Ainohelena Väli-Klemelä

WHAT AFFECTS THE INTENTION TO CHANGE INFORMATION SECURITY BEHAVIOR WHEN USING BIOMETRIC AUTHENTICATION IN MOBILE PAYMENTS?

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2021

ABSTRACT

Väli-Klemelä, Ainohelena
What affects the intention to change information security behavior when using biometric authentication in mobile payments?
Jyväskylä: University of Jyväskylä, 2021, 76 pp.
Information Systems Science, Master's Thesis
Supervisor: Woods, Naomi

Mobile payments and the use of mobile payment applications have increased significantly over the past years. Several different types of authentication methods are used to make mobile payments, one of them being biometric authentication. The most common biometric authentication methods in mobile payments are fingerprint and facial recognition. However, due to the increased number of users, the information security threats towards mobile payments and biometric authentication have also increased. The users are forced to change their information security behavior accordingly. This thesis aimed to research what are the main factors that affect information security behavior change when using biometric authentication in mobile payments. In addition, it was researched whether there can be seen a difference between information security professionals and non-security professionals. The thesis consists of a literature review and an empirical research, that was conducted as a qualitative study. The data for this study was gathered by conducting semi-structured interviews with information security professionals and non-professionals. The data was analyzed through 7 different themes identified in the interviews: usability, trust and confidence, information security knowledge, the behavior of others, new perspective on life, new legislation and regulations, and perceived risks, threats, vulnerabilities and incidents. The results show that usability is the key factor affecting the information security behavior change. Users are willing to sacrifice their security in order to gain usability. In addition, trust towards the manufacturers affects the behavior. It was also observed that threats and incidents have an effect on the behavior, but the increased severity of the threat or incident also increases the effect. No significant differences were observed between the information security professionals and non-security professionals, which indicates that the information security knowledge of non-security professionals may have increased recently, and it should be researched more.

Keywords: biometric authentication, information security behavior, information security behavior change, information security professionals, mobile payment

TIIVISTELMÄ

Väli-Klemelä, Ainohelena
Mitkä asiat vaikuttavat tietoturvakäyttäytymisen aiottuun muutokseen käyttäessä biometrista tunnistautumista mobiilimaksaessa?
Jyväskylä: Jyväskylän yliopisto, 2021, 76 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Woods, Naomi

Mobiilimaksut ja mobiilimaksusovellusten käyttö ovat lisääntyneet merkittävästi viime vuosina. Käyttäjät käyttävät erityyppisiä tunnistautumismenetelmiä mobiilimaksujen suorittamiseen, mukaan lukien biometrinen tunnistautuminen. Yleisimmät mobiilimaksamisen biometriset tunnistustavat ovat sormenjälki- ja kasvojentunnistus. Käyttäjien määrän lisääntymisen myötä myös tietoturvauhat mobiilimaksuille ja biometriseen tunnistamiseen ovat lisääntyneet. Tämä johtaa siihen, että käyttäjien on pakko muuttaa tietoturvakäyttäytymistään vastaavasti. Tämän pro-gradu -tutkielman tarkoituksena oli tutkia, mitkä ovat tärkeimmät tekijät, jotka vaikuttavat tietoturvakäyttäytymisen muutoksiin, kun käytetään biometristä tunnistautumista mobiilimaksaessa. Lisäksi selvitettiin, onko tietoturva-alan ammattilaisten ja muiden kuin turvallisuusalan ammattilaisten välillä eroa. Tämä tutkielma koostuu kirjallisuuskatsauksesta ja empiirisestä tutkimuksesta, joka tehtiin kvalitatiivisena tutkimuksena. Tämän tutkimuksen tiedot kerättiin tekemällä puolistrukturoituja haastatteluja tietoturva-alan ammattilaisten ja ei-ammattilaisten kanssa. Tiedot analysoitiin haastatteluissa havaittujen seitsemän eri teeman avulla: käytettävyys, luottamus ja itsevarmuus, tietoturvatietoisuus, muiden käyttäytyminen, uusi näkökulma elämään, uudet lainsäädännöt ja määräykset sekä havaitut riskit, uhat, haavoittuvuudet ja tapahtumat. Tulokset osoittavat, että käytettävyys on keskeinen tekijä, joka vaikuttaa tietoturvakäyttäytymisen muutokseen. Käyttäjät ovat valmiita uhraamaan turvallisuutensa saadakseen käytettävyyttä. Lisäksi luottamus valmistajia kohtaan vaikuttaa käyttäytymiseen. Tutkielmassa havaittiin myös, että tietoturvauhilla ja -tapahtumilla on vaikutusta käyttäytymiseen, mutta uhan tai tapahtuman lisääntynyt vakavuus lisää myös sen vaikutusta. Tietoturva-alan ammattilaisten ja muiden kuin ammattilaisten välillä ei havaittu merkittäviä eroja, mikä saattaa osoittaa, että muiden kuin turvallisuusalan ammattilaistenkin tietoturvaosaaminen on nykyään melko korkea, ja sitä kannattaisi tutkia enemmän.

Asiasanat: biometrinen tunnistautuminen, tietoturvakäyttäytyminen, tietoturvakäyttäytymisen muutos, tietoturva-ammattilainen, mobiilimaksaminen

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Background

Using cash as a payment method has decreased rapidly over the past years, especially during the COVID-19 pandemic in 2020 and 2021, and using credit cards and other payment methods have increased. Mobile payments are one method that is quickly gaining users as owning a smartphone is becoming more common. This transition has taken place due to changes in the economy, technological developments on the Internet, the proliferation of social networks, and increased use of mobile devices. (Ramos de Luna, et al., 2019.) According to Statista, there's 3.8 billion smartphone users in the world in 2021, and the global amount of smartphone users increased by 40% between the years 2016 and 2020. Because smartphones are nowadays a widespread commodity, consumers benefit from the ease and convenience of paying for goods and services with this new payment channel. Mobile payment systems have adapted not only to mostly digital and mobile-free reality but also a new business environment that makes it easier to do business anywhere, at any time and to anyone. (Ramos de Luna, et al., 2019.)

Most smartphones also provide a biometric authentication, usually with fingerprint recognition and facial recognition technologies. Biometric authentication can work as an alternative to passwords as they do not need to be remembered. Biometric authentication can provide many benefits to users compared to traditional authentication methods, and thus many mobile payment application providers also provide the possibility to use biometric authentication methods to authenticate the user when making a payment. However, using physical features to identify oneself also brings new issues and threats compared to passwords and other traditional authentication methods. Biometric identifiers can reveal sensitive information about users, such as race, gender, or disease. (Phillips, Zou, & Li, 2017.) Providing biometric data to a company could compromise privacy and

eventually even lead to illegal espionage by governments or law enforcement agencies (Memon, 2017).

These threats can be minimized with sufficient information security behavior. Individual's information security behavior can be affected by many things, for example the user may change their information security behavior for the better as their knowledge and awareness of information security threats and countermeasures increase and they understand the impact of their own actions on the possible threats. (Lebek, et al. 2011.) The atmosphere and attitudes of the user's circle of acquaintances can also affect the user's behavior, if the circle of acquaintances become more security critical. (Wu, 2009.)

Mobile payments, biometric authentication and information security behavior are all quite well researched topics in the past. Previous research has looked into, for example, the security threats of mobile payments (Huh, et al. 2017), the adaptation of biometric authentication (Wolf, Kuber & Aviv, 2018 and 2019) and the comparison of security practices between information security professionals and non-security professionals (Ion, Reeder & Consolvo, 2015). However, there's no current studies examining all these aspects when they are combined, even though the amount of users using biometric authentication in mobile payments has increased significantly (Ahmed, et al. 2020; Choi, et al. 2020). This research focuses to examine what are the factors that affect the possible change of information security behavior when using biometric authentication in mobile payments. The study focuses on mobile payment applications and the use of biometric authentication methods in them and examines how information security behavior can change when using them. The aim is also to understand how much does increased information security knowledge influence the intended change. The research questions in this research are as follows "*What factors would affect the intention to change information security behavior in the context of using biometric authentication in mobile payments?*" and "*What differences can be seen in the intention to change information security behavior comparing information security professionals and non-professionals, in the context of using biometric authentication in mobile payments?*".

The first part of this study has been carried out as a literature review, so it provides a clear a review of scientific articles and literature in the field. In the search for sources the main databases have been Scopus and Google Scholar together with the JYKDOK database of the University of Jyväskylä. Top search terms have been "biometric authentication" combined with the terms "information security behavior", "change" and "mobile payments". Various combinations have also been used in the search phrases from the above terms. The main criteria for selecting sources are in addition to the content of the text, the reliability of the sources. Reliability has been assessed based on the number of citations, the publication channel, and other work by the authors. In addition, the content of the sources has been evaluated based on their year of publication to ensure up-to-date information.

A qualitative research was chosen as the research method in this study. A qualitative study focuses on a deeper understanding of the subject matter and research problem compared to a quantitative study that focuses on a large sample and statistics. In the case of this research, cloud services and their management

in organizations from a security perspective. The qualitative research will be conducted by interviewing a group of IT professionals specializing in information security and a group of people that have not studied nor worked within the information security field. The empirical material of the research is collected from these interviews.

1.2 Structure of thesis

The structure of the literature review of the research is as follows: chapter two defines mobile payment and discusses the information security related threats towards it that has been found in previous literature. Next, chapter three defines authentication in general and introduces different types of authentication methods, and defines the information security risks related to using biometric authentication in mobile payments. Chapter four gives a brief introduction to information security behavior as a concept, the differences in behavior between information security professionals and non-security professionals, and introduces the theoretical framework used in this research. The empirical research of the study begins in chapter five, which introduces the research method and the progress of the research. Chapter six presents the detailed results of the research interviews, and presents the recurring themes found in the interviews. Chapter seven then presents the reflection of the study and discusses the found results and compares them to the previous literature. Chapter eight is a summary of the study.

2 MOBILE PAYMENTS

Nowadays many refer to mobile commerce, which is an addition to the wider e-commerce industry. Mobile commerce can be defined as a form of electronic business that focuses specifically on mobile devices. The key forms of the mobile commerce include mobile payment and mobile banking. The clear distinction between the two is challenging, since they contain overlapping functions and can be part of the same entity (Jovanovic & Muñoz-Organero, 2011), and are susceptible to information security risks. In the next chapter I will elucidate on these definitions and refer further to the related information security risks.

2.1 The definition of mobile payment

At its widest, mobile payment is defined as any payment transaction using a mobile device such as a smartphone or tablet to initiate, activate and / or approve a payment transaction (Karnoukos, 2004). Alternatively, one definition of mobile payment is that at least the payer uses a mobile device to make the payment (Au & Kauffmann, 2008). These definitions therefore do not limit mobile payment to any specific application, and the definitions are not dependent on the location of the payer or payee. It should also be noted that mobile payments are not only limited to mobile or smartphone payments but are possible with any device using wireless network technologies (Karnouskos, 2004). It is important to notice that there's various ways to perform mobile payments, such as SMS messages and dedicated applications. In this literature review the focus is set on dedicated mobile payment applications.

It is common practice for mobile payments to be divided into two different types based on their method of operation: remote and local payments, also called contactless payments. In a remote payment, the user connects to the back end system of a mobile payment service using a mobile device and through mobile networks, whereas in a contactless payment the user makes a payment using a mobile device and short-range communication technologies (Agarwal, Khapra,

Menezes & Uchat, 2007). The use of mobile payment systems requires the customer to sign up for the service, which often includes installing an application on your mobile device. The customer can then use the application on a mobile device to make a payment. The customer may have pre-paid money in their account, or the service may charge directly from an associated bank account (Taylor, 2016).

Short-range Radio Frequency Identification technology (RFID) is often used for contactless payments. The technology is based on NFC (Near Field Communication), which enables data transfer between two devices, such as a consumer mobile device and a retail payment terminal. The payer takes their mobile device close to the payment terminal, usually less than 20 centimeters from the device to make a purchase. The payer usually has to verify the transaction by entering a password or a security code on the mobile device. (Liu, Kostakos & Deng, 2013.)

It is also worth noting that the mobile payment may be a so-called peer-to-peer (P2P) or consumer-to-business (C2B) payment. P2P payment is private payment between two service users, and they are typically remote. A commercial payment platform may be involved in the transaction, but the transaction itself is directly between two persons. P2P payments are popular, especially in developing countries, and are estimated to have enormous growth potential. For example, over 40 million money transfers, so-called red envelopes, were sent via WeChat in China, during Chinese New Year 2015 alone. The C2B payment, is a purchase transaction where the customer pays a company for the product or service. (Wang, Hahn & Sutrave, 2016.)

When using mobile payment applications, the payer needs to either sign into the application with a password or verify the payment within the application with a password. In the modern mobile devices, these passwords can be replaced by verifying the purchase with biometric authentication methods such as fingerprint recognition or facial recognition. A few identified mobile payment applications for contactless payment that allow the use of biometric authentication methods are briefly introduced in the following chapters.

2.2 Mobile payment applications

Mobile payments have been around already for over 20 years and several applications have been introduced during that period (Dahlberg, Huurros & Ainamo, 2008). In the past few years, plenty of new applications have been published and a few of them have become firmly established in the everyday life of Finnish consumers. The most downloaded and used mobile apps in the Finnish market are MobilePay, Pivo and Apple Pay.

MobilePay is a mobile payment application launched by Danske Bank in 2013 and was differentiated to an independent subsidiary MobilePay Finland Oy in 2018. MobilePay has over 5.8 million users in the Nordic countries. The app has been downloaded more than 1.6 million times in Finland. The application can be used by a customer at any bank, and according to MobilePay, more than half of those downloading the application use something else as their primary bank

than Danske Bank. With MobilePay, user can send and receive money P2P with phone number. In addition, users can pay with MobilePay at checkout or online with contactless payment, a 5-digit code or a QR-code. MobilePay requires an Android or iOS operating system from a smart device. Contactless payments in MobilePay use NFC and BLE (Bluetooth Low Energy) technologies. The BLE technology also allows iOS users to use MobilePay as a contactless payment method. (MobilePay, 2021.)

Pivo is an application developed by a Finnish bank Osuuspankki and its likewise launched in 2013. Initially, the main purpose of the application was to help track the revenue and expenditure of one's finances, but its goal from the beginning was to develop a mobile payment application. Now with Pivo, users can send and receive money P2P by phone number, pay at checkout as well as pay online. Pivo can be used by any bank's client and it works on Android, iOS, and Windows phones and it has over 1.2 million users in Finland. However, the contactless payment in Pivo can be used only with Android phones with NFC technology and by Osuuspankki clients. (Pivo, 2021.)

Apple Pay was launched for the Finnish market in 2017. With the application user can pay for both in online shops and in stores with contactless payment technologies. Prior to Apple Pay, many contactless payment methods, excluding MobilePay, have been successful only on Android devices because Apple has limited the Apple devices' NFC technology use only for themselves. Apple Pay works with all of Apple's latest devices by adding debit or credit card information to the application. However, Apple Pay doesn't support all credit and debit cards and in Finland it is only limited to 23 different card suppliers, including Nordea, Aktia, Danske Bank, Osuuspankki and American Express. (Apple, 2021.)

2.3 The information security of mobile payments

Users require confidentiality, authentication, data integrity, as well as non-repudiation as essential needs for making safe and secure transactions over the internet (Sharma, 2017.) The electronic payment systems need to have all the above protection attributes, as in a competitive market, users will not rely on an unsecure mobile system. As well as this, trust is exceptionally essential to gain approval from the users. (Hassan et al., 2020.) Many of the information security risks associated with mobile payment are the result of the mobile payment device being used for many different purposes and containing many different applications. Installing mobile device security and software updates is typically the responsibility of the user, which can further reduce device security. (Wang, Streff & Raman, 2012.) This may cause the device to be vulnerable for attacks and malwares. In addition to possible malware, mobile payment threats also include the loss or theft of a mobile device and the risks of malfunction. (Me, 2003)

Malware is one of the biggest threats to mobile payment systems and they are constantly growing in number (Bosamia & Patel, 2019; Wang et al., 2016). The

malware that threatens smart devices can be divided into three main categories: spyware, viruses, and trojans. Viruses spread from one device to another by replicating themselves. Often, they are hidden in a file that is downloaded on the mobile device. Viruses can also be transmitted via Bluetooth. Trojans are often disguised as games, security updates or other desired application that the user downloads to their device. Most of the malware on smartphones belongs to the group of spywares that aims to collect user information unobserved. It is estimated that over 60 percent of the Android operating system malware is spyware. (Wang et al., 2012)

Many mobile payment systems rely on SSL / TLS protocols to protect the data on the network. However, there are critical vulnerabilities found in these protocols that could be exploited by attackers. (Wang et al., 2016.) Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are encryption protocols designed to protect communications (Oppliger, 2016). In 2014 a major vulnerability called Heartbleed Bug was revealed in OpenSSL, an open source SSL / TLS implementation. By exploiting this vulnerability, a hacker could gain access to personal data such as credit card numbers, usernames, and passwords. Perhaps most worrying was that it also allowed the hijacking of encryption keys and appearing as or controlling a server. Many of the most popular online services, such as Facebook, Google and Twitter, were affected by this vulnerability. (Gujrathi, 2014.) SSL / TLS protocols are also vulnerable to Man in the Middle attacks, which are a known threat in mobile payments (Bosamia & Patel, 2019).

In SRFC2828, a Man in the Middle (MitM or MITM) attack is defined as an active eavesdropping attack in which an attacker intercepts and selectively transforms data in order to disguise itself as one or more of connective parties. (Shirey, 2003) In a typical MitM attack, the attacker is set between the user and the server so that they can communicate separately with both parties. This way both the user and the server think that they are communicating directly with one another without knowing the presence of the attacker. Although SSL / TLS protocols in principle provide sufficient protection to MitM attacks, the attacks are a serious threat to many SSL / TLS based web applications. There are two main reasons for this: firstly SSL / TLS server authentication is often poorly implemented or not implemented at all by a naive end user. This results in a situation where the user ends up talking to a dishonest intermediary and thus gives away information to them. Second, SSL / TLS session setup is often not connected to the user authentication, which allows the attacker to cheat the server with the authentication information obtained. (Oppliger, Hauser & Basin, 2006.)

Bosamia and Patel (2019) also raise tampering with the mobile payment application and the use of root kits as a vulnerability for the mobile payment applications. This means that an attacker chooses to backdoor a mobile payment application to capture login details and send these to an attacker-controlled server. By this attacker can download and upload any data from user application. According to Bosamia and Patel (2019), other application-based threats are, for example, weaknesses in biometric identification for initial authorization of transactions, which may cause unauthorized access to the application, and that the credit

card information is not stored encrypted in Secure Element or processed in Trusted Execution Environment, which may cause the credit card information to be available in plain text to an attacker. (Bosamia & Patel, 2019.)

The information security of mobile payments can be enhanced with various methods. Encryption technologies play an important role in protecting mobile payments in the open networks that have very little or no physical security. (Isaac & Sherali, 2014) Protecting mobile devices from malware is also extremely important. There are different models for detecting and preventing malicious software, and it includes participation from both the application developers and end users. The developers should follow secure programming and privacy practices to minimize the access to unnecessary information that could be exploited by attackers. The end user of the mobile device must ensure that they install a good quality mobile security solution to the device and only download applications from trusted marketplaces. (Ramu, 2012.)

User authentication is an extremely important function of mobile payment for safety. Mobile devices themselves often contain authentication methods such as Personal Identification Number (PIN) and Personal Unblocking Key (PUK). These authentication methods utilize a common SIM card in mobile devices. The most common approach to enhance the information security is to make the user use username and password sign-up when performing mobile payments. (Kadhiwal & Zulfiquar, 2007.) Authentication is explained in more detail in the next chapter.

3 AUTHENTICATION

We need to authenticate ourselves to different services and environments every day at work and in everyday life. We need access to workstations, emails, internet services and business environments. The most commonly used means of authentication is username and password (Sabzevar & Stavrou, 2008), but it is not the only authentication method in use. Using only username and password for authentication are seen to be less secure, because a perpetrator can easily guess or get to know the password. Thus, there are more secure authentication methods in use nowadays, such as biometric authentication methods (Wang, et al., 2020.), which will be presented in more detail in this chapter.

The authentication process consists of two parts, the information system factor identification and verification of a presumed identity (Bailey, Okolica & Peterson, 2014). In this literature review, the focus is on human-to-machine authentication or in other words user authentication. In user authentication, the most important target of the authentication process is to answer the question "Is this person the one they claim to be?" (O'Gorman, 2003.) This chapter describes the definition of authentication and gives a brief introduction to different types of authentication methods.

3.1 Definition and methods of authentication

Authentication is one of the most important aspects of an information system's components (Barkadehi et al., 2018). It is a process in a distributed information system or other information network whereby one factor affecting an information system entity verifies its own identity to another. Verifiable information system factors may include, for example, human, computer or network service. (Altinkemer & Wang, 2011.) At its simplest, authentication can be described with one phrase: authentication is the verification of the identity of the source of information.

Authentication is often a prerequisite for accessing the resources of the target system (Braz & Robert, 2006) and is considered as one of the security infrastructures key components (Burrows, Abadi & Needham, 1990). Proper authentication can effectively reduce, for example, the risk of impersonation such as impersonating another person or organization, which is considered one of the greatest security threats to information systems. According to O'Gorman (2003), authentication between a human and a computer or other network service is much less secure than authentication between two computers or a service on a network. A person who identifies has limitations and weaknesses, such as capacity and performance; user authentication can even be considered to be the Achilles heel of secure systems (O'Gorman, 2003).

Most often, authentication is based on some encryption key or other information shared by the parties (Burrows et al., 1990). Menkus (1988) has divided the authentication methods used into three different authentication factors. According to Menkus, authentication can be based either on a person's knowledge, possession or inherence. Knowledge-based authentication methods are the most commonly used methods for identifying information systems. They are based on the questions "what do you know" or "what do you remember". The most well-known authentication type in the category is the traditional string-based password that has retained position as the most used authentication type (O'Gorman, 2003), even though researchers have identified the associated security and availability issues already for 40 years (Bonneau et al., 2012). The drawback of the knowledge-based method is that the authentication information it requires, such as a password, can be revealed and thus used by the wrong person, which exposes the target system to impersonation (Bailey, Okolica & Peterson, 2014, Wang, et al., 2020).

The possession-based authentication method means that a physical object, such as a debit or smart card, is required for authentication. The device may also be, for example, an active device that generates single-use authentication codes for the user. Possession-based methods are based on the question of "what do you own". (O'Gorman, 2003.) A drawback to the possession-based authentication method is that the authentication device may be lost or stolen, which can get it into the wrong hands (O'Gorman, 2003; Bailey et al.,2014). In addition, one of the problems of possession-based authentication methods is that authentication or system access will be prevented if the authentication tool is not available.

Because using fingerprint recognition and facial recognition as the authentication method of performing mobile payments is increasing significantly, this research focuses more deeply on inheritance-based authentication methods, also referred to later as biometric authentication methods. An inherence-based authentication method means that a single user can be identified by a specific physical or chemical property or based on a measurable specific characteristic that is based on user behavior. Instead of identifying yourself with the questions "what do you own", "what do you know" or "what do you remember", a person-specific authentication method can answer the question of "who you are". Compared to knowledge-based and possession-based authentication methods, an inherence-

based approach better addresses the question of the identity of an identifiable person by combining both components, i.e. user identification and identity verification (Bailey et al., 2014), because the issue of authentication is with the person themselves and not with the information being shared or the physical object itself. However, the knowledge-based authentication methods are relatively easy to use and quite familiar to broader userbase. Thus, the knowledge-based authentication methods usually show very high usability and adaption rate. But as mentioned before, the knowledge-based passwords are also easy to be leaked or guessed by an attacker, leading to a low security level. (Wang, et al., 2020.) Although an authentication device based on a person's special characteristics is more secure, copying or imitating it is possible, though much more challenging than other authentication methods. (O'Gorman, 2003; Jain, Flynn & Ross, 2007) Biometrics are generally divided into physiological and behavioral biometrics (Bergadano, Gunetti & Picardi, 2002). These methods are explained more in depth in the following chapters.

3.2 Biometric authentication methods

As mentioned in the previous chapter, biometric authentication methods can be divided into two categories: behavioral and physiological. A good biometric method should contain seven features. The first characteristic is universality, everyone must have that feature. The second requirement is individuality, as the feature should be able to distinguish between two people. Third, the property should be permanent, something that is independent of time or changing climatic conditions. Fourth, the feature should be collectible and quantifiable. Fifth, feature should be generally accepted, meaning that people should be able to use technology without feeling it irritating or intrusive. Sixth, the feature must be capable of good performance in recognition accuracy and recognition duration. Lastly, the ability of fraudulent people and techniques to cheat the biometric system should be very insignificant. (Clarke, 1994.)

Many industries are already using biometrics or are in the process of implementing them. Elliott, O'connor, Bartlow, Robertson and Guest (2015) refer to the use of biometric technologies in the automated border management, banking and healthcare sectors. The use of biometrics has also been chosen widely for high security access control (Meenakshi & Padmavathi, 2009). They have also become increasingly common in consumer information system applications, particularly in mobile technology, thanks to evolving facial and fingerprint recognition technologies. (Jain et al., 2007.) This chapter describes different types of biometric authentication methods, behavioral biometrics and physical biometrics, and the information security related risks especially when using biometric authentication in mobile payments.

3.2.1 Behavioral biometrics

Behavioral biometrics measures the characteristics of an individual's behavior. It is usually used as an authentication method on various information systems based on features such as voice recognition (Renaud, 2005), keyboard dynamics (Bergadano et al., 2002), mouse dynamics (Ahmed & Traore, 2007), or other analysis of graphical user interface and user interaction (Bailey et al., 2014). The method is based on analyzing behavior by utilizing previously recorded behavior data from the user.

Authentication can be either static or dynamic. Static authentication means that a user is identified once, for example, at login, which is the method that is most used in knowledge, possession and inherent authentication methods. (Ahmed & Traore, 2007.) Behavioral authentication has the advantage of dynamic authentication, which means that the user can be constantly identified in the background also after the actual logon event. Dynamic authentication prevents a user of a secure information system from switching users during an authenticated session. (Bailey et al., 2014; Ahmed & Traore, 2007.)

Voice recognition requires methods to identify a person by voice sample to voice samples in the database (voice print) by comparison. Taking a sound sample is easy, it does not require very much devices like many other biometric identifiers. The sound sample also does not take much time, although due to the reliability of the sample it should be taken two to three times. The sound or speech generation is unique mainly to the vocal organs because of immutability. Instead, speech can be different at the time of the sound sample, because the mental and physical state of the person influences the sound produced. A sound sample can be provided by means of communication and thus does not require the physical presence of a person. Automatic speaker recognition can be divided into text-based or text-independent recognition. (Bhattacharyya et al. 2009.)

Keyboard and mouse dynamics can be seen as another type of behavioral authentication method. According to some research, the use of a computer keyboard and the resulting tapping rhythm are individually distinguishable from others. Pato and Millet (2010) claim, however, that keyboard dynamics are very much dependent on circumstance. A person's emotional state can influence at what pace the person is using the keyboard. In addition, the person's posture and the position in which they are typing affect the use of the keyboard. The type of computer keyboard might also have an effect on typing. A mouse tap and movement can be unique and recognizable and thus it could be used as a biometric authentication method. (Pato & Millet, 2010.)

3.2.2 Physiological biometrics

If behavioral biometrics focus on how a person does things, physiological biometrics are the characteristics that a person has that usually can’t be changed easily. According to Bolle et al. (2013) the most commonly used physiological biometrics are handprint recognition, iris recognition, face recognition and fingerprint recognition.

Handprint recognition is a technology where a person is identified by using the geometric and structural features of their hand. In adulthood, these characteristics are stable for a long time. In addition to not changing, two persons' handprints can't be identical. (Kong et al., 2008.) According to Pato and Millet (2010), obtaining the geometry of a hand is easy because it can be measured with the width of the palm and the width and length of the fingers. There are two types of hand geometry recognition techniques: the back of the hand and the side profile can be used or the image or print of the palm. A handprint recognition can also be done with infrared cameras that detect the vascular systems in hands. (Pato & Millet, 2010.)

Iris recognition utilizes the unique features of one or both eyes, patterns inside the eye. Iris recognition is popular because they are clearly visible but well protected from the effect of time and the environment. In addition, they can be seen from a distance. (Daugman, 2009.) Like handprint or fingerprint, iris textures are stable and unique, even with identical twins, and are very difficult to fake surgically (Leo, De Marco & Distante, 2014). According to Connell, Ratha, Gentile and Bolle (2013), the popularity of iris recognition has increased because it is accurate, the sensors it requires are inexpensive and have better usability than touch biometric methods such as fingerprinting authentication.

Fingerprint authentication traditionally refers to automatic biometric method that attempts to authenticate two comparative fingerprints based on previously collected data from fingerprints. The fingerprint recognition device can capture the imprint with an optical camera, ultrasound or capacitance sensors (Maeva & Severin, 2009). In addition to traditional fingerprint pattern recognition, a finger can be used for biometric recognition by depicting its vascular pattern (Kathuria, 2010) or by swiping a finger over the temperature sensor (Coventry, De Angeli & Johnson., 2003). Fingerprint recognition technology is present in people's everyday lives, even on a daily basis. The increase in the number of touch-enabled smart devices has increased the need for compatible authentication methods (Koundinya et al., 2014) and several manufacturers of mobile phones, tablets, and other smart devices have added fingerprint-based sign-in to their devices.

Facial recognition captures the spatial geometry of facial features. It can be done with mobile devices that have a high-quality camera. Different vendors use different face recognition methods, but all focus on measuring key facial features. Because human face can be captured by the camera at a distance, face detection can be done without the subject may knowing that they have been detected. (Woodward Jr et al., 2003.) Facial recognition verifies the user by measuring the facial features such as the distance between eyes or corners of mouth. The face recognition process does not require users to adjust their faces to a predetermined fixed point, but rather to take a facial image only by looking at the screen of their mobile devices so that their face should be included in whole in the image. (Ijiri, Sakuragi & Lao, 2006.)

Physiological biometrics are used for identification also by governments, for example, by issuing biometric passports. Biometric passports contain machine-readable biometric data of the person to whom they are issued in addition

to the traditional information contained in the passport. The standard for biometric passports is defined by the International Civil Aviation Organization, which allows for the collection and storage of the following biometric features: face, fingerprints and iris. The picture of the passport holder is stored in all biometric passports, but storing other biometric data is optional. The biometric passport is similar to traditional passports, but additional biometric information can be read from the passport at the border and can be used for automatic identification of the passenger. For example, in Finland the biometric passports contain a photo of the person for facial recognition and also fingerprint information for fingerprint recognition. (Heimo, Hakkala & Kimppa, 2011.)

Using a biometric authentication method instead of username and password or just instead of password is increasing also in mobile payments, and it in turn increases the possibilities to many new information security issues. The information security of biometric authentication methods is described in the following chapter.

3.3 The information security of biometric authentication in mobile payments

From all the biometric authentication methods presented in this literature review, the most widely used ones for making mobile payments are fingerprint and facial recognition technologies. The reliability of biometric authentication methods can be evaluated with false acceptance rate (FAR) and false rejection rate (FRR). The false acceptance rate measures the probability that the biometric authentication method will accept the wrong person's login attempt. Instead, the false rejection rate is used to measure the likelihood of the right person signing in with a failed attempt. The lower the meter values, the more reliable the biometric authentication method is. (Jain et al., 2007.)

The advantage of a biometric authentication method is that it is difficult to duplicate the authentication source and that the authentication data can hardly be passed on to another person, so it effectively prevents multiple people from signing in with the same user information (O'Gorman, 2003). However, according to O'Gorman (2003), static biometric signals can be easily captured without sufficient hardware and network security, so biometric authentication should not be used without multi-factor authentication. Captured biometric information can be used for example as a replay attack or spoofing tool.

Replay attack is a major threat to biometric authentication. This is done by sending back the information previously provided by the legitimate user to the verifier. An attacker can retrieve data either through a sniffing device or sniffer software during a successful authentication process or by collecting the remaining result on the sensor after successful authentication.

Spoofing is an attack where a malicious individual pretends to be someone else. In biometrics, spoofing means a process that cheats a biometric system by

providing a forged biometric copy of legitimate user biometrics. Spoofing techniques are different between the biometric technologies, but one thing they have in common is that they all involve presenting a fake biometric sample to the sensor.

In addition to the technical attacks, the most common threats towards biometric authentication systems include falsification of biometric features and attacks on the database. (Jain et al., 2016.) In the event of an attack towards the database and possible consequent data leak, biometric data, such as models of users' fingerprints, can fall into the wrong hands, which can cause widespread inconvenience to users. (Jain & Nandakumar, 2012.) If an attacker cannot modify the database, it still might have the ability, for example, to prevent legitimate users from authenticating or to allow outsiders to access the system. (Ratha et al., 2001). What makes the leakage of biometric data problematic is that users cannot change biometric features in the same way compared to traditional alphanumerical passwords, making the leaked biometric feature unusable for authentication. (Jain & Nandakumar, 2012).

Since the biometric features used for identification and authentication are not secret like a memory based password or similar can be, and have sometimes even been published on the internet when posting pictures of individuals on social media, an attacker can attack the biometric system through data simulation or falsification. However, majority of the research shows that an attacker would need a great amount of effort to create a synthetic biometric feature. (Xiao, 2005.) Furthermore, in recent years, cheating the biometric authentication systems has become more difficult as the authentication methods have evolved and, for example, fingerprint and face detectors have introduced technologies that identify a living person (Rui & Yan, 2018). This development can be seen, for example, in the study of Sadasivuni, Houkan, Taha and Cabibiha (2017) in which they were able to identify an artificial fingerprint with 100 percent certainty among 300 fingerprints with the device they developed. On the other hand, in his research Adler (2003) found out that when trying to reconstruct a facial image, his method only needs a few thousand iterations to form an image that can be mixed with the original image at a very high level of confidence. This could potentially fool a biometric authentication sensor. Also, the possibility of automatic face detection without the user's permission has raised concerns about people's privacy and security (Guo, Xiang, & Li, 2019). The concern is not pointless, as facial recognition has already been proven to be used for mass surveillance of people in addition to social media and smart devices (Lehto, 2019).

When using authentication based on the person's characteristics one of the advantages is that the authentication tool is always available. The downside is that feature-based authentication is prevented if the feature used to identify a person changes, for example, as a result of aging. Human aging has direct effects, among other things to skin elasticity, lung oxygen uptake, and muscle strength, which affect features such as face, fingerprint, palm geometry, and sound. (Lanitis, 2010.) For example, with fingerprint recognition, it must be recognized that aging leads to a loss of collagen, leaving the aging skin loose and dry. This then

affects the quality of fingerprints, which makes the sensors not work properly. The quality of fingerprints varies by age group and the variance is more pronounced in the age groups of 62 years and older. (Modi et al., 2007.) Facial features also change with age, as the aging of soft and hard tissue reshapes the features, which yet again may cause the sensors used in facial recognition technology not to recognize the user. (Leung, Fong & Hui, 2007). In addition to the direct effects of natural aging, human biometrics are also affected by various injuries and illnesses such as diabetes which may cause the person to gain weight fast and face recognition might stop working. (Lanitis, 2010.) The changing of the biometric features can be seen as the most common security risk for biometric authentication.

4 INFORMATION SECURITY BEHAVIOR AND THE THEORETICAL FRAMEWORK OF INFORMATION SECURITY BEHAVIOR CHANGE

The following chapter describes some of the factors affecting user information security behavior and highlights the differences between information security professionals and non-professionals. The theoretical framework of information security behavior change used in this research is presented in the section 4.4.

4.1 The definition of information security behavior

For the purposes of this research, information security behavior refers to the way a user behaves on their mobile device and in networks and how they consider information security in their behavior. Information security behavior also refers to the activities that end users must follow to maintain security and are defined in security guidelines (Padayachee, 2012). For home users, however, there are no security guidelines and the user is self responsible for the choices they make considering information security. When talking about information security behavior, it is important to acknowledge the difference between planned behavior and actual behavior. This means that although the individual is aware of possible information security problems and they plan to behave in a certain way, it is a different matter whether they follow the planned behavior. (Thomson & von Solms, 1998.)

Most times, users access the internet from their personal device, which is very often a desktop computer, laptop, mobile device, or tablet. Personal devices usually contain confidential information and when devices containing such information are connected to the internet, the risks of data theft or loss increase. In addition, the owner of the device is often personally responsible for the security of the device. However, traditional desktops and laptops and their browsers are often better protected than, for example, mobile devices and tablets and the browsers offered for them (Virvilis, et al., 2014; Alasuutari, 2016.) In the future,

as much attention should be paid to the security of mobile devices as to computers, as mobile devices are often used in the same way as computers, and both contain information that is sensitive to the user, such as payment data from the mobile payment applications.

The information security behavior is strongly influenced by information security awareness (Hwang et al., 2019). It has been suggested that information security awareness is the most significant mitigating factor in security breaches. Good information security awareness is usually a key factor in successful information security. (Furnell & Clarke, 2012.) The effects of information security awareness to information security behavior are explained in more detail in the following section.

4.2 Information security awareness

It has been studied that the general level of education does not significantly affect an individual's security awareness. However, educational background related to information security clearly correlates with information security awareness. (Pattinson, Butavicius, Parsons, McCormac & Calic, 2015.) The problem with security-related training for non-professional users is its cost-effectiveness and problems with availability. Very few non-professionals are able to participate in information security training (Li & Siponen, 2011.) It can be claimed that often non-professionals are not even aware of the possibility of training, because they do not understand the relevance of information security or know how to seek training.

Studies have found that security awareness and security behavior often go hand in hand. When the user's awareness of various risks and threats grow, so does their attitude towards information security and the individual behavior becomes safer. However, in some cases, there is no change in security behavior, though security awareness would increase or be high from the starting point. (Öğütçü, Testik, & Chouseinoglou, 2016.) Several studies have found that non-professional users are unlikely to significantly improve their information security behavior, even if they are offered information about different risks and security solutions and their information security awareness would increase (Aytes & Connolly, 2004; Edwards, 2015).

Siponen (2001) has divided information security awareness into five different dimensions, which address security awareness from a different perspective. These dimensions are the organizational dimension, the general public dimension, socio-political dimension, the computer ethical dimension and the institutional education dimension. The general public dimension can be divided into two target groups: IT/computer/IS professionals and other end users. The skills of an IT professionals should include certain information in information security aspects. According to Siponen (2001), the result should be professional qualifications that harmonize and develop these skills alongside others. In addition, professional associations should work with educational institutions to manage

procedures and determine the content of relevant knowledge and skills for professionals related to information security. The main idea of this dimension is based on the argument that there are some key information security issues that every citizen using information technology should be aware of. (Siponen, 2001.) However, it can be argued that education and profession related to information security usually increases the information security awareness of an individual evidently. The next section provides more details from past studies about information security professionals' and non-professionals' actual information security behavior.

4.3 Differences between information security professionals and non-security professionals

Most non-security professionals are able to name some of the internet threats, such as viruses, and at least understand the link between that threat and security. Most also realize that they are responsible for their own security. Nevertheless, entry-level users are very rarely able to name solutions or better practices for the security issues they are familiar with. In addition, users do not seem very interested in improving their own security, even if they understand that there are problems. (Furnell, Tsaganidi & Phippen, 2010.)

It has been widely studied that non-security professionals think security differently than information security professionals. Professionals and non-professionals are seen to have a gap in their mental models (an internal conception for how something works in the real world) against information security risks, which can lead to the non-professionals to experience ineffective risk communication and therefore the lack of knowledge on the likelihood and severity of a threat (Asgharpour, Liu & Camp, 2007.) In addition, non-professionals are seen less likely to even think about topics such as information security or risk factors and consequences of threats (Bravo-Lillo, et al. 2010; Bartsch & Volkamer, 2013). Although they are aware that they are responsible for their own security, non-professionals are also less likely to think they can actually protect themselves and thus give more trust towards the service providers and are more likely to think that, for example, a website can be trusted to protect users' information security (Theofanos, et al., 2017). To enforce that a website will protect their information, non-professionals are more likely to think about if a website looks professional when deciding whether it is trustworthy (Bravo-Lillo, et al., 2010).

It can be even claimed that non-professionals sometimes even make conscious decisions not to behave in a secure way. For example, studies show that sometimes non-professionals choose not to guard their passwords with a password management tool or to not install operating system or application updates, even though they know that it could improve their security posture. (Ion, Reeder & Consolvo, 2015; Vaniea, Rader & Wash, 2014.)

Ion, Reeder and Consolvo (2015) found in their studies that one thing strongly affecting the non-professionals information security behavior was usability. Usability was mentioned for example to be one of the reasons non-professionals do not use password managers. According to Ion, Reeder and Consolvo (2015), non-professional users tend to emphasize usability compared to information security professionals, which means that usually professionals are more willing to use applications or systems with poor usability if it enhances their security behavior.

Usability has also seen important when adapting the use of biometric authentication. Wolf, Kuber and Aviv (2018 & 2019) have studied the adaptation of biometrics within information security professionals, and with professionals compared to non-professionals. They found that both user groups are prone to stop using biometrics if the usability is seen bad. The perceived security of the mobile device also affected the adaptation of biometric authentication, especially within the information security professionals. The information security professionals showed distrust against using biometric authentication in mobile platforms in general. It was also observed that professionals found Apple products to be more secure and to have better usability compared to products with Android operating systems. (Wolf, Kuber & Aviv, 2018 & 2019.)

Wolf, Kuber and Aviv (2918 & 2019) also found that the information security professionals are more influenced by work/bring-your-own-device (BYOD) authentication requirements that come from their employer compared to non-professionals. Furthermore, the professionals were more likely to try biometrics immediately once available and were somewhat more likely to view biometric authentication as a good idea in principle, and thus were more likely to recommend the use of biometrics. (Wolf, Kuber & Aviv, 2018 & 2019.)

The information security professionals showed more concern about securing their mobile devices and were seen with a higher degree of concern towards compromising their data than non-professionals. This concern molded both their willingness to try out new authentication methods and simultaneously their distrust towards using biometric authentication with sensitive data or transactions. One of the observations of the study was also that the non-professionals were more trusting of biometric authorization for financial applications, such as mobile payment applications. (Wolf, Kuber & Aviv, 2019.)

4.4 The theoretical framework of information security behavior change

There are multiple well-known theories and theoretical frameworks developed when studying information security behavior, such as the Technology Acceptance Model (TAM) (Davis, 1989), Theory of planned behavior (Ajzen, 1991), and Technology threat avoidance Theory (TTAT) (Liang & Xue, 2009). For example, TAM has been created to explain why users accept or reject information

technology. TAM suggests that perceived ease of use (PEOU), and perceived usefulness (PU) are the two most important factors in explaining information system usage. (Davis, 1989.) The Theory of the planned behavior studies individual's intention to perform certain behavior. It claims that the stronger the intention to engage in a particular behavior, the more likely the individual is to do so. (Ajzen, 1991.) The TTAT on the other hand suggests that individual's perception of threat is based on how likely the individual sees the threat and how severe the consequences of the threat would be. Based on TTAT, an individual takes actions against the threat based on the likeliness of the threat. (Liang & Xue, 2009.) Although all the theories mentioned could be used to study this subject, they were not chosen because the aim was to study the individual's information security behavioral change in more detail. Therefore, the theoretical framework used in this research is based on the framework created by Alasuutari (2016) to explain information security behavioral change. The framework is presented in figure 1.

Alasuutari has based her framework on three theories. First component is Searle's (1983) theory of behavior change connected to the subjective reality, second is the needs and motivational psychology that is based on Maslow's (1954 & 2007), Alderfer's (1969), McClelland's (1961) and Reiss' (2004) theories of needs. The third component of the framework is appraisal theory, based on the research of Ellsworth and Schrerer (2003). The framework was chosen to be used in this thesis as it is developed to help examine explicitly information security behavior. In addition, Alasuutari's framework is developed to study individual home users and even though this research examines the differences between information security professionals and non-professionals, the aim is not to study any organizational level factors that the professionals might face, but the emphasis is on the security behavior of individuals and in the context of this study, the security professionals are also treated as individuals. The following subchapters describe in more detail the three theories forming Alasuutari's framework and the framework itself.

4.4.1 Subjective reality

Behavior is considered to be changing in nature. (Bridle et al., 2005) John Searle (1995 & 1983) provides a theoretical explanation for behavior change through his thoughts on the creation of reality and the purposefulness of experience. Each individual subjectively creates an image of reality through their own consciousness (Nagel, 1974; Searle, 1983). The formation of this subjective image is mainly influenced by the individual's own experiences but influences also come through interaction with the world around us and other people. As a person reflects on their own experiences, the events that have taken place, and the meanings of everything around them, their subjective view of reality changes. (Searle, 1983.)

On the other hand, a change in subjective perception affects a person's behavior when they understand the consequences of their own and other people's actions and, for example, gain acceptance among other people. Behavior change affects all behavior, so changes in subjective reality can drive a person to both good and bad behavior. (Searle, 1983.)

Subjective reality also affects information security behavior. Mobile payment users may change their security behavior for the better as their knowledge and awareness of security threats increases and they understand the impact of their own actions on countering threats. In turn, security behavior can also change for the worse if the user is not sufficiently informed about potential threats or if they interact mostly with people who treat information security indifferently.

According to Alasuutari (2016), Searles thoughts about each individual creating a reality based on their needs gives a new perspective to information security behavior. User's information security behavior may change for example between different elements as a result of interaction rather than explaining the behavior with factors that are always valid in all situations and at all times. Users experience security issues and interact with other people and things. They reflect on what these experiences mean for them and for their own intentioned security. Thus, new experiences and interactions can further change a person's beliefs and thoughts, which in turn can bring a change in behavior. (Alasuutari, 2016)

4.4.2 Needs and motivational psychology

The objective of needs and motivational psychology is to explain people's behavior and thinking when they have different options at their use (Nurmi & Salmela-Aro, 2002). Over the years, several theories explaining motivation and needs have emerged. One of the most famous needs theories is Maslow's hierarchy of needs. In addition to it, some the most commonly used theories are McClelland's theory of needs and Alderfer's ERG theory which extends Maslow's hierarchy of needs (Hersey, Blanchard, & Johnson, 1996; Ruohotie, 1998.)

Maslow's hierarchy of needs (1954 & 2007) approaches the motivating factors of the individual from the perspective of different needs and deficiency. Maslow argues that people have different motives for deprivation and development. The first category (deprivation needs) includes security needs and different needs for social appreciation, while the second category (development needs) includes different aesthetic, intellectual and self-actualization needs. The two categories include basic needs in five different categories. Maslow has named the categories as follows: 1) physiological needs, 2) safety needs, 3) love needs, 4) esteem needs, and 5) self-actualization needs. (Maslow, 1954)

Alderfer's ERG theory expands Maslow's hierarchy of needs and presents the basic needs of humans in three different categories. Alderfer has identified the categories of needs as follows: 1) existence needs, 2) relatedness needs, and 3) growth needs. (Peltonen & Ruohotie, 1987; Robbins, 1993). The needs belonging to the existence needs are material and, according to Alasuutari (2016), include the deprivation needs presented in Maslow's hierarchy of needs. The second category, relatedness needs, includes the needs with which people strive to maintain their social relations (Peltonen & Ruohotie, 1987). The relatedness needs include Maslow's needs for cohesion in the hierarchy of needs and, in part, also the motives for social appreciation (Alasuutari, 2016). Needs belonging to the third category, growth needs, are related to individuals' desire to develop (Peltonen &

Ruohotie, 1987). According to Alasuutari (2016), these also include the developmental needs presented in the context of Maslow's hierarchy of needs and, to some extent, the needs of social appreciation.

McClelland's theory of needs suggests that people have three key needs: 1) the need for achievement, 2) the need for power, and 3) the need for affiliation. (Harrell & Stahl, 1984; McClelland & Burnham, 1995). According to Alasuutari (2016), McClelland's theory of needs has been used in psychological literature to study, for example, the impact of an individual's desire for power on decision-making (Magee & Lanner, 2008) and the relationship of McClelland's motives to people's well-being and the flow of life (Schüler et al., 2013).

According to Alasuutari (2016), Reiss' (2004) Theory of 16 basic desires represents one of the most recent theories explaining motivation and has been formed as a result of empirical research. The motives identified in Reiss' (2004) theory are based on the perception of more than 2,500 people who participated in the study of what motivated them. Alasuutari (2016) states that in terms of information security behavior, the most important elements presented in Reiss's (2004) motive theory are curiosity, saving / collecting, social contacts, and acceptance and tranquility.

In her framework, Alasuutari (2016) has adapted all of the previously described needs and motivational theories to suit the needs of technology and information security, as the theories themselves do not take, for example, technology into consideration. Alasuutari (2016) uses the example of Alderfer's ERG theory (Robbins, 1993; Peltonen & Ruhotie, 1987), and analyses that the described need for existence emphasizes a person's need to protect themselves from physical and emotional harm, but does not take a closer look at the possibility of physical harm to technology or the security needs do not refer to information security.

4.4.3 Appraisal theory

In addition to needs, emotions can also be seen to have a significant effect on behavior (Helkama et al., 2015; Vilkko-Riihelä, 1999). According to Vilkko-Riihelä (1999), motives are related to emotions, because, for example, a certain action or activity can be associated with many different emotions and, on the other hand, emotion itself can also act as a motive for behavior.

The starting point of the appraisal theory is that people's assessment of the prevailing environmental conditions plays a significant role in the expression of emotions. Thus, the appraisal theory emphasizes the connection between emotions and the prevailing environment (Ellsworth & Scherer, 2003; Smith & Lazarus, 1990). More specifically, emotions can be seen as a kind of adaptation reaction to the world around us, as people constantly evaluate the changes in their environment and their significance for their well-being (Ellsworth & Scherer, 2003).

According to the appraisal theory, emotional experience is a continuous process in which the appraisal of circumstances changes the nature of emotional experience (Ellsworth & Scherer, 2003). In addition, re-appraisal refers to a person's ongoing assessment of environmental events and the person's active

response to feedback from the environment (Smith & Lazarus, 1990). Topics of particular interest for information security behavior are negative emotions and related themes, as Alasuutari (2016) found that negative experiences related to information security often arouse negative feelings, such as fear and shame. According to Alasuutari (2016), a person also has a tendency to try to get rid of negative feelings, and this tendency continues to affect the person's actions. Thus, for example, the leakage or loss of personal information could arouse negative feelings in a person that the person would seek to get rid of, and that effort would then affect the person's actions.

Alasuutari (2016) explains in her study that the appraisal theory complements Searle's thoughts on subjective reality and ideas of motivational psychology on the impact of needs to behavior. In the theoretical framework (Figure 1) at level 1, the user conducts an appraisal of circumstances in a security-related operating environment, which evokes different emotions that lead to a state of uncertainty and consideration of solutions to how that uncertainty could be overcome. After a change in behavior (level 3), the user makes a new appraisal in a security-related operating environment, which in turn leads to the awakening of new emotions. After a change in behavior, the user experiences an interaction that leads to an exception. This evokes various emotions which motivate the user to deviate, either temporarily or permanently, from the use of a protection measure that had been already adopted. (Alasuutari, 2016.)

The purpose of this study is to examine what can affect the intention to change information security behavior when using biometric authentication methods in mobile payment, and whether there can be seen a difference between information security professionals and non-professionals. Based on the literature review, it can be claimed that information security professionals have a higher knowledge in information security awareness and thus the purpose is to examine how much does increased information security awareness affect the intention change information security behavior.

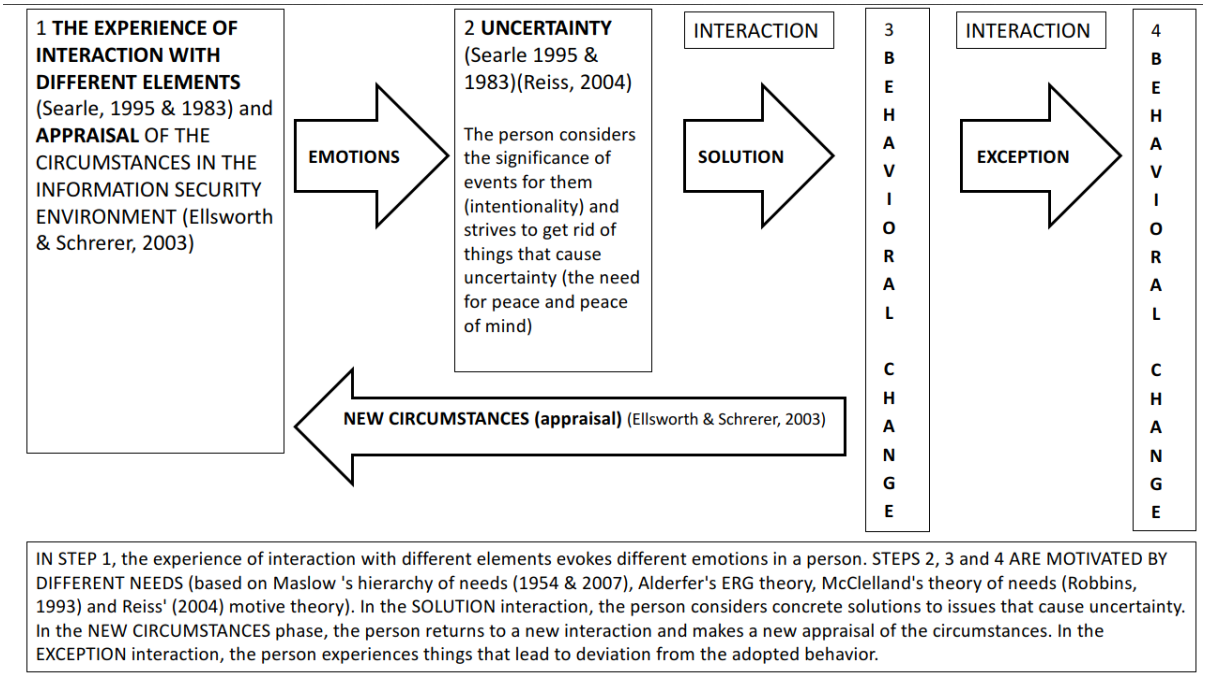

Figure 1 The theoretical framework of information security behavior change, translated from Alasuutari, 2016.

5 EMPIRICAL RESEARCH

The study aimed in finding answers for the two research questions regarding intention of change of information security behavior:

- *What factors would affect the intention to change information security behavior in the context of using biometric authentication in mobile payments?*
- *What differences can be seen in the intention to change information security behavior comparing information security professionals and non-professionals, in the context of using biometric authentication in mobile payments?*

Previous chapters examined the research questions by reviewing previous literature of the topic. In these following chapters, the research questions are examined by completing an empirical research. This chapter describes the research method used. First, the chosen research method is presented. The method of data collection is then explained, and the final chapter describes the analysis of the data.

5.1 Research methods

A qualitative research method is suitable for research when the researcher wants to find out the meaning and context of the behavior. Qualitative research can utilize two different approaches to data collection: observation and interviews. Examples of observation are, for example, ethnographic research and observational research. The observation-based researches examine the behavior of people in different situations. (Hirsjärvi, Remes & Sajavaara, 2016.)

In a qualitative study, the analysis is often performed inductively. The aim of the research is to uncover as yet unknown and sometimes unexpected information. Inductive analysis may bring out unexpected and important information and thus the researcher does not decide which is important, but instead the material gathered reveals the important facts. Therefore, the goal is not to test hypotheses, but to investigate material in detail and multilaterally without

prejudice or special expectations. (Hirsjärvi et al., 2016.) The observations made in the qualitative research can be seen as subjective rather than objective, since the observation present the view of the interviewee and the researcher about a certain phenomenon. The researcher also uses their own understanding when analyzing the collected data. (Tuomi & Sarajärvi, 2018.)

In qualitative research, research materials are usually collected in natural situations and the source of information is usually a human. Key data collection methods in qualitative research are interviews, observations, biographies and information from several documents (Hirsjärvi et al., 2016.) These data collection methods reveal an individual's personal views and opinions on a research topic. When the results are presented in qualitative research, the researcher usually uses direct citations from the interviewees. This emphasizes the researcher's analysis of the topic. (Tuomi & Sarajärvi, 2018.)

5.2 Data collection

When aiming to understand why something is happening, an interview is a good choice. Interviews are a great way to gain material and thus understanding when dealing with abstract things and phenomena. The format of the interview should be consistent with the research questions, the research objective, and the research strategy. When conducting the research by interviews, the significance of behavior and context can be elucidated because an interview brings present the interviewees experience and observations of the situations, and allows factors related to the interviewees past and development to be taken into account. (Hirsjärvi & Hurme, 2015.) An interview based qualitative research method was chosen for this research, because the interview takes into account the interviewee's assumptions and experiences of the object under study.

Interviews can be divided into many different ways, but most commonly interviews are divided as follows: semi-structured interviews, unstructured in-depth interviews, group interviews, and structured interviews. A semi-structured theme interview method was considered the most suitable for this research, as according to Hirsjärvi and Hurme (2015), in a semi-structured interview, the interview questions are formulated in the same way for all interviewees, which facilitates the comparison of the results of the interviews. The most important factor for theme interviews is that the themes and subject matters remain the same for all interviewees. The theme interview can be used to take into account the key issues such as people's interpretations and the meanings they give to things. (Hirsjärvi & Hurme, 2015.) In this study, the topics of the interview questions were based on the themes of the research framework: the importance of information security, information security behavior, issues and experiences that have influenced information security behavior and intended changes in information security behavior. According to Schultze & Avital (2011), using a framework as the basis of the interview structure aids the interviewer in leading the interview meaningfully and helps to obtain detailed and substantial information.

In addition, in a semi-structured interview, the interviewer has the possibility to change the order of the questions if it is appropriate for the results of the interview. A semi-structured interview also allows the interviewees to answer in their own words and is not tied to answer options. This was seen as important so that the interviewed information security professionals could use their expertise to also steer the interview in a direction that serves their core competencies the best. (Hirsjärvi & Hurme, 2015.) In addition, the advantages of a semi-structured interview method include that it offers some structure and direction for the interview, but on the other hand it offers a lot of flexibility in an interview, for example, when a surprising or interesting information emerges in an interview situation (Hair, Page & Brunsveld, 2019).

Discretionary sampling is generally used in qualitative research, meaning that the people interviewed are appropriately selected (Hirsjärvi & Hurme, 2015). The possible bias of interview data is mitigated by interviewing numerous and highly knowledgeable informants who view the studied phenomenon from different perspectives (Eisenhardt & Graebner, 2007). The purpose of this research is to understand the information security behavior when biometric authentication methods are used within mobile payments in the Finnish markets and the difference of information security professionals compared to non-professionals. Therefore, it is appropriate to select two groups of Finnish people to participate in the interviews, one forming from information security professionals and the other from non-professionals. The information security professionals selected for this study have all studied or worked within the field for several years and currently work as information security professionals. They are all employees in a multinational company that offers consulting services within the information security and cybersecurity field. The non-security professionals were selected from various occupations and so that they don't have any educational or professional background in information security.

In a qualitative study, it is difficult to determine the optimal number of interviewees because the purpose of the study is not to look for average correlations or statistical regularities (Hirsjärvi et al., 2016). The main goal of the research is to understand the research subject holistically. Guest, Bunce and Johnson (2006) have determined that if the goal is to describe a shared perception, belief or behavior among a relatively homogeneous group, then a sample of 12 is enough. However, if the aim is to understand how two or more groups differ in a certain dimension, one should most likely use some sort of stratified sample and may intentionally select for example 12 participants per group of interest. The exact sample size for this study was determined according to the available information security professionals. Eight information security professionals participated in the interviews and thus the number of non-professionals was selected to match the amount of professionals to have sufficient representation of both groups. This means that the sample size for this research is in total 16 interviewees. The amount was considered to be sufficient to obtain versatile information, as the appropriate amount is always determined definitively by the purpose of

the study (Hirsjärvi et al., 2016). The background of the interviewees is presented in more detail in the chapter 5.2.1.

The interviews were conducted via videoconference application Microsoft Teams or in person. Because it was important to find the real opinions of the interviewees comprehensively and honestly, an individual interview was seen best suited for this research. In this way, the influence of other people and other distractions to the responses were minimized. The length of the interviews varied from 17 minutes to 35 minutes and all interviews were recorded with the permission of the interviewee. The interviewees were promised complete anonymity, which means their personal information from which they can be identified would not be linked to the material at any time.

The interview questions are presented in appendix 1. The questions were based on the framework described in chapter 6.3. Some of the questions were altered, added or removed compared to the original questions presented in Alasuutari's research due to the reason that the original framework was built to describe the intention of change of information security behavior when using personal computers and this research focused on a more specific topic of information security behavioral change intentions when using biometric authentication methods with mobile devices and in mobile payment. Because the type of interview was semi-structured, it provided an opportunity to ask improvised but pertinent additional questions in some of the interviews. In most interviews, some questions, concepts, and/or related terms were explained to the interviewee in more detail. Not all questions were asked in the interviews because they were not relevant to all interviewees or if the interviewee had no knowledge of the topic. The order of the questions was also changed if necessary.

5.2.1 Interviewee background information

In total of 16 individuals were interviewed for this research. Eight of them have studied and/or work within the information security field and in the context of this study, are considered to be information security professionals. All of the information security professionals interviewed currently work in a same multinational and large consulting company as cyber security consultants. Their background of studies and work experience are presented in more detail in table 1. The other eight have not studied nor worked within information security and currently work within various positions, such as Marketing Lead, Event Producer, Communications Planner or Interior Architect. In the context of this study they are referred as non-professionals. Their background is also presented in more detail in table 1.

The only requirement set for the interviewees was the use of mobile payment applications. However, the use of biometric authentication methods was not required. The information security professionals are listed as interviewees 1 to 8 and the non-professionals are listed as interviewees 9 to 16.

Table 1 Interviewee background

Interviewees	Age	Education	Work experience within information security
Information security professionals: 8 (Interviewees 1-8)	25-30: 6 31-35: 1 36-40:1	Master's degree: 5 Bachelor's degree: 3	Less than a year: 2 1-4 years: 4 5-9 years: 1 over 10 years: 1
Non-security professionals: 8 (Interviewees 9-16)	25-30: 7 31-35: 1 36-40: 0	Master's degree: 5 Bachelor's degree: 3	N/A

5.3 Data analysis

Because the study was conducted using a qualitative research method, qualitative analysis was chosen as the method of analysis. In qualitative analysis, the researcher uses either inductive or abductive reasoning. In inductive reasoning research material is central and new facts are sought from the material. In abductive reasoning, the researcher has some original theoretical ideas that they try to prove through interviews. (Hirsjärvi & Hurme, 2015) The inductive reasoning was chosen as the reasoning method for this study because this study does not seek to prove any hypotheses but seeks to find reasonings behind a behavioral change and differences of two groups. According to Hirsjärvi et al. (2016), typical features of qualitative analysis include performing the analysis already at the interview stage, storing the interview materials in writing, and varying with the analytical techniques because there is no single true analytical technique used for qualitative research. When the research is done by conducting interviews, the researcher is able to draw conclusions of interviews, finding connections and specialties already during the interview phase. Thus, the purpose of the analysis performed in this study was to find similarities already in the interview phase.

There are two ways to break down the collected material: by transcribing the material into text, or by drawing conclusions or coding themes directly from the recorded material without writing the material into text. (Hirsjärvi & Hurme, 2015.) In this study, the interviews were recorded using a telephone recording function or directly with the Microsoft Teams application to facilitate transcribing afterwards. The analysis of transcribed material can be done in three steps according to Hirsjärvi and Hurme (2015). Initially, the material is arranged, and its structure is highlighted. The material is then clarified, for example irrelevant elements such as repetitions and non-essential elements are deleted. Lastly the actual analysis of the material is carried out, and the material is summarized, categorized and interpreted.

Because the interviews were conducted as semi-structured theme interviews, it is natural that the material was categorized according to the themes, as

each theme focuses on a specific topic with its own purpose. Within the interview themes, the material was then coded into response themes, according to the answers provided to perform thematic analysis. Thematic analysis provides a highly flexible approach that can be tailored to the needs of many studies, providing rich and detailed but complex information about the data. Thematic analysis gives the researcher a way to see collective or shared meanings from the interviews, and it should not be used to identify experiences from a single data item. However, in thematic analysis it is important to understand that what is common is not necessarily important for the research. The importance of the occurring themes need to be considered in relation to the particular topic and research questions. (Braun & Clarke, 2012.)

The written material was organized in such a way that an excel document was created including all interview details and the responses from information security professionals and non-professionals were placed in different tabs to facilitate the easier comparison between the two groups. The responses were also categorized according to the identified themes. Categorizing the results with the themes allows results to be compared with each other and the regularities of the responses can be observed. (Hirsjärvi & Hurme, 2015). As mentioned previously, the four themes used in the interviews were the importance of information security, information security behavior, issues and experiences that have influenced information security behavior and intended changes in information security behavior, and the response themes identified from the answers to perform the thematic analysis were usability, trust and confidence, information security knowledge, the behavior of others, new perspective on life, new legislation and regulations, and perceived risks, threats, vulnerabilities and incidents. The relation of the themes and response themes is presented in table 2. The results of the analysis are presented in the next chapter.

Table 2 Interview themes and response themes

Interview themes	**Response themes**
Importance of information security	Trust and confidence
	Information security knowledge
	Perceived risks, threats, vulnerabilities and incidents
	Usability
Information security behavior	Trust and confidence
	Information security knowledge
	Perceived risks, threats, vulnerabilities and incidents
	Usability
Issues and experiences that have influenced information security behavior	Trust and confidence
	Information security knowledge
	Perceived risks, threats, vulnerabilities and incidents
	Usability
	The behavior of others
	New perspective on life

	New legislation
Intended changes in information security behavior	Perceived risks, threats, vulnerabilities and incidents
	Usability
	The behavior of others
	New legislation

6 RESULTS

The results of the empirical research are presented in this chapter. First, the background of the interviewees use of biometric authentication methods and mobile payment applications is presented. The results are then described according to the order indicated by the themes described in chapter 6: usability, trust and confidence, information security knowledge, the behavior of others, new perspective on life, new legislation and regulations, and perceived risks, threats, vulnerabilities and incidents.

6.1 Use of biometric authentication and mobile payment applications

As mentioned in the previous chapter, the interviewees were required to use at least one mobile payment application but not required to use biometric authentication. To determine the use of the mobile payment applications and biometric authentication, the interviewees were asked four questions: do they use biometric authentication methods in general and if so, what type, which mobile payment applications they use, and do they use the biometric authentication methods in the mobile payment applications and if so, what type and how often. The results can be seen in figures 2, 3, 4 and 5. Figure 2 describes the use of biometric authentication in general, figure 3 describes the use of mobile payment applications, figure 4 presents the use of biometric authentication in mobile payments and figure 5 describes how often the biometric authentication methods are used in mobile payments.

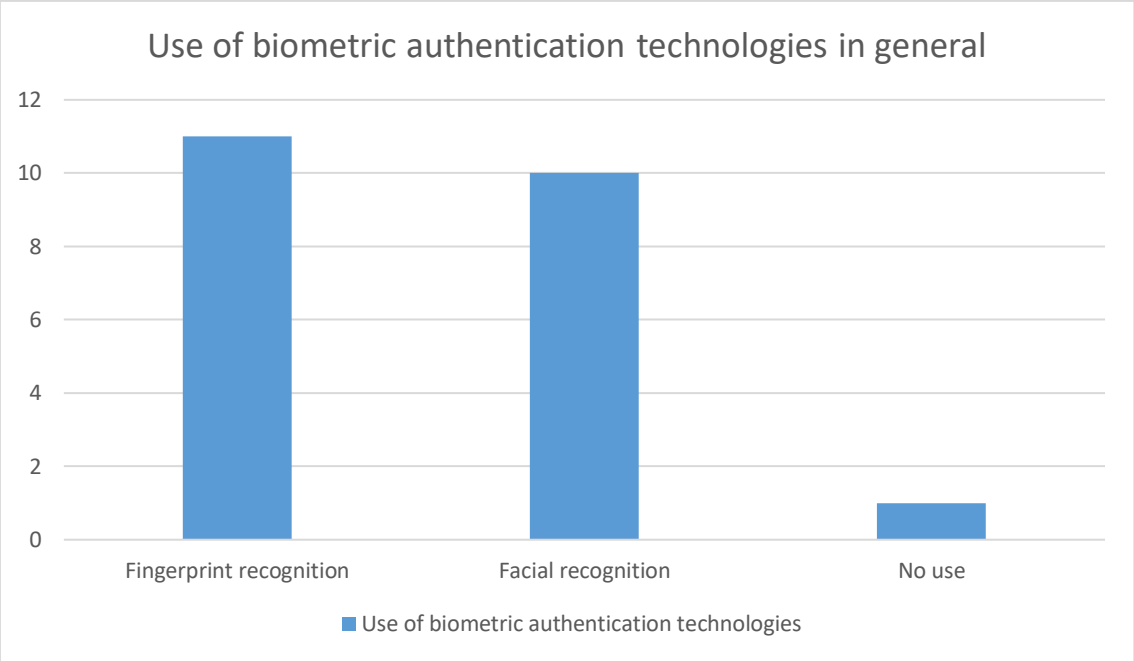

Figure 2 Use of biometric authentication technologies in general

Out of the 16 interviewees, 15 used some biometric authentication method and only one of the interviewees (interviewee 6) didn't use any biometric authentication methods. However, three of the interviewees (interviewees 1, 6 and 8) that uses biometric authentication methods in general don't use them for mobile payment applications. 11 out of the 15 interviewees that use biometric authentication in general use fingerprint recognition. In addition, 10 of the 15 interviewees use facial recognition. This means that out of the 15 interviewees that use biometric authentication methods in general, six uses both fingerprint and facial recognition technologies. Five of the information security professionals use both, only one of the non-professionals. Also, five interviewees use only fingerprint recognition (two professionals and three non-professionals) and four use only facial recognition, all of them non-professionals. None of the interviewees used other biometric authentication technologies.

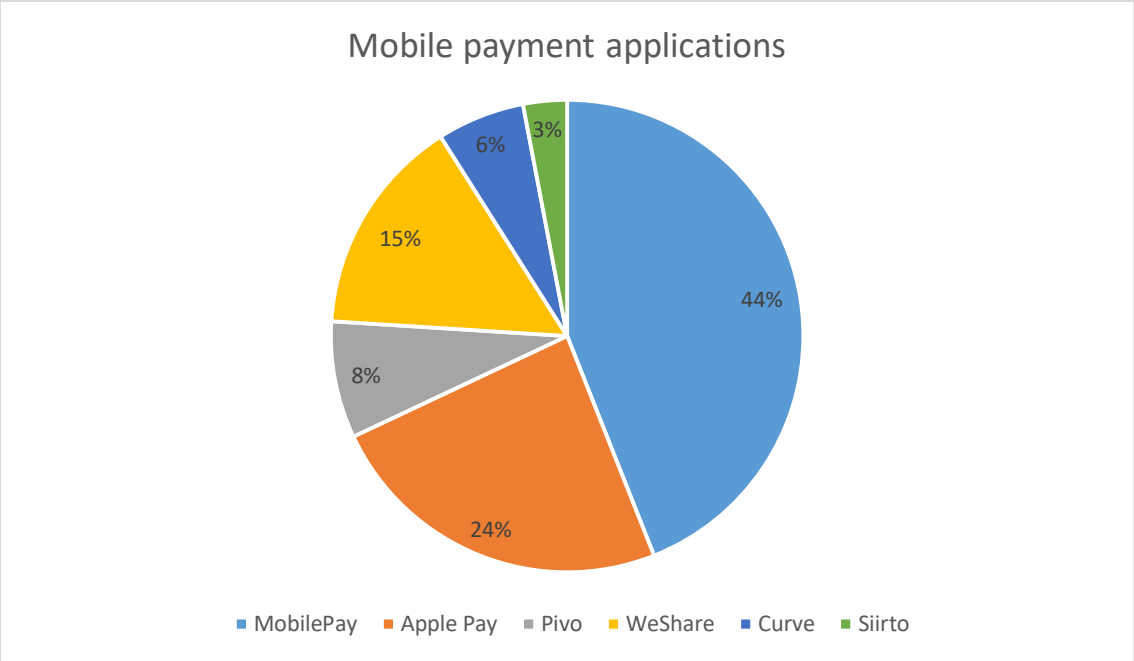

Figure 3 Use of mobile payment applications

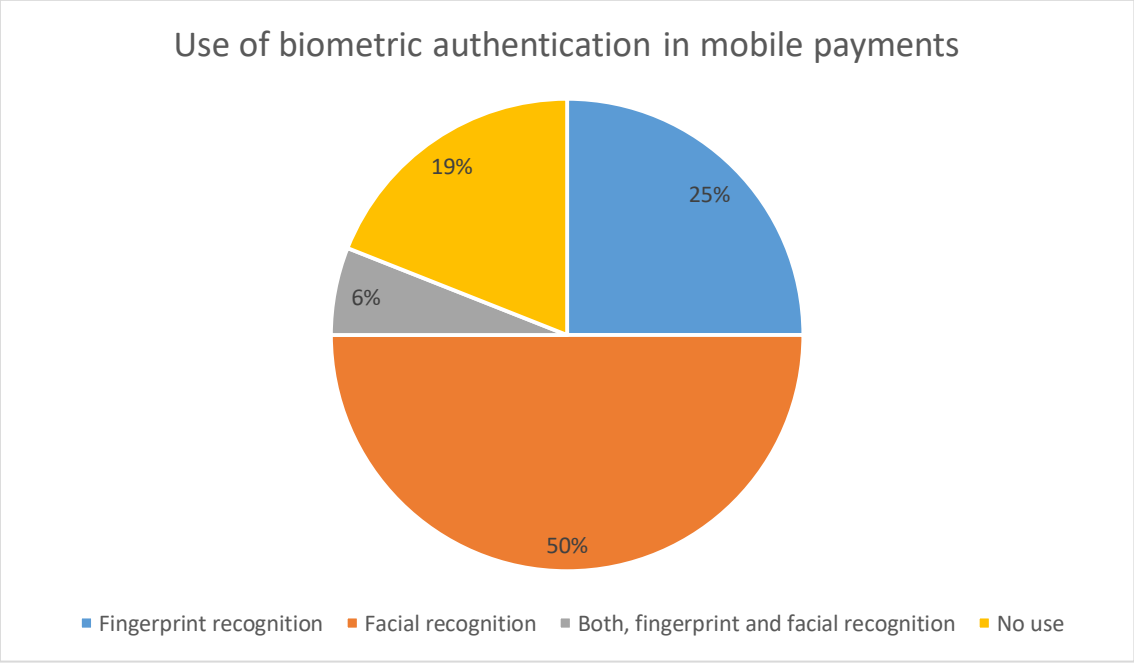

Figure 4 Use of biometric authentication in mobile payments

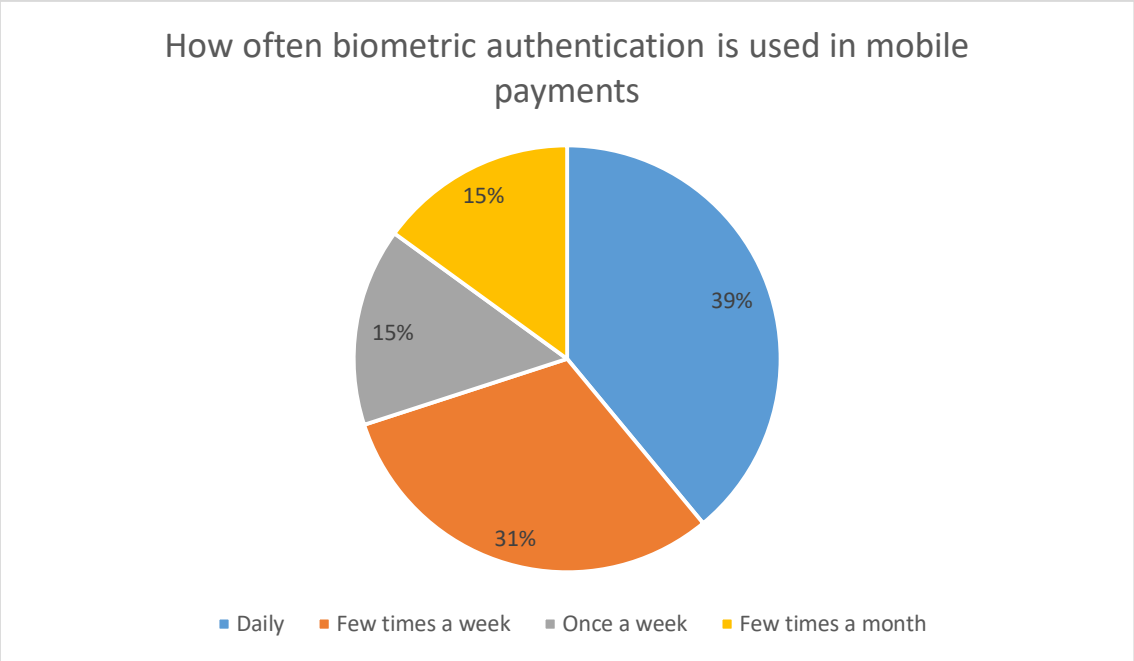

Figure 5 How often biometric authentication is used in mobile payments

When it comes to the use of mobile payment applications, 15 out of the 16 interviewees use MobilePay. Only interviewee 5 doesn't use MobilePay. Five from the 15 mention to also use WeShare, which is an additional application developed by MobilePay to use when sharing expenses (MobilePay, 2021). Eight interviewees use Apple Pay, three of them information security professionals and five of them non-professionals. Only three interviewees mentioned to use Pivo (one professional and two non-professionals). In addition, two of the interviewees, 2 and 5, mention to use Curve, which is a mobile credit card that can be used with cards that are connected to Apple Pay (Curve, 2021). Interviewee 16 also mentions to use Nordea Siirto, which is a mobile payment application similar to MobilePay developed by the Nordic bank Nordea, and in Finland can be used by clients from Nordea, Osuuspankki, S-Bank and Bank of Åland (Nordea, 2021).

Three of the interviewees, 1, 6 and 8, do not use biometric authentication methods in mobile payment applications. All of them are information security professionals. From the remaining 13, eight use facial recognition and four use fingerprint recognition. Only interviewee 4 uses both, fingerprint and facial recognition, in mobile payment applications. Two of the interviewees, 10 and 11, use the biometric authentication methods, facial recognition to be specific, only in Apple Pay, although using other mobile payment applications as well.

From the 13 interviewees who use biometric authentication in mobile payments, five use it daily. Four interviewees, 2, 13, 14 and 16, use it a few times a week and two, interviewees 7 and 12, use it once a week. Two of the interviewees, 3 and 10, use biometric authentication in mobile payments less frequently, only a few times a month.

6.2 Understanding of information security behavior

The interviewees were asked about their understanding of what information security behavior is to gain knowledge if the perceived understanding differs. All of the interviewees understood information security behavior in a similar way and described it to be behavior where a user takes information security into consideration when using applications. Some of the mentioned behavioral aspects were password protection and mitigating information security risks in general.

> From the individual's point of view, the way in which an individual behaves in relation to information security, if they are a conscious person and implement information security instructions or other thing. In an academic sense, maybe something else. – Interviewee 7

> It's about doing the right things and making sure that all the possible ways of securing information is used. But in the end, it's about your own actions that matters. -Interviewee 9

> I would see it as how good to take care of data security, in example whether the passwords are the same. But to myself it's a bit distant thing. I think it's also something about if you have antivirus installed on your mobile phone and computer. -Interviewee 10

Only interviewee 5, an information security professional, mentioned that they don't consider information security behavior to be some special behavior, but instead something that everyone does when they use applications and internet, consciously or not.

> Well, really, I do not understand it because it's part of the behavior of what you do when you're connected to the internet and information technology. So, it's just behavior with some level of idea of secure behavior. If the idea doesn't exist, then maybe it's bad security behavior. Some kind of continuum, I would say. – Interviewee 5

6.3 Usability

Usability was one of the recurring themes in all of the questions. The interviewees described usability to be a factor when deciding whether to use biometric authentication at all, and also when contemplating the use in the future. After determining the understanding of information security behavior, the interviewees were asked to describe their own information security behavior when using mobile payment applications, and biometric authentication methods in them. Interviewees 6 and 8, that don't use biometric authentication methods, described the reason to be more on the usability side than information security related, and do not think that biometric authentication could give them any benefits. However, they

describe to take information security into consideration when using mobile payment applications.

> The fact that I'm not using biometrics is not a security choice, I do not trust that the face recognition works. However, I always look very carefully that the recipients for mobile payments are right, that nothing odd has happened when opening the app. So, if I order something and pay with MobilePay, then I check that there is nothing suspicious about it. Because sometimes it has happened that the app has offered a double charge. – Interviewee 6

> I don't use biometrics because I don't feel it necessary. So, it's not a security choice. When paying, I am more concerned about the security of the payment itself, in example that the subject of the payment is correct, but I don't consider that to be information security issue. – Interviewee 8

Four of the interviewees said that they feel like they achieve more usability when behaving like they described. This referred to the use of biometric authentication methods that the interviewees consider to be easier to use compared to alphanumeric passwords.

> When I use fingerprint recognition, it's just pretty much more convenient. – Interviewee 4

> I feel like I am achieving safety, a sense of security. And in fact, it's that it's easier because I have a really hard time remembering passwords, I don't need to remember any password, it's always enabled, so it's easy and fast. I feel that the fingerprint, though, would be even more convenient, it's annoying that it can't be chosen. For example, sunglasses and a cap or the mask makes face recognition more difficult, fingerprint would be easier. – Interviewee 11

Similar themes recurred when asked what the interviewee's think they would lose if they didn't behave in their described way. The interviewees described that they would lose the usability or that they would feel more insecure about their information.

> I would lose the ease of use and the possibilities of what biometric authentication brings, it would take a lot more time and effort. – Interviewee 5

> I may not lose, well maybe the loss of usability. The phone unlock code is quite long, for example, I feel that it is easier to use, and it would be more difficult and slower. And the fact that if someone found out the PIN code, it would be easier to hack. - Interviewee 11

After contemplating what they would gain or lose, the interviewees were asked four questions about things may have affected their information security behavior. The first question was regards if someone had experienced any information security related issues when using biometric authentication in mobile payments. None of the interviewees had experienced any direct information security related issues. However, some of them mentioned experiencing usability

issues, and most facial recognition users said that during COVID-19 the use of the facial recognition technology has been challenging due to the use of protective face masks. Two of the interviewees also said that they think their information security is at risk when they have to use the PIN code instead of the facial recognition. The details are presented in figure 6.

> I have not, other than troubles with a mask. I have to think will I enter an PIN code, which is a bigger risk when someone can see it, or will I take off the mask for a moment so that the phone can recognize my face. The way I choose depends on the situation. – Interviewee 5

> It doesn't work so well with a mask and I have to have a pin code along with biometric authentication which makes it more vulnerable as someone can see my pin code. – Interviewee 9

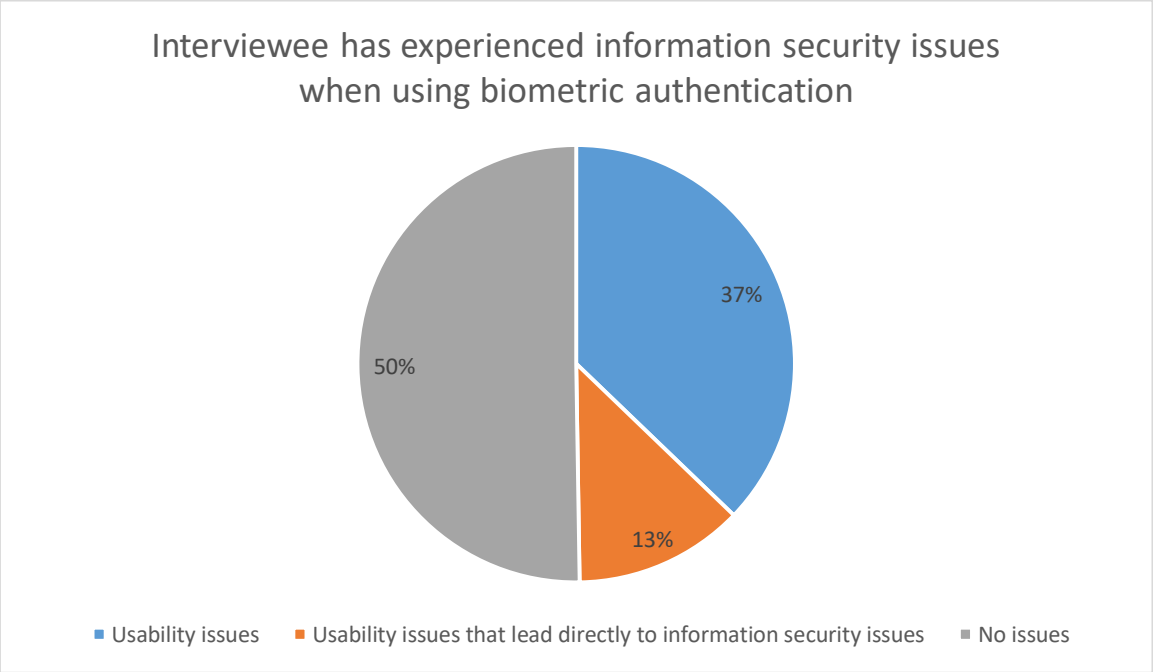

Figure 6 Experienced information security issues when using biometric authentication

The majority, nine of the interviewees, think that their information security behavior is on a sufficient enough level, but they see points for improvement. For example, the non-professional interviewees 10 and 16 mention that even though they think their information security behavior is at a good enough level, their password management could be improved. Again, four interviewees from the professionals, 3, 5, 6 and 7, mention that their information security behavior is only at sufficient level because of usability.

> I feel it is at an adequate level, thinking back to risk management and balancing with usability. Good or very good costs something, time and effort, and I do not want to be neurotic, because risks are always there. It's about considering how much risks am I willing to take versus how much I'm willing to make changes. - Interviewee 5

> I think it's at a relatively good level, could be better. Perhaps I should be more aware of the different risks. More aware that what is good security in general. It feels like when an iPhone offers fingerprint recognition or face recognition, then I don't know how many people think about security aspects when the solution is offered on a tray, that this is easy, then you might not think about how secure it is and if there are any risks involved because they haven't been told. – Interviewee 14

> Yes, it is at a quite good level. Still, in my opinion there is always room for improvement regarding security behavior. Using more complex passwords and changing them more often. – Interviewee 16

Lastly, the interviewees were asked what could prevent them from making changes to your information security behavior they think could be useful. All of the interviewees, except for interviewee 16, mentioned that usability is the main reason why they would continue with their information security behavior even though they think it could be improved. They consider that if more secure behavior would make the use slower of harder, they wouldn't make the changes. Interviewee 16 didn't come up with of anything that would prevent them from making changes.

> Probably laziness is the main reason that secure behavior usually requires more, and the mentality is that "I don't have time to do this". So, the usability aspect. If I think about it more broadly, then I actually currently don't recycle passwords because it's hard to remember and manage them. So, if it becomes too hard versus what I personally am willing to spend time on. – Interviewee 7

> If it's terribly hard because I also want ease of use, and if it's extremely hard, then I'm looking for easiness and speed, meaning I might use face recognition even if there would be a better way. – Interviewee 11

Two of the interviewees, 1 and 13, consider the importance and the sensitivity of the data that would be in risk compared to usability. They say that if the data is not so sensitive, they most probably wouldn't make changes to their behavior due to the loss of usability.

> If I have created usernames for services that do not matter so much, then I'm not going to bring passwords to the central password management system, for example. So, if it needs a huge effort then maybe not. Maybe it's not so much about whether the service is important, but rather what kind of information is in the service. – Interviewee 1

> Ease of use. And it affects what it is all about. If it comes to money, I would switch right away. If it was Facebook or Instagram, for example, I would still continue to use it. But if I read even from Helsingin Sanomat that facial recognition is no longer good, then I might not change, but if I got information from friends, then I would change. Also, considering the personal information I would protect, the limit goes in that if someone gets my name, city of residence and birthday, then that's fine, but the more specific information I want to protect. – Interviewee 13

6.4 Trust and confidence

In addition to usability, trusting the device or application manufacturer was seen as one of the most important things to consider whether to use biometric authentication now or in the future. One of the interviewees that doesn't use biometric authentication methods described it to be an information security related choice and said that they don't want the manufacturer of their mobile phone to have their biometric information.

> I do not use, one reason why I do not use the fingerprint on my phone is because I do not want to give my own fingerprint to the manufacturer, Xiaomi, but for example, I can give my fingerprint to Apple, which is the manufacturer of my work phone and I use the fingerprint to log into that phone. But I'm also aware that fingerprint authentication may not be the most secure option. – Interviewee 1

Trusting the manufacturer of the device or the application is also a recurrent theme in the answers of others. In addition to interviewee 1, 10 other interviewees (six professionals and four non-professionals) described that they take the reputation and trustworthiness of the service provider into consideration when choosing whether to use the mobile payment applications, and if they choose to use biometric authentication in them.

> It's a narrow aisle, I take into consideration the overall security of the device, whether the device locks automatically, and I don't rely on biometric only, according to Financial Supervision Authority guidelines. I also use multi-level authentication, e.g. balances can only be viewed with a biometric identifier, but payments are then made behind several verification steps. Device and application reliability are important. – Interviewee 3

> Well, I just do nothing but choose which apps to use. With Curve, it doesn't collect the information of my face itself, it goes through Apple. That is, I rely on the apps I use, and Apple and Curve. At the behavioral level, perhaps I can't say I take security into account. I use biometrics in general because I trust the service providers. Security and usability go hand in hand to some extent, and then you need to take informed risks if you want usability. So, I accept the risk of handing over biometric data to Apple. – Interviewee 5

> I only use applications and software providers that are well-known and widely used. I also try to read about information security problems from newspapers and other news outlets to learn more about them and to find out if there are problems in applications that I am using. Otherwise I don't give much effort to investigate the security and safety of biometric authentication methods in mobile payments. – Interviewee 15

Interviewee 12 also adds that they trust that the manufacturer of the mobile payment application has already considered the information security issues and thus they don't necessarily take any extra measures to make their information security behavior more secure.

> Information security is very important to me since there is so much data gathered from all of us in digital form. I expect that information security issues have been considered when designing the devices and application I use, especially with applications that use sensitive data such as mobile payment applications. I also understand that information security is not just the technical side of devices and applications but a broader concept that includes users and their behaviors. However, I think it is vital that the designers of devices and applications have made it easy for the user to achieve a strong enough level of information security when using their products and services. – Interviewee 12

Interviewee 11 uses biometric authentication in mobile payments because they consider it to be safer than for example using a four-digit code (PIN code) to authenticate. In addition, interviewee 13 considers that facial recognition is safer to use than fingerprint recognition technology. This means that they trust the method itself more and therefore are willing to use it.

> All I do is feel that PIN code is more secure, because I am one of those people who keeps PIN codes in password apps because I don't remember them, so I feel that face recognition is more secure than that someone could have hacked into my password app. – Interviewee 11

> At least I want to choose what I think is a reliable way to authenticate, I find facial recognition more reliable than a fingerprint. If there was no authentication, then I would not agree to use, I would not pay, because I would assume that there's a bug or I've been hacked. I also think about the reliability of the app when downloading, but if I've already downloaded it, then I don't think anymore. I think information security a lot because in my own opinion I don't understand it at all, so I actively try to think it to understand more. – Interviewee 13

During the interviews, it was determined what the interviewees consider they gain when they behave in the way they described in the previous question and what they think they would lose if their information security behavior wasn't at the level they had just described to get more understanding around what kind of events the interviewees consider to matter the most. Over half of the interviewees mentioned that they feel like they achieve a certain level of confidence that their information is safe. The confidence was also something that was mentioned to be lost if they didn't behave in the way they had described. In addition, one of the interviewees, interviewee 3, mentioned that information security increases their confidence and trust towards the device and application manufacturers.

> Information security increases my confidence in payment instruments, and in society. Increases confidence in mobile payments, too. Improving in information security means the manufacturer can take risks and innovate more. – Interviewee 3

> I can sleep my nights without a worrying about stolen data or money when I behave like I described. – Interviewee 3

> I like to be sure, so that there is no need to later think about whether something strange happened when you're thinking information security already in the moment. Of

> course, as I already said, I feel also that I achieve the protection of my own data and money. – Interviewee 6

> I am more confident that my data is safe, and also peace of mind regarding security aspects. – Interviewee 16

> I will lose free time and perhaps be more stressed if I start worrying and protecting my information in every possible way. On the other hand, if I would not consider at all what kind of applications, I would use I believe I could be in greater risk of criminals stealing my personal information and perhaps money. – Interviewee 15

6.5 Information security knowledge

13 out of the 16 interviewees mention that information security is important to them. Four of the information security professionals mention that information security is important to them because it's their profession and they make a living out of it. However, this was not the only reason they mentioned about the importance of information security for any of them. Gaining information security knowledge was seen as one of the factors affecting the information security behavior.

> A broad question, information security is my profession and provides a living, so it plays a big part in my life. I follow a lot of industry news from several news sources. And from Twitter too. I also listen to podcasts related to the topic. Personally, the importance has changed since I started working in the field. Before I became a consultant, I knew at a basic level that weak passwords should not be used for reason X. Nowadays, when I know the risks, I have been much more active in changing passwords, updating systems, and implementing MFA, for example. I consider it to have big impact in my life, e.g. when reading technology news, you may start to think about the security angle. – Interviewee 1

> Means pretty much, it has a lot of importance to what services I use, but I don't do any more in-depth research on how data, etc. is encrypted, I rely on the research of others. – Interviewee 2

However, three of the security professional interviewees, 4, 7 and 8, admit that although they are information security professionals and know that information security is important, they might not behave in a secure manner in their personal lives. Also, two of the non-professionals, 13 and 14, admit that they might not always behave in a secure manner, but this is due to the fact that they don't understand what information security is or they haven't thought about information security aspects.

> It affects quite much because that way I earn a living. In my personal life, I may not go to extremes, I am ready to use WhatsApp, for example. I proportion the information security to what I use, and I understand that in some cases I am a product. I try to control on social media platforms what I share there, which means I share things quite

> moderately, but I don't go to extremes in there either in information security either. – Interviewee 4

> Of course, I am interested in security in the sense that I acknowledge what it means, and I am more aware of security risks than others, but I may still use the service. I consider it important, but sometimes I don't behave securely. – Interviewee 7

> It's my profession, so it's pretty important to me. But in my spare time, I am not a big security enthusiast. – Interviewee 8

> I think my information security is pretty bad, should be better. It's important, but a little unusual and strange, and I would like to know more. But I think information security should be easy and easily accessible to everyone. – Interviewee 13

Interviewee 14, a non-professional, mentions that in addition to usability, the fact that they think that they don't know enough about information security would prevent them from making necessary changes. They add that they feel like the information security threats do not affect them because they haven't heard of anyone having issues or have had information security related issues themselves. Furthermore, interviewee 14 admits that they have not considered information security at all when using biometric authentication in mobile payments.

> I've never thought about it, I don't know how security should be considered. When I press one button, it opens the face detection. So, it's quick and easy, but I've never thought about how easy it would be to abuse. I'm not sure how security should be taken into account. – Interviewee 14

6.6 The behavior of others

One other recurring theme found in the interviews is that four of the interviewees want to read about user experiences and wait for new apps and systems to come into broader use before starting to use them their selves. The interviewees consider that to be an information security related decision, and it can be seen also to be one of the aspects about only using apps and devices that are trusted.

> When it came, it was not among the first to start using it, perhaps only when it began to become familiar. I have confidence in Apple's ecosystem, that is, in that ecosystem I don't worry about the use. I actually do not even use biometrics in other contexts. So pretty much depending on trust. Once authentication happens through the Apple ecosystem, applications under it can be deployed. – Interviewee 4

When asked if the interviewees think that the information security behavior of others has affected their own behavior, most of the interviewees, 12 out of 16, think that other's behavior has affected theirs (figure 7). The information security professionals mostly consider that if there is an impact, it is because they work within the field and know many security-oriented people, who have even more

knowledge and better behavior. The non-professionals usually mentioned that the behavior of relatives and friends have affected them the most.

> Certainly, in really many ways. For example, of course, I work with smart colleagues and my friends are woke, I always get good tips and thoughts from there, and the security thinking stays on, which boosts my own security behavior. On the other hand, maybe if there is someone who doesn't take security aspects into account, I take it so that I myself want to compensate even more and want to take even more care of my behavior. And I think about connections that someone else's behavior can raise my own risk too. – Interviewee 5

> Yes, it affects that way, that for example I have a friend who is very familiar with everything security related, so if she tells some tips, then I take them as part of my own behavior. For example, two-stage authentication. I don't think security so much myself, but if someone else brings it up, or there's news about passwords leaked to the web, then I make changes. – Interviewee 11

> I feel like my dad, for example, is pretty security conscious. His passwords and usernames are pretty cryptic, and if he needs my help with technology, he never gives them to me in the same messages but uses separate ones. I may not have adopted that scale to my own security behavior, but if someone who knows things well, e.g. a friend, can explain or advise in a simple way, then that's the best way to make an impact to my behavior. – Interviewee 14

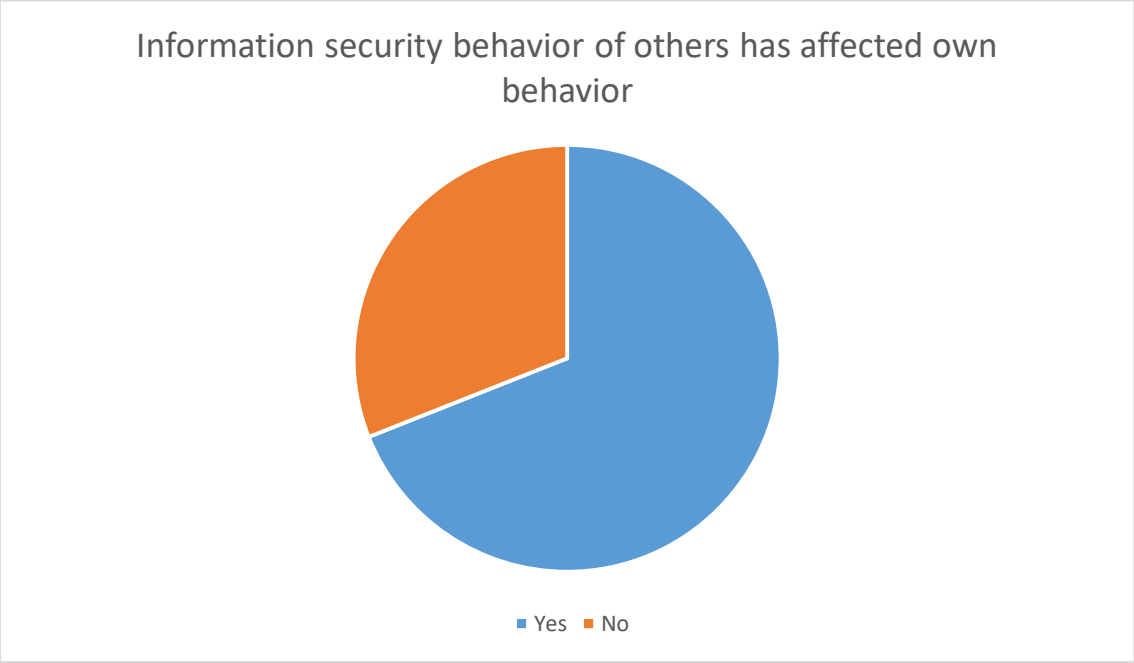

Figure 7 Effect of others on information security behavior

When asked whether the interviewees think that their information security behavior is at a good lever or if they want to change it somehow, interviewee 11 also mentions that tips from others might affect their future behavior.

> I feel that is at a good level. I have changed it for the better. Let's just say I belong to that "lazy" type of person who cares about things, but I don't want to take the effort. If someone says tips, then I might grab the tip for use. I feel that at least it's at a better level than a while ago. – Interviewee 11

6.7 Perceived risks, threats, vulnerabilities and incidents

Threats, vulnerabilities and incidents were raised as one of the most affecting factors of information security behavior. The loss of money and personal information worried a lot of the interviewees, and some consider that to be the greatest risk that they see if they would change their information security behavior. For example, interviewee 9 mentioned that they would worry that someone that found their phone could just start making payments.

> The risk in particular is that if you don't use a credit card, or MobilePay for terribly large sums, then maybe you don't need to be that precise. In the worst case, you can lose your money. – Interviewee 8

> I feel that security breach to my personal data would cause practical issues that would affect on everyday life. I wouldn't know who has all the information about me and how would they use that. From work point of view, impacts would be very large in company level and cause a lot of issues. – Interviewee 16

In addition to interviewee 16 that mentions they wouldn't know who has the data and how they would use it, two other interviewees mention identity theft as one of the major things that would bother them if they didn't behave securely.

> Payments could go to a different place than they should, or I could maybe not get some product, or someone could take my money, but I don't see that as such a strong risk. However, I feel like that in biometric identification, the risk of identity theft increases. - Interviewee 3

> I probably imagine that someone could hack into online banking and take the money, or someone would take my identity and I'd have to change my social security number. – Interviewee 13

None of the interviewees had experienced any information security issues except from usability when using biometric authentication. However, when the interviewees were asked whether they know someone or have heard about someone that has experienced information security related issues when using biometric authentication in mobile payments, some mentioned hearing about incidents that had happened to someone. None of the interviewees relatives or friends had experienced any issues, but some told that they have heard about security issues from the news or read about them, or that some person not close

to them has experienced issues. Figure 8 presents if the interviewees have heard that someone has experienced issues relating to information security.

> There are no outright incidents related to biometrics, but I've heard about incidents in the public about the facial recognition being deceived with a reconstructed picture from celebrity pictures. – Interviewee 2

> I have, but I don't remember it in detail. Someone once said that facial recognition had worked with someone else's face. I don't know about it in more depth. – Interviewee 10

> I have heard of someone stealing another person's phone and being able to access payment applications despite biometric authentication. – Interviewee 15

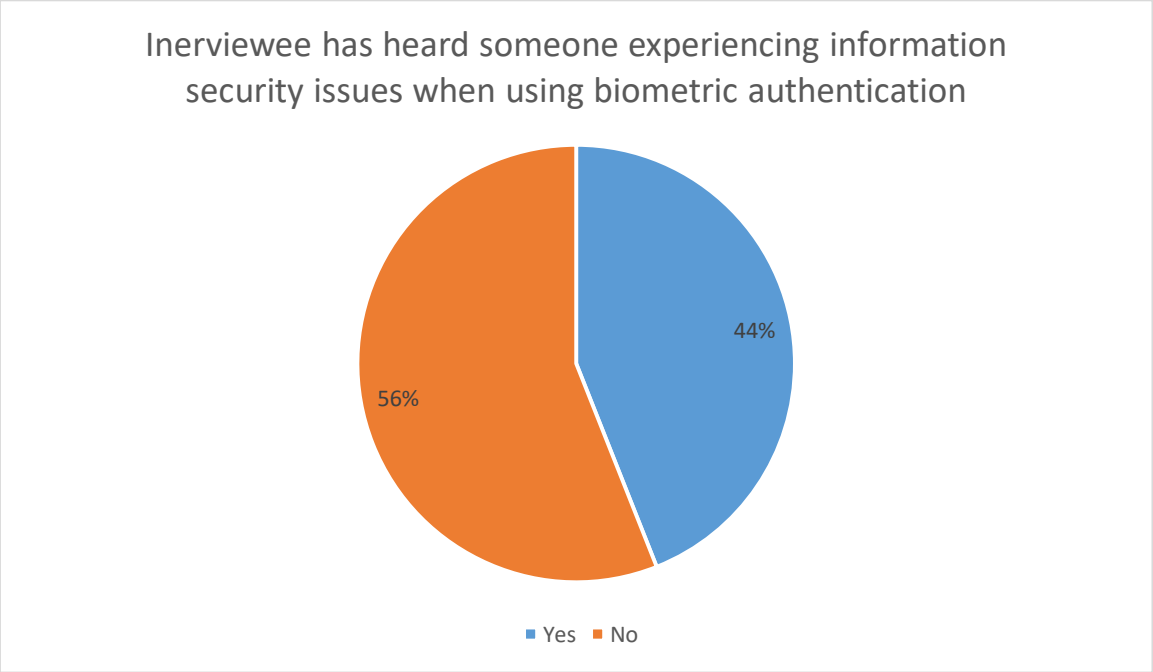

Figure 8 Has heard someone has experienced information security issues when using biometric authentication

When asked a series of questions what would change their behavior, and what kind of events would it require, 14 out of the 16 interviewees mention, that a breach to their personal data, or banking data would cause them to change their behavior. In addition, most of the interviewees mention that if a threat, vulnerability or an incident was widely reported in the news, they would consider changing their behavior.

> I think if my data was involved in some really big data leak with some personal information, then I could change my behavior. – Interviewee 7

> Certainly, if something happened that someone would misuse my information. If I were to be the target of a security attack, it would change radically. Also, if a loved one can give practical tips that resonate with me, because the security risk doesn't always

> feel like it would happen to myself. I think more that I don't have such kind of information or money that someone would want to steal. Although, on the other hand, data collection is quite ordinary. Of course, misuse of my data or any other event could make a difference. – Interviewee 14

> Widely reported issues in information security in applications that I am using. Cyber criminals stealing personal information that results in losing money, blackmailing, accessing my phone or other impact on my personal life. – Interviewee 15

One recurring theme in the non-professional interviewees answers was that some consider that the information of threats and vulnerabilities should be told to them in an easy way, or by a friend or other close person, and just reading them from news wouldn't make them change their behavior. Also, the ease of the required change is mentioned to be something that would affect the possible behavioral change.

> Recommendations from qualified friends who are more knowledgeable about things. Expert recommendations would make an impact, but they should be easy to do. But it should be in a language that is easily understandable. And that my data is stolen. Then I would change, but that would be learning through the hard wat. Also, if there was an easier way to secure the data more, I would be immediately prepared to change it. – Interviewee 13

The others mentioned quite similar responses than to the previous questions but emphasized the fact that the breach or vulnerability should be quite severe or in a large scale in order for them to completely stop using biometric authentication methods.

> If something like, it turned out to be really insecure, that even the media would talk about it a lot that biometric identifiers have been misused a lot. Of course, it also involves the idea that the phone has scanned my facial features, so what is possibly done with that data. That is, if it turned out something that that the facial data could be misused somehow. If, in one's own close circle, friend or family member would say something has happened, so it hits close, or some social fuss would raise. Or on the other hand, if I happened to read some research, but that would demand something really major. – Interviewee 14

6.8 New perspective on life

When asked about what would change their information security behavior, two of the interviewees, 10 and 11, mention that since having their own children, they have started to think more about information security and their own information security behavior, in addition to other factors. They consider it to be a big life change, that has had them thinking about many aspects of their security behavior.

> If I was part of a data leak or someone managed to hack me, it would change. Or if someone close to me would be part of a leak. At the moment, it feels relatively distant,

> however. But after the birth of my own child, I have become more thoughtful. I've started pondering what to download to the internet or should I even download anything at all, and giving permission for others to downlead content about my family. – Interviewee 10

> I would change if I found out that my personal pictures have been leaked to the web or if I spotted them from some weird website, or pictures of my child or persons I know would be misused. Would make me more cautious. After having a child, I've changed my Instagram profile to private, for example, I don't accept followers I don't know, and I've removed unknown followers. Become much more cautious after having children. Maybe I think social media differently than before, before thought that I make content for everyone, but now I want to share my life only with my friends. – Interviewee 11

6.9 New legislation and regulations

The final question related to the information security past experiences was if the interviewees consider that legislation, such as the GDPR, has affected their information security behavior. Four of the interviewees, 1, 5, 12 and 16, consider that new legislation has had an effect to their personal information security behavior. In addition, six other interviewees think that new legislation has influenced how they behave regarding information security at work. That leaves five of the interviewees that do not see any effect of the legislation to their information security behavior. Figure 9 presents the details if the interviewees think that the new legislation has affected their behavior.

> Perhaps in the sense that, as a security professional, the data processing and all that, GDPR brings to mind that it should be better researched. – Interviewee 3

> No, not knowingly at least. – Interviewee 8

> Yeah at work, but not so much in my personal life. Maybe so that I find it even harder to understand. That I don't really have the latest information on how to act, the uncertainty increases every time more information comes. – Interviewee 13

> Yes, for example I am more careful of sharing sensitive data and always use secure ways to do that. – Interviewee 16

In addition, two of the interviewees, 5 and 6, mention that if a new legislation would come that would either require to change the behavior or make data handling even more restricted, they would change their behavior. Interviewee 6 also mentions, that if their employer would require changes, they would make them. Restrictive legislation was also mentioned to be one of the possible reasons why to change information security behavior. Interviewee 5 also mentions that they would stop using biometric authentication if they would have to consent to

some terms and conditions where it was said that the information can be stored by The National Security Agency (NSA) or similar.

> Probably if there was a really massive breach or something where the whole concept would be completely questioned. Or if tighter regulation were to come, or if it would be banned altogether. So, a pretty big change. – Interviewee 4

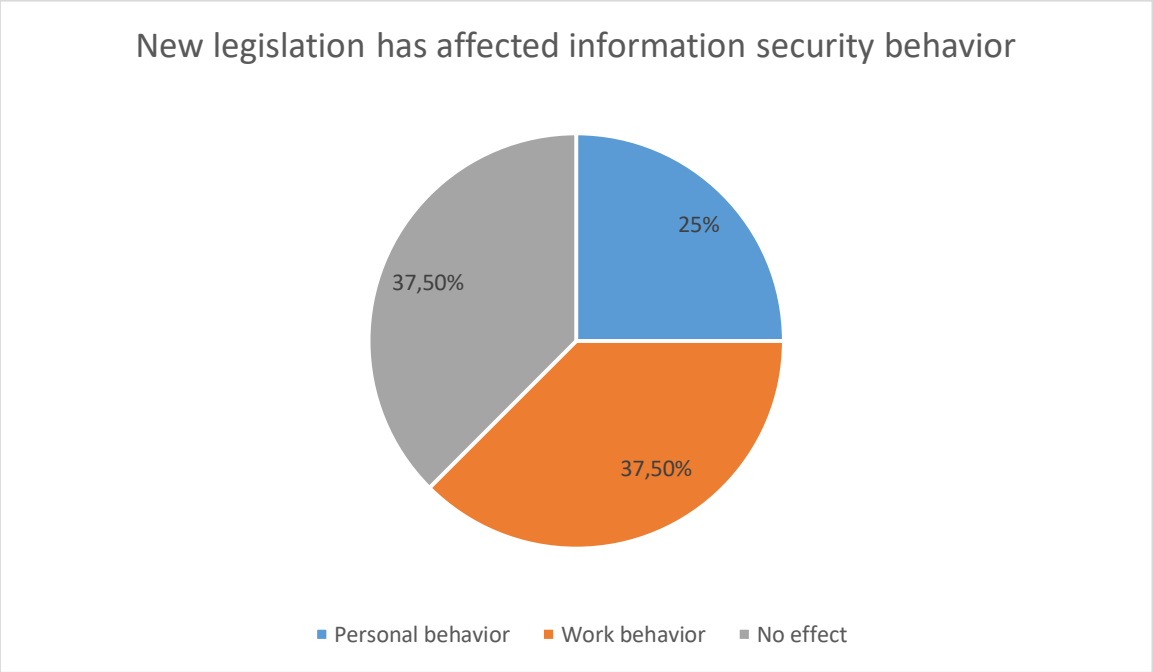

Figure 9 Legislation affects information security behavior

6.10 No intention to change information security behavior

The last interview theme had five questions around the possible future changes to interviewee's information security behavior. The first question was a subjective question in which the interviewees were asked if they consider their information security behavior to be currently at a good level, or if they wanted to change it somehow. When asking this question, it was also explained that the changes can be towards more secure behavior or even towards not behaving so securely. Five out of the 16 interviewees, three professionals and two non-professionals, consider that their information security is at a good level and do not want to change it in any way.

> It's at a pretty good level, and I would not want to change it. Generally, I think it's at a better level than with normal people. – Interviewee 2

Only two of the interviewees, non-professionals 13 and 15, consider that their information security behavior is not on a good level. However, interviewee 15 doesn't want to change their behavior either. Interviewee 13 mentions that

they think they're currently "easily hackable", and they would like to improve their password management and use more biometric authentication methods instead of alphanumeric passwords.

To achieve even more deeper understanding of intended change behavior, the interviewees who use biometric authentication methods were asked what type of events it would require for them to completely stop using the biometric authentication in mobile payments. Two of the interviewees, 3 and 13, mentioned, that they can't think of any events that would stop them using the biometric authentication. Interviewee 3 reasoned the statement with that they don't consider biometric authentication to be in such a large role in their life and thus can't think of anything. Interviewee 13 said that they think biometric authentication is so easy to use, that they would rather stop using the application or device connected to it than biometric authentication.

7 DISCUSSION

This chapter reviews and discusses the results of the study against the research questions and considers the relevance of the research results. In the third chapter, the reliability and validity of the study are examined, and generalization of the results is contemplated. The limitations of the study are also assessed.

7.1 Factors affecting the intention of changing information security behavior

One of the major findings of this research is that the results of the empirical research support the previously researched information that was described in the literature review. Most of the interviewees said that information security is important to them and they had made conscious information security choices in their behavior. They also described that with their current information security behavior, they want to gain confidence that their personal information is safe. This observation supports that security and safety needs direct the user's behavior. Usability was also mentioned to be one of the factors that has led the interviewees to behave in a certain way with information security. Both these observations, the need of safety and the need of the ease of use, can be found also from the theories of needs by Maslow and Alderfer. Most of the previous changes had come from their own experiences and from interactions with others, which can be seen to in Searle's (1983) theory of subjective reality and the social appreciation needs identified by Maslow and Alderfer.

When it comes to the factors that might affect the future information security behavior, the interviewees listed many things. The most commonly mentioned were reported threats, vulnerabilities and incidents, and especially to their own data or money. It thus can be claimed that the user is more concerned and prone do change their behavior if the security issue is relating to something important to them and the threat happening directly against them rather than if they hear that the issue has happened to someone else. Users need a confirmation

that their personal information is secured and that they don't need to be concerned.

The results also show that the bigger the threat, the bigger the response to the threat. The interviewees mentioned that if the vulnerability or incident was severe, they would completely stop using biometric authentication and this would cause a major change to their information security behavior. The severity was also highlighted to be dependent about whether the incident is against their own personal data, and money or financial data. This supports the previously made claim, that individuals have the tendency to change the behavior especially when they feel like it is a benefit to themselves. Maslow's hierarchy of needs (1983) also supports this observation, as the safety needs identified in it are described as people want to experience order, predictability and control in their own lives.

New perspective on life, or a new subjective reality according to the theories, such as having a child was also mentioned to be an influencing factor to change the behavior. It's said that having a child is a huge emotional change, and emotional change is the basis of behavioral change according to Alasuutari (2016). So, it is not a surprise that a significant change in somebody's life also affects the behavior.

Although most of the interviewees said that the information security behavior of others has affected their current behavior when directly asked, only a few mentioned that recommendations from others would affect their behavior in the future. According to this, it's hard to withdraw a conclusion if aspects such as social acceptance and belongingness needs really have an impact to the information security behavior change.

Other significant finding was that in addition to usability being one of the most important things that affects the current information security behavior of an individual, usability was also named as one of the prominent factors affecting the behavioral change. Most interviewees explained that if the usability would suffer from the information security behavior change, they wouldn't make the change. However, it is unrealistic to expect to achieve maximum usability and at the same tame maximum security in all secure systems. In most systems, it can be considered as a trade-off between security and usability. The goal can be seen to be minimizing the possibility of threat scenarios and maximizing the usability. (Kainda, Flechais & Roscoe, 2010.) Based on these claims, it can be said that users seek for convenience also with their information security behavior. Thus, they might not behave in the most secure way, even though they understand it's importance. This can lead to the discussion whether the users really have an understanding of the risks their behavior can result in. This would suggest that adding information security awareness and awareness of the impact of user's own actions on countering threats. However, it seems that higher information security awareness doesn't always resolve in having better and more secure information security behavior. This is discussed more in the next chapter.

7.2 Differences between information security professionals and non-professionals

The main observation regards the differences of information security professionals compared to non-professionals of the research is that the professionals considered more that the information security behavior of others does not affect theirs. This might be due to the fact that the information security knowledge and awareness can be claimed to be usually already quite high within the information security professionals, so they feel like they do not need information security tips from others. The information security professionals might also feel like they don't need advising or tips from other since they should be the most conscious of the information security aspects. This is also in line with the previous studies that show that information security professionals usually have a better understanding of information security risks, and therefore perhaps don't need any guidance from others. The only time the information security professionals mentioned that the information security behavior of others has affected theirs was when they referred to their co-worker's behavior. This might be due to the fact that Wolf, Kuber and Aviv (2018 and 2019) also observed in their research, that information security professionals are usually more influenced by work requirements. Even though co-workers' recommendations do not directly link to work requirements, it is worth to remember that all of the information security professionals interviewed for this research were working for the same employer and thus have the same requirements for information security at work.

As mentioned in the previous chapter, usability was named as one of the most important factors affecting information security behavior and the interviewees said that they might not change their information security behavior for the better if it affects negatively to the usability. There were no significant differences in this regardless the level of information security knowledge, as both information security professionals and non-professionals answered the question similarly. Although the information security professionals seemed to be more aware of the risks, they still chose not to change their behavior if usability would be impacted. Thus, it can be claimed that usability plays such an important role in the user experience that it might affect the information security behavior negatively, despite the information security knowledge. The previous research supports this, although usually the non-professionals were seen as the ones not performing securely even with the knowledge. However, usability has already previously been seen as having a big impact on information security behavior for both information security professionals and non-professionals, as was studied for example by Wolf, Kuber and Aviv (2019).

Other differences were not found in this research. The responses to the interview questions were relatively similar, no matter if the respondent was considered to be an information security professional or a non-professional. However, this is an observation itself and shows that the information security behavior is nowadays perhaps so familiar to even non-professionals, that their

information security awareness is already quite high despite the lack of education or experience in the field. This can be claimed to be due to the fact that information technology, such as smartphones with biometric authentication methods, are mostly part of our everyday life and not considered to be a luxury that only few can afford, and this forces everyone to contemplate their choices when it comes to information security. This observation also differs from previous studies, as previous studies have seen a clear distinction between information security professionals and non-professionals, for example when it comes to the adaptation of the use of biometric authentication and the trust. Almost all of the non-professionals interviewed in this study were quite aware of the risks and threats that are connected with biometric authentication, which differs from previous studies.

7.3 Validity, reliability, generalization and limitations of the study

Reliability and validity are an indication of credibility in scientific research. They can be evaluated differently in quantitative and qualitative research. Reliability refers to whether a researcher collects data that can be trusted. Because qualitative research is characterized by a mixture of structured and unstructured knowledge rather than specific research instruments, reliability should be addressed with different aspects compared to quantitative research. On the other hand, validity can be defined as the relevance of the findings collected. In other words, it is a question of whether the phenomenon studied is what the researcher seeks to study (Hirsjärvi & Hurme, 2015.)

The validity of the study is increased by using a framework that is suitable to study the topic. The research framework used was created to be used in the empirical research to explore the information behavior change. The interview questions were formed based on the research framework. As the interview phase progressed and more interviews were conducted, the framework was found to be appropriate to explore the topic, as the interviews provided information on the themes presented in the framework. The data collected was very rich in information on some topics. Thus, it can be assumed that the research framework is suitable for researching the presented research questions, which increases the validity and reliability of the research. The validity and reliability of a study can be also increased by having another researcher go through the observed information. (Franklin & Ballan, 2001.) This study is revised by researchers from the University of Jyväskylä, which increases the validity and reliability.

The non-professional interviewees were selected by discretionary sampling which is common in qualitative research (Hirsjärvi & Hurme, 2015). The interviewees worked in various occupations and they also had different educational backgrounds. The aim of the interviewee selection was to obtain as comprehensive depiction of the research subject as possible, which increases the reliability

and validity of the study and the possibility of generalization. The professional interviewees were selected from the same organization and occupation in hopes to ensure similar level of information security knowledge. However, the possibility of generalization of the results regarding the difference of the two groups might be reduced by the small sample size. The different groups were only conducted from 8 interviewees, but the suggested amount to be able to compare different groups is to have 12 interviewees each. (Guest, Bunce & Johnson, 2006.) Nonetheless, the amount was found to be an appropriate since the interviews generated new information from each theme and topic.

The interviews were received only from Finnish citizens who all had an academic degree, which may limit the generalization of the results. One possible limitation is also the age of the interviewees. All of the interviewees were from age group 25 to 38 and can be considered to be more prone to be familiar with the use of different emerging technologies. Thus, they might have a greater understanding of the threats the technologies face than possibly an elderly person would have, and the results cannot be fully generalized.

The interviews were conducted as semi-structured interviews because qualitative research requires openness, flexibility, and improvisation. The aim was to obtain as diverse information as possible on research topics, and the semi-structured interview method was considered to provide the best opportunity to gather such information. Choosing a semi-structured interview method as a data collection method thus increases the reliability and validity of the study. Using the framework in interviews helps to obtain detailed and rich information, which increases the validity of the study. It is also desirable to use the framework as a basis for the interview structure as it helps the interviewer to lead the interview towards the research topics.

Sometimes the interviewee may misunderstand the question, leading to incorrect answers. The likelihood of this happening was reduced during the interviews by carefully explaining the questions and reformulating the question if the interviewee seemed to misunderstand it. The influence of other people was also removed from the interview design by conducting the interviews as individual interviews where other people could not influence the respondent.

Interviews have some weaknesses so using interviews as the data collection method can in some cases be a threat to the reliability and validity of a study. The researcher should be trained in creating a valid interview frame and conducting an interview. Poorly conducted interview can lead to distorted answers. Other reasons can also affect the distortion of the answers. The interviewee may experience the interview setting to be threatening which may affect their answers. People also have a tendency to give socially acceptable answers in interviews. In this study, the focus was on information security behavior, and it is possible that some of the interviewees might have altered their responses to create a more secure description of their information security behavior.

The reliability of research is often difficult to assess when research is conducted using qualitative methods. Accurate and truthful descriptions of people, methods, and cases are central to assessing the reliability of qualitative research.

Reliability is increased by describing the implementation of the study as accurately as possible. (Hirsjärvi & Hurme, 2015) The implementation of empirical research is described in detail in previous chapters, and therefore it can be said that reliability of the research is increased by the accurate description.

7.4 Recommendations for practice and suggestions for further study

It was observed that all of the interviewees for this study considered information security to be important. However, some of the non-security professionals mentioned that they think that information about the information security risks and threats is often presented so that they do not understand it and they feel like that is the reason why their behavior might be unsecure. Therefore, it would be good to pay attention to how the instructions or news about information security are written, so that they are not only understandable for the information security professionals, but for a wider audience as well. Furthermore, more information security training should be available for the non-professionals.

This research mainly supported the existing studies about the relevant subjects. Even though the non-security professionals mentioned they don't necessarily understand all the requirements for secure behavior, the results show quite high information security awareness of the non-security professionals, which can be interpreted that more research should be done to observe the actual current information security knowledge level of non-professional users. It seems, that due to the increased amount of information security threats, the level of information security awareness of an information technology everyday user has increased as well.

Other aspect that would be worth studying is how much does the perceived severity of the threat affect the information security behavior, especially with emerging technologies such as biometric authentication. The interviewees of this study emphasized that the bigger the threat, the bigger the effect on them. However, where can we draw the line? It would be interesting to know what threats can be seen not severe enough for the information security behavior not to change.

8 CONCLUSION

The aim for this Master's Thesis was to identify the factors which affect the information security behavior change when using biometric authentication in mobile payments. Previous studies had looked into the security issues of biometric authentication, information security behavioral change and the differences between information security professionals and non-security professionals. However, no recent studies had combined all these three aspects, even though the amount of mobile payment users has increased, and biometric technologies have evolved rapidly over the past years. In addition, it is interesting to understand what kind of differences good information security knowledge brings to information security behavior. The results show that usability is seen as a key factor when deciding information security behavior, even to the level that the users are willing to behave insecurely if it increases usability. Furthermore, the information security awareness of non-security professionals is at a high level, which suggest that the information security awareness level of an average mobile device user could be even more examined.

The research questions for this study were *"What factors would affect the intention to change information security behavior in the context of using biometric authentication in mobile payments?"* and *"What differences can be seen in the intention to change information security behavior comparing information security professionals and non-professionals, in the context of using biometric authentication in mobile payments?"*. These themes were studied through a literature review and an empirical study. The empirical study was conducted as a qualitative research and the interviews were conducted as semi-structured interviews. The interview was constructed based on framework identified by Alasuutari (2016) and the information identified in the literature review. Although the information security behavior and factors that affect it have previously studied extensively, there is no data about the change in information security behavior when it comes to biometric authentication in mobile payments. Because using biometric authentication in mobile payment applications has increased significantly during the past years, it was important to conclude research from this aspect as well.

In the second chapter, the definition of mobile payment and the information security related threats towards it were discussed. In the third chapter, authentication in general and different types of authentication methods were introduced. Chapter four discussed the biometric authentication methods in more detail and defines the information security risks related to using biometric authentication in mobile payments. Chapter five then gave a brief introduction to information security behavior as a concept and introduced the theoretical framework used in this research. The sixth chapter describes the research method for empirical study and the scope of the study. In the seventh chapter, the results of the empirical study are discussed. In the eight chapter, the results are discussed and analyzed. The final chapter of this study concludes the study.

This research aimed to find answers for the defined research questions by conducting literature review and an empirical study. The empirical study followed the findings of the literature review to some extent, but new findings were made as well. It needs to be reminded that due to the limitations of this study, it might not provide generalizable findings but nevertheless, the findings of the study provide an interesting angle to the information security behavior of mobile payment applications users. For this research to be more generalizable, a larger population with even more diverse background could have been interviewed to get a boarder view of the topic.

These research questions were answered by observing seven different themes: usability, trust and confidence, information security knowledge, the behavior of others, new perspective on life, new legislation and regulations, and perceived risks, threats, vulnerabilities and incidents. As an answer for the first research question about the factors affecting the intention to change the behavior, it was observed that the most general factors were experienced threats, vulnerabilities and incidents, the behavior of others, and usability. The experienced threats, vulnerabilities and incidents were perceived to have a more notable changes to the behavior depending on the severity and the involved information or asset. Usability, on the other hand, was usually seen to have a negative impact on information security behavior change. This finding suggests that that usability plays such an important role in the user experience that the user is ready to behave in an unsecure way.

For the second research question, no significant differences were found besides that information security professionals tend to feel like the information security behavior of others doesn't affect theirs. This can be claimed to be connected to the higher level of information security awareness an individual considers having. In addition, it was discussed that the lack of findings for the second research question can be influenced by the information technology and therefore also information security issues becoming more common. The observations for the second research question can be seen emphasizing the importance of information security awareness affecting information security behavior.

REFERENCES

Adler, A. (2003). Sample images can be independently restored from face recognition templates. *CCECE 2003-Canadian Conference on Electrical and Computer Engineering. Toward a Caring and Humane Technology,* Vol. 2, 1163-1166. IEEE.

Agarwal, S., Khapra, M., Menezes, B., & Uchat, N. (2007). Security issues in mobile payment systems. *Proceedings of ICEG 2007: The 5th International Conference on E-Governance*, 142-152.

Ahmed, A. E. E. & Traore, I. (2007). A New Biometric Technology Based on Mouse Dynamics. *IEEE Transactions on Dependable and Secure Computing, 4*(3), 165-179.

Ahmed, W., Rasool, A., Nebhen, J., Kumar, N., Shahzad, F., RehmanJaved, A., & Jalil, Z. (2021). Security in Next Generation Mobile Payment Systems: A Comprehensive Survey. *arXiv e-prints, arXiv-2105*.

Alasuutari, M. (2016). Prosessiteoreettinen näkökulma, joka selittää henkilökohtaisen tietokoneen käyttöön liittyvää tietoturvakäyttäytymisen muutosta. *Jyväskylä studies in computing,* (234).

Altinkemer, K., & Wang, T. (2011). Cost and benefit analysis of authentication systems. *Decision Support Systems, 51*(3), 394-404.

Anderson, C. L., Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *Management Information Systems : Mis Quarterly, 34*(3), 613-643.

Apple. (8.6.2021) Apple Pay. Retrieved from https://www.apple.com/fi/apple-pay/

Asgharpour, F., Liu, D., & Camp, L. J. (2007). Mental models of security risks. *International conference on financial cryptography and data security* (367-377). Springer, Berlin, Heidelberg.

Au, Y. A. & Kauffman, R. J. (2008). The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application. *Electronic Commerce Research and Applications, 7*(2), 141-164.

Aytes, K., & Connolly, T. (2004). Computer Security and Risky Computing Practices: A Rational Choice Perspective. *Journal of Organizational and End User Computing (JOEUC), 16*(3), 22-40.

Bailey, K. O., Okolica, J. S., & Peterson, G. L. (2014). User identification and authentication using multi-modal behavioral biometrics. *Computers & Security,* 43, 77-89.

Barkadehi, M. H., Nilashi, M., Ibrahim, O., Fardi, A. Z., & Samad, S. (2018). Authentication systems: A literature review and classification. *Telematics and Informatics, 35*(5), 1491-1511.

Bartsch, S., & Volkamer, M. (2013). Effectively Communicate Risks for Diverse Users: A Mental-Models Approach for Individualized Security Interventions. *M. Horbach, INFORMATIK 2013 – Informatik angepasst an Mensch, Organisation und Umwelt. Bonn, Gesellschaft für Informatik e.V.,* 1971-1984.

Bergadano, F., Gunetti, D., & Picardi, C. (2002). User authentication through keystroke dynamics. *ACM Transactions on Information and System Security (TISSEC), 5*(4), 367-397.

Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology, 2*(3), 13-28.

Bridle, C. C., Riemsma, R. P., Pattenden, J. J., Sowden, A. J., Mather, L. L., Watt, S., & Walker, A. A. (2005). Systematic review of the effectiveness of health behavior interventions based on the transtheoretical model. *Psychology & Health, 20*(3), 283-301.

Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., & Senior, A. W. (2013). *Guide to biometrics.* Springer Science & Business Media.

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. *2012 IEEE Symposium on Security and Privacy,* 553-567. IEEE.

Bosamia, M., & Patel, D. (2019). Wallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures. *Int. J. Comput. Sci. Eng, 7*(1), 810-817.

Bravo-Lillo, C., Cranor, L. F., Downs, J., & Komanduri, S. (2010). Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy, 9*(2), 18-26.

Braz, C., & Robert, J. M. (2006). Security and usability: the case of the user authentication methods. *IHM Vol. 6*, 199-203.

Burrows, M., Abadi, M. & Needham, R. (1990). A logic of authentication. *ACM Transactions on Computer Systems, 8*(1), 18-36.

Choi, H., Park, J., Kim, J., & Jung, Y. (2020). Consumer preferences of attributes of mobile payment services in South Korea. *Telematics and Informatics, 51,* 101-397.

Clarke, R. (1994). Human identification in information systems: Management challenges and public policy issues. *Information Technology & People, 7*(4), 6-37.

Connell, J., Ratha, N., Gentile, J., & Bolle, R. (2013). Fake iris detection using structured light. *Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference,* 8692-8696. IEEE.

Coventry, L., De Angeli, A., & Johnson, G. (2003). Biometric verification at a self service interface. *Contemporary ergonomics,* 247-25

Curve, (21.6.2021) Curve mobile credit card. Retrieved from https://www.curve.com/

Dahlberg, T., Huurros, M., & Ainamo, A. (2008). Lost opportunity why has dominant design failed to emerge for the mobile payment services market in Finland?. *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008),* 83-83. IEEE.

Daugman, J. (2009). *How iris recognition works. In The essential guide to image processing*, 715-739. Academic Press.

Edwards, K. (2015). Examining the security awareness, information privacy, and the security behaviors of home computer users. *Nova Southeastern University, College of Engineering and Computing.,* 947

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of management journal, 50*(1), 25-32.

Elliott, S. J., O'connor, K., Bartlow, E., Robertson, J. J., & Guest, R. M. (2015). Expanding the human-biometric sensor interaction model to identity claim scenarios. *IEEE International Conference on Identity, Security and Behavior Analysis (ISBA 2015),* 1-6. IEEE.

Ellsworth, P. C. & Schrerer, K. R. (2003). *Appraisal processes in emotion. In R.J. Davidson, K.R. Screrer & H. Hill Goldsmith (Eds) Handbook of affective sciences.* Oxford; New York: Oxford University Press.

Franklin, C., & Ballan, M. (2001). *Reliability and validity in qualitative research. The handbook of social work research methods*, 4(273-292).

Furnell, S. & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security,* 31, 983–988.

Furnell, S., Tsaganidi, V. & Phippen, A. (2008). Security beliefs and barriers for novice Internet users. *Computers & security* (27), 235-240.

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field methods, 18*(1), 59-82.

Goode, A. (2014). Bring your own finger – how mobile is bringing biometrics to consumers. *Biometric Technology Today, 2014*(5), 5-9.

Gujrathi, S. (2014). Heartbleed bug: An openssl heartbeat vulnerability. *International Journal of Computer Science and Engine ter Science and Engineering, 2*(5), 61-64.

Guo, S., Xiang, T., & Li, X. (2019). Towards Efficient Privacy-Preserving Face Recognition in the Cloud. *Signal Processing.*

Hair, J. F., Page, M., & Brunsveld, N. (2019). *Essentials of business research methods.* Routledge.

Harrel, A.M. & Stahl, M.J. (1984). McClelland's trichotomy of needs theory and the job satisfaction and work performance of CPA firm professionals. *Accounting, organizations and society 9* (3), 241-252.

Hassan, M. A., Shukur, Z., Hasan, M. K., & Al-Khaleefa, A. S. (2020). A review on electronic payments security. *Symmetry, 12*(8), 1344.

Heimo, O. I., Hakkala, A., & Kimppa, K. K. (2011). The problems with security and privacy in eGovernment-Case: Biometric passports in Finland. *Ethicomp 2011 Conference Proceedings, Andy Bisset, Terrell Ward Bynum, Ann Light, Angela Lauener, Simon Rogerson (Eds.),* 210-217.

Helkama, K., Myllyniemi, R. & Liebkind, K. (1998). *Johdatus sosiaalipsykologiaan*. Helsinki. Edita.

Hirsjärvi, S. & Hurme, H. (2015). *Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö.* Helsinki: Gaudeamus Helsinki University Press

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2016). *Tutki ja kirjoita (21. uud. painos).* Helsinki: Tammi.

Huh, J. H., Verma, S., Rayala, S. S. V., Bobba, R. B., Beznosov, K., & Kim, H. (2017). I Don't Use Apple Pay because it's less secure...: perception of security and usability in mobile tap-and-pay. *Workshop on Usable Security, San Diego, CA.*

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2019). Security awareness: The first step in information security compliance behavior. *Journal of Computer Information Systems,* 1-12.

Ijiri, Y., Sakuragi, M., & Lao, S. (2006, May). Security management for mobile devices by face recognition. *7th International Conference on Mobile Data Management (MDM'06*)(49-49). IEEE.

Ion, I., Reeder, R., & Consolvo, S. (2015). "... no one can hack my mind": Comparing Expert and Non-Expert Security Practices. *Eleventh Symposium On Usable Privacy and Security (SOUPS). ACM Press, Ottawa, Canada,* 327-346.

Isaac, J. T., & Sherali, Z. (2014). Secure mobile payment systems. *IT Professional, 16(*3), 36-43.

Jain, A. K., Flynn, P., & Ross, A. A. (Eds.). (2007). *Handbook of biometrics.* Springer Science & Business Media.

Jain, A. K., & Nandakumar, K. (2012). Biometric Authentication: System Security and User Privacy. *IEEE Computer, 45*(11), 87-92.

Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters, 79,* 80-105.

Jovanovic, M., & Muñoz-Organero, M. (2011). Analysis of the latest trends in mobile commerce using the NFC technology. *Journal of Selected Areas in Telecommunications (JSAT), May Edition, 2011,* 1-12

Kadhiwal, S., & Zulfiquar, A. U. S. (2007). Analysis of mobile payment security measures and different standards. *Computer Fraud & Security, 2007*(6), 12-16.

Kainda, R., Flechais, I., & Roscoe, A. W. (2010). Security and usability: Analysis and evaluation. *2010 International Conference on Availability, Reliability and Security*, 275-282. IEEE.

Karnouskos, S. (2004). Mobile payment: A journey through existing procedures and standardization initiatives. *IEEE Communications Surveys & Tutorials, 6*(4), 44-66.

Kathuria, M. (2010). Design of a Vein Based Personal Identification System. *Advances in Recent Technologies in Communication and Computing (ARTCom), 2010 International Conference*, 284-286. IEEE.

Kong, J., Lu, Y., Wang, S., Qi, M., & Li, H. (2008). A two stage neural network-based personal identification system using handprint. *Neurocomputing, 71*(4-6), 641-647.

Koundinya, P., Theril, S., Feng, T., Prakash, V., Bao, J., & Shi, W. (2014). Multi resolution touch panel with built-in fingerprint sensing support. *Proceedings of the conference on Design, Automation & Test in Europe,* 245. European Design and Automation Association.

Lanitis, A. (2010). *Facial age estimation*. Scholarpedia, 5(1), 9701.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review.*

Lehto, M. (2019). Ihmisten tunnistaminen tehostuu - uhka yksityisyydelle? Retrieved on 5.7.2021 from https://www.upseeriliitto.fi/sotilasaikakauslehti/1_2019/ihmisten_tunnistaminen_tehostuu_-_uhka_yksityisyydelle

Leo, M., De Marco, T., & Distante, C. (2014). Highly usable and accurate iris segmentation. *2014 22nd International Conference on Pattern Recognition (ICPR),* 2489-2494. IEEE

Leung, M. K., Fong, A. C. M., & Hui, S. C. (2007). Palmprint verification for controlling access to shared computing resources. *Pervasive Computing, IEEE, 6*(4), 40-47.

Li, Y., Siponen, M. (2011) A Call For Research On Home Users' Information Security Behaviour. *PACIS 2011 Proceedings*, 112

Liu, Y., Kostakos, V., & Deng, S. (2013). Risks of using NFC mobile payment: Investigating the moderating effect of demographic attributes. *Effective, Agile and Trusted eServices Co-Creation*, 125.

Maeva, A., & Severin, F. (2009). High resolution ultrasonic method for 3D fingerprint recognizable characteristics in biometrics identification. *2009 IEEE International Ultrasonics Symposium,* 2260-2263. IEEE.

Magee, J. C., & Langner, C. A. (2008). How personalized and socialized power motivation facilitate antisocial and prosocial decision-making. *Journal Of Research In Personality, 42*(6), 1547-1559.

Maslow, A.H. (1954). *Motivation and personality.* New York. Harper & Brothers.

Maslow, A.H. (2007). *Motivation and personality.* New Delhi. Pearson.

McClelland, D.C. & Burnham, D.H. (1995). Power is the great motivator. Harward business review 73 (1) , pp. 126-139.

Me, Me, G. (2003). Security overview for m-payed virtual ticketing. *14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003. Vol.* 1, 844-848. IEEE.

Meenakshi, V. S., & Padmavathi, G. (2009). Security analysis of password hardened multimodal biometric fuzzy vault. *World Acad. Sci. Eng. Tech, 56*, 312-320.

Menkus, B. (1988). Understanding the use of passwords. *Computers & Security, 7*(2), 132-136.

MobilePay (8.6.2021) Retrieved from https://mobilepay.fi/

Modi, S. K., Elliott, S. J., Whetsone, J., & Hakil Kim. (2007). Impact of age groups on fingerprint recognition performance. *Automatic Identification Advanced Technologies, 2007 IEEE Workshop,* 19-23.

Nordea (21.6.2021) Nordea Siirto. Retrieved from https://www.nordea.fi/en/personal/our-services/online-mobile-services/siirto.html

Nurmi, J.E. & Salmela-Aro, K. (2002). *Modernin motivaatiopsykologian perusta ja käsitteet.* Jyväskylä. PS-kustannus.

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE, 91*(12), 2021-2040.

Oppliger, R. (2016). *SSL and TLS: Theory and Practice.* Artech House.

Oppliger, R., Hauser, R., & Basin, D. (2006). SSL/TLS session-aware user authentication–Or how to effectively thwart the man-in-the-middle. *Computer Communications, 29*(12), 2238-2246.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security, 31*(5), 673-680.

Pato, J. & Millet, L. (2010). *Biometric recognition: challenges and opportunities*. National Academies Press.

Pattinson M., Butavicius M., Parsons K., McCormac A., Calic D. (2015) Factors that Influence Information Security Behavior: An Australian Web-Based Study. *Human Aspects of Information Security, Privacy, and Trust, HAS 2015*, 231-241

Peltonen & Ruohotie (1987). *Motivaatio. Menetelmiä työhalun parantamiseksi.* Helsinki. Otava.

Phillips, T., Zou, X., & Li, F. (2017). A Cancellable and Privacy-Preserving Facial Biometric Authentication Scheme. *Proceedings - 14th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2017*, 545–549.

Pivo. (8.6.2021) Retrieved from https://pivo.fi/

Ramos de Luna, I., Liébana-Cabanillas, F., Sánchez-Fernández, J., & Muñoz-Leiva, F. (2019). Mobile payment is not all the same: The adoption of mobile payment systems depending on the technology applied. *Technological Forecasting and Social Change, 146*, 931-944.

Ramu, S. (2012). Mobile malware evolution, detection and defense. *EECE 571B, Term Survey Paper*

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journal, 40*(3), 614- 634.

Renaud K. (2005). Evaluating Authentication Mechanisms. *Security and usability: Designing secure systems that people can use,* 103-128

Robbins, S.P. (1993). *Organizational behavior: concepts, controversies and applications.* Englewood Cliffs (N. J.): Prentice Hall, cop.

Rui, Z., & Yan, Z. (2018). A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification. *IEEE Access, 7*, 5994-6009.

Sabzevar, A. P. & Stavrou, A. (2008) Universal multi-factor authentication using graphical passwords. *2008 IEEE international conference on signal image technology and internet based systems,* 625-632. IEEE.

Sadasivuni, K. K., Houkan, M. T., Taha, M. S., & Cabibihan, J. J. (2017). Antispoofing device for biometric fingerprint scanners. *IEEE International Conference on Mechatronics and Automation (ICMA)* (683-687). IEEE.

Schultze, U., & Avital, M. (2011). Designing interviews to generate rich data for information systems research. *Information and Organization, 21*(1), 1–16

Schüler, J., Brandstätter, V., & Sheldon, K. (2013). Do implicit motives and basic psychological needs interact to predict well-being and flow? Testing a universal hypothesis and a matching hypothesis. *Motivation & Emotion, 37(*3), 480-495.

Searle, J. (1995). *The construction of social reality.* New York. Free press.

Searle, J. (1983). *Intentionality. An essay in the philosophy of mind.* Cambridge: Cambridge University Press.

Sharma, M.K. (2017) Electronic Cash over the Internet and Security Solutions. *Int. J. Adv. Res. Comput. Sci*, 8, 229.

Shirey, R. (2003). RFC 2828–Internet security glossary, 2000.

Siponen, M. (2001) Five dimensions of information security awareness. *Computers and society, 31*(2), 24-29

Smith, C. A., & Lazarus, R. S. (1990). Emotion and adaptation. *Handbook of personality: Theory and research,* 609-637.

Taylor, E. (2016). Mobile payment technologies in retail: A review of potential benefits and risks. *International Journal of Retail & Distribution Management, 44*(2), 159-177.

Theofanos, M.F., Stanton, B., Furman, S., Prettyman, S.S., & Garfinkel, S. (2017). Be Prepared: How US Government Experts Think About Cybersecurity. *Network and Distributed System Security Symposium (NDSS). Information Society, San Diego, CA,* 1-11.

Thomson, M. E., & von Solms, R. (1998). Information security awareness: educating your users effectively. *Information management & computer security.*

Vaniea, K.A., Rader, E., & Wash, R. (2014). Betrayed by updates: how negative experiences affect future security. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, Toronto, ON*, 2671-2674.

Vilkko-Riihelä, A. (1999). *Psyyke: psykologian käsikirja.* WSOY.

Virvilis, N., Tsalis, N., Mylonas, A., & Gritzalis, D. (2014). Mobile devices: A phisher's paradise. *2014 11th International Conference on Security and Cryptography (SECRYPT)* (1-9). IEEE.

Wang, Y., Hahn, C., & Sutrave, K. (2016). Mobile payment security, threats, and challenges. *2016 second international conference on mobile and secure services (MobiSecServ),* 1-5. IEEE.

Wang, Y., Streff, K., & Raman, S. (2012). Smartphone security challenges. *Computer, 45*(12), 52-58.

Wang, C., Wang, Y., Chen, Y., Liu, H., & Liu, J. (2020). User authentication on mobile devices: Approaches, threats and trends. *Computer Networks, 170,* 107-118.

Wolf, F., Kuber, R., & Aviv, A. J. (2018). How do we talk ourselves into these things? Challenges with adoption of biometric authentication for expert and non-expert users. *UMBC Student Collection.*

Wolf, F., Kuber, R., & Aviv, A. J. (2019). " Pretty Close to a Must-Have" Balancing Usability Desire and Security Concern in Biometric Adoption. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1-12.

Woodward Jr, J. D., Horn, C., Gatune, J., & Thomas, A. (2003). *Biometrics: A look at facial recognition*. RAND CORP SANTA MONICA CA.

Wu, Y. (2009). Influence of social context and affect on individuals' implementation of information security safeguards. *ICIS 2009 Proceedings, 70*.

Xiao, Q. (2005). Security issues in biometric authentication. *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop,* 8-13. IEEE.

Öğütçü, G., Testik, Ö. M., Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security 56,* 83-93.

APPENDIX 1 THE SEMI-STRUCTURED INTERVIEW FRAME

Interview questions:

1. Background information
    a. Age
    b. Education
    c. Occupation and work experience if occupation is in the field of information security
    d. Use of mobile payments and biometric authentication
        i. What type of biometric authentication methods do you use?
        ii. What mobile payment applications do you use?
        iii. What biometric authentication methods do you use in mobile payments and how often?

2. The importance of information security and information security behavior
    a. What does information security mean to you? How does it affect you?
    b. What is your understanding of information security behavior?
    c. Describe how do you take into account information security when using biometric authentication in mobile payments

3. Issues and experiences that have influenced the development of current information security behavior
    a. What do you feel you will achieve when you follow your described information security behavior?
    b. What do you feel you will lose if you do not follow your described information security behavior?
    c. Have you experienced information security issues when using biometric authentication in mobile payments? What kind of?
    d. Have you heard of others experiencing information security issues when they have used biometric authentication in mobile payments? What kind of?
    e. Do you feel the information security behavior of others has affected yours?
    f. Do you feel that new legislation, such as the GDPR, has affected your information security behavior?

4. Possible future changes in information security behavior
    a. Do you feel that your information security behavior is at a good level? Would you want to change it somehow?
    b. What would change your information security behavior?
    c. What kind of events would it require for you to change your information security behavior?

d. What kind of events would it require you to completely stop using biometric authentication in mobile payments?
e. What could prevent you from making changes to your information security behavior you consider could be useful?