailed, Supported
Cookie perceptions, positive: IT expertise	H6a: There will be a significant difference in positive cookie perceptions between IT experts and non-IT experts.	*t* = 3.202, df = 78, *p* = 0.002, two-tailed, Supported
Cookie perceptions, negative: IT expertise	H6b: There will be a significant difference in negative cookie perceptions between IT experts and non-IT experts.	*t* = 1.744, df = 78, *p* = 0.084, two-tailed, Not supported
Cookie perceptions, positive: Security awareness	H7a: There will be a negative correlation between security awareness and positive cookie perceptions.	r = -0.018, n = 80, *p* = 0.874, two tailed, Not supported
Cookie perceptions, negative: Security awareness	H7b: There will be a positive correlation between security awareness and negative cookie perceptions.	r = -0.319, n = 80, *p* = 0.004, two tailed, Supported

6.5 Other findings

The difference with participants self-assessed level of information technology knowledge and their reported IT expertise gained through studies or work experience was analysed, and it was found that the self-assessment of participants aligned with their reported experience levels (*t* = 6.975, df = 78, *p* < 0.001, two-tailed). This was measured to ensure the participants had a realistic idea of their own information technology expertise, so the analysis could be ensured that the results of this thesis would be more reliable.

To analyze the correlation between sum variable cookie awareness and consent habits, Spearmans Rho was conducted to analyze the correlation between the two variables since both of the variables were not normally distributed. The analysis shows that no significant correlation was found between cookie awareness and consent habits in the analysis (rho = -0.009, n = 80, *p* = 0.934, two-tailed).

No significant correlations were also found between age (rho = 0.047, N = 80, *p* = 0.682), gender (U = 835.500, N = 80, *p* = 0.565, two tailed) or education level (rho = -0.105, N = 80, p = 0.356, two tailed) with cookie consent habits. There was also not found any significant correlation between age (rho = 0.070, N = 80, *p* = 0.538), gender (U = 669.500, N = 80, *p* = 0.280) or education level (rho = -0.006, N = 80, *p* = 0.955) with security awareness.

6.6 Analysis of open question responses

In the survey, multiple open answers were collected to enrich the results on how IT expertise and security awareness affect cookie consent habits and perceptions. The open answers given are discussed in the following chapter.

6.6.1 Participants' perceptions of cookies

To provide a more profound answer for the security awareness portion of the research questions, open answers were collected and analyzed. In this section, survey items 14 and 16 (Appendix 1) were considered.

In the survey, after five-point Likert scale questions on whether participants feel that there a positive, and/or negative aspects to website cookies, open answers were collected to better understand the thoughts behind the perceptions.

43 out of the 46 experts provided explanations why they felt that there are positive aspects to website cookies. All the non-experts answered the open question. With both experts and non-experts who felt like there are positive aspects to website cookies, participants referred to better personalization whilst using a website, whether that mean more accurately targeted ads, or a better user experience (Table 12). The majority (N=13) of participants who reported feeling neural about the statement, explained that they do not really know what website cookies are or do (Table 12). The participants who stated to disagree with the statement, described to find cookies intrusive or exploitive (Table 12).

Table 12 Open answers to statement that there are positive aspects to website cookies

Standpoint	Group	N	% of group	Category (mentioned in how many answers) (
Agree	Experts	31	67,4%	Better user experience and saved information (7) Better and accurately targeted ads (31) Personalization on websites (24)
	Non-experts	12	35,3%	
Neutral	Experts	13	28,2%	Technologically mandatory (8) Do not know what cookies do (13) Difficult to say if they are positive or negative (6)

	Non-experts	14	41,2%	
Disagree	Experts	2	4,4%	Cookies are intrusive (7) Cookies are exploitive (9)
	Non-experts	8	23,5%	

43 of the 46 IT experts provided explanations why they felt that there are positive aspects to website cookies. All the non-experts answered the open question. Both experts and non-experts who felt like there are negative aspects to website cookies, participants referred to do so to avoid exploitive and intrusive behaviors of website providers. A number (N=12) of participants also reported with agreeing with the statement since they find the cookie collecting technology decisions to be unethical. The majority of participants who reported to feel neutral about the statement, reasons their decision by not really knowing what website cookies are or do (Table 13). Three (N=3) participants also stated that it's difficult to state if they find cookies more positive or negative, and one stated that they feel neutral about the subject since technology is mandatory (Table 13). The participants who disagreed with the statement that there are negative aspects to website cookies, did so because they feel like the positives like a better user experience or personalization outweigh the negative aspects (Table 13).

Table 13 Open answers to statement that there are negative aspects to website cookies

Standpoint	Group	N	% of group	Category (mentioned in how many answers)
Agree	Experts	35	76,1%	Cookies are intrusive (20) Cookies are exploitive (24) Cookies are unethical (12)
	Non-experts	20	58,8%	
Neutral	Experts	10	21,7%	Do not know what cookies do (18) Difficult to say if they are positive or negative (3) Technologically mandatory (1)
	Non-experts	12	35,3%	
Disagree	Experts	1	2,2%	Better user experience and saved information (3) Personalization on websites (1)
	Non-Experts	2	5,9%	

6.6.2 Reasoning for consent habits

In Table 14 is specified the most common reasons for users' cookie consent habits, participants provided in their open answers. The Table 14 consists of standpoints and the three categories under them. Standpoints are divided into options of accepting and declining cookies as well as feeling neutral towards them or doing both. Answers always accept and usually accept were grouped to form the accept -standpoint. A similar measure was followed with the decline -standpoint. Categories name the reasons why people chose the option and the number states how many gave the same reasoning in their open answers.

The Table 14 presents the most common reasons for users to accept cookies on websites. The most common of them provided by twelve (N=12) participants is that they accept cookies because they feel that the website is safe and familiar. This aligns with fifteen (N=15) people also stating that they declined cookies on sites that they felt like are dangerous or unfamiliar to them. Some users added that they like to accept sites that are Finnish and foreign only if they are a big notable brand. The second most common answer provided by eleven (N=11) participants was that they have accepted cookies since it was the easy option. Some users noted that this was against how they felt towards cookies, even feeling negative towards them yet accepting them on for the "easy way out". A couple of users did note that they do decline the cookies if a choice is made easy but rarely is that the case in their opinion. Another reason for accepting the cookies given by six (N=6) participants was that they believed that this gave them the best user experience on the site. It was mentioned that accepting cookies provides them with the best and most accurately targeted ads as well as smooth operating website with functions such as password saving and a faster website.

A portion of users noted that they feel neutral towards cookies and select which ever choice is made easier on the website. Most of the users who felt neutral towards cookies (N=10) based their selection on randomness and they noted that they felt ignorant towards cookies overall. A few of the participants (N=5) stated that they try and always accept only the required cookies since they felt like it's the most neutral choice for a website surfing.

The largest group of participants (N=42) stated that they decline cookies on websites. The most common reasoning behind this decision was that the website felt dangerous or unfamiliar to them, stated by 15 participants. In perceived dangerous and unknown websites, participants felt like their data is not in safe hands and that the site or the company may exploit their data. Ten (N=10) of the users also felt that accepting cookies is often made too difficult. This maliciousness and misleadingness of users causes them to have a opposite reaction and provoking a want to fight the "forced" cookie consent. This was reason why some users said that they decline cookies along with users who feel like cookies contain a lot of privacy issues stated by four (N=4) participants. These issues relate to unknown sites and companies and the fear of data leaks and selling of personal data was mentioned in the answer's multiple times. Six (N=6) users also noted that they decline cookies since they do not know enough about them. This lack of understanding of cookies and what they do was also noted as a large portion of people's perceptions about cookies overall. It was also mentioned that cookie consent popups do not provide information about where and how the information gathered is being used and this causes some users to feel like they rather decline the cookies than use them.

Table 14 Reasoning for cookie consent habits

Standpoint	Accepted cookies	25
	Neutral	13
	Declined cookies	42
	Total	80
Categories and how many answers in each one		
Accept	Accepted cookies on safe and familiar websites (12)	
	Accepted cookies since it was the easy option (11)	
	Believe cookies provide them with better user experience (6)	
	Accept the cookies unwillingly since declining was made too difficult (2)	
Neutral	Accept only required cookies (5)	
	Feel neutral about cookies or base their selection to randomness (10)	
Decline	Decline cookies since they don't know what they are used for (6)	
	Decline cookies on dangerous and unknown websites (15)	
	Decline cookies since accepting cookies is made too easy and they want to be against that or if declining is an easy option (10)	
	Decline cookies since they feel like they are intrusive with data collection and privacy issues (4)	
	Decline cookies since they feel like they are exploitive selling your information away (5)	

7 DISCUSSION

The purpose of this chapter is to discuss the main findings of the study, the outlined research questions and practical implementations based on the results of the study. In addition, limitations and possibilities for future research are discussed. Previous research has found that individuals with an IT background are more likely to share their personal information and data online (Chanchary & Chiasson, 2015). The primary objective of this thesis was to examine the possible correlation between IT expertise and security awareness with website cookie consent.

7.1 Cookie consent habits

This thesis explored the effects of using your background two website cookie consent habits and perceptions. The thesis focused especially on comparing the consent habits and perceptions of IT experts and non-experts as well as different levels of security awareness. Data was collected via an online survey from 80 participants, and it was found that security awareness correlates with website cookie consent negatively. This aligns with previous research outlining that perceived privacy risks affect users sharing personal information online negatively (Bhatia & Breaux, 2018; Torabi & Beznosov, 2013; Torten et al., 2018). These findings align with the privacy calculus theory, as the perceived benefits of declining cookies are higher for the more security awareness. However, surprisingly in this thesis it was found that IT expertise does not significantly correlate with website cookie consent habits. A previous study by Chanchary & Chiasson, (2015) has found that there is a positive correlation with an IT background and cookie consent, the findings of this study do not provide additional confirmation to these results. The possible explanations for these results are discussed in the limitation and future research section of this chapter.

It has been studied that user awareness and user experience (Habib et al., 2022), the design of the user interface (Jayakumar, 2021), the website cookie banner (Bavel & Rodríguez-Priego, 2016) and website familiarity and trustworthiness (Hovnik et al., 2022; Jayakumar, 2021) can affect website cookie consent habits. All of these findings align with the open answers collected about cookie consent habits. Several participants reported website familiarity, user experience, the cookie banner, and the lack of knowledge on website cookies affect their consent habits.

7.2 Cookie perceptions

When analyzing the data collected on website cookie perceptions, it was found that between IT experts and non-IT experts, the IT experts find significantly more positive aspects about website cookies. The main reasonings for positive perception on website cookies were better user experience and better and more accurate ads. Interestingly, the same result was not found when analyzing the correlation between security awareness and positive cookie perceptions. The same continues when analyzing the negative perceptions of website cookies. There was found a significant positive correlation with security awareness and negative perceptions on website cookies. However, there was not found a significant difference in negative perceptions between IT experts and non-experts. This is surprising, since it was also found in the research that IT expertise positively correlates with security awareness. The possible reasonings for the conflicting results is discussed in the limitations and future research.

7.3 Contribution and practical implications

The results of this thesis contribute to user centric website cookie research greatly, as there is not much current research on how IT expertise and security awareness correlate with cookie consent or perceptions. There has been research on the non-technical users attitudes towards website cookies (Ur et al., 2012), however the viewpoint and comparison specifically of technical users has been missing. The open answers provided more information to the field and research about cookie consent habits and perceptions.

Understanding that security awareness affects cookie consent and perceptions, has practical implications. This can not only contribute to the academic research made in the field but also holds practical implications for web developers, policymakers, and educators striving to create digital environments that align with user expectations and security best practices. Several participants (N=20) reported to being unsure what website cookie do in general, this aligns with prior research in the field (Jayakumar, 2021). This finding shows that more education on the topic must be provided to everyday users. Hopefully these results will ultimately encourage a safer, more user-centric digital environment as well as offer a deeper understanding of the factors shaping our online experiences.

7.4 Limitations and future research

There are some limitations in the current research. In terms of the literature review, all the research in the discussed subjects may not be included. The search of relevant research was also limited by some publications being behind a paywall, which resulted them not being included in the literature review.

A larger sample size of individuals might be used to replicate the empirical investigation. The sample size of the research was relatively small (N=80). Nonetheless, the sample size is adequate when compared to another comparable research. In addition, the respondents' age or professionality distribution deviates from Finland's national average (Tilastokeskus, 2024), this could be because the survey was spread out online on social media channels like LinkedIn and in IT companies, that are more popular among younger individuals (Tilastokeskus, 2023). It is also notable to mention, that most of the participants were presumably Finnish and therefore the result may not be applicable for different cultures and backgrounds.

User consent habits were gathered with one survey item, which can leave space for interpretation and other influencing factors on the results. It has been researched that multiple factors affect users consent choices, for example the type of information collected by the website owner (Leon et al., 2013), wording used on the cookie banner (Kulyk et al., 2018) and the level of trust on the website (Hovnik et al., 2022) have all been found to affect user consent habits. There were open answers, to understand user consent choices better, however the study left room for speculation which other factors strongly determine user consent choices. It is also notable to mention that technical factors alone do not determine security awareness levels, as individual differences in cognitive abilities, habits, and behavioral intention can also play a role in shaping individuals' responses to cybersecurity threats.

This study measured information technology knowledge on a very general level, and exploring the effects of expertise to website cookie consent and perceptions is one of the possible angles of future research. Cookie consent habits were also gathered in a self-assessed format, this also proposes domain for future research as another possibility for future research would be to implement a study with an actual cookie consent situations that participants could deal with in a way, they do normally online. In a self-assessed survey format it can be more challenging to gather a realistic picture of the participants knowledge and actions (Dunning et al., 2004).

8 CONCLUSION

The purpose of this thesis was to find out if the level of expertise in the field of information technology or security awareness causes difference in cookie consent habits and perceptions. This research provides a viewpoint on everyday phenomenon of accepting or declining cookies and the user perceptions behind it.

Prior research on the topic is increasingly common through the increase of time people spend online and though legal guidelines like the GDPR that have brough website cookies to the knowledge of everyday users. Studies have been done on a variety of topics, such as how users respond to cookie disclaimers (Kulyk et al., 2018), how non-technical users feel about cookies (Ur et al., 2012), and general worries about the subject of tracking users online(Leon et al., 2013). This thesis aimed to provide further insight into whether IT expertise affects cookie consent habits and perceptions. Correlation between security awareness and cookie consent and perceptions was also examined, since IT expertise does not necessarily have a positive correlation with security awareness (Clarke et al., 2016). Past studies have also shown that most users lack sufficient knowledge about cookies and their uses (Smith et al., 2006; Wheeler et al., 2022). The thesis aimed to provide more information to these topics, to shed light on why individuals interact and perceive cookies in certain ways.

The results of this thesis suggest that security awareness significantly negative correlates with cookie consent habits. IT expertise was also found to negatively correlate with cookie consent habits, but not on a significant level. The results also suggest that there is a significant positive correlation between IT experts and positive cookie perceptions. There was also found to a slight correlation between security awareness and positive cookie perceptions but not on a significant level. The results of the study suggest that there is a significant positive correlation between security awareness and negative cookie perceptions. There was also found a slight positive correlation between IT expertise and negative cookie perceptions, but not on a significant level. The chosen research method based on the nature of the study was an online survey. The research questions set were answered based on the research. Both research questions, "Does the level of IT knowledge influence website cookie consent habits" and "Does increased security awareness influence website cookie consent habits?" can be answered based on the conducted research. Open answers were included, to gain a better understanding of participants perceptions of cookies and insight into their consent habits. The most common reasoning for accepting cookies was reported to be either the familiarity of the website or ease of consent. The most common reasons provided to why participants decline cookies was when being on seemingly dangerous or unknown websites.

The main limitations of the study was a rather small sample size (N=80), not demographically evenly representing Finland's population (Tilastokeskus, 2024). In addition, it has been researched that cookie consent habits are based on multiple different internal and external factors, so the level of IT expertise or security awareness is just one affecting factor with user choices. There is also always certain limitations when conducting an self-assessed online survey(Dunning et al., 2004), more accurate results could be achieved with more hands on methods where participants would face real life cookie consent decisions.

In conclusion, this study found that security awareness negatively correlates with cookie consent. This adds to prior research on the field and paves the way for future research on a user centric viewpoint on cookie consent and perceptions.

REFERENCES

Aladeokin, A., Zavarsky, P., & Memon, N. (2017). Analysis and compliance evaluation of cookies-setting websites with privacy protection laws. *2017 Twelfth International Conference on Digital Information Management (ICDIM)*, 121–126. https://doi.org/10.1109/ICDIM.2017.8244646

Alwahaishi, S., Ali, Z., Al-Ahmadi, M. S., & Al-Jabri, I. (2023). Privacy Calculus and Personal Data Disclosure: Investigating the Roles of Personality Traits. *2023 9th International Conference on Control, Decision and Information Technologies (CoDIT)*, 2158–2163. https://doi.org/10.1109/CoDIT58514.2023.10284222

Bandi, S. (2016). *AN EMPIRICAL ASSESSMENT OF USER ONLINE SECURITY BEHAVIOR: EVIDENCE FROM A UNIVERSITY*. http://hdl.handle.net/1903/18829

Bartold, P. M. (2018). Are you an expert? *Australian Dental Journal*, *63*(4), 393–393. https://doi.org/10.1111/adj.12664

Bavel, R. van, & Rodríguez-Priego, N. (2016). Testing the Effect of the Cookie Banners on Behaviour. *JRC Research Reports*, Article JRC103997. https://ideas.repec.org//p/ipt/iptwpa/jrc103997.html

Benjamin, G. (2017). Privacy as a Cultural Phenomenon. *Journal of Media Critiques*, *3*(10), 55–74.

Bermejo Fernandez, C., Chatzopoulos, D., Papadopoulos, D., & Hui, P. (2021). This Website Uses Nudging: MTurk Workers' Behaviour on Cookie

Consent Notices. *Proc. ACM Hum.-Comput. Interact.*, *5*(CSCW2), 346:1-346:22. https://doi.org/10.1145/3476087

Bhatia, J., & Breaux, T. D. (2018). Empirical Measurement of Perceived Privacy Risk. *ACM Trans. Comput.-Hum. Interact.*, *25*(6), 34:1-34:47. https://doi.org/10.1145/3267808

Bilal Khan. (2011). Effectiveness of information security awareness methods based on psychological theories. *AFRICAN JOURNAL OF BUSINESS MANAGEMENT*, *5*(26). https://doi.org/10.5897/AJBM11.067

Biselli, T., Utz, L., & Reuter, C. (2024). Supporting Informed Choices about Browser Cookies: The Impact of Personalised Cookie Banners. *Proceedings on Privacy Enhancing Technologies*. https://petsymposium.org/popets/2024/popets-2024-0011.php

Borberg, I. M., Hougaard, R., Rafnsson, W., & Kulyk, O. (2022). 'So I Sold My Soul': Effects of Dark Patterns in Cookie Notices on End-User Behavior and Perceptions. *Proceedings 2022 Symposium on Usable Security*. Symposium on Usable Security, San Diego, CA. https://doi.org/10.14722/usec.2022.23026

Bortz, A., Barth, A., & Czeskis, A. (2011). Origin Cookies: Session Integrity for Web Applications. *Web 2.0 Security and Privacy (W2SP)*.

Bostan, A. (2015). Impact of education on security practices in ICT. *Tehnicki Vjesnik - Technical Gazette*, *22*(1), 161–168. https://doi.org/10.17559/TV-20140403122930

Chanchary, F., & Chiasson, S. (2015). *User Perceptions of Sharing, Advertising, and Tracking*. 53–67. https://www.usenix.org/conference/soups2015/proceedings/presentation/chanchary

Chen, C. C., Dawn Medlin, B., & Shaw, R. S. (2008). A cross-cultural investigation of situational information security awareness programs. *Information Management & Computer Security*, *16*(4), 360–376. https://doi.org/10.1108/09685220810908787

Clarke, N., Li, F., Furnell, S., Stengel, I., & Ganis, G. (2016). Information security and practice: 11th International Conference on Cyber Warfare and Security. *Proceedings of the 11th International Conference on Cyber Warfare and Security, ICCWS 2016*, 81–89.

Dincelli, E., & Goel, S. (2015). *Research Design for Study of Cultural and Societal Influence on Online Privacy Behavior*.

Dunning, D., Heath, C., & Suls, J. M. (2004). Flawed Self-Assessment: Implications for Health, Education, and the Workplace. *Psychological Science in the Public Interest*, *5*(3), 69–106. https://doi.org/10.1111/j.1529-1006.2004.00018.x

Ericsson, A., Prietula, M., & Cokely, E. T. (2007). The making of an expert. *Harvard Business Review*. https://www.semanticscholar.org/paper/The-making-of-an-expert.-Ericsson-Prietula/6e7ecb2754cc3150c90ac83c106f5be7066cde73

Ericsson, K. A., Hoffman, R. R., Kozbelt, A., & Williams, A. M. (Eds.). (2018). *The Cambridge Handbook of Expertise and Expert Performance* (2nd ed.). Cambridge University Press. https://doi.org/10.1017/9781316480748

EUR-Lex. (2009, November 25). *Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws*. Your Europe. http://data.europa.eu/eli/dir/2009/136/oj

EUR-Lex. (2016, April 27). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Http://Data.Europa.Eu/Eli/Reg/2016/679/Oj. http://data.europa.eu/eli/reg/2016/679/oj

Fernandes, T., & Pereira, N. (2021). Revisiting the privacy calculus: Why are consumers (really) willing to disclose personal data online? *Telematics and Informatics*, *65*, 101717. https://doi.org/10.1016/j.tele.2021.101717

Fertig, T., & Schütz, A. (2020). *About the Measuring of Information Security Awareness: A Systematic Literature Review*. https://doi.org/10.24251/HICSS.2020.798

Flinn, S. (n.d.). *A Flock of Birds, Safely Staged*.

Furnell, S. (2005). Internet threats to end-users: Hunting easy prey. *Network Security*, *2005*(7), 5–9. https://doi.org/10.1016/S1353-4858(05)70258-0

Gironda, J. T., & Korgaonkar, P. K. (2018). iSpy? Tailored versus Invasive Ads and Consumers' Perceptions of Personalized Advertising. *Electronic Commerce Research and Applications*, *29*, 64–77. https://doi.org/10.1016/j.elerap.2018.03.007

Gobet, F. (2006). *The Cambridge handbook of expertise and expert performance*. https://www.semanticscholar.org/paper/The-Cambridge-handbook-of-expertise-and-expert-Gobet/69d233b61d0101c14b2ef1cbb9e9673420247c7e

Graßl, P., Schraffenberger, H., Zuiderveen Borgesius, F., & Buijzen, M. (2021). Dark and Bright Patterns in Cookie Consent Requests. *Journal of Digital Social Research*, *3*(1), 1–38. https://doi.org/10.33621/jdsr.v3i1.54

Greenberg, E. A., & Long, C. O. (2003). What are cookies?: *Nursing*, *33*(6), 76. https://doi.org/10.1097/00152193-200306000-00059

Ha, V., Inkpen, K., Al Shaar, F., & Hdeib, L. (2006a). An examination of user perception and misconception of internet cookies. *CHI '06 Extended Abstracts on Human Factors in Computing Systems*, 833–838. https://doi.org/10.1145/1125451.1125615

Ha, V., Inkpen, K., Al Shaar, F., & Hdeib, L. (2006b). An examination of user perception and misconception of internet cookies. *CHI '06 Extended*

Abstracts on Human Factors in Computing Systems, 833–838. https://doi.org/10.1145/1125451.1125615

Habib, H., Li, M., Young, E., & Cranor, L. (2022). "Okay, whatever": An Evaluation of Cookie Consent Interfaces. *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, 1–27. https://doi.org/10.1145/3491102.3501985

Hänsch, N., & Benenson, Z. (2014). Specifying IT Security Awareness. *2014 25th International Workshop on Database and Expert Systems Applications*, 326–330. https://doi.org/10.1109/DEXA.2014.71

Hovnik, A., Jelovčan, L., Mihelic, A., & Vrhovec, S. (2022). Exploring the Associations between Website Trustworthiness, Cookie Consent and Taking an Online Survey | Request PDF. *ResearchGate*. EICC 2022: European Interdisciplinary Cybersecurity Conference. https://doi.org/10.1145/3528580.3532991

Jayakumar, L. N. (2021). Cookies 'n' Consent: An empirical study on the factors influencing of website users' attitude towards cookie consent in the EU. *DBS Business Review*, *4*. https://doi.org/10.22375/dbr.v4i0.72

Jiang, X., Goh, T.-T., & Liu, M. (2022). On Students' Willingness to Use Online Learning: A Privacy Calculus Theory Approach. *Frontiers in Psychology*, *13*. https://doi.org/10.3389/fpsyg.2022.880261

Johnson, K. (2010). Expertise in language learning and teaching. *ELT Journal*, *64*(2), 217–218. https://doi.org/10.1093/elt/ccp104

Kruger, H., Flowerday, S., Drevin, L., & Steyn, T. (2011, August 1). *An assessment of the role of cultural factors in information security awareness*. https://doi.org/10.1109/ISSA.2011.6027505

Kulyk, O., Hilt, A., Gerber, N., & Volkamer, M. (2018). 'This Website Uses Cookies': Users' Perceptions and Reactions to the Cookie Disclaimer. *Proceedings 3rd European Workshop on Usable Security*. European Workshop on Usable Security, London, England. https://doi.org/10.14722/eurousec.2018.23012

Leon, P. G., Ur, B., Wang, Y., Sleeper, M., Balebako, R., Shay, R., Bauer, L., Christodorescu, M., & Cranor, L. F. (2013). What matters to users? Factors that affect users' willingness to share information with online advertisers. *Proceedings of the Ninth Symposium on Usable Privacy and Security*, 1–12. https://doi.org/10.1145/2501604.2501611

Leonard, D., Barton, G., & Barton, M. (2013). Make yourself an expert. *Harvard Business Review*, *91*(4), 127–131, 143.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, *54*(1), 471–481. https://doi.org/10.1016/j.dss.2012.06.010

Li, Y., Kobsa, A., Knijnenburg, B. P., & Nguyen, M.-H. C. (2017). Cross-Cultural Privacy Prediction. *Proceedings on Privacy Enhancing Technologies*. https://petsymposium.org/popets/2017/popets-2017-0019.php

Ma, E., & Birrell, E. (2022). Prospective Consent: The Effect of Framing on Cookie Consent Decisions. *Extended Abstracts of the 2022 CHI Conference* *on Human Factors in Computing Systems*, 1–6. https://doi.org/10.1145/3491101.3519687

Majumdar, A., & Bose, I. (2016). Privacy Calculus Theory and Its Applicability for Emerging Technologies. In V. Sugumaran, V. Yoon, & M. J. Shaw (Eds.), *E-Life: Web-Enabled Convergence of Commerce, Work, and Social Life* (pp. 191–195). Springer International Publishing. https://doi.org/10.1007/978-3-319-45408-5_20

Mallela, S. S., & Jonnalagadda, S. K. (2018). Internet Security—A Brief Review. In J. Anguera, S. C. Satapathy, V. Bhateja, & K. V. N. Sunitha (Eds.), *Microelectronics, Electromagnetics and Telecommunications* (pp. 889–894). Springer. https://doi.org/10.1007/978-981-10-7329-8_92

McDonald, A., & Cranor, L. (2010). *Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising*.

Mittal, S. (2016). *Understanding the Human Dimension of Cyber Security* (SSRN Scholarly Paper No. 2975924). https://papers.ssrn.com/abstract=2975924

Montero, B. G. (2016). *Thought in Action: Expertise and the Conscious Mind*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199596775.001.0001

Njenga, K., & Ndlovu, S. (2012). On privacy calculus and underlying consumer concerns influencing mobile banking subscriptions. *2012 Information Security for South Africa*, 1–9. https://doi.org/10.1109/ISSA.2012.6320453

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020a). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10.1145/3313831.3376321

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020b). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10.1145/3313831.3376321

Núnez-Barriopedro, E., Cuesta-Valiño, P., & Mansori-Amar, S. (2022). The role of perceived usefulness and annoyance on programmatic advertising: The moderating effect of Internet user privacy and cookies. *Corporate Communications: An International Journal*, *28*(2), 311–324. https://doi.org/10.1108/CCIJ-03-2022-0033

Passmore, C., Dobbie, A., Parchman, M., & Tysinger, J. (2002). Guidelines for constructing a survey. *Family Medicine*, *34*, 281–286.

Rahman, M. S. (2019). Does Privacy Matters When We are Sick? An Extended Privacy Calculus Model for Healthcare Technology Adoption Behavior. *2019 10th International Conference on Information and Communication Systems (ICICS)*, 41–46. https://doi.org/10.1109/IACS.2019.8809175

Rasaii, A., Singh, S., Gosain, D., & Gasser, O. (2023). Exploring the Cookieverse: A Multi-Perspective Analysis of Web Cookies. In A. Brunstrom, M. Flores, & M. Fiore (Eds.), *Passive and Active Measurement* (Vol. 13882, pp.

623–651). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-28486-1_26

Robertson, O., & Evans, S. (2020). Just how reliable is your internal reliability? An overview of Cronbach's alpha (α). *PsyPag Quarterly*, *1*(115), 23–27.

San Nicolas-Rocca, T., & Burkhard, R. J. (2019). Information Security in Libraries: Examining the Effects of Knowledge Transfer. *Information Technology and Libraries*, *38*(2), 58–71. https://doi.org/10.6017/ital.v38i2.10973

Schipper, B. C. (2014). *Awareness* (SSRN Scholarly Paper No. 2401352). https://doi.org/10.2139/ssrn.2401352

Schomakers, E.-M., Lidynia, C., & Ziefle, M. (2022). The Role of Privacy in the Acceptance of Smart Technologies: Applying the Privacy Calculus to Technology Acceptance. *International Journal of Human–Computer Interaction*, *38*(13), 1276–1289. https://doi.org/10.1080/10447318.2021.1994211

Sipior, J. C., Ward, B. T., & Mendoza, R. A. (2011). Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons. *Journal of Internet Commerce*, *10*(1), 1–16. https://doi.org/10.1080/15332861.2011.558454

Smit, E. G., Van Noort, G., & Voorveld, H. A. M. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior*, *32*, 15–22. https://doi.org/10.1016/j.chb.2013.11.008

Smith, A. F., Pope, C., Goodwin, D., & Mort, M. (2006). What defines expertise in regional anaesthesia? An observational analysis of practice†. *BJA: British Journal of Anaesthesia*, *97*(3), 401–407. https://doi.org/10.1093/bja/ael175

Srivastava, D. K., & Roychoudhury, B. (2021). Understanding the Factors that Influence Adoption of Privacy Protection Features in Online Social Networks. *Journal of Global Information Technology Management*, *24*(3), 164–182. https://doi.org/10.1080/1097198X.2021.1954416

Strycharz, J., Smit, E., Helberger, N., & van Noort, G. (2021). No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies. *Computers in Human Behavior*, *120*(106750). https://doi.org/10.1016/j.chb.2021.106750

Tilastokeskus. (2023, December 12). *Väestön tieto- ja viestintätekniikan käyttö | Tilastokeskus*. https://stat.fi/tilasto/sutivi

Tilastokeskus. (2024, October 24). *Väestörakenne | Tilastokeskus*. https://stat.fi/tilasto/vaerak

Torabi, S., & Beznosov, K. (2013). Privacy Aspects of Health Related Information Sharing in Online Social Networks. *HealthTech*. https://www.semanticscholar.org/paper/Privacy-Aspects-of-Health-Related-Information-in-Torabi-Beznosov/d009e382cea86dbe22c06052d12887fbd3369191

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security Awareness on information technology professionals' behavior. *Computers & Security*, *79*, 68–79. https://doi.org/10.1016/j.cose.2018.08.007

Trevisan, M., Traverso, S., Bassi, E., & Mellia, M. (2019). 4 Years of EU Cookie Law: Results and Lessons Learned. *Proceedings on Privacy Enhancing Technologies*, *2019*(2), 126–145. https://doi.org/10.2478/popets-2019-0023

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2010). Analyzing Information Security Awareness through Networks of Association. In S. Katsikas, J. Lopez, & M. Soriano (Eds.), *Trust, Privacy and Security in Digital Business* (pp. 227–237). Springer. https://doi.org/10.1007/978-3-642-15152-1_20

Ur, B., Leon, P. G., Cranor, L. F., Shay, R., & Wang, Y. (2012). Smart, useful, scary, creepy: Perceptions of online behavioral advertising. *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 1–15. https://doi.org/10.1145/2335356.2335362

Vásquez Duque, O. (2024). *Beyond the Banner: Exploring User Knowledge of Cookies and Attitudes Toward Targeted Advertising* (SSRN Scholarly Paper No. 4815717). Social Science Research Network. https://doi.org/10.2139/ssrn.4815717

Wheeler, M., Saka, S., & Das, S. (2022). *User Perception and Actions Through Risk Analysis Concerning Cookies* (No. arXiv:2211.07366). arXiv. https://doi.org/10.48550/arXiv.2211.07366

White, R. W., Dumais, S. T., & Teevan, J. (2009). Characterizing the influence of domain expertise on web search behavior. *Proceedings of the Second ACM International Conference on Web Search and Data Mining*, 132–141. https://doi.org/10.1145/1498759.1498819

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

APPENDIX 1 SURVEY FORM

Website cookie consent and perception survey

Hello and thank you for participating in this study!

The purpose of this study is to investigate how user background affects consent habits and perception of website cookies.

The information provided by the respondents will be processed anonymously and cannot be linked to the respondents. The information provided for research purposes will be treated with absolute confidentiality. Participation in the study is voluntary. By participating in the study, you agree that the provided information will be used for scientific research purposes.

By submitting your responses, you express your consent to the contents outlined in the research notice, privacy statement, and consent form found above.

You can withdraw your consent to participate in the study at any stage of the research.

For more information about the study, you can contact Emilia Kariuki at emamwako@jyu.fi.

Website cookies are small text files that the browser stores on the user's device. They contain information related to a specific website, such as login credentials, preferences, and details of tracking targeted advertising. Since 2018, the EU's General Data Protection Regulation came into force in Europe, according to which a company must obtain consent to the processing of personal data and clearly inform users about the collected data and its purpose.

Every response counts. Responding to the survey will only take about 5-10 minutes. The information provided by the respondents will be processed anonymously and cannot be linked to the respondents. Please respond to the questions as honestly and truthfully as possible.

Thank you for your time!

1. **I have work or study experience in the IT field. (This could mean computer science, software development, web development or similar computer related fields.)**

- Yes, I have work or study experience in the information technology field.
- No, I do not have work or study experience in the information technology field.
- Rule: Skip the next two questions if answered yes

2. **I have work experience in computer science, software development, web development or similar computer-related fields.**
- No work experience
- Over 0 - under 2 (years)
- Over 2 - under 4 (years)
- Over 4 - under 6 (years)
- Over 6 - under 8 (years)
- Over 8 - under 10 (years)
- Over 10 (years)

3. **I have study experience, a degree, or extensive training in computer science, software development, web development or similar computer-related fields.**
- Upper secondary school/vocational studies
- Polytechnic
- Bachelor's degree
- Master's degree
- Doctoral degree
- Occupational training (learning on the job)
- Other (please specify)

4. **How would you rate your level of expertise with computers/information technology?** (1 = I don't know anything about information technology, 5 = I am an expert in information technology)

5. **I decide not to use a website or purchase something online because I was unsure how my personal information would be used.** (1 = Never, 5 = Always)

6. **I read a website's privacy policy.** (1 = Never, 5 = Always)

7. **I delete cookies from my web browser.** (1 = Never, 5 = Always)

8. **I activate the "do not track" option in web browsers or use any tracking prevention tools.** (1 = Never, 5 = Always)

9. **I refuse to give information to a website because I feel it is too personal or unnecessary.** (1 = Never, 5 = Always)

10. **I feel like I have a general idea of what website cookies do**. (1 = Strongly disagree, 5 = Strongly agree)

11. **I feel like I have a general idea of what kind of information is stored/transmitted with website cookies** (1 = Strongly disagree, 5 = Strongly agree)

12. **I feel like website cookies can benefit internet users.** (1 = Strongly disagree, 5 = Strongly agree)

13. **I feel like there are positive aspects to website cookies.** (1 = Strongly disagree, 5 = Strongly agree)

14. **Please state why you chose that particular option in the previous question (question 13)**

15. **I feel like there are negative aspects to website cookies**. (1 = Strongly disagree, 5 = Strongly agree)

16. **Please state why you chose that particular option in the previous question (question 15)**

17. **How would you describe website cookies? Please use this space to respond freely about your thoughts and feelings about the subject.** (You can use bullet points, individual words or sentences)

18. **How do you generally deal with website cookies**? (1= Always decline, 5= Always accept)

19. **What kind of factors affect you accepting/declining the use of website cookies?** This could mean for example choosing one of the options because it's easier to choose, less harmful to you or just because you don't really know what website cookies do. Also, for example the reasoning could be that you believe website cookies have a positive or negative impact on your user experience.

20. **What is your gender?**
- Male
- Female
- Other

21. **What is your age?**
- Under 20
- 20-29
- 30-39
- 40-49

- 50-59
- 60 and older

22. **Education**

- Upper secondary school/vocational studies
- Polytechnic
- Bachelor's degree
- Master's degree
- Doctoral degree
- Occupational training (learning on the job)
- Other (please specify)