Miika Aunola

SUBJECTIVE NORM IN PASSWORD SELECTION

UNIVERSITY OF JYVÄSKYLÄ
DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION SYSTEMS
2020

TIIVISTELMÄ

Aunola, Miika
Subjective norm in password selection
Jyväskylä: Jyväskylän yliopisto, 2020, 63 s
Tietojenkäsittelytiede, kybertuvallisuus, pro gradu -tutkielma
Ohjaaja: Siponen, Mikko

Salasanoja käytetään yleisesti pääasiallisena todentamismenetelmänä ja siksi ne ovat näyttelevt suurta roolia käyttäjän tietoturvassa. Epäturvalliset salasanat voivat monin tavoin vaarantaa käyttäjän tietoturvan. Tässä tutkielmassa pyritään selvittämään miten subjektiiviset normit vaikuttavat käyttäjän salasanavalintaan. Subjektiivinen normi on osatekijä useissa käyttäytymistieteiden teorioissa ja sillä tarkoitetaan sosiaalisen ympäristön luomia odotuksia, joita yksilö kokee sekä tämän motivaatiota toimia näiden odotusen mukaisesti (Fishbein & Ajzen, 1975). Subjektiivisen normin merkitystä kyseenalaistettu (Ahtola 1976) ja sitä koskeva tutkimus on tuottanut vaihtelevia tuloksia (Sommestad et al. 2014). Tässä tutkielmassa tarkasteltiin subjektiivisten normien merkitystä salasanan valintaan kirjallisuuskatsauksella sekä tätä seuranneella käsitteellis-analyyttisellä tutkimuksmenetelmällä. Käsitteellis-analyyttisessä osiossa kirjallisuuskatsauksen löydöksiä analysoitiin kolmen erillisen skenaarion kautta.

Tutkimuksessa ilmeni että subjektiivisten normien merkittävyys salasanan valintaa selittävänä osatekijänä on kyseenalainen. Aikaisempi tutkimusnäyttö sen merkityksestä on vaihtelevaa ja osittain ristiriitaista. Subjektiivisten normien merkitys näyttää riippuvan vahvasti myös asiayhteydestä sekä tilanteesta. Näistä seikoista johtuen tutkielman johtopäätöksissä todetaan että subjektiivinen normi voi joissain olosuhteissa vaikuttaa salasanan valintaan, mutta se ei useimmiten ole luotettavin tai merkittävin osatekijä.

Avainsanat: subjektiivinen normi, normatiivinen uskomus, TBA, TAM, UTAUT, TRA, käsitteellis-analyyttinen tutkimus, kirjallisuuskatsaus, salasana

ABSTRACT

Aunola, Miika
Subjective norm in password selection
Jyväskylä: University of Jyväskylä, 2020, 63 p.
Information systems science, Cyber Security, Master's Thesis
Supervisor: Siponen, Mikko

Passwords play a significant role in users' information security and serve as the primary means of authentication. Insecure choice of passwords can compromise information security in several ways. This study aimed to increase the understanding of how can subjective norm, a construct of several behavioural models and theories that has also been used to explain information security related behaviour, affect individuals' selection of passwords.

Subjective norm is defined a "perceived expectations of the specific referent individuals or groups, and by the person's motivation to comply with those expectations"(Fishbein & Ajzen, 1975, p. 302). The use of subjective norm as a construct has been questioned (Ahtola, 1976) and the use of it in studies has yielded varying results (Sommestad et al. 2014). This paper studied the role of subjective norm in password selection by a literature review that considered the results of over 40 previous studies of which 10 were chosen for an in-depth examination. The literature review was followed by a conceptual analysis. In this phase the findings of the literature review were analysed in three different scenarios.

This study found that the use of subjective norm as a construct and a predictor for password selection can be seen questionable due to varying and sometimes contradicting results in previous studies. The significance of subjective norm in password selection appeared to differ considerably depending on the context in which it was used. Therefore, this study concluded that while under certain circumstances subjective norm can be used to explain individuals' selection of passwords, it is often not the relevant predictor.

Keywords: subjective norm, password, normative beliefs, TBA, TAM, UTAUT, TRA, conceptual analysis, literature review, password

FIGURES

TABLES

TABLE OF CONTENTS

1 DESCRIPTION OF THE TOPIC

The role of human behaviour frequently referred to as the weak link in an organization's information security infrastructure which is no surprise given the effect that a single person can have in the entire organization (Jalkanen, 2019). Regardless of whether or not the statement is true, the importance of good information security behaviour is not limited to professional life as digital and online services become increasingly significant aspects in our lives. Previous research often explains information security behaviour by attitude, subjective norms, self-efficacy, and threat appraisal (Pahnila, Siponen, Mahmood, 2007; Lee & Larsen, 2017; Sommestad et al. 2014). Passwords are an obvious contributor to an individual's information security as they are the dominant authentication method (Florêncio & Herley, 2007; Woods & Siponen, 2017; Woods & Siponen, 2019). The number of passwords users have on average as grown significantly and while there are several tools to help users to choose secure passwords and manage them securely, it is important to understand the underlying reasons of a password selection on a behavioural level. As established above, information security behaviour is often explained by the well-established behavioural and technology acceptance theories such as Theory of Planned Behaviour, TPB (Ajzen, 1991), Theory of Reasoned Action, TRA (Fishbein & Ajzen, 1975), Technology Acceptance Model, TAM (Davis, 1985; Davis, 1989), and Unified Theory of Acceptance and Use of Technology, UTAUT (Venkatesh et al., 2003; Venkatesh et al., 2012). A determinant present in some of these theories is subjective norm which according to TRA is determined by normative beliefs and motivation to comply. Subjective norm as a term is defined as "perceived expectations of the specific referent individuals or groups, and by the person's motivation to comply with those expectations"(Fishbein & Ajzen, 1975, p. 302). The selection of a passwords can take place under different circumstances and the significance of the subjective norm in password selection can vary based on the situation.

1.1 Research objective

Organizations are spending an increasing amount of money on information security related products and services. The worldwide spending increased from $101,5 billion in 2017 to $124,1 billion in 2019 (Gartner, 2018). While the exact amount spent on password related services, products and incidents is unknown it is likely that organizations would be keen to reduce the related overhead. Understanding the significance of subjective norms of the users and how they affect their behaviour can help service providers and other organizations such as workplaces optimize the way they want to convey the message of good password related behaviour. The benefits of this can be two-fold. First, the opportunity for organizations to minimize costs can be significant. Second, good password practices can contribute towards more secure passwords and less password related incidents. This can consequently reduce the number users who experience the mental, financial, and reputational hardships that can result from having one's password compromised. The aim of the thesis relates to subjective norm, which has been advanced as a predictor for IS security behaviour, and passwords (Taylor & Todd, 1995; Venkatesh & Davis, 2000; Hu et al., 2001; Dinev & Hu, 2007; Herath & Rao, 2009; Yoon & Kim, 2013; Yazdanmehr & Wang, 2016; Jafarkarimi et al., 2016; Johnson, 2017; Kusyanti et al., 2019). To be more precise, the aim of this study is to argue that generally subjective norm may not be a predictor for information security behaviour, specifically in the password selection.

1.2 Thesis structure

The study consists of seven chapters and is organized as follows. The first chapter is introductory and as such describes the aim of the study, its background together with the motivation to conduct it and the significance of the topic. The research approach and methodology will also be introduced in this chapter.

The second chapter includes a general description of passwords and how they are used. The second chapter will be based on a thorough literature review.

Next, the third chapter reviews and describes some of the best known and most widely researched technology acceptance theories that are based on the behavioral sciences. The theories selected are well established and include subjective norms a component. The fourth chapter presents the proposed research methodology, explains the qualitative research approach as well as literature review as a mean of examining the topic.

The fifth chapter describes the findings and interpretations. The sixth chapter also discusses the practical and theoretical implications of the study together with its limitations and potential future research opportunities. The seventh chapter concludes the thesis and summarizes its main contributions.

2 PASSWORDS

Techterms, an online computer dictionary, defines password as "...a string of characters used for authenticating a user on a computer system. For example, you may have an account on your computer that requires you to log in. In order to successfully access your account, you must provide a valid username and password. This combination is often referred to as a login. While usernames are generally public information, passwords are private to each user." (Techterms, 2020).

Passwords originate from the Roman military where they were called watchwords and have been adopted for the use of computer since the early days of computing. The first computer system to implement password login was The Compatible Time-Sharing System (CTSS) which is an operating system introduced in MIT in 1961 (Troy Hunt, 2017a). Since then passwords have become the most common form of authentication for web users and as such play an incremental part of user's experience. The number of web users and different accounts they access is expected to increase and they are being used to control access to some of our most important information in many of our devices (Chiasson et al., 2009).

Together with user ID password plays a significant role in personal information security. However, the significance of user ID from information security perspective is questionable. It is considered as public information as it can often be determined with reasonable effort. Despite the term "password" it should not' necessarily be a word but rather a string characters that is memorable for the user but difficult to guess for everyone else (Traficom, 2014).

2.1 A simplified description of passwords in an online environment

Entering credentials to gain access to an online account triggers a chain of events. The password is sent to a server to authenticate whether access can be granted. This transfer is mainly completed using either HTTP (Hypertext Transfer Protocol) or HTTPS protocol (Harvard University, 2014). HTTP is a non-encrypted ASCII transport protocol used for data transfer between client and a web server. This protocol transfers the data in a readable format, and which leaves the data vulnerable to several threats. In HTTPS the "S" stands for "Secure". This protocol adds a layer of encryption to the data that is being transferred. While HTTPS not immune to threats the extra layer of encryption means that the data is not readable when transferred (IETF documents, 1999).

In HTTP a client submits information to the web server and waits for a response. The request contains information of both the request and the requested contents. There are two methods of HTTP requests: GET and POST. GET method carries the request parameters appended in the URL string making it less secure for passing on sensitive information. The upside to this method is that they can be bookmarked, cached, and remain in the browser history. POST method carries the request parameter in the message making it the more secure option. This, however, means that they cannot be bookmarked and are not stored in browser history (GeeksForGeeks, 2017).

Once transferred to a web server, the password is then compared with the database where user credentials are stored in one of three ways: Plaintext, hashed or salted and hashed. Storing passwords in plaintext is generally regarded as an outdated practice that places users' information at risk for both internal and external threats (Bauman et al., 2015). Hashing passwords prevents them from being readable and thus adds a layer of protection for the users' information (Hendrickson, 2019).

Password hashing means calculating plaintext into an unintelligible series of numbers and letters using a hashing algorithm. While this does not make accessing the passwords any more difficult, it renders them cumbersome for a bad actor to utilize. It is important to note, however, that even hashed passwords are vulnerable to brute force attack techniques such as dictionary attack. A way of protecting against attacks like this is password salting which means adding random characters to a password before hashing it (Jung, 2019). The process of password salting and hashing is illustrated in the figure below (FIGURE 1). Here salt, a string of random characters "c6aX@*" is added to a password "hovercraft". After salt is added, the password is hashed from "hovercraft" into "Jxa/hKjam*/9Nb2gh". Combined, salting and hashing have turned the password "hovercraft" into "c6aX@* Jxa/hKjam*/9Nb2gh".

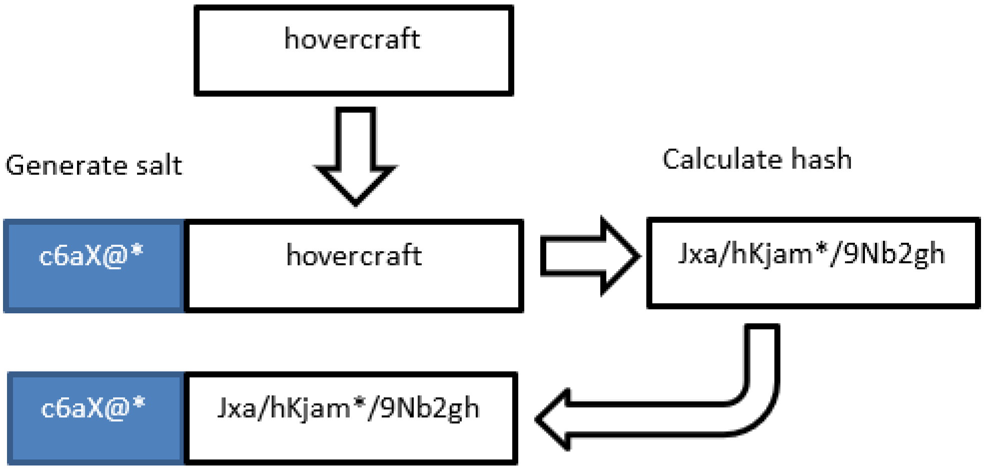


FIGURE 1 Password salting and hashing

2.2 Password security

2.2.1 Password strength

Despite newer, alternative authentication methods, text-based passwords remain dominant (Florêncio & Herley, 2007; Woods & Siponen, 2017; Woods & Siponen, 2019). Modern authentication methods such as use of biometrics or graphical authentication still rely on passwords as an alternative way of authenticating a user for example in the event that graphical password is forgotten. (Kleucker, 2013). Consequently, password cracking methods have become significantly more advanced. To combat these threats policies that define the parameters for passwords in organizations and services have become more complex (Kelley et al., 2012).

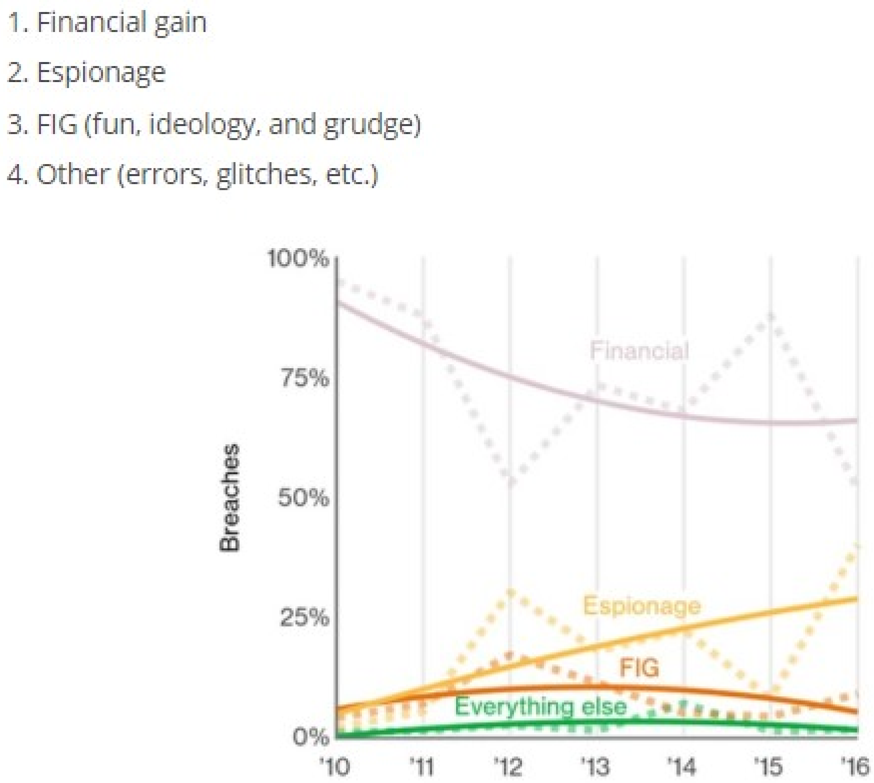
While in the past there has been some debate over the extent to which the complexity or use of non-alphabetical characters contribute to the robustness of a password it is commonly accepted that length does strengthen them. The Cybersecurity and Infrastructure Security Agency of United States (CISA) recommends the using upper and lowercase letters, numbers and special characters and suggests that together with sufficient password length the make a strong password (Cybersecurity & Infrastructure Security Agency, 2019). The argument against the use of non-alphabetical characters relies on the notion that use of such characters makes passwords less memorable and makes users rely in reusing same passwords or writing them down and storing them non a non-secure manner. In their study Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms, Kelley et al. (2012) compared different password policies against simulated password cracking algorithms and found that a 16 character long password with no specific requirements appeared to be more secure than a 8 character long password that included upper and lowercase letters, a symbol and a digit. They do note, however, that the strength of password against a cracking algorithm relies heavily on the type of dictionary that is used for the cracking.

2.2.2 Threats

Data breaches and incidents regarding leaked or hacked user credentials have become a frequently covered topic in today's mainstream media. While the total number on incidents remains unclear as not all them are discovered, let alone reported it may be safe to say that the attention the topic has received is reflective of its importance in today's society.

Troy Hunt (2017b), the creator of haveibeenpwned.com – a website that allows users to search across multiple data breaches to see if their email addresses have been compromised, noted that during its existence more than 10.1 billion user accounts have been compromised. It is worth noting that the service is not a comprehensive source of all user accounts affected by a breach. They recognize this themselves by stating: "Whilst HIBP is kept up to date with as much data as possible, it contains but a small subset of all the records that have been breached over the years. Many breaches never result in the public release of data and indeed many breaches even go entirely undetected. "Absence of evidence is not evidence of absence" or in other words, just because your email address wasn't found here doesn't mean that is hasn't been compromised in another breach." (Troy Hunt, 2017b).

The primary motivation behind hacking appears to be financial gain. Calyptix, an IT security company analyzed the 2017 version of Verizon Data Breach Investigations Report and found that 93% of breached studied were motivated by financial gains. The proportion of each motivational factor is illustrated in the graph below, extracted from Calyptix's website (Calyptix Security, 2017). While the proportion of hacking that is motivated by financial gains has decreased to 86%, it remains dominant (Verizon, 2020).



1. Financial gain
2. Espionage
3. FIG (fun, ideology, and grudge)
4. Other (errors, glitches, etc.)

FIGURE 2 Hacking motivators (Calyptix Security, 2017)

The figure (FIGURE 2) illustrates that the main motivation for hacking is financial gain. While espionage as a motive has been found to increase over the year, it still only accounts for around 25% of the breaches. FIGs and other motivators account for a very small portion of breaches. The main marketplaces for stolen user account credentials reside in The Onion Router (TOR) network where these credentials hold monetary value (Peltomäki & Norppa, 2015). There are a number of ways for an attacker to gain access to the desired information that can be sold. There are several techniques for acquiring or cracking a password. Techniques include phishing, shoulder surfing, dumpster diving, password cracking and social engineering. In this chapter we focus strictly on password cracking as most of the current identity authentication attacks are based on them (Chou et al., 2009). The most common techniques used for it are brute force approach, dictionary attack and hybrid attack. All these methods, in principle, are based on guessing the right password and in no way alter password protection works or the level of security it provides.

Brute force approach is heavily reliant on the raw computing power that is available. It consists of the attacker submitting several passwords with the hope of eventually guessing the correct one. A simplified example of a brute force attack would be cracking a six-digit PIN. In a brute force attack the cracker would first guess "000000". If unsuccessful, they would try "000001", "000002" and so on. A match would occur at some point between "000000" and "999999". The principle of a real-world brute force attack is roughly the same with the only difference being a greater number of characters that make up a password. The number and variety of characters makes the number of possible combinations greater which in turn increases the amount of time needed guess the correct one. A strong enough password can render brute force attacks impractical. This method is especially quick and suitable for cracking shorter passwords. Longer passwords have more possible values which makes them exponentially more difficult and time consuming to crack. However, theoretically brute force approach should be able to crack nearly any password if there are no time constraints (Erminôte, 2020).

Dictionary attack is a method that relies on users' tendency to choose simple passwords. It utilizes large lists of words which are often found on the internet and are based on passwords recovered from past data breaches. These lists can contain hundreds of millions of passwords. A file containing the list of passwords is loaded into a cracking application. The file is then run against user accounts that are located in the application (Erminôte, 2020).

A hybrid attack as the name would suggest, is a combination of brute force and dictionary attacks. It can be used to target passwords that have been created to meet strong password requirements by adding one or more digits in the beginning or end of the password. Hybrid approach enhances a dictionary attack by placing a string of brute force characters to the beginning or end of the dictionary words. For instance, a word "dog" would be given values such as "001dog", "002dog" or "dog003". The limitations of this method are obvious as the brute force characters are added either in the beginning or the end of the dictionary word (Cyclonis, 2018).

There are several alternatives and methods derived available for more specific purposes. Alternative password cracking methods include for example mask attack, permutation attack PRINCE attack, rule-based attack, table-lookup attack, and toggle-case attack.

2.3 The use of passwords and tools

The number of people with access to internet has grown significantly over the last two decades. The number of people using the internet in 2000 was roughly 413 million whereas in 2016 it was over 3.4 billion. Similar increase has been observed in the time we spend online. In United States the average time spent online in 2010 was around 3 hours whereas in 2018 it was over 6 hours (Roser et al. 2015). Given our growing online presence it is logical that more and more services are provided to us on the internet. Some of these services require us to create an account with a password. There are several estimates of how many online user accounts and average person has. These estimates range from 38 (LogMeIn, 2020) up to 150 (Caruthers, 2018). Caruthers observed that the majority of users underestimated the number of accounts they have. Remembering and managing a large number of unique and complex passwords can be difficult. Users want to protect data that is important to them but feel justified to adopt non-secure behaviors such as reuse of passwords in the name of practicality. Users say they are unable to remember all their passwords and reusing them makes it easier to manage them (Gaw & Felten, 2016).

2.3.1 Digital password managers

Some research points to users' inability to remember a larger number of passwords and claims that memorizing text-based passwords places a significant load on users. Consequently, this leads to users selecting simple passwords or reusing them (Chiasson et al, 2009). Interestingly, in a recent study Too many passwords?: How understanding our memory can increase password memorability the authors found this to be inaccurate as they state "Our results show that correct password recall had no correlation to the memory capabilities of the user, but was correlated to the users' perceptions of their capacity to recall passwords correctly, their control over their memory for passwords, their level of motivation to remember passwords, and their understanding of how passwords can be made more memorable." (Woods & Siponen, 2017 p. 34).

Neither study denies the notion that users tend to rely on poor password practices at least partly because of the number of accounts they have. A number of digital password managers exist to help users manage their user account credentials including passwords. These password managers enable user to save their passwords along with other account credentials and store them either on the user's device or in the service providers cloud.

2.3.2 Password meters

Password meters are tools that aim to help users create stronger passwords. They are usually placed in an account registration page and can provide a variety of feedback when user is entering a proposed password. This feedback can be a visual cue such as a colour bar that changes from red to green depending on the strength of the password. It can also be a simple plain text feedback such as "strong" or "weak".

In their study How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation authors (Ur et al, 2012) focused on examining the effects of websites' password meters in security and usability of passwords. They found that the inclusion of a password meter lead to users creating longer passwords and passwords with more digits, symbols, and uppercase letters that were also found to be more resistant to password-cracking algorithms. Interestingly, the use of password meters also affected the process of password creation. Sites with password meters that provide visual feedback saw their users spend more time on creating their passwords and were more likely to change the password while entering it. Also, they were most likely to find the meter annoying.

Similar conclusions were drawn by Serge Egelman et al (2013). They observed that the presence of password meters did in fact yield significantly stronger passwords. It is worthwhile noting, however, that this was found to be true only for important accounts. The authors performed a follow-up study for an unimportant account and did not find an observable difference in the strength of passwords. Users simply reused the weak passwords that they used for other unimportant accounts. Moreover, Woods & Siponen (2019) found that the process of creating passwords can have an effect on its memorability and ultimately could reduce insecure password behaviors. They discovered that by "increasing the number of verifications can make passwords more memorable while not concurrently increasing user inconvenience. Second, this change could reduce the chance of forgetting passwords, and the financial consequences that can then occur." (Woods & Siponen, 2019, p.10).

3 TECHNOLOGY ACCEPTANCE THEORIES

The theoretical foundation of this study is based on theoretical models of human behaviour that include subjective norm as a construct. Acceptance and use of information technology are one of the most studied and mature aspects of information systems research, understanding it is necessary for this study. Researchers have adopted theories of human behaviour to study technology acceptance for years (Davis, 1985; Venkatesh et al., 2003). The purpose of this chapter is to present the most merited and widely applied theories and models that utilize the concept of subjective norm. The theories examined in this chapter are Theory of Reasoned Action (TRA) (Fishbein & Ajzen, 1975), Theory of Planned Behaviour (TPB) (Ajzen, 1991), Technology Acceptance Model (TAM) (Davis, 1985; Davis, 1989), Technology Acceptance Model 2 (TAM 2) (Venkatesh & Davis, 2000), Unified Theory of Acceptance and Use of Technology (UTAUT & UTAUT2) (Venkatesh et al., 2003; Venkatesh et al., 2012). While TRA and TPB were designed to explain human behaviour in general, TAM and UTAUT models were developed to explain the acceptance of technology. All of these theories share a component of subjective norm and are therefore relevant for this study. Moreover, these theories are well established, widely used and serve as a foundation in most recent studies as well. Reviewing the models, the author expects to find minor deviations on the role that subjective norm is perceived to play. Finally, at the end of this section author presents comprised a table (TABLE 1) that synthesizes the theories presented in section 3, summarizes the components, and provides definitions.

3.1 Theory of Reasoned Action (TRA)

Theory of reasoned action, TRA, explains how behavioural intentions and preexisting attitudes affect individuals' behaviour (Fishbein & Ajzen, 1975). It is based on the notion that an individual's decision to engage in a particular behaviour is based on the expected outcome of the behaviour. TRA relies on the assumption that an actual behaviour is always preceded by an intention to perform that exact behaviour (Ajzen & Madden, 1986). The concept of TRA was first introduced by Fishbein (1967) and later further developed by Fishbein & Ajzen (1975) and was initially meant to explain human behaviour on a very general level (Ajzen & Fishbein, 1980). TRA has also been called the extended Fishbein model.

The theory was developed to explain and predict specific behaviour in a defined situation. According to Fishbein and Ajzen (1975), the TRA comprises of three equations. First equation suggests that individual's actual behaviour is directly dependent on his or her behavioural intention which refers to the individual's subjective likelihood of performing the behaviour. This, in turn is dictated by the individual's attitude or "evaluative affect" toward a behaviour as defined by Davis (1986, p16) and subjective norm which is defined as one's perception on whether the behaviour in question is favoured by the people important to him or her. The second equation of the model describes individual's attitude as a result his or her beliefs of the outcome of the behaviour that are multiplied by evaluation of the outcome. The third equation is described as "the perceived expectations of the specific referent individuals or groups, and by the person's motivation to comply with those expectations"(Fishbein & Ajzen, 1975, p. 302). According to the authors, subjective norm is the least understood part of the model and "very little research ... has dealt with the formation of normative beliefs (Fishbein & Ajzen, 1975, p. 304).

Given that TRA is a broadly applicable theory and general in nature, it does not indicate which beliefs affect the individual's attitude in a given context. The authors suggest that an individual can possess several beliefs about an object and that only a small number of those will actually influence his or her attitude in any given moment. It is then the responsibility of the researcher to discover those beliefs (Ajzen & Fishbein, 1980).

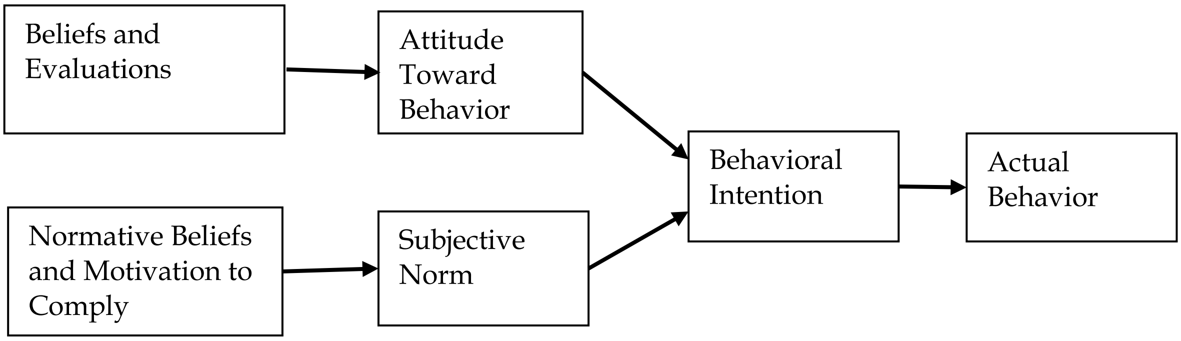


FIGURE 3 Theory of Reasoned Action (Fishbein & Ajzen 1975)

It appears that the significance of intention in the model can be reduced in certain instances. First, if a behaviour is obligatory, and the individual has no voluntary control over it the predictiveness of the intention on the actual behaviour is reduced. Second, the time between measuring intention and actual behaviour has an impact on the reliability of accuracy of the predicative power of the intention (Ajzen & Fishbein, 1980; Bagozzi, 1981).

3.2 Theory of Planned Behaviour (TPB)

Theory of planned behaviour is based on the Theory of Reasoned Action (Fishbein & Ajzen, 1975; Ajzen & Fishbein, 1980). The new theory (Theory of planned behaviour) incorporated an element of perceived behavioural control that the original model did not include. Whereas theory of reasoned action suggests that behaviour is determined by attitude toward it and subjective norm, theory of planned behaviour suggests that perceived behavioural control has an effect on the intention and therefore the behaviour that often results from the intention.

To support the addition of perceived behavioural control, Ajzen (1991) provided in his paper "The Theory of Planned Behaviour" two key rationales. First, assuming that intention remains constant, perceived behavioural control is likely to be increased with the effort expended to successfully conclude a course of behaviour. This means that when two people have equally strong intentions to learn a new skill, the person who with more confidence in mastering the skill is more likely to persevere. The second rationale for the existence of a direct link between behavioural achievement and perceived behavioural control is that behavioural control can often be used as a substitute for a measure of actual control (Ajzen, 1991). The figure (FIGURE 4) below illustrates how perceived behavioural control affects intention and ultimately the behaviour that results.

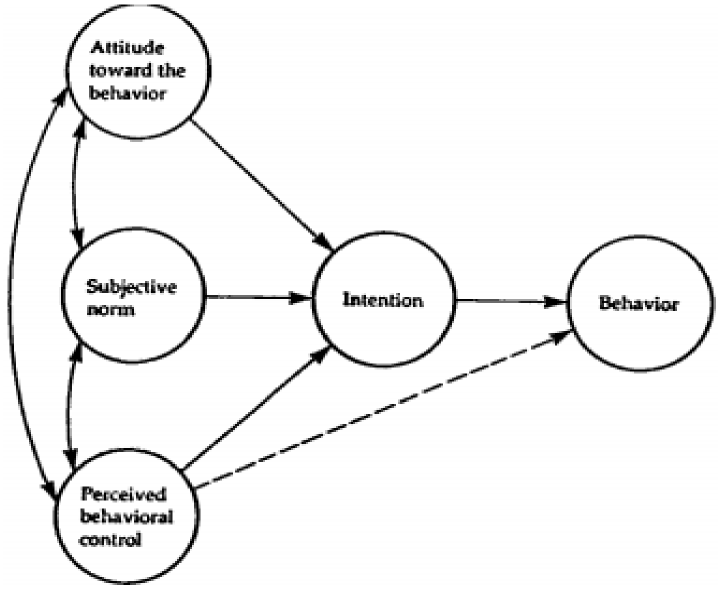


FIGURE 4 Theory of planned behavior (Ajzen, 1985)

3.3 Technology Acceptance Model (TAM)

TAM is a theory designed to explain computer usage behaviour. Davis (1986), who developed TAM, based it on the work of Fishbein & Ajzen (1975) with TRA. Instead of creating a general theory like TRA, the aim was to specify the variables relevant in explaining the end-user computer usage. Davis et al. (1989) recognize the merits of TRA in several aspects. Firstly, the model incorporates several theories that previously focused intentions, beliefs, and behaviour separately. Secondly, TRA has been empirically tested and applied in several different research settings and has therefore accumulated understanding of the model's key limitations and predictiveness. Thirdly, TRA defines constructs and causal relationships between the variables in a detailed manner (Davis, 1986). Unlike TRA, which includes subjective norm as one of the key variables, Davis decided to omit it from TAM.

The initial TAM introduced by Davis (1986) suggests that two beliefs: perceived ease of use and perceived usefulness dictate the individual's intention to use a system and that intention is major determinant of individuals attitude toward the system. "A Key purpose of TAM, therefore, is to provide a basis for tracing the impact of external factors on internal beliefs, attitudes, and intentions." (Legris et al. 2001, p.192). The revised TAM by Davis et al. (1989) suggests however, that in an organizational context attitude is irrelevant as people, despite their feelings, form intentions toward performing behaviours. The notions, therefore, points to a direct effect between perceived ease of use and perceived usefulness, disregarding the attitude. The figures (FIGURE 5) and (FIGURE 6) demonstrate the relationships of constructs represented in TAM and how the omission of attitude towards use of a system result in perceived ease of use and perceived usefulness having a direct influence in behavioural intention.

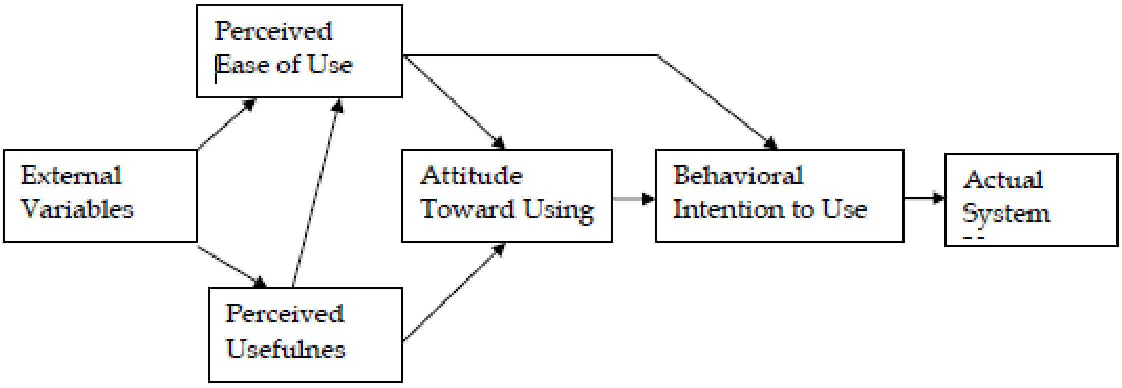


FIGURE 5 Technology Acceptance Model (Davis., 1985)

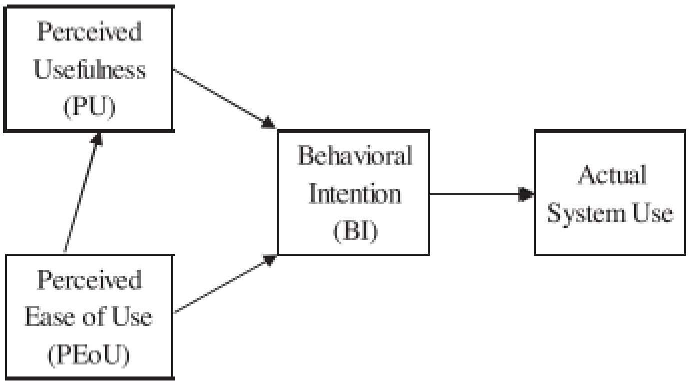

Perceived Usefulness (PU)
Perceived Ease of Use (PEoU)
Behavioral Intention (BI)
Actual System Use

FIGURE 6 Technology Acceptance Theory (Davis et al., 1989)

3.4 Technology Acceptance Model 2 (TAM2)

TAM has later been extensively researched and revised, most notably by Venkatesh & Davis (2000) when developing TAM2. Based on TAM the TAM2 introduced the aspects of social influence and cognitive instrumental processes. These include subjective norm, image constructs and voluntariness which can directly affect the usage intention. Furthermore, experience and subjective norm can influence perceived usefulness jointly with other constructs such as image, job relevance, output quality and the demonstrability of results. Linkages between the constructs are demonstrated in the figure below (FIGURE 7).

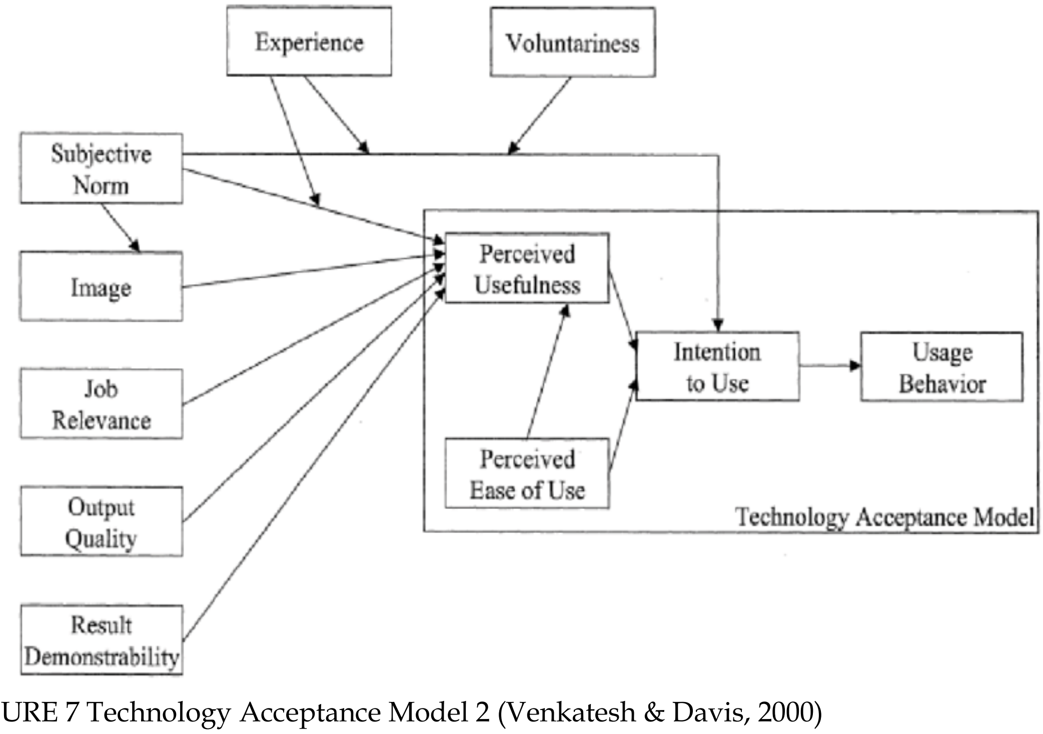
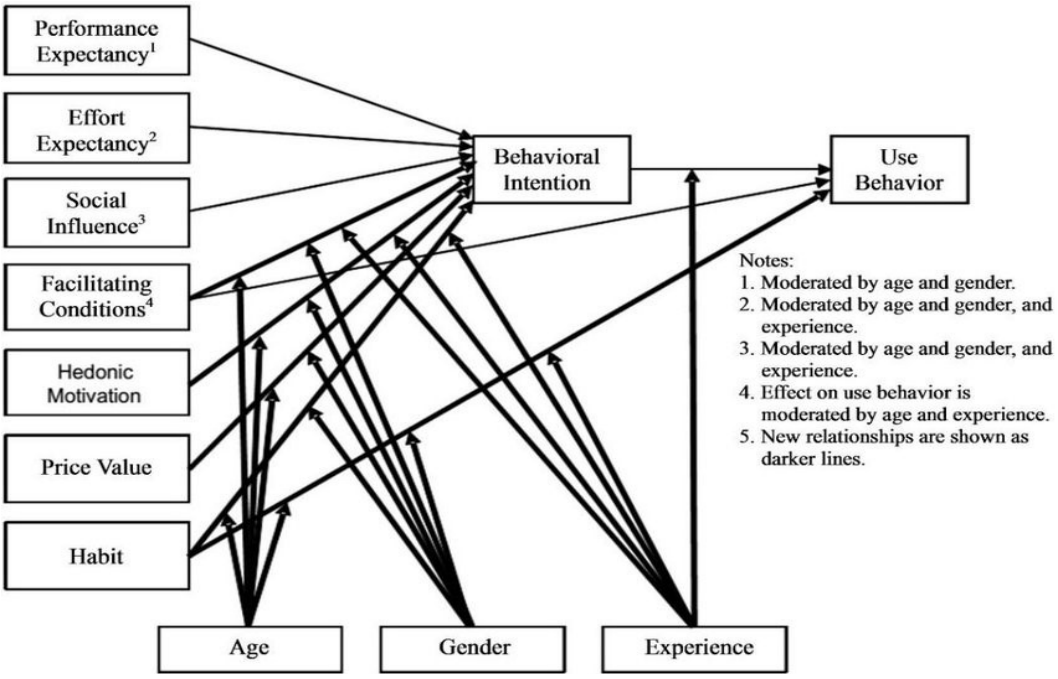


FIGURE 7 Technology Acceptance Model 2 (Venkatesh & Davis, 2000)

3.5 Unified Theory of Acceptance and Use of Technology (UTAUT and UTAUT 2)

UTAUT is a result of a review of eight technology acceptance theories and was formulated by Venkatesh et al. (2003). The need for UTAUT according to Venkatesh et al. (2003) was due to the existence of several user acceptance theories that allowed the researchers to pick the most suitable ones while ignoring the rest. The model presents key constructs: performance expectancy, effort expectancy and social influence which are direct determinants of usage intention and behavior. In addition, the fourth key construct which is facilitating conditions is a direct determinant of user behavior. Moreover, the four key constructs are influenced by moderators: age, gender, experience, and voluntariness. The relationships between the key constructs and moderators is illustrated in figure 3. UTAUT has been applied in a number of studies, some of which focused on technology acceptance determinants in consumers which on its part demonstrates the applicability of it when studying user acceptance of protected email.

UTAUT2 being an extension of UTAUT constructed by Venkatesh et al. (2012) introduces a more consumer centric approach to the model. In addition to the constructs of UTAUT, the authors incorporated three additional ones based on IS research and literature review on buyer behavior. These new constructs are hedonic motivation, price value and habit. FIGURE 5 below presents both UTAUT and UTAUT2 by differentiating the thicker lines as additions made in UTAUT2 and thinner lines representing the original UTAUT.



Notes:
1. Moderated by age and gender.
2. Moderated by age and gender, and experience.
3. Moderated by age and gender, and experience.
4. Effect on use behavior is moderated by age and experience.
5. New relationships are shown as darker lines.

FIGURE 8 Unified Theory of Acceptance and Use of Technology (Venkatesh et al., 2012)

Theory	Components	Definitions	Source
Theory of Reasoned Action (TRA)	Attitude toward behaviour	"an individual's positive or negative feeling (evaluative effect) about performing the target behavior"	Fishbein & Ajzen, 1975, p.218
	Subjective norm	"person's perception that most people who are important to him think he should or should not perform the behavior in question"	Fishbein & Ajzen, 1975, p.302
Theory of Planned Behavior (TPB)	Attitude toward behaviour	Adapted from TRA	
	Subjective norm	Adapted from TRA	
	Perceived behavioral control	"perceived ease or difficulty of performing the behavior"	Ajzen, 1991, p.188
Technology Acceptance Model (TAM)	Perceived usefulness	"the degree to which a person believes that using a particular system would enhance his/her job performance"	Davis, 1989, p.320
	Perceived ease of use	"the degree to which a person believes that using a particular system would be free from effort"	Davis, 1989, p.320
	Subjective norm	Adapted from TRA	
Technology Acceptance Model 2 (TAM2)	Perceived usefulness	Adopted from TAM	
	Perceived ease of use	Adopted from TAM	
	Subjective norm	Adopted from TRA	

Unified Theory of Acceptance and Use of Technology (UTAUT)	Performance expectancy	"The degree to which an individual believes that using ICT will help him or her to attain gains in job performance"	Venkatesh et al., 2003, p. 447
	Effort expectancy	"The degree of ease associated with the use of the system"	Venkatesh et al., 2003, p. 450
	Social influences	"The degree to which an individual perceives that important others believe he or she should use a technology"	Venkatesh et al., 2003, p. 451
	Facilitating conditions	"The degree to which an individual believes that an organizational and technical infrastructure exists to support use of the system"	Venkatesh et al., 2003, p. 453
Unified Theory of Acceptance and Use of Technology 2 (UTAUT2)	Hedonic motivation	The fun or pleasure derived from using a technology	Venkatesh et al., 2012, p. 161
	Price value	“Consumers' cognitive tradeoff between the perceived benefits of the applications and the monetary cost of using them”	Venkatesh et al., 2012, p. 161
	Habit	“A perceptual construct that reflects the results of prior experiences”	Venkatesh et al., 2012, p. 161

TABLE 1 Synthesis of theories

3.6 Subjective norm

As established, subjective norm is one of the dominant determinants in many of the abovementioned theories. The definition of subjective norm according to Fishbein and Ajzen (1975) is "perceived expectations of the specific referent individuals or groups, and by the person's motivation to comply with those expectations" (Fishbein & Ajzen, 1975, p. 302). This definition has been further refined in several different contexts. One of the examples comes from the domain of security in home computers by Ng and Rahim (2005) as "a person's perception of the social pressure to perform or not to perform the behavior under consideration, in this case, to practice computer security in home computers." (Ng & Rahim, 2005 p. 238.)

According to Fishbein and Ajzen (1975) subjective norms are a construct of normative beliefs and motivation to comply. On his University of Massachusetts website Ajzen describes normative beliefs as "the perceived behavioral expectations of such important referent individuals or groups as the person's spouse, family, friends, and – depending on the population and behavior studied – teacher, doctor, supervisor, and coworkers. It is assumed that normative beliefs — in combination with the person's motivation to comply with the different referents — determine the prevailing subjective norm. Specifically, the motivation to comply with each referent contributes to the subjective norm in direct proportion to the person's subjective probability that the referent thinks the person should perform the behavior in question." (Ajzen, 2019). Conversely, the likelihood for an individual to perform the behavior decreases if the referents were less likely to approve of the behavior. Fishbein and Ajzen (1975) define motivation to comply as "On both theoretical and empirical grounds it appears that motivation to comply is best conceived as the person's general tendency to accept the directives of a given reference group or individual."

Subjective norm as a construct has been criticized. Fishbein and Ajzen point out that the concept of subjective norm works under the assumption that subjects will intend to perform positive behaviors with respect to people they like and, conversely, negative behaviors with respect to people they dislike (Fishbein & Ajzen, 1975).

The concept of normative beliefs is based on the premise that people form a generalized opinion of "important referent individuals". It would seem plausible that within this group there are members that hold relatively homogenous norm about expected behaviours. However, it seems very unlikely that all members of the group hold similar expectations. The existence of a generalized subjective norm in people's cognitive structure as an idea can be called to question (Ahtola, 1976).

Ahtola (1976) also points out that the second component of subjective norm – motivation to comply- can be problematic as it may not be truly independent component. Ahtola (1976) elaborates: "There seems to be considerable uncertainty about the exact meaning of this component. Should it be independent of the referent's particular demands, or should it be specific to the particular behaviour or behavioural domain under consideration, or should it be defined as the subject's general motivation to comply with the referent? The last conceptualization is advocated by Fishbein (Fishbein and Ajzen, 1975). The theoretical grounds for this choice are not referred to, but the guess of this author is that the grounds are to make the "motivation to comply" component independent of the "normative belief" component." This assumption might not be conceptually sound and consistent. A father might want to comply with his child's wishes in if presented as polite requests but would not be happy to comply with the child's strong demands or threats. Fishbein and Ajzen (1975) also acknowledge the problems that may arise from several possible interpretations.

4 METHODOLOGY AND THE RESEARCH PROCESS

The methodologies used in this research are two-fold: first, a thorough literature review is conducted by executing a range of searches in different databases and libraries using a variety of keywords; second, a conceptual-analytical approach is to be taken. The main objective of this paper is to argue that generally subjective norm may not be a predictor for information security behaviour, specifically in the password selection.

As established in previous chapters, most of the dominant theories consider subjective norm as a contributor towards user behaviour. Given this, a presumption can be made that subjective norms also influence users' selection of a password. Therefore, to challenge this one must discover if there are instances where the use of subjective norm as a predictor might not be ideal or valid. A literature review is a natural and necessary starting point as it can provide an understanding of existing knowledge. Building on the literature review a conceptual analysis will be conducted where the aim is to discover if there are scenarios in which, in the light of previous research, subjective norms do not contribute to users' selection of a password or their effect is minimal.

4.1 Literature review

Existing knowledge is generally the basis for scientific research. Literature reviews are therefore an important part of research. Miller & Yang (2007, p. 62) described literature review as "The literature review is a comprehensive survey of previous inquiries related to a research question. Although it can often be wide in scope, covering decades, perhaps even centuries of material, it should also be narrowly tailored, addressing only the scholarship that is directly related to the research question." According to Easterby-Smith et al. (2009), literature review is an essential step as it is used to summarize existing research, by identifying themes and patterns. It also helps to generate research ideas and as such provides a good starting point for research. Literature review as a research methodology draws on and evaluates different types of sources including professional and academic journal articles, web-based resources, and books. Literature review consist of the following stages: scanning, taking notes, structuring the literature review, writing the literature review, and building a bibliography (Rowley & Slack, 2004)

This research follows the structure presented by Rowley & Slack (2004) as it provides a clear and comprehensive process for conducting a literature review. First, research databases were scanned for relevant literature. These database searches consisted of, in addition to Google Scholar, well-established IS research libraries such as MIS Quarterly, IEEE Xplore, AIS Electronic Library and ACM Digital Library. The search process was conducted manually. As the search resulted in a broad variety of articles from different academic and professional fields, they were filtered based on their relevance. The relevance was deemed on the basis of the field of research.

Second, notes were taken to deem the relevance of a given piece of literature which was determined by whether the publication had an information security aspect to it and whether it included a subjective norm as a construct. The inclusion criterions therefore are:

- Study must be conducted in the field of information security
- Study must examine information security from a behavioral standpoint
- Study must include a subjective norm as a construct
- Study must be in English or in Finnish

Third, key information of the relevant articles was constructed into a table to provide a summary of the information distilled from the literature. 10 articles were chosen for closer examination. Next, the literature review was written before building the bibliography that is positioned at the end of this thesis. Written literature review serves as a natural base and a starting point for the conceptual analysis.

4.2 Conceptual analysis

Furner (2004) defines conceptual analysis as "…a technique that treats concepts as classes of objects, events, properties, or relationships. The technique involves precisely defining the meaning of a given concept by identifying and specifying the conditions under which any entity or phenomenon is (or could be) classified under the concept in question. The goal in using conceptual analysis as a method of inquiry into a given field of interest is to improve our understanding of the ways in which particular concepts are (or could be) used for communicating ideas about that field." (Furner, 2004 p. 233-234).

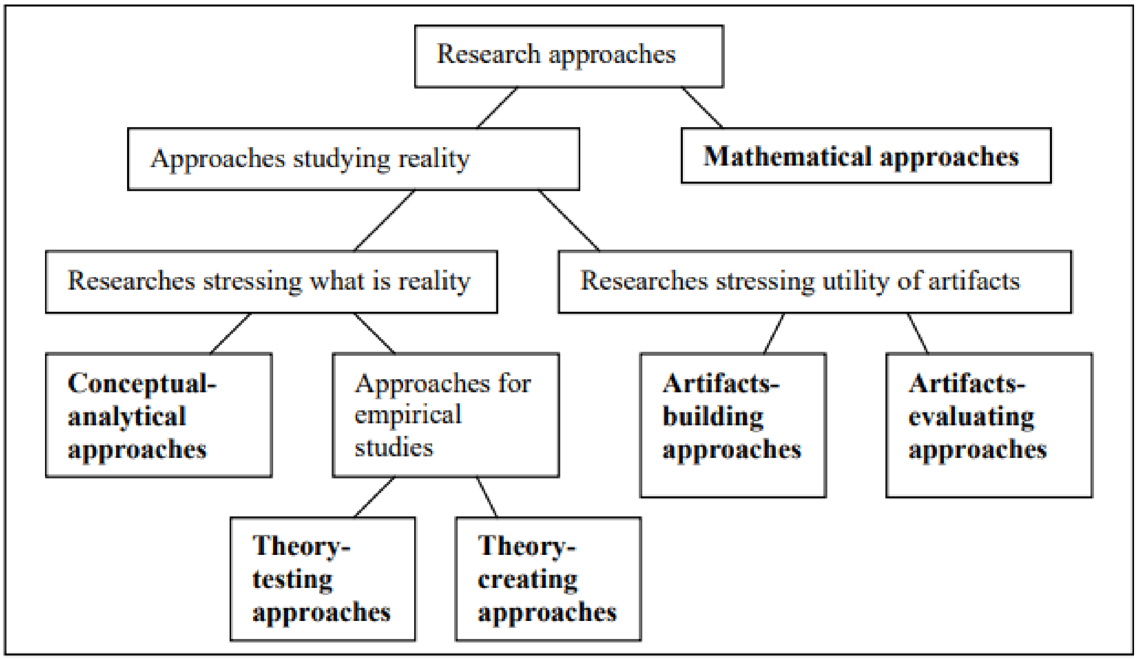

Research approaches
Approaches studying reality
Mathematical approaches
Researches stressing what is reality
Researches stressing utility of artifacts
Conceptual-analytical approaches
Approaches for empirical studies
Artifacts-building approaches
Artifacts-evaluating approaches
Theory-testing approaches
Theory-creating approaches

FIGURE 9 A classification of IS research approaches (Järvinen 2004)

Järvinen (2004) divides and categorizes IS research approaches as illustrated above in FIGURE 9. In the taxonomy a top-down principle is applied. IS research approaches are divided into the ones that study reality and the ones that that a mathematical approach. "Mathematical approaches" are differentiated from them rest as they are utilized to study formal languages, units, words or symbols that do not have a direct reference to objects in reality. "Approaches that study reality" can be subdivided into "research stressing what reality is" and "researches stressing utility of artefacts". The latter is further differentiated by whether artefacts are being built or evaluated. "Researches stressing what reality is" is divided into "Conceptual-analytical approach" and "Approaches for empirical studies". The latter is further subdivided into "Theory testing approach" and "Theory creating approach" depending on the aim of the research approach.

This paper aims to synthesize knowledge from previous work and question existing assumptions regarding the use of subjective norm as a predictor in information security behavior, specifically in the context of password selection. As such this paper is not intended to present original data, test theories nor create new ones. This paper sets out to discover and discuss the role of subjective norms in password selection by examining existing empirical research, analyzing the research settings and findings.

Following the logic presented in figure 9 conceptual analytical approach appears best suited to accomplish the goals of this research. IS researchers have applied methods from several different disciplines such as psychology, philosophy, mathematics and sociology (Siponen, 2002). Conceptual analysis is widely used to study abstract ideas in philosophy but can be used to benefit other academic disciplines as well (USC Libraries, 2020). Conceptual analysis as a research approach has, not unlike other research methodologies, been critiqued and questioned. There are objections to the notion that conceptual analysis can produce substantial knowledge especially in philosophical domain. While this may be true, the author of this paper wants to note that the aim of this research is to examine and analyze existing empirical research and draw conclusions based on them. As such this paper aims to act as a springboard to new empirical research that can improve our understanding of subjective norms in this context (Kipper, 2012).

5 LITERATURE REVIEW

Studies were chosen based on parameters described above in section 4.1. Literature review. This section discusses the results and implications of those 10 studies and focuses on the role subjective norm plays in each of them. The studies are examined particularly in the light of research objective (to argue that generally subjective norm may not be a predictor for information security behaviour, specifically in the password selection). Due to the lack research on subjective norms and passwords other information security behavior related studies were also included.

The emphasis of this section is in the role subjective norm plays in each of the studies examined. All the studies were conducted in the field of information security and focused on human behavior as opposed to technical solutions. All of them utilized an empirical research approach. The findings in each research show a considerable variation and at a glance can appear to contradict with each other. While the results are indeed inconsistent, there are underlying differences that can at least partly explain why the significance of subjective norm varies between the studies. Out of the 10 studies chosen, 8 utilized a survey or questionnaire as a research method, one relied on a systematic literature review and one conducted an experiment on the participants.

5.1 Studies in an organizational context

Organizations can address password security rules and requirements in the information security policies. Depending on the extent of the information security policy framework it can be embedded in a general information security policy or as a separate, standalone password policy. Regardless, in order to understand how subjective norms, relate to individuals' password selection, it is vital to consider the element of information security policy compliance. Research on subjective norms as predictors for information security compliance have shown mixed results over the years with (Yoon & Kim, 2013) finding them insignificant, (Yazdanmehr & Wang, 2016) as strong, and weak (Dinev & Hu, 2007;

Jafarkarimi et al., 2016) as weak. Järvinen (2018) conducted a survey that yielded 408 responses from students in the University of Helsinki and National Defense University. In the research model author combined the Theory of Reasoned Action and personality traits as predictors of information security behavior. In addition to personality assessments, the participants were presented with three different scenarios where information security was at risk. Based on the scenarios the participants were asked to rate their probability to act in a similar way as well as their evaluation of the presented act. The ratings provided information about participants' intention and attitude towards the scenarios. Interestingly, the author found that while attitude and subjective norms combined accounted for 33% of the variance in information security behavior, the former was found to be significantly stronger predictor for conscious cautious information security behavior compared to the latter. Organization's instructions on information security accounted for 37% of the variance in subjective norms and the covariance between the two was found to be quite strong (Järvinen, 2018). Similar conclusions were drawn by Safa et al. (2015) based on their research "Information security conscious care behavior formation in organizations". The authors found that the relationships between attitude and subjective norms towards information security conscious care behavior were positive. Furthermore, Safa et al. (2015) also found that organizations information security policies have a positive effect on subjective norms towards performing information security conscious care behavior. They note, however, that this may also be due to the mandatory nature of the policies. These findings are also supported by Herath & Rao (2009) in their paper "Protection motivation and deterrence: A framework for security policy compliance in organizations". The research was conducted online as a survey to employees in various roles and positions across 10 different organizations and found that subjective norms have a significant on policy compliance intention. The authors do note that out of the five items (boss, colleague, computer specialist, top management and IS security department) related to subjective norms, two (top management and IS security department) were found to be insignificant. They speculate that this may be due to the lack of a dedicated IS security department in some organizations and the employees not knowing the expectations of the top management. Hu et al. (2001) concluded in their research "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture" that "We confirmed that the established behavioral determinants—attitudes, subjective norm, and perceived behavioral control—indeed significantly influence an individual's behavioral intention toward compliance with information security policies" (Hu et al. 2001, p.44). Similar findings were reported by Johnson (2017) in his research "How Attitude Toward the Behavior, Subjective Norm, and Perceived Behavioral Control Affects Information Security Behavior Intention" where he applied Theory of Planner Behavior (TPB) to examine "how attitude toward the behavior, subjective norm, and perceived behavioral control affected the intention of computer end users in a K-12 environment to follow information security policies"(Johnson, 2019 p.

3). He discovered that TPB accounted for over 30% of the variance in intention to comply with these policies. Notably, subjective norms were a significant predictor of intention in the model.

In the light of the research examined here, there appears to be a varying degree of influence that subjective norms have over intention to comply with information security policies. Similar conclusions were drawn by Sommestad et al (2014) based on a systematic review of 29 studies and aimed to identify variables that influence compliance with information security policies of organizations and to establish the significance of these variables. The authors found "soft" variables more important than "hard" ones but none of the variables explained a significant part of variation in people's behavior. Moreover, when the variables were investigated in multiple studies the findings showed considerable variation. Finally, Taylor & Todd (1995) found subjective norm to be a more accurate predictor if intention among inexperienced users in a study they conducted in a student computing information resource center. In their study Venkatesh & Davis (2000) found subjective norm to affect intention especially under mandatory situations. They also discovered that it weakened over time.

5.2 Studies in a non-organizational environment

Hazari et al. (2008) went outside the organizational computing environment to study employees who perform work related duties from home. The notable differences between organizational computing and home computing can be the levels of management and technical controls. In their study Hazari et al. (2008) extended the TBP to predict behavior of employees who perform work related computing on home computer and their information security awareness. The study utilized a questionnaire that included 12 scale items relating to information security awareness taxonomy categories. The study was conducted in a university in United States and all participants were subject to a knowledge quiz. The authors found that while all three variables of TPB, attitude, subjective norm and perceived behavioral control showed strong path coefficients, subjective norm was by far the least weighted. The authors note that while some of the shortcomings of information security behavior in work related home computing can be addressed with training and technical solutions, the managers of the organizations should be cognizant that psychological and social factors play important role in sustaining such behavior.

Chi et al. (2012) studied "influence of end users' perceived risk on usage intention of cloud computing services and to examine whether subjective norm is a moderating variable between the relationship of perceived risk and usage intention" (Chi et al. 2012, p. 95). The study was conducted in Taiwan and dispatched in companies, internet cafes and computer classrooms. The authors discovered that the influence of subjective norm is higher than perceived risks on the usage intention. This implies that users are willing to accept a degree of security risk to join social networks to develop human relationships. Subjective norm was found to have a moderating effect which means that under the interactive effect of subjective norm and perceived risk the user intention will gradually decline. Kusyanti et al (2019) also studied the effect of subjective norm on security intention. The authors conducted a case study where they used 12 construct variables adapted from Protection Motivation Theory (PMT) to analyze Facebook account and found that subjective norm has significant influence towards user behavior intention. Based on the results of their research, the authors concluded that "If a friend or family of an individual advises that the user increases security measures in protecting their online account, then the user will increase the security measures and vice versa" (Kusyanti et al. 2019, p. 8).

The element of subjective norm was also studied by Khan (2017) in a thesis "Effects of Peer Feedback on Password Strength" where the author studied the effects of peer influence on password strength by utilizing a peer-feedback password meter for a pool of 48 university students. Khan compared the results of a peer-feedback password meter to a traditional one and found that the former produced stronger passwords only when administered alongside explicit instructions. However, in the absence of explicit instructions there was no significant statistical difference between the two. Finally, the authors hypothesize that a peer-feedback password meter would most benefit on platforms such as social media, that depend upon social connections between users. Conversely, this could imply that elements of subjective norms, here peer-feedback, might not play a significant role in the creation of a strong passwords unless explicit instructions are administered and the service for which the password is created is dependent on social connections between users. The significance of subjective norm in this study is not explicitly addressed, but it would appear that it alone is not significant enough to result in the creation of strong passwords.

6 CONCEPTUAL ANALYSIS

In this section, the author presents three separate scenarios of information security behaviour related to password selection. The aim is to consider conceptually the role of subjective norm as predictor in in these scenarios. The scenarios represent the findings of the literature review by making the distinction between organizational and non-organizational context. By applying conceptual-analytical research approach and using scenarios the author wants to underline and expound instances where subjective norm might not be a strong contributor in the given behaviour. Conceptual-analytical research approach presented and justified in greater detail in section 4.2.

6.1 Password for a work-related account

Creating easy-to-guess passwords is one of the most important and common IS security issues in organizations (Siponen and Vance, 2010). As discussed above in the previous section, there can be rules in place to either restrict or guide the creation of a password but because there are ways around these, the issue persists.

Creating passwords in a work environment can differ from personal use as there is an element of accountability that stems from workplace information security and password related policies. These policies typically mandate the use of strong and frequent refreshed passwords (Aurigemma et al., 2017). This is not the case with home end-users who rarely change their relatively weak passwords (Florencio & Herley, 2007).

The presumption that the rules of secure password selection are mandated in each organization's information security and/or password policies means this section focuses on information security policy compliance. Behavioral research on information systems security has produced several different models to explain information security policy compliance. Unified Model of Information Security Compliance (UMISPC) reviews 11 of these theories that contribute to the majority of information security models. Authors Moody et al.

(2018) found subjective norms to be insignificant in their model but as the study utilized distinct scenarios based on the previous work of Siponen & Vance (2010), the authors note that the results may differ depending on the scenarios presented to the subjects. Based on their empirical analysis of the UMISPC Moody et al. (2018) discovered that role values were the most significant component of towards information security policy compliance. The authors described role values as "The required ISS policy compliance act is appropriate, justified, and acceptable, keeping in mind the nature of the work and the task the person is performing" (Moody et al., 2018 p.16).

In this paper the author has examined a number of studies that have found subjective norm to have positive influence over information security policy compliance (Hu et al.,2001; Johnson, 2017; Herath et al., 2009; Safa et al., 2015). In contrast, Sommestad et al. (2014) conducted a review of 29 studies that included different 61 variable in the effort to identify the ones that influence compliance with information security policies without conclusive results. The authors speculate this could be because of measurement errors introduced by lower quality studies. Despite the inconclusive results, the authors were able to identify predictors that were generally good predictor for information security compliance: perceived behavioral control, perceived justice of punishment, perceived legitimacy, threat appraisal, information security awareness, descriptive norm, information security policy fairness, normative beliefs and perceived value congruence. While the list includes normative beliefs, a component of subjective norms, it did not include the motivation to comply which is the other component of subjective norms. Furthermore, the fact that the list includes 9 predictors may serve as testament to the significant variance in results across different studies conducted on information security policy compliance.

In the light of previous research, it is questionable if that subjective norm is generally as a reliable predictor for the password behavior. Consider, for example, the following scenario A (FIGURE 10). In this scenario subjective norm cannot be considered as a significant contributor towards such behavior. Rather the author speculates instead that role values may be a more significant contributor. The reason is that Albert was aware and previously willing to comply with the company's password policy. The decision to adopt less secure information security related behavior in the form of password re-usage in this scenario was a conscious one. Albert reasoned can be seen appropriate and justified given the new circumstances.

Similarly, in scenario B (FIGURE 11) the decision to use a less secure password was arguably not motivated by subjective norm. Instead, the decision could have been affected by the sense of urgency and pressure caused by other people behind him in the line. As such the presence of other passengers may have contributed towards Betty's decision to choose the password. However, subjective norm is defined as "person's perception that most people who are important to him think he should or should not perform the behavior in question" (Fishbein & Ajzen, 1975, p.302). The author argues that it would be a stretch to consider other passengers as "important". Furthermore, while it is plausible that among the co-passengers there may have been for example a colleague, it is difficult to see how the perceived behavioral expectations of him or her could have been of significance. Moreover, as Ahtola (1976) noted, the concept of normative beliefs which is a construct if subjective norm, relies on the idea of a homogenous norm about expected behaviors by those of importance to the person. Therefore, for subjective norm to hold significance in scenario B (FIGURE 11) all of the following would have to be true: (1) Betty considers her co-passengers expectations important to her, (2) Betty perceives her co-passengers expectations homogenous, and (3) Betty is motivated to comply with these expectations. The author speculates that it is more likely the sense of urgency in the situation and perhaps exuded by the co-passengers collectively could have played a more significant role in Betty's decision to choose a less secure password for a temporary use and therefore, violate the company policy. It is also worth noting that there was an intention to switch to a more secure password and therefore to comply with the company policy. Similar to scenario A (FIGURE 10), in scenario B (FIGURE 11) it is far more likely that the key contributor to this behavior were role values as the decision was a conscious one. It is perceivable that Betty reasoned that the risk of having a less secure password for a short period of time is insignificant enough to warrant her behavior.

Description of scenario A:

Albert was recently promoted to a manager for a team of consultants. As a former consultant in the company he is no stranger to the company's obligatory annual trainings that include those about secure and compliant information security behavior. His password is due to expire and it is time for a first refresh since he started in the new position. Albert has usually created complex passwords and avoided re-using them as is required by the company policy. However, Albert no longer needs to visit clients and even has his own office. Given this, he reasons that it is secure enough if he simply used the same password he used previously and just added the number "1" at the end of it.

FIGURE 10 Description of scenario A

Description of scenario B:

Betty is boarding a plane for a business trip. Betty has her boarding pass in the inbox of her company email account. She is struggling to remember the password for the app and realizes there is a queue forming behind her. She decides to hit the "Forgot your password" link that sends her a one-time password via email. When used the application requires users to create a new password. Due to a sense of urgency, Betty decides to set the password to "Betty123" for now and switch it later. The company Betty works for has strict requirements to use secure passwords set forth in the company policy. Despite this, the intention to change the password is soon forgotten.

FIGURE 11 Description of scenario B

6.2 Password for a private email account

The most popular email clients from Apple, Google and Microsoft hold a market share about 83% (Litmus Labs, 2020). While there is an abundance of alternative email providers to choose from, the overwhelming majority email users appear to prefer one of the aforementioned companies' solutions. Each of the companies' email clients deploy a set rules that govern the creation of a password for an account. The purpose of such rules is to prevent users' from creating weak passwords and they are in-line with what was established in section 2.2.1 Password strength of this thesis. While the parameters for an acceptable password are set forth by the email service providers, it is still possible to create less secure passwords that satisfy the requirements, for example by selecting a password that is easy to guess or similar to the user account name.

Although the results of the study by Kusyanti et al. (2019) suggest that subjective norm has a significant influence towards user behavior, it is worth noting that the study was conducted in the context of Facebook, a social media platform, users' passwords. Khan (2017) had similar findings when conducting research on a password meter that would utilize a peer-feedback mechanism but went on to speculate that it could prove to be most effective on platforms that depend upon social connections between the users. While the two studies are not entirely compatible, the findings by Khan (2017) would suggest that the context and nature of the service in which subjective norm is examined should not be overlooked. Given that Kusyanti et al. (2019) conducted their study on Facebook users, the findings may not be applicable in the context of creating a password for an email account. The authors, too, acknowledge this limitation themselves and state that "Deeper investigation may be required like adding some constructs from different model to obtain a better comprehension on protecting online accounts."

Some of the previous research points towards willingness to accept a degree of security risk to join social networks to develop human relationships (Chi et al., 2012). Similarly, users are more susceptible for influence by others in situations where social connections are present or of relevance (Kusyanti et al. 2019; Khan, 2017).

Consider also the scenario (FIGURE 12) presented below, which is about user was creating a private email account. The author speculates that while an email account could be used for building social networks, it might not be accurate to consider it as the primary motivation in this scenario. Instead, arguably, the motivation was to avoid cluttering the user's primary email with emails of less importance like newsletters. As the element of social networks and human relationships is insignificant or absent, the research findings related to the significance of subjective norms introduced above become less significant. Subjective norm, therefore, could not be considered as a significant contributor in the following scenario B (FIGURE 11). It is perceivable that the decision to apply length and complexity to her password could have been influenced by the email service providers' password requirements. However, as stated above, they cannot prevent re-use of passwords from other services or prevent users from creating easy-to-guess or dictionary-based passwords. In scenario C (FIGURE 12), the decision to apply these features of a secure password could stem from user's habit that influenced the behavioral intention. This is particularly plausible given that the user appears to be accustomed to using secure passwords.

Description of scenario C:

Carl secures his private email account with a complex and difficult-to-guess password. He uses this email account for almost everything of importance, for example as a back-up for his mobile phone. The account is also linked to his photos and contacts list. Carl applies similar criteria to his other important passwords for example for social media accounts.

Carl wants to create another email address that he can use for less important matters such as subscribing to a newsletter to receive a one-time discount code for an online store. He decides to secure this account with an equally secure password that is completely different to the one he already has for her primary email account.

FIGURE 12 Description of scenario C

7 DISCUSSION

Subjective norms are used as a predictor in some of the most prominent and well-established theories and behavioural models. However, the role of subjective norm as a predictor in information security related behaviour has been widely and frequently contested. This may be due to considerable variation in results from different studies across the field. This paper studied how subjective norms affect individuals' selection of passwords by the means of literature review followed by a conceptual-analytical research approach.

7.1 Findings

Literature review provided confirmation that the significance of subjective norm as a construct or a predictor in various information security related behaviours and scenarios is unclear and dependent on several factors. Previous research related to subjective norms in the context of password selection is sparse and therefore a decision was made to expand the scope of the literature review to information security related behaviour pieces with subjective role as a construct.

Literature review synthesized a number of studies utilizing a variety of behavioural models and theories under different circumstances. It became apparent that a distinction between an organizational environment and non-organizational environment was a necessary one to make as studying the former would mean incorporating an element of information security policy compliance with its constructs which as such are not relevant nor applicable in a non-organizational environment.

The literature review of the studies conducted in non-organizational environments points to subjective norm having an impact on security intention especially. However, the significance and type of impact remain unclear. On one hand, it is suggested that subjective norm has a significant positive impact on users' information security intention (Kusyanti et al., 2019) while on the other hand a study found subjective norm to have an insignificant effect on password selection unless administered with explicit instructions (Khan, 2017). Latter hypothesized that social norm may have a relatively significant role as a contributor towards information security behavior, such as good password practices, in the context of services built upon social networks, such as social medias. Conceptual analysis supports these findings while adding that rules and requirements regarding passwords can sometimes make it more difficult to choose a weak password

Studies conducted in an organizational context concentrate on information security policy compliance and show mixed results in terms of the significance of subjective norm as a contributor towards compliant behaviour. While there are several studies that have identified subjective norm as a predictor for information security policy compliance, those studies also identified other more significant predictors. It is worth noting that most the studies included in this paper examine relationships statistically (e.g., by means of statistical significances). Therefore, significant predictor herein means a statistical generalization, which are not universal but rather probabilistic statements (Siponen & Klaavuniemi 2020).

The issue of using subjective norm as a predictor was questioned by Safa et al. (2015) as they argued that the distinction between the influence of subjective norm and the mandatory nature of information security policy compliance can be difficult to make. While several studies found subjective norm to contribute towards information security policy compliance, and as such the selection of passwords in an organizational environment, they are in no way consistent. This was also well noted by Sommestad et al. (2014) who were unable to identify the best predictors toward infosec policy compliance behaviour in their research that consisted of 29 studies.

The inconsistent, and in some cases contradicting research findings make it difficult to establish scenarios where subjective norm can be reliably used as a predictor for information security intent and information security policy compliance. Building on this, the criticism of subjective norm as a concept presented in section 3.6. makes it challenging to justify the use of subjective norm as a major predictor in the aforementioned scenarios and, therefore also for password selection in both organizational and non-organizational environment.

7.2 Limitations

Existing research on the significance of subjective norm in the context of password selection is sparse. Because of these limitations the author chose to expand the scope of the literature review to include information security related behaviour in general as opposed to limiting it just to passwords. While this decision might have had a negative effect on the reliability of the study, it was necessary to increase the validity to an acceptable level. Furthermore, the limitations of the research method are obvious. The aims of literature review and conceptual analysis are to synthesize information. Findings presented in the previous chapter need to be further studied and validated perhaps by empirical means.

8 CONCLUSION

The motivation for the present study stemmed from the authors interest in individuals' information security related behaviour. Subjective norm as a construct and a predictor for this type of behaviour has been widely contested. The aim of this study therefore was to examine if subjective norm can be used to explain individuals' selection of passwords. To examine this, the present study included a literature review supplemented with a conceptual analysis. The literature review consisted of an in-depth analysis of 10 previous studies on information security behaviour. One of the studies analysed was a structured literature review of 29 studies. The findings of the literature review were then applied in a conceptual analysis where the author presented three hypothetical scenarios: two in an organizational and one in a non-organizational context. In both scenarios, subjective norm was assessed for its significance as contributor towards user behaviour. The results from the literature review proved to inconclusive and in some cases contradicting, which was also reflected in the conceptual analysis. The author of speculates that this can be due to the low validity of some of the previous studies which in turn can be because of wide selection of different variables used across them.

This study provides further evidence that the use of subjective norm as a predictor of behaviour in the context of information security and indeed password selection is questionable. Furthermore, this study underpins the great deal of variance in the results of existing studies. The extent to which subjective norm can be reliably used to explain this kind of behaviour remains unclear and more empirical studies are needed.

REFRENCES

Ahtola, O. (1976), Toward a Vector Model of Intentions. NA - Advances in Consumer Research Volume 03, eds. Beverlee B. Anderson, Cincinnati, OH: Association for Consumer Research, Pages: 481-484.

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behavior. Englewood Cliffs NY Prentice Hall (Vol. 278).

Ajzen, I., & Madden, T. (1986). Prediction of goal-directed behaviour: Attitudes, intentions, and perceived behavioural control. Journal of Experimental Social Psychology. 22: 453-474

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. Action control pp. 11-39.

Ajzen, I. (1991). The Theory of Planned Behavior. Organizational Behavior and Human Decision Processes 50, 179-211.

Ajzen, I. (2019). Normative Beliefs. Accessed 26.7.2020 from https://people.umass.edu/aizen/nb.html

Aurigemma, S., Mattson, T. & Leonard, L. (2017). So Much Promise, So Little Use: What is Stopping Home End-Users from Using Password Manager Applications?

Bagozzi, Richard (1981). "Attitudes, intentions, and behavior: A test of some key hypotheses". Journal of Personality and Social Psychology. 41 (4): 607–627.

Bauman, E., Lu, Y. & Lin, Z. (2015). Half a Century of Practice: Who Is Still Storing Plaintext Passwords?. In: Lopez J., Wu Y. (eds) Information Security Practice and Experience. ISPEC 2015. Lecture Notes in Computer Science, vol 9065. Springer, Cham

Boer, H., & Seydel, E.R. (1996). Protection motivation theory. In M. Connor and P. Norman (Eds.) Predicting Health Behavior. Buckingham: Open University Press.

Calyptix Security. (2017). What Motivates Hackers? Money, Secrets, and Fun. Accessed 10.6.2020 from https://www.calyptix.com/top-threats/motivates-hackers-money-secrets-fun/#:~:text=Financial%20gain%20is%20what%20motivates%20hackers%20most%20often.&text=Hackers%20were%20able%20to%20nab,the%20bank's%20international%20transaction%20account.

Caruthers, M. (2018). World Password Day: How to Improve Your Passwords. Accessed 11.6.2020 from https://blog.dashlane.com/world-password-day/

Chi, H., Yeh, H. & Hung, W-C. (2012). The Moderating Effect of Subjective Norm on Cloud Computing Users' Perceived Risk and Usage Intention. International Journal of Marketing Studies; Vol. 4, No. 6; 2012

Chiasson S., Forget. A, Stobert, E., van Oorschot, P. & Biddle, R. (2009). Multiple password interference in text passwords and click-based graphical passwords. Conference: Proceedings of the 2009 ACM Conference on Computer and Communications Security, CCS 2009

Chou, H-C., Lee, H-C., Yu, H-J., Lai, F-P., Huang, K-H. & Hsueh, C-W. (2012). Password cracking based on learned patterns from disclosed passwords. International Journal of Innovative Computing, Information and Control ICIC International ©2013 ISSN 1349-4198 Volume 9, Number 2, February 2013

Chuttur, M.Y. (2009), Overview of the Technology Acceptance Model: Origins, Developments and Future Directions, Indiana University, USA, Sprouts: Working Papers on Information Systems.

Cybersecurity & Infrastructure Security Agency. (2019). Security Tip (ST04-002) Choosing and Protecting Passwords. Accessed 5.6.2020 from https://us-cert.cisa.gov/ncas/tips/ST04-002

Cyclonis. (2018). What Is a Hybrid Password Attack? How Is It Used in Password Cracking? Accessed 11.6.2020 from https://www.cyclonis.com/what-is-hybrid-password-attack-how-used-password-cracking/

D'Arcy, J., Hovav, A., and Galletta, D. F. 2009. "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," Information Systems Research (23:1), pp. 79-98.

Davis, F. (1985). A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results. Massachusetts Institute of Technology.

Davis, F. D. (1986). PhD Thesis - Massachusetts Institute of Technology.

Davis, F. D. (1989), "Perceived usefulness, perceived ease of use, and user acceptance of information technology", MIS Quarterly, 13 (3): 319–340.

Davis, F., Bagozzi, R. & Warshaw, P. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. Management Science. 35. 982-1003.

Florencio, D. and Herley, C. (2007). A large-scale study of web password habits, Proceedings of the 16th international conference on World Wide Web, ACM, 2007, pp. 657-666

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. Journal of the Association for Information Systems, 8(7), 386–408.

Easterby-Smith, M., Thorpe, R., & Lowe, A. (2002). Management research. London: Sage Publications

Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K., & Herley, C. (2013). Does my password go up to eleven?: the impact of password meters on password selection. Conference on Human Factors in Computing Systems - Proceedings. 2379-2388.

Erminôte, D. (2020). Cyber Raid — Potentiate Brute-force and dictionary attack on hashed real-world passwords cracker. Accessed 11.6.2020 from https://medium.com/@daric_erminote/cyber-raid-potentiate-brute-force-and-dictionary-attack-on-hashed-real-world-passwords-cracker-a8d7bd50a24d

Fishbein, M. (1967). Attitude and the prediction of behaviour in Readings in Attitude Theory and Measurement.

Fishbein, M., & Ajzen, I. (1975). Belief, Attitude, Intention, and Behavior. Addison-Wesley Series in Social Psychology.

Florêncio, D., & Herley, C. (2007). A large-scale study of web password habits. In 16th international conference on World Wide Web (pp. 657-666). ACM.

Furner, J. (2004). Conceptual Analysis: A Method for Understanding Information as Evidence, and Evidence as Information. Archival Science.

Gartner (2018). Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019. Accessed 12.10.2020 from https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

Gaw, S. & Felten, E. (2006). Password management strategies for online accounts. In Proceedings of the second symposium on Usable privacy and security (SOUPS '06). Association for Computing Machinery, New York, NY, USA, 44–55.

GeeksForGeeks. (2017). HTTP GET and POST Methods in PHP. Accessed 8.6.2020 from https://www.geeksforgeeks.org/http-get-post-methods-php/

Harward University. (2014). Behind The Login Screen: Understanding Web Authentication Protocols. Accessed 3.6.2020 from https://iam.harvard.edu/resources/behind-login-screen

Hazari, S., Hargrave, W. & Clenney, B. (2008). An Empirical Investigation of Factors Influencing Information Security Behavior. Journal of Information Privacy and Security.

Hendrickson, J. (2019). Why are companies still storing passwords in plain text. Accessed 8.6.2020 from https://www.howtogeek.com/434930/why-are-companies-still-storing-passwords-in-plain-text/

Herath, T. & Rao, R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. EJIS.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43(4), 615–660.

IETF Documents. (1999). Hypertext Transfer Protocol. Accessed 7.6.2020 from https://tools.ietf.org/html/rfc2616

Jalkanen, J. (2019). Is human the weakest link in information security, 2019 University of Jyväskylä, Faculty of Information Technology.

Jafarkarimi, H., Saadatdoost, R., Sim, A. T. H., & Hee, J. M. (2016). Behavioral intention in social networking sites ethical dilemmas: An extended model based on theory of planned behavior. Computers in Human Behavior, 62, 545–561.

Johnston, A. C., and Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly (34:3), pp. 549-566.

Johnson, D. (2017). How Attitude Toward the Behavior, Subjective Norm, and Perceived Behavioral Control Affects Information Security Behavior Intention.

Jung, J. (2019). What are Salted Passwords and Password Hashing?. Accessed 8.6.2020 from https://www.okta.com/blog/2019/03/what-are-salted-passwords-and-password-hashing/

Järvinen P (2004), Research questions guiding selection of an appropriate research method. Proceedings of the 8th European Conference on Information Systems (ECIS 2000), Vienna, Austria.

Järvinen, H. (2018). Human factors in information security – personality and reasoned actions behind information security behaviour. Master's thesis. Faculty of Medicine / Department of psycholofy and logopedics. University of Helsinki.

Kamasak, R., Kar, A., Yavuz, M. & Baykut, S. (2017). Qualitative methods in organizational research: An example of grounded theory data analysis.

Kipper, J. (2012). A Two-Dimensionalist Guide to Conceptual Analysis. De Gruyter (April 15, 2012)

Kelley, P., Komanduri, S., Mazurek, M., Shay, R. Vidas, T., Bauer, L., Christin, N., Cranor, L. & Lopez, J. (2012). Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms," 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, 2012, pp. 523-537

Kleucker, M. (2013). Fallback Authentication. Beyond the Desktop Hauptseminar Medieninformatik WS 2012/2013 Technical Report LMU-MI-2013-1, April, 2013

Kusyanti, A., Catherina, H., Puspa, A. & Sari, Y. (2019). Protecting Facebook Password: Indonesian Users' Motivation. Procedia Computer Science.

Lee, M. (2013). Encryption Works: How to Protect Your Privacy in the Age of NSA Surveillance. Freedom of the Press Foundation.

Legris, P., Ingham, J., Collerette, P. (2001). Why do people use information tec nology? A critical review of the technology acceptance model. Information & Management 40 (2003) 191–204.

Litmus Labs. (2020). Email Client Market Share. Accessed 2.10.2020 from https://emailclientmarketshare.com/

LogMeIn, (2020). Psychology Of passwords: The online Behavior that's Putting you at risk. Accessed 11.6.2020 from https://lpcdn.lastpass.com/lporcamedia/documentlibrary/lastpass/pdf/en/LastPass-B2C-Assets-Ebook.pdf

McNeill, P., & Chapman, S. (2005). Research methods. Third edition.

Moody, G., Siponen, M & Pahnila, S. (2018) Toward a Unified Model of Information Security Policy Compliance. MIS Quarterly Vol. 42.

Ng, B-Y.& Rahim, M. (2005). A Socio-Behavioral Study of Home Computer Users' Intention to Practice Security." PACIS (2005).

Pahnila, S, Siponen, M & Mahmood, A. (2007). Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study. PACIS 2007 Proceedings. 73.

Peltomäki, J., & Norppa, K. (2015). Rikos meni verkkoon: Näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen. Helsinki: Talentum

Rogers, E. M. (1995). Diffusion of innovations. Macmillian Publishing Co. Schneier, B. (1995) E-mail Security: How to Keep Your Electronic Messages Private. Wiley; 1 edition (January 25, 1995).

Roser, M., Ritchie, H. & Ortiz-Ospina, E. (2015). Internet. Accessed 11.6.2020 from https://ourworldindata.org/internet

Rowley, J. & Slack, F. (2004). Conducting a literature review. Management Research News. 27.

Safa, N., Solms, R., Sookhak, M. & Ghani, N. (2015). Information security conscious care behavior formation in organizations, Computers & Security, 53, 65-78.

Siponen, M. (2002). Designing secure information systems and software:

Critical evaluation of the existing approaches and a new paradigm. Academic Dissertation to be presented with the assent of the Faculty of Science, University of Oulu.

Siponen, M. & Klaavuniemi, T. (2020). Why is the hypothetico-deductive (H-D) method in information systems not an H-D method? Information and Organization 30 (2020).

Siponen, M. T. & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487–502.

Sommestad, T., Hallberg, J., Lundholm, K. & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. Information Management & Computer Security.

Taylor, S. & Todd, P. (1995). Assessing IT Usage -The Role of Prior Experience. MIS Quarterly, Vol. 19, No. 4. (Dec. 1995), pp. 561-570.

Techterms (2020). Password Definition. Accessed 3.6.2020 from https://techterms.com/definition/password

Traficom. (2014). Salasanalla on väliä. Accessed 5.6.2020 from https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2014/12/ttn201412031257.html

Troy Hunt (2017a). Passwords Evolved: Authentication Guidance for the Modern Era. Accessed 3.6.2020 https://www.troyhunt.com/passwords-evolved-authentication-guidance-for-the-modern-era/

Troy Hunt. (2017b). FAQs. Need to know something about Have I Been Pwned (HIBP)? Accessed 5.6.2020 from https://haveibeenpwned.com/FAQs

Ur, B., Kelly, P., Komanduri, S., Lee, J., Maass, M., Mazurek, M., Passaro, T. Shay, R., Vidas, T., Bauer, L, Christin, N., & Cranor, L. (2012). How does your password measure up? The effect of strength meters on password creation. Proc. Security '12, USENIX Association.

USC Libraries. (2020). Humanities Research Strategies: Conceptual Analysis. Accessed 10.9.2020 https://libguides.usc.edu/humanitiesresearch/conceptual

Venkatesh, V.; Davis, F. D. (2000), "A theoretical extension of the technology acceptance model: Four longitudinal field studies", Management Science, 46 (2): 186–204.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3).

Venkatesh, V., Thong, J. Y. L. & Xu, X. (2012), 'Consumer Acceptance and Use of information technology: Extending the unified theory of acceptance and use of technology', MIS Quarterly 36(1), 157–178.

Verizon. (2020). 2020 Data Breach Investigations Report. Accessed 10.6.2020 from
https://enterprise.verizon.com/resources/reports/dbir/

Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," MIS Quarterly, (37:1), pp. 1-20.

Woods, N., & Siponen, M. (2017). Too many passwords?: How understanding our memory can increase password memorability.
International Journal of Human Computer Studies, 111, 36-48.

Woods, N & Siponen, M. (2019). Improving password memorability, while not inconveniencing the user. International Journal of Human-Computer Studies, 128.

Yang, K. & Miller, G. (2007). Handbook of Research Methods in Public Administration. CRC Press; 2nd Edition (November 14, 2007)

Yazdanmehr, A. & Wang, J. (2015). Employees' information security policy compliance: A norm activation perspective. Decision Support Systems, 92, 36–46.

Yoon, C. & Kim, H. (2013). Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. Information Technology & People, 26(4), 401–419.

Younghwa, L. & Larsen, K. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. European Journal of Information Systems, Volume 18.

APPENDIX 1 TABLE OF PREVIOUS STUDIES

Study name	Authors	Descripton	Description of the research set up	Effect of Subjective Norm
Human factors in information security – personality and reasoned actions behind information security behaviour (Ihminen osana tietoturvaa: persoonallisuus ja perusteltu toiminta tietoturvakäyttäytymisen taustalla)	Heini Järviö	“The objective of this study was to investigate what kind of individual and organisational factors affect the way we act with personal and organisational data. The research model of this study combined the Theory of Reasoned Action (TRA) and personality traits as predictors of information security behaviour. In TRA, the best predictor of an action is the intention to do it, which in turn is affected by the attitude towards the action and subjective norms. Scenario method was used to investigate if TRA predicts actions also in concrete scenarios The included personality theories were Big Five and Dark Triad theo-	“The data in this study was a sample of the students in the University of Helsinki and the National Defense University (N=408). The participants completed a survey which measured personality traits and the elements of TRA. Personality was assessed with Short Five and Short Dark Triad inventories. In addition, the participants read three scenarios where information security was at risk. After this they rated their probability to act in a similar way (intention) and their evaluation of the presented act (attitude). The scenarios in this study where divided in three groups according to their level of risk and each participant received scenarios only from a same level. The relationship between personality traits and responses in scenario situations was assessed with regression analysis. The measurement model was as-	The TRA structure was found to predict attitudes in concrete situations. Attitude (β = .48, p<.001) was found to be a stronger predictor for conscious cautious information security behaviour than subjective norms (.25, p<.001). Combined these two accounted for 33% of the variance in information security behaviour. Organization’s instructions on information security accounted for 37% of the variance in subjective norms and the covariance between the two is quite strong (β=.61, p<.001).

		ries, of which the latter has not yet been studied in information security research.”	sessed with path analysis.”	
Information security conscious care behaviour formation in organizations	Nader Sohrabi Safa Mehdi Sookhak, Rossouw Von Solms, Steven Furnell, Norjihan Abdul Ghani, Tutut Herawan	“The study investigated the role of penalties, pressure, and the perceived effectiveness of employee action in information security organization policies. Intrinsic and extrinsic motivations affect employees' behaviour towards compliance with organization security policies.”	“Two hundred and twelve questionnaires remained for data analysis, of which, 51.4% were from male respondents and 48.6% were from female respondents. The gender was relatively equal. Approximately 46.2% of participants were experts in information security and 53.8% were information technology professionals (e.g. roles, such as systems analyst, designer, developer, and so on).”	“The results of the study showed that the pressures exerted by subjective norms and peer behaviour influence employee information security behaviour. Information security policies in my organization are important for my colleagues. Mean: 3.92. STD: 0.949, CFA Loading 0.685 My colleagues' information security behaviour influences my behaviour. Mean: 3.65, STD: 0.915, CFA Loading 0.754

				Information security culture in my organization influences my behaviour. Mean: 4.41, STD: 0.848, CFA Loading: 0.799 My boss's information security behaviour influences my behaviour. Mean: 3.68. STD: 0.868, CFA Loading 0.683”
Protection motivation and deterrence: A framework for security policy compliance in organizations	Herath, T. & Rao, R	“Our study is informed by the literature on IS adoption, protection-motivation theory, deterrence theory, and organisational behaviour, and is motivated by the fundamental premise that the adoption of information security practices and policies is affected by organisational, environmental, and behavioural factors.	“Theoretical model with a data set representing the survey responses of 312 employees from 78 organizations.” “Employees from several organizations were requested to participate in the web-based survey (10 employees from each organization). The 312 responses represent employees from 78 organizations. The average age of participants was 42.3 years, ranging from 18 to	H12: "Subjective norms will positively affect intention to comply with organizational information security policies" “In support of H12, the subjective norm was found to have a significant impact on policy compliance intention.” “We would like to note

		We develop an Integrated Protection Motivation and Deterrence model of security policy compliance under the umbrella of Taylor-Todd's Decomposed Theory of Planned Behaviour. Furthermore, we evaluate the effect of organizational commitment on employee security compliance intentions."	70 years. The participants worked in various roles, including IT personnel, non-IT personnel, engineers, technicians, accounting managers, medical professionals, administrative assistants, etc. 46% of the respondents were female, whereas 54% of the respondents were male"	here that in the formative construction of the five items related to subjective norms, three weights (boss, colleague, and computer specialist) were found to be significant whereas two weights (top management and IS security department) were found to be insignificant. This may be due to the fact that not all organisations have separate security department. Also, employees may not be aware of the top management's expectations.
Protecting Facebook Password: Indonesian Users' Motivation	Ari Kusyanti, Harin Puspa Ayu Catherinab, Yustiyana April Lia	"To be able to enjoy various services from Facebook, a user is required to have a Facebook account. In the registration process to create a new Facebook account, the user is	Data was collected from Facebook users with 300 questionnaires. There was 24 outliers and 276 eligible responses. Users were age 18-24 and the questionnaire used a five-point Likert-scale.	"H6: Subjective norm has a significant positive effect on security intention. "It concluded that Subjective Norm has signifi-

	Sarib	prompted to create a password to protect his account. The password policy service applied by Facebook requires all users to create and use a password for their Facebook account in accordance with the policies. This study aims to analyze user behavior with case study of Facebook account by using 12 construct variables adapted from Protection Motivation Theory (PMT). “		cant influence towards user behavior intention. The results of this study are similar to the results of research conducted by [20] who suggested that the existence of social influences such as: friends or family of a user can influence a user to continue security measures. If a friend or family of an individual advises that the user increases security measures in protecting their online account, then the user will increase the security measures and vice versa.”
Effects of Peer Feedback on Password Strength	Faisal Irfan Yar Khan, 2017	“Lack of strong passwords means that it is the single most vulnerable point to gain unauthorized access to the resource as prior studies have uncovered	“To address this question, we conducted an experiment on a pool of 48 university students. In the design of this experiment, we had two forms of password meters, one was the traditional	“H1: Using peer-feedback password meters increases the password strength as compared to using the traditional password meter.”

	that most passwords are significantly weak and hence, easy to crack. Consequently, exploring mechanisms which improve password security has been the main focus of a significant body of research. To this end, we introduced a peer-feedback password meter which shows how the strength of the user’s password compares to the strength of passwords used by other users. To achieve this goal, we conducted a user study where we asked users to create an account on a hypothetical website. The users were either shown a traditional password meter or a peer-feedback meter.”	password meter and the other was a peer-feedback password meter”. “Age 20-24 students, voluntary set-up. In our study, we informed each participant that this system is being developed specifically for UW students to assist them in collaborating on group projects. Hence, we created a perception amongst the participants that this was a real prototype website soon to be launched for them and they had a real stake in it.”	“Our results suggest that the peer-feedback meter, when administered alongside explicit instructions, would create relatively stronger passwords as compared to traditional password meters. However, when no explicit instructions were given, we did not find a statistically significant difference.”

The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies	Qing Hu	A study of user behavioral intention toward protective technologies based on the framework of the theory of planned behavior.	“Students enrolled in various classes were asked to complete the online questionnaire during class time. Alternatively, students who did not have access to computers in their classes were asked to fill out a paper survey. Additionally, we initiated an e-mail campaign with a request for IS professionals who graduated from this university with MIS/CS degrees to particcipate in this study. We posted links to the online survey on our web sites. Over a period of four weeks, we received 339 responses.”	“We find that awareness of the threats posed by negative technologies is a strong predictor of user behavioral intention toward the use of protective technologies. More interestingly, in the presence of awareness, the influence of subjective norm on individual behavioral intention is weaker among basic technology users but stronger among advanced technology users. Furthermore, while our results are consistent with many of the previously established relationships in the context of positive technologies, we find that the determinants “perceived ease of use” and “computer self-efficacy” are no longer significant in the context of protective

				technologies.”
An Empirical Investigation of Factors Influencing Information Security Behaviour	Hazari, S Hargrave, W. Clenney, B.	“This study uses Ajzen’s Theory of Planned Behaviour to investigate factors related to WRHC (Work Related Home Computing) users’ information security awareness. Demographic, characteristics, attitude, subjective norm, and perceived behavioral control that affect behavioral intention were studied to identify determinants of information security behavior. “	“Approximately 200 business students in a US University completed an online questionnaire. Questionnaire included 12 scale items relating to Information security awareness taxonomy categories. All participants were subject to a knowledge quiz.”	“The study showed that attitudes, subjective norm and perceived behavioral control are related to maintaining information security awareness. Study shows strong path coefficients between these three. Subjective norm, however was found to have weighed the least.”
Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture	Hu, Q, Dinev, T. Hart, P. Cooke, D.	“We develop an individual behavioral model that integrates the role of top management and organizational culture into the theory of planned behavior in an attempt to better understand how top management can influence security compli-	“Alumni of the MIS and MBA programs of a large public university in the US. This yielded a total of 148 responses.” “Measurement items for each construct in the model are based on a 5-point Likert scale.”	“Stronger subjective norm about information security policy compliance leads to stronger behavioral intention to comply with the policies.” “This is in stark contrast

	ance behavior of employees. Using survey data and structural equation modeling, we test hypotheses on the relationships among top management participation, organizational culture, and key determinants of employee compliance with information security policies." "We set out to study two central research questions that have not been adequately investigated in the information security literature: (i) What is the role of organizational culture in shaping employee intention to comply with information security policies? (ii) How does the top management influence employee intention to comply with information security policies?"		with Dinev and Hu (2007) and Pavlou and Fygenson (2006) where the influence of subjective norm is found to be insignificant on individual behavior intentions. The difference may be explained by the different context where subjective norm was measured. The subjective norm in the Dinev and Hu (2007) and Pavlou and Fygenson (2006) studies was about voluntary and proactive behavior and was measured in terms of the influence from an individual's social circle (friends and relatives). In this study, the subjective norm is about compliance behavior in an organization."

The Moderating Effect of Subjective Norm on Cloud Computing Users' Perceived Risk and Usage Intention	Hsinkuang Chi, Hueryren Yeh & Weichien Hung	"The study aims to explore the influence of end users' perceived risk on usage intention of cloud computing services and the interactive effect of perceived risk and subjective norm on usage intention."	"The study dispatched 350 questionnaires to internet users. The amount of valid questionnaires is 238 and the effective response rate is 68%. Conducted in Taiwan and dispatched in companies, internet cafes and computer classrooms. The study uses the questionnaire as research instrument with a 7-point Likert scale (1=strongly disagree; 7=strongly agree)."	"The study also discovered the influence of subjective norm is higher than perceived risk on usage intention. It tells that the influence of individual perceived behavior on usage intention is subject to the effects of society, culture, family , and reference groups' pressures. Hence, it implies that users will use cloud computing services or join social networks to develop human relationships even if there is an internet security risk. Subjective norm has a moderating effect which signifies that under the interactive effect of perceived risk and subjective norm, usage intention will gradually diminish. However, high level

				subject norm group will not reduce usage intention, even following the increase of perceived risk. It is to say that peers’ or social communities’ pressures can increase usage intention.”
How Attitude Toward the Behavior, Subjective Norm, and Perceived Behavioral Control Affects Information Security Behavior Intention	David Philip Johnson, Walden University	“To what extent does attitude toward the behavior, subjective norm, and perceived behavioral control affect the intention of computer end users in a K-12 environment in the Bigg County Public School System located in Northeast Georgia to follow information security policy?”	“Data collection was from 165 K-12 school administrators in Northeast Georgia using an online survey instrument. Data analysis occurred applying multiple linear regression and logistic regression.”	"SN was a significant predictor of intention in the model.....These findings suggest improvement to K-12 SETA programs can occur by addressing normative beliefs of the individual."

Variables influencing information security policy compliance: a systematic review of quantitative studies	Teodo Sommestad, Jonas Hallberg, Kristoffer Lundholm, Johan Bengtsson	“To identify variables that influence compliance with information security policies of organizations and to identify how important these variables are.”	“A systematic review of empirical studies described in extant literature is performed. This review found 29 studies meeting its inclusion criterion. The investigated variables in these studies and the effect size reported for them were extracted and analysed.”	“Unfortunately, no clear winners can be found among the theories, prediction models and variables. While emotional (“soft”) variables seems to be more important than cerebral (“hard”) variables, each of the variables and models only explain a small part of the variation in people’s behaviour. In addition, when a variable has been investigated in multiple studies, the findings show a considerable variation.”