PASSWORD BEHAVIOUR: Still a threat to cyber security.

A study of future financial sector employee's password behaviour

Lucy C. Gabrielsen*

* Senior Lecturer
lcga@iba.dk
+45 2496 6595
Faculty of Finance
INTERNATIONAL BUSINESS ACADEMY
Kolding
6000
Denmark

Abstract

The threat of cybersecurity breaches in Denmark is assessed as the highest ranking of national security threats and has been given top priority attention with dedicated initiatives including the Ministry of Defence's "Centre of cybersecurity". Several sectors are considered the most vulnerable. At the top of the most vulnerable ranking is the financial sector. Organisations, both private and public, concentrate security efforts on software systems, often overlooking the human factor, yet numerous reports present repeated cases of cybersecurity breaches caused by end user behaviour. The human factor is a threat to cyber security when considering that the most common security access modes for malicious adversaries are email and passwords. This paper concentrates on password behaviour by future financial sector employees in Denmark. There is a lack of research on password behaviour focusing on the most vulnerable financial sector. This paper aims to close the gap by focusing data collection on students studying specifically to pursue a future in the financial sector. Born in the mid 1900's and nearing the end of their studies, the vast majority of these students are digital natives, known as Generation Z. Due to their digital upbringing, the study explores if their behaviours and attitudes towards password security. Leaning on social psychological theories, including social engineering and behavioural psychology, the study uses focus groups to explore behaviours and attitudes of the future generation of financial sector employees. The findings demonstrate that behaviours and attitudes towards password security, of digital natives studying for a career in the sector most vulnerable to cyber-attack, are no different from any other group. This presents a high-risk factor for society.

Key words: cybersecurity, passwords, social engineering, financial sector, Generation Z, digital natives.

Content

Introduction

Cybersecurity is at the top of the executive agenda with governments around the world focusing efforts on solutions to cyber-attacks. Both the state and private organisations are investing in research and software systems, creating stringent policies, protocols, reporting procedures and training to minimize the risk of cyber-attacks with investment in precautionary measures focusing heavily on systems software. While this is an improvement on the preceding situation, the question is whether enough is being done about user-controlled access.

Several reports demonstrate that one of the weakest links in organisations, regardless of size, industry or country of operation, is the user [1-5], as individual employees are an easy target through which malicious adversaries can gain access using social engineering. The high threat probability of cyber-attacks from user-controlled access, lies within two somewhat embarrassingly simple and seemingly uncomplicated areas; accessing malware emails and insecure passwords. This paper focus on the latter.

Threat through unknown manipulation

Traditional confidence trickster behaviour of psychological manipulation is in essence fraud through the act of manipulating[1] others [3], with the purpose of gaining access to or eliciting information from victims by skilfully manoeuvring the victim into taking action that they would not usually take, and that may or may not be in the victim's best interest. In today's digital world, the improved and increasing number of attack vectors[2] provide a wealth of personal information from open sources that allows for sophisticated collection, in depth social network analysis, psychological profiling and evaluation, resulting in highly customised and personal attacks as social engineering makes use of human intelligence using direct interpersonal interaction between malicious adversaries, commonly known as hackers, and their potential targets with the purpose of eliciting sensitive information. By this means, malicious adversaries[3] design trustworthy, targeted cyber-attacks to gain access to internally "secured" public and private corporate networks and data through user vulnerabilities.

IT industry reports identify human error as the root cause, at 95%, of all cybersecurity incidents from 2014-19 [1] [4]. Business takes precautions by installing and updating anti-virus, anti-Malware and Firewalls, all which play an essential role in securing networks. Limited by design, this approach is historical based upon cyber-attacks that have already occurred with a mere lack of timeously system updates allowing malicious adversaries to access systems [5]. Compounded by the internet not originally built with the intention of

[1] Defined as when an adversary manipulates an individual to conduct a specific action with the sole purpose to cause a cyberattack [2].
[2] Points of attack exposure, including amongst others email, SMS and social media.
[3] Often referred to as Blackhats [17].

protecting against cyber criminals, but rather to accommodate computer-based communications in a trusted global community for the purpose of communication and trade, it was designed for maximum efficiency without regard for security [6].

A definition of security in terms of computing is "the protection against unwanted disclosure, modification, or destruction of data in a system and also the safeguarding of systems themselves" comprising both technical and human aspects and as such, areas that should be included in the designing of Cybersecurity measures for businesses should include procedural, administrative, and personnel considerations [7].

The list of unintentional threats caused by user error are numerous and include design of hardware, software and information systems, programming, testing, data, collection, data entry, authorisation, negligence, inadequate employee training and password behaviour, including sharing with others. Focusing on the latter three; negligence, inadequate employee training and passwords, the threat is confounded when considering user access and individual online behaviour whereby significant amounts of personal information is left behind on open sources across the internet.

The Social Vulnerability and Assessment Framework (SAVE) project carried out by a consortium of highly regarded institutions[4], proves that in Denmark, a country with a high level of graduates and a mature digital infrastructure, Danes leave a large digital footprint that can be successfully accessed and utilised if planning an attack. So that technological precautions by business, in the form of firewalls and antivirus software, do not provide the necessary security. As organisations concentrate their efforts and focus on IT software, they often neglect considering the end user, a vulnerable link that can open the gateway for attack by malicious adversaries' exploitation of individual employees who have systems access [8]..

Regardless of the size of spend governments and private companies use on preventative measures against cyber threats. Social engineering, the psychological manipulation of individuals - here employees - to perform specific actions, remains a threat with serious consequences of compromising an organisation's security, by unconsciously giving system access to malicious adversaries [9]. As Turban, et al. [6] point out, cyber fraud is aimed mostly at individuals and that malicious adversaries are increasingly attacking the most critical areas of infrastructure and, when it comes to cyber war attacks, along with political espionage, corporate espionage is a target due to the wealth of valuable information held.

[4] The consortium is made up of the following institutions:
Danish Institute of Fire and Security Technology (DBI) leading knowledge center in the field of fire safety and security.
The Alexandra institute (ALX) non-profit organisation that participates in several Danish and EU research projects and recognized by the Danish government as an advanced technology provider.
Center for Defence, Space and Security (CenSec) an industrial cluster and network center for SME vendors and potential vendors to the defence security and/or space industry.

Individuals increasingly create content that they share with others, both individuals known to them in the physical and cyber sphere and strangers Pieters et al. [10]. Thus, access to individuals' personal information becomes increasingly easy for social engineers resulting in increased security threats [10]. The rate of incident of attack rises in correlation to increasing social media, e-commerce and electronic communication use [9], as individuals share their wealth of personal information in their trusted environment of social networks.

Considered a high value commodity on par with oil [11], data became considered as a valuable resource around three decades back when the American "Computer Science and Telecommunications Board" (CSTB) proposed that future "terrorists may be able to do more damage with a keyboard than with a bomb" [7]. As with all assets of value, there is a positive correlation with security.

Irrespective of the number of reports produced, highlighting the complacency of individuals in society, citizens still do not appreciate the enormity of the danger, even in the instance where a large number of individuals in society have been exposed to a cyber-attack [12]. This provides an indication that behaviour does not change with significant correlation to exposure of threat.

In a 2019 survey, a mere 17% of Danish respondents reported they withhold or limit their personal details on social media. Restriction of internet use due to fear of cybersecurity breach became significantly less important since 2015, indicating an increased trust in inbuilt security compared to previous years [13].

Increased online activity together with increased trust of inbuilt cybersecurity indicates that individuals as employees, at every level regardless of the size of the business, are increasingly exposed to and targets of malicious adversaries who use popular social media platforms in their efforts to cajole individuals into giving access, often in unsophisticated, basic manipulation, without the individual's knowledge. In fact, Turban, et al. [6] state that insiders – employees working for attacked businesses – are responsible for almost half of cybersecurity problems - with the newest recruits often bringing added security threats with them.

The threat is enhanced when considering that information accessible on social networks is machine-readable and open to automatized collection of unstructured data, information processes and analysis [9]. Data obtained illegally is subsequently published or processed and used to access confidential information only available and disclosed to authorised employees. Authorised information access by an employee is typically via something they know; a password, or something they possess; an entry token, and can be something unique to the person, in the form of biometrics; a fingerprint or face scan.

Research on password behaviour concentrates primarily on theory and non-specific situations. The literature does not cover the coupling of theoretical insight directly to implications for a specific business sector. Cybersecurity is the risk causing most concern within the financial sector. A risk compounded by the sector's

dependence on IT. Results of a recent (2020) trust and risk survey of respondents responsible for risk in the financial sector, shows a slight decrease in concern by respondents, from 81% in 2019 to 74% in 2020. The 7% decline could be an indication of one of two factors; namely, an increased effort in the investment or that other risks have become more challenging. Either way, they agree that cybercrime adversaries, social engineers, are continually more skilled and advanced criminals [14]. This paper aims to explore future financial sector employees' password attitudes and behaviours, the sector identified by the Danish Ministry of Defence's Centre for Cybersecurity as the most susceptible to cyber-attack in Denmark [5].

The underlying purpose of this research stems from unexpected outcomes of focus groups with future financial sector employees [15], namely their attitudes towards their personal data. These results were prior to the 25th May 2018 effectuation of the EU's General Data Protection Regulation (GDPR) [16].

Future financial sector employees

Based on the working age of 18-65, with a standard deviation of two years and not considering any handicaps, Generation Z (Gen Z) make up 11,25% of the Danish workforce [17]. By 2020, one in four will have lived their entire life in a digital world. According to Schultz Hansen [18] as future employees, these "Digital Natives" find it strange to be met in an environment where social media is not an integrated part of their day. Born around 1995 this generation group follows the Millennials. They are the first generation to have internet technology readily available from a young age [19], having grown up with the internet they are unaware of a world without it. The generation having grown up with mobile phones, they are more mobile than previous generations, expect more from technology and less from each other [20]. Turkle postulates that Gen Z find online life more satisfying than real life, describing real life as "just one more window," and not necessarily their best [20].

A surprising if not disturbing result from a previous study was the attitude that Gen Z demonstrated towards their private data sharing. They expressed little to no interest in terms and conditions of social media platforms or apps. In fact, when probed further, the only private data that they would not consider sharing is their social security number. For some, the choice of social media platform or app and number of users currently known to them was more important to them. Personal risk was assessed through the experiences, or rather lack thereof, of their friends as expressed by one participant saying that nothing has happened to friends yet, so it is accepted by them. Overall, they did not consider that they have any personal information that should be held private [15].

Results from existing research into attitudes towards cybersecurity demonstrate that users in general are unmotivated [21][22] and too unknowledgeable to understand and thereby follow complex security guidelines [23][24].

Attitudes of Gen Z is not due to their lack of knowledge of their personal data for profit gains. In fact, they expressed conscious knowledge of their personal data being used by large international organisations and brands and consider sharing private information part of existing today naming examples such as Google and Facebook.

Gen Z believe that they cannot function as a person without giving their private information [15]. This confirms Benhamou's notion of their "fear of missing out" [25]. Generation Z is ready to give their private details without hesitation. In fact, they are 'quick' to give out personal, sensitive details [26]. Schultz Hansen [18] argues that one must not stereotype and suppose that just because they use the internet to connect with others that they do not worry about their private lives. On the contrary, they research, test, reflect on and problematise distinguishing between open and closed profiles, smaller limited groups utilising a selection of varied social media depending on the use, including private and professional. Despite their reflection, experience and almost virtuoso use of the internet and social media there exists a displacement of the term privacy.

The premises on which they interact in the netsphere is turned inside-out so that the basis for dialogue and other interaction is public whereupon an active choice is necessary to make such interaction private. As such, the private arena, including personal information, is not something that their internet behaviour has in advance as a default setting, i.e., it is not the premise upon which individuals act and as such protect, but something that they must actively and constantly re-establish.

Social media for this generation is more social and less exclusively dedicated to a one-to-one dialogue and companionship. They automatically share an increasing amount of themselves and increasingly more from their private sphere. In considering borders between private and public behaviour on the internet, digital natives perceive borderlessness as the natural premise and the universal starting point where effort is required to shut off and be private [18].
By focusing on what to keep private rather than what to publicize, they often inadvertently play into another common rhetorical crutch—the notion that privacy is necessary only for those who have something to hide [27]. Furthermore, privacy for these individuals no longer exists individually, rather a new form of privacy exists consisting of calculated and set boundaries and divisions into different types and groups of friends. Group has become the new private [18].

Chia and Andreas's [28] study on the influence of how closer circle (in-groups) of related users might guide individuals' security decision making, when looking to install applications on their smart phones, resulted in community positive reviews being overlooked when the closer circle of in-group "friends" contradicted the positive review with negative. The result demonstrates that advice from close ties of value homophily is regarded higher than whole weaker tie communities. Sotirakopoulos [29] argues that this is down to the

effectiveness of peer pressure enforced by value homophily as the feeling of the internal pressure of guilt is more effective than the external pressure of shame.

The research question driving the study is thus "*Are future financial sector employees' online attitudes and behaviours towards passwords putting the sector at risk of cyber-attacks?".* The study explores future financial sector employees', Generation Z, attitudes and behaviours towards cybersecurity, specifically their password behaviour.

Methodology

The philosophy and approach is a combination of post positivistic and interpretivism combined with an inductive approach permitting unexpected outcomes.

The study aims to explore password attitudes and behaviour by Generation Z in Denmark. Here literature gives considerable attention to the use of social scientific and primarily qualitative approaches, Carrasco and Lucas [30] together with Stinger [31] and Baron and Byrne [32] are in consensus in that attitudinal studies focusing primarily on individuals should go beyond simple explanations of behaviours and preferences in order to capture a wider range of psychological and social influencers of individuals' behavioural outcomes. Carrasco and Lucas [30] further argue that qualitative methods are particularly useful for several results; exploring previously unknown areas, causal effects of individuals' behaviours and complex aspects of the individual's decision making processes [30]. The post positivistic approach considers both quantitative and qualitative methods of data collection as valid approaches. Draper [33] and Fade [34] discuss in detail the complementary role of qualitative data in researching human behaviours, feelings and attitudes. To lay the foundation of the extent of the vulnerability that the end user presents, the theoretical section of the paper provides a concise overview of social engineering, behaviour economics and password behaviour. The data collection method is via focus groups as focus groups are more conducive to data collection where the objective is to capture attitude formation and decision making. Conducive to exploratory research topics it allows data collection from the group interaction while simultaneously increasing the sample size when compared to individual interviews [35] and [36]. Rabiee [37] argues that focus groups have the added advantage over interviews that they can be used to highlight different perspectives, both between participants within an individual group and between each of the focus groups. In line with Green et al. [38] stating that the added advantages of holding focus groups is the generation of data based not only on what is said, that is the dialogue and actual utterances between participants, but also the interaction between group members [38].

The method relies on researcher focus to produce concentrated amounts of data on precisely the topic of interest. As well as the group's interaction, the groups' discussions provide direct evidence about similarities

and differences in the participants' opinions and experiences as opposed to reaching such conclusions post analysis of separate individual interviews. The trade-off being that focus groups provide less depth and detail about the opinions and experiences of the individual participants from individual interviews where communication is closer between the interviewer and the individual respondent [39]. In addition, verification of the usefulness of this method lies in how active and easily respondents are willing to discuss the topic of interest [36]. In the case of this study cyber security and most specifically password behaviour.

Limitations

Academic literature pays considerable attention to the influence that awareness raising has on individuals' attitudes and consequently behaviour [21-23] cited in [30]. Whilst the author does not deny these causal affects, the probable likelihood of the effects of GDPR awareness-raising following the implementation from 25th May 2018 does not form a primary role in this study, as the specific intention of the study is to capture current attitudes and behaviours towards cyber security rather than to measure any change in attitude.

Theoretical review informing the study

Effort and memory in Pa55w0rd creation and use

Historically, security plays a secondary role in system development and has evolved to consist of three layers, Authentication, Authorisation and Encryption. It is within the first, that passwords play a substantial role as a key controlling access [41]. The definition of passwords is explicit. The word pass meaning right of entry to access "pass", in this case a system including data, by means of using the correct "word" [41]. "Word" in this instance does not necessarily mean a dictionary based, sense making semantic. In fact, a deliberate, focused move away from dictionary-based words is significantly more conducive to the very purpose of passwords, heightened security. The first line of defence against cyber-attacks, passwords as an access authentication method, are not without flaws [42], as results from previous studies demonstrate. Vulnerabilities arising from human limitations [42], including, decision making [43], human memory [44] and socio-cultural contexts [45] create weaknesses in password authentication methods, with academics considering this method to be one of the most likely human error risk factors to impact IT systems. [46]. Thus,

Creating secure passwords

The most common of authentication methods, passwords include the use of alphanumeric based words known only to the users [41] [42]. Organisations and academics alike advise the creation of good passwords by using a reasonably long passwords, using a large character set, specifically special characters simultaneously being easy to remember [44]. A good password according to Yan, et al. [44] should not consist of words found in the dictionary, should not be written down in an easily accessible place and can either be in capital or small type letters, specifically, it is the rich combination of lower and upper case letters, random characters, numbers, special characters to form non-dictionary, non-sense making and lengthy "words" that moves an

individual's password towards a higher level of security [44]. A good/strong/secure password should seem random, be hard to guess, and never written down or stored in plain text.

Yet, a later study found that over half of respondents had only alphabetical characters, one third letters and numbers, with less than 2% including special characters in their passwords [47]. A more specific example of weak and insecure passwords is observed in the 2019 report featuring the most common passwords used in attacks on connected devices, Internet of Things (IoT), as demonstrated in table one below.

Table 1: Top passwords, in order of frequency, used in IoT attacks in 2019.

123456
(BLANK)
system
sh
shell
admin
password
enable
12345

Source: adapted from Symantec (2019) [48].

Table one above clearly demonstrates the weakness of limited memory and the illusion of unlimited choices. This insecure cyber behaviour could be a causal effect of low Consideration of Future Consequences (CFC) [49], a measure of consideration given by individuals to potential future outcomes, low CFC results in an individual acting on immediate needs and concerns and high CFC guides the individual by future consequences [49].

The limitation of the human memory is a recurring theme spanning literature on the threat of human error in password creation. Earlier studies demonstrate the resulting causal effect of human memory limitations being the choice of too short and easy to remember passwords, compromising the very essence for why they exist [50] [41]. The difficulty of remembering an unlimited number of passwords that would be required to access each and every system essential to the daily functioning of modern life, together with the increasing necessity for more complex passwords and the human weakness of limited memory becomes clearly apparent.

Individuals continue to produce insecure passwords including using names of prominent famous people, with a meagre 10% choosing passwords made up of random strings of letters, numbers and symbols [51]. Thus, a

balancing act arises, the creation of strong passwords versus the effort involved in both creating and remembering them with the unlimited possibilities becoming an illusion [52].

Password guidance for employees

A further weakness happens after original password creation, at the point of renewal. Individuals, when forced to renew and change their password, prevented from using a previous password, act rapidly moving through their historical list of passwords yet defaulting to their favourite, easily memorable password [53]. Over three decades of literature highlight that the majority of organisations and website vendors offer users guidance by means of simplified strength meters providing real-time assessment, forcing individuals to reconsider the information they use to create their password. Yan, et al. [44] found that while many users willingly adhere to the advice, they often create weak passwords, e.g. Brian06 for June and Brian07 for July [44] similar to the phenomenon of keyboard walking. Thus, well intentioned security advice and rules within organisational policies, that of systematically, periodically renewing passwords is itself flawed.

Considering password composition rule enforcement, studies dating over a decade back found that these do not necessarily discourage individuals to utilise their personal information; including date of birth and names when creating a new password [54]. As early as 2000, Yan et al.'s experiments demonstrated that for each experiment there was a small number (10%) of individuals within the test groups whom simply ignored the advice given them regarding length of password and whom, through their disregard for instruction, chose more insecure passwords than the rest of their group [44].

The results of Zviran and Haga's [53] study on renewal and memory of passwords demonstrates individuals recall of password was higher for self-selected passwords, than for randomly assigned password, 23%. The number of subjects keeping a written copy of their self-selected password, 14% versus 66% keeping a written copy of the randomly assigned password. For the majority of users, security is a secondary consideration, a means to an end and often considered an obstacle causing users to find shortcuts in order to gain access to the desired system.[29]. Individuals prefer delegating security to their organization; specifically trusted individuals they consider knowledgeable on security [29]. This creates a challenge for Compliance Officers who concentrate on writing and enforcing security procedures with the expected outcome being employee compliance.

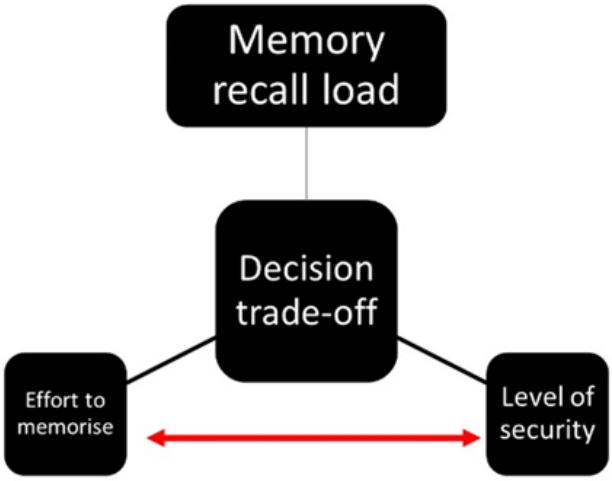
4g0turPa55word?

With secure password creation, there follows a further trade-off with individuals, due to the human limitation of memory, resorting to insecure backup authentication including written records [44]. Likewise, individuals assigned random passwords have a higher degree of difficulty in remembering them, coping by recording

them in writing and having not effectively managed or made the effort to memorise the randomly selected password, utilising the written recording as reference for a longer period [44].

Trade-offs between convenience and security due to text-based passwords necessitate the right combination of human intelligence and senses in order to result in the "best-possible security mechanism" [41]. The trade-of can be linked to Strathman, et al.'s CFC results [49] when considering the perceived consequence, security breach or not, to individuals and the timeframe of said consequence; i.e. short-term, long-term. The perceived immediacy of the consequence is here weighted against the cost of effort based on perceived and subjective measurement of convenience, or lack thereof, when creating a strong and memorable password. Figure one below demonstrates the decision trade-off of password selection, i.e. A password that is effortless to memorise has a lower level of security, an effortful password has a higher level of security yet is more difficult to remember.

Figure 1. Password choice trade-off.



Source: own working based on [55]

Decision making trade-off.

The trade-off of security level versus effortful/effortless memory recall together with Consideration of Future Consequences (CFC) [49] and the compulsion by individuals to continually default towards insecure passwords can be directly linked to Kahneman's [43] two-system notion of psychology of human decision making, lending insight into attitudes and behhaviours of password selection.

Table two below provides a basic diagram of the system one and system two decision-making concept. System one an unconscious and automatic process, necessitated by the limitations of the human mind [43]. Influenced by ignorance of over confidence in own abilities and the world around them, individuals are prone to the danger of overestimating, thus underestimating the role of chance events, such as a cyber-attack [43]. Guided by impressions and feelings, the confidence individuals possess in their intuitive beliefs and

preferences is usually, but not always justified [43]. Utilised in decision making as observed, and documented by previous studies stated, system one guides individuals' password choices, resulting in effortless, low security level passwords.

Table 2: Decision making

System 1 (current state)	**System 2 (desired state)**
Independent of working memory	Limited by working working memory capacity
Autonomous	Deliberate
Fast	Slow
Effortless - independent of cognitive ability	Effortful – dependent on cognitive ability
Automatic	Controlled
Nonconscious	Conscious
Biased responses	Normative responses
Contextualised	Abstract
Associative – experience-based decision making	Rule-based – consequential decision making
Pragmatic	Logical
Simple decisions	Complex decisions
Error prone	Reliable

Source: Adapted from [56].

The deliberate and effortful form of thinking, system two is based on self-relatedness, the process by which individuals encode the strength of stimulus's relation to the self and to environmental contexts. It is the desired state of decision making when choosing password authentication. In system two decision making, individuals modify awareness using cognitive modulation, through self-awareness or self-consciousness by taking an observing, analytical perspective of themselves.

To move from the current state of system one to the desired state of system two, cognitive modulation can be achieved through sense of agency.

In an attempt to combat the problem of effort and memory, studies have explored cued recognition based on daily experiences [57] as effortless aids to memory recall, also the use of graphical icons as a more secure and robust method of memory recall have been exploited [52]. These priming efforts do not sufficiently negate influential effects such as user fatigue and mood. Balzacq [58] lends insight into a way around limitations, suggesting the organisation's ability to identify with individuals "feelings, needs and interests" as essential key factors in a successful security strategy [58]. As with Dhamija and Perrig's [57], Balzacq [58] too suggests focusing on appealing to individuals' own experiences, adding that this be executed by linking fears

and threats to feelings, needs and interests by highlighting the individual's responsibility, liability, and threat as a partner in the fight against cybercrime. One suggestion to protect organisations' network security is by mobilising individuals' experiences, through partnership and by resonating with the individual's lived experiences as suggested by Hansen [59] thereby building on the existing "sensible bridge" between the individual and the password as suggested by Qureshi et al. [41].

Learning via error

Sense of agency is typically defined as the wellbeing of controlling one's actions and their consequences. It involves adjustment and openness, a two-way dynamic implying continual modulation between action and reaction. Di Costa, et al.'s results suggest a relationship between sense of agency and reinforcement learning with negative outcomes triggering adaptive changes in subsequent action selection processing, in turn increasing sense of agency. The study found stronger action binding following a non-rewarded outcome than following a rewarded outcome, suggesting that post-error binding may reflect a specific strategic adaptation to the information value of an action following an error. This adaptation reflects the fact that errors may be highly informative for future action as individuals experience unfavourable outcomes, feeling more control, not less in the next attempt. Thus, error feedback might transiently boost participants' feeling of agency, as action failures more strongly motivate the requirement to act appropriately on subsequent occasions and encourage learning what actions are appropriate [60].

Having established the theoretical background, the following section focuses on future financial sector employees.

Data collection approach

Data collection design

With respect to the number of participants in the sessions, Morgan [39] argues that the size of the group is not important in contradiction, earlier literature [61] and [35] suggests that groups should be small enough that everybody has an opportunity to share his perceptions, and big enough to provide diversity of perceptions. Larger groups bring with them challenges increasing difficulty in managing, as they demand higher moderator involvement for maintaining discipline and inhibiting parallel chats [62].

Population size

Focus group recruitment for this study was targeted at students studying on the finance graduate and undergraduate degree programs, a target group not previously explored by academics in their research on password creation and use, the total possible population size was 142 students across five classes. Allowances were made for illness, rarely attending students, class lists not updated with inactive students, disinterest due

to subject, disinterest due to project week workload etc. The estimation calculation M=(O+3G+P)/5[5] [63] was used to estimate the probable number of individual participants and focus groups. Thus M=(60+3*20+12)/5 calculated as number of students and M=(10+3*5+3)/5 calculated as number of possible focus groups. The calculations result in a rounded off total estimated number of students expected to participate 26 with six focus groups in total. The actual number of focus groups and individual participants exceeded the expected sample size with seven focus groups consisting of a total of 32 participants.

Participant recruitment

Individuals were invited twice at the latter end of the week prior (Danish calendar week 14, 2019) to a project week (Danish calendar week 15, 2019). The invitations were sent via the project week forum, as project weeks are mandatory to attend and actively participate in. Participants were to sign up voluntarily, as such it was anticipated that the likelihood of the participants signing up within their designated study groups was relatively high.

The high probability of group size being around four students was concluded to be a low risk negative effect when reflecting on Freitas, et al.'s [62] positive effects of small groups; i.e. all participants having the opportunity to share their perceptions, ease of managing the group with lower moderator involvement for maintaining discipline and inhibiting parallel chats.

Considerations were made of the probable negative effects of highly homogeneous groups, i.e. hampered diversity of perceptions and the probability of the groups' existing established norms and thus similar opinions and thinking especially as study groups are, for the most part, self-chosen groups, thus prone to be formed on the basis of the sociopsychology phenomenon of homophily (similarity-likeness attraction) [64] and [65]. To counteract the probability of homogeneous perspectives and minimise non-productive discussions, the invitation was designed in line with [62]. Keeping a fine balance by providing participants with enough information to peak interest and desire to participate, yet at the same time, not providing too much information of the topic of research.

In considering the lesser objective approach of post positivism compared to positivism, it is important to point out that the topic in this study, was pre-determined by the research, as such, it is the study's interest that provides the focus, yet it is the groups' interaction, here both individuals within the group and the group as a whole, that provides the data [39].

[5] Where M is the middle value, G, the probable, O, the optimistic and P, the pessimistic estimation.

Data collection

Stage one: Introduction

The first stage of the focus group data collection included introductions and prepping the groups and was conducted orally in Danish. The background to the project together with the purpose of the focus group and the benefits to the students was explained. To counteract language misunderstanding and ambiguity, the participants where then asked if they understood what was expected of them and if they had any questions prior to proceeding to stage two.

Stage two: Implementation

According to Krueger [35] participants may be increasingly affected by social desirability within the group, thus inhibiting their contribution. To counteract this phenomenon, it was explicitly made clear in the introduction to participants that there was no expected consensus with one another's behaviours, nor was it expected that there be a conclusion as to right or wrong answer within the discussions. Furthermore, the researcher/facilitator's role was explained.

Emphasis here was on the primary role as facilitator with the purpose of ensuring firstly that judgement within the group was not made by participants - thus securing all behaviours and opinions - and secondly, promoting as much as possible, equal participation by all participants; whilst simultaneously promoting each participant to share their opinions and behaviours; even where these appeared not to be in consensus with the group. The secondary roles were too explained, i.e., that of observer, note taker and timekeeper.

Freitas et al. [62] note that participants who are known to one another are likely to have difficulty concentrating on the topic of study, regardless of context. Attempts to counteract this phenomenon was made via the focus group design and facilitation of the implementation as follows.

The trade-off between giving control to the group, possibly resulting in focus moving away from the topic and directly controlling the group, possibly resulting in a loss of free-flowing, natural discussion [39].

With the main purpose of balancing the trade-off and simultaneously counteract language misunderstanding and ambiguity, and in considering the negative impact of a rigid method [62], pre formulated questions and statements, as in table three below, were printed on an A4 piece of paper, cut out, folded over, and finally put into a non-distinctive white bowl with the order then mixed up.

Table 3: Focus group data collection questions and statements - ENG

How many passwords do you have?
I change my password(s) regularly

How do you remember your password(s)?
There are some passwords that are stronger than others
Do you use special characters when you create a password?
Have you ever considered not sharing your personal information online?
It is okay to use your work computer for personal use
Does responsibility for password creation lie with the employer or with the employee?
There is no difference between private passwords and work passwords.

Using the pre-printed, mixed questions/statements in random order for each session, was not viewed as an obstruction to obtaining similar content, as it was the content, i.e., the attitudes and opinions that were of the highest importance when using this data collection method. To a certain extent, any patterns or divergences from the themes were seen in themselves to form part of the data for analysis and, where participants deviated largely from the themes, the moderator used the printed questions/statements to bring them back on topic by merely bringing their attention back to the questions/statements that had been drawn. Utilising the same approach for all focus groups served the purpose of minimising any perceived bias in results caused by differing approaches, including the facilitator unconsciously affecting results through voice changes in asking questions or reading statements. As such the facilitator role and thus effect was kept to a minimal during the focus group implementation.

A secondary purpose of this method was to eliminate any bias in over structuring and over formalizing the implementation to create a fun and relaxed environment conducive to encouraging natural participation. Furthermore, the method was designed to ensure discussions were organized so that each focus group received the same questions and statements with the primary aim of counteracting any structural bias.

Elimination of the probability of occurrence of a 'leader' picking and reading out a question/statement was established by implicitly encouraging the group to share the task of picking out a statement/question in turn. Yet another aim of the design was for the purpose of analysis and comparison among the groups.

In addition, the design was to:

- Ensure all participants developed their own order, if any, within the group.
- Promote participation to provide as specific as possible, in-depth data by encouraging iterative reviewing of and reflection on the statement/question drawn during the discussion.
- Promote interaction by giving equal opportunity to answer.
- Ensure all participants remained focused on the data collection and cover the maximum number of relevant topics.

Stage three: Closing

At the end of drawing the last question/statement from the bowl, participants were given time to continue with discussions. As the discussions came to a natural end with longer and more regular pauses, the respondents were asked whether they had any additional comments or final statements they would like to add based on the questions/statements they had drawn during the session.

The focus group session closed with a reconfirmation of the data usage, including confidentiality and anonymity.

Participants were then asked and informed of the following information to be recorded for the purposes of analysis:

- Name and class ID, for further notification/contact, recommendation letter and participant prize draw.
- Year of birth, to establish validity, by confirming participants belong to Generation Z, the focus target group of the study.
- Gender, for analysis reliability purposes, based on decision making and risk-taking differences in gender.

Finally, participants were thanked for their time and left in high spirits.

Analysis of data collection method

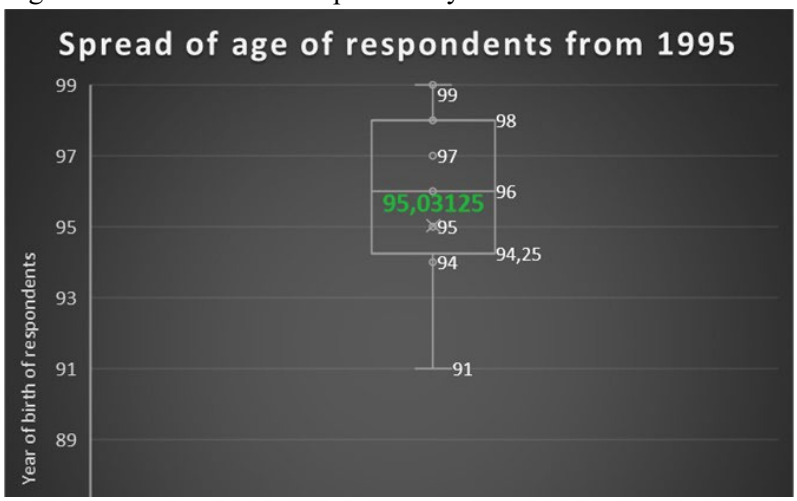
Validity of age

Figure two and three below provide the qualitative data caputred for the purpose of defending the reliability of the qualitative data on attitudes and behaviour as being captured from Generation Z.

Generation Z is defined as being born in the mid 1990's. If taken as an exact figure, this would be all those born in 1995. However, there will always exist a degree of subjectivity as to what charaterizes mid 1990's. For this purpose, respondents participating in the focus groups were purposefully not sought as those specifically born in 1995 rather, all volunteering respondents were included in the focus groups, after which an analysis of the deviation from the year 1995 was conducted by means of a box plot, the result of which is demonstrated in figure three below.

Figure two below demonstrates clearly that the median birth year of respondents is 1996 with the mode being 95,03125. The data is bunched together demonstrating a lower variety between the birth years of respondents. When calculating the inner quartile range of the upper and lower quartiles, no outliners are present as demonstrated by the calculations.

Figure 2. Distribution of respondents year of birth.



Source: own working

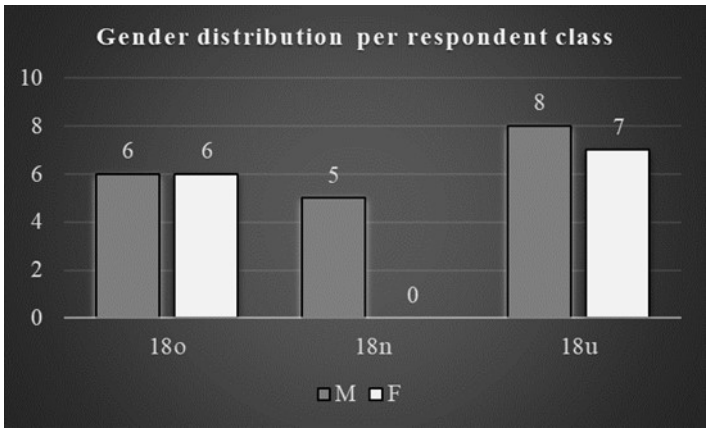
In analysing the validity of participants in the focus groups as belonging to Generation Z, the box plot method was used. The year of birth of respondents at the lower quartile is 1984. The lower quartile median being 87 and the interquartile range calculated at 10. The lower quartile date of birth, at 1984, is at a further distance that the calculated outlier number of 1972, than from the overall data set median of 1995,03.

The year of birth of respondents at the upper quartile is 1999. The upper quartile median being 1997 and the interquartile range calculated at 15. The upper quartile date of birth, at 1999, is at a further distance from the calculated outlier number of 2012, than from the overall data set median of 1995,03

Validity of gender

There exists a wealth of literature on the differences between males and females in, amongst others, both risk taking and decision making [66] [67]. Thus, an analysis of gender distribution of the respondents participating in the focus groups is provided. Figure three below demonstrates the results of the analysis.

Figure 3. Gender distribution per respondent per class.



Source: own working

The gender distribution for one Financial Management class, namely 18o, is exactly equal at six female and six male respondents whereas for the second Financial Management class, 18n, the distribution of male versus female respondents is greatly distorted as all five respondents participating were male with no female respondents participating. Gender distribution of respondents studying on the Bachelor of Finance program, 18u, demonstrates a more even distribution. When considering the total gender distribution, a ratio 19:13 males to females, the two extremes are equidistant to the median of 16 out of the total 32 respondents and closely bunched together indicating less variety and as such a higher reliability.

Data collection analysis design

According to Robson [68] the aim of data analysis is to reduce the data. Yin [69] suggests a number of stages including; examining, categorising and combining, or recombining, the data focusing on the overall aim of the study. Krueger and Casey [70] further emphasis that the aim of the study must drive the analysis [70]. It is these suggested strategies that form the backbone of the analysis design of the focus group interviews.

The use of qualitative data analysis, to bring meaning to situations, presents an obvious challenge of the interchange between researcher and the data, i.e. the risk of bias through subjective selection and interpretation of the data generated by each group and between each group [71]. Guba and Lincoln [72] propose a pragmatic solution to minimise the risk of potential bias iterated by Krueger and Casey's [70] suggestion to carry out a systematic analysis in a sequential manner, a method that Guba and Lincoln [72] argued will increase the extent of dependability, consistency and conformability of the data and in doing so provide a path of evidence; of great importance for ensuring quality [73].

There exists several approaches to systematic qualitative data analysis and most academics make use of a combination of approaches of which Krueger's [35] framework carries an advantage due to the clear series of steps it provides for managing the complexity of the data. This is particularly important with data collection where the interaction between participants constitutes and generates an important amount of valuable data. The framework approach is a process of analysis involving interconnected stages [74] and as such conducive to focus group analysis. The approach is thematic, i.e., themes are allowed to develop from both the research questions and the participant responses. Raibee [37] provides an overview of the stages depicted in four parts as demonstrated in table four below.

Table 4. Framework approach to thematization.

1	Facilitation of the discussion during the data collection	• Generation of rich data from the interview. • Observational notes. • Reviewing the recorded information.

2	Familiarisation with the data	• Reading the observational notes. • Summarising the notes. • Watching and listening to the video recordings.
3	Emerging patterns	• Sifting data by highlighting and sorting quotes. • Category development. • Making comparisons (within and across focus groups).
4	Conceptualising	• Combining and re-arranging quotes from their original. context under appropriate thematic content.

Source: Own working created from Rabiee (2004) [37].

Stage one: Facilitation of the discussion during the data collection

Having established the framework for focus group data analysis. Stage one, as suggested by Ritchie and Spencer [74], and Rabiee [37] was carried out during the focus group interviews by way of facilitating the discussions, ensuring that all participants participated, and all questions and statements were considered. Additional time was given at the end of each focus group to encourage dialogue and thus furthermore generate rich data. Facilitator notes were made using a pre-printed A4 page of the questions and statements. These were used as a backup to log the order of the questions, the time taken for answering each question and the answers to the questions and statements themselves. At the end of each focus group the recorded information, both facilitator notes and audio and visual recordings, was reviewed.

Stage two: Familiarisation with the data

The thematical framework approach of analysis involving interconnected stages as suggested by Ritchie & Spencer [74] was further utilised for the focus group analysis. The analysis here consisted of a cumulation of the second and third stage of the framework approach. As observational notes were used to summarise the data. The process of sifting and categorising the data, making comparisons within the individual focus groups was carried out simultaneously.

Stage three: Emerging patterns

The third stage, emerging patterns, is primarily concerned with sifting and sorting data with the aim of reducing the data, the very aim of data analysis according to Robson [68]. For this purpose, Rabiee [37] recommends Krueger's [35] seven headings for interpreting focus group data over Krueger and Casey's five [70] headings, whilst simultaneously adding an eighth by separating extensiveness from frequency. The data collection and design of this study is based on these eight headings as demonstrated in table five below.

Table 5. Headings used to interpret and analyse focus group data.

Krueger (2000)	**Rabiee (2005)**	**Krueger & Casey (2015)**	**Gabrielsen data collection and analysis design**
Words	Words		**Words** *Achieved during data collection, captured during data analysis stage 1.*
Context	Context		**Context** *Achieved through the questions and statements designed during the pre-data analysis design as part of the methodological approach design.*
Internal Consistency	Internal Consistency		**Internal Consistency** *Captured during data analysis stage 3 and 4.*
Frequency and extensiveness	Frequency	Frequency	**Frequency** *Captured through numeration during data analysis stage 4.*
Intensity of comments	Intensity of comments	Motion	**Intensity of comments** *Covered by "Words" and "Specificity of responses".*
Specificity of responses	Specificity of responses	Specificity of responses	**Specificity of responses** *Captured during stage 1 and covered by "Words".*
	Extensiveness	Extensiveness	***Extensiveness*** *Captured through numeration during data analysis stage 4.*
Big ideas	Big picture	Big picture	**Big picture** *Covered by "Words", "Specificity of responses", Internal Consistency" and "Extensiveness" during analysis stage 1, 2, 3 and 4, and illustrated in figure 4.*

Source: Adapted form Krueger, Rabiee, and Krueger & Casey [35], [37] and [70].

The approach to the final analysis design was carried out by means of creating a colour coded key of themes, utilised to sift and categorise by highlighting in colour the emerging themes matching to the key, to make comparisons within and across the focus groups. The key pattern code was developed throughout the analysis process, refer to supplementary data one in appendix one.

Stage four: Conceptualisation

Having utilised the third stage of focus group analysis suggested by Robson [68], the analysis of facilitators notes proceeded to employ the last of the suggested headings for interpreting focus group data, thus focusing primarily on the consensual "Big ideas, Big Picture" as suggested by Krueger [35], Krueger & Casey [70], Rabiee [37] and included in the adapted recommended headings by the researcher as per table five above.

Words

According to Smithson [75], opinions of the group should not be viewed as individual, previously formed, and static, but rather as constructs within the social situation. Thus, the focus of analysis here was on the discourses constructed within the context rather than on the mere explicit utterances of participants. The advantage is that discussions within the groups highlight current debates, contradictions, and tensions prevalent within public discourse. Thus, as participants discuss the term "passwords", any relationship between their attitudes and actual behaviour was observed directly with their understanding.

Internal consistency

The wording of the questions and subsequent comments made by the other participants influences the context within which the comments are made. Here the wording of the questions/statements was formed prior using slips of paper to be selected from the bowl. With no single participant taking charge of selecting from the bowl and reading the question allowed to the others.

Frequency, four. Specificity of response, and five. Big picture

Frequency, specificity of response and big picture were sorted and analysed simultaneously, see supplementary data one and two.

Results

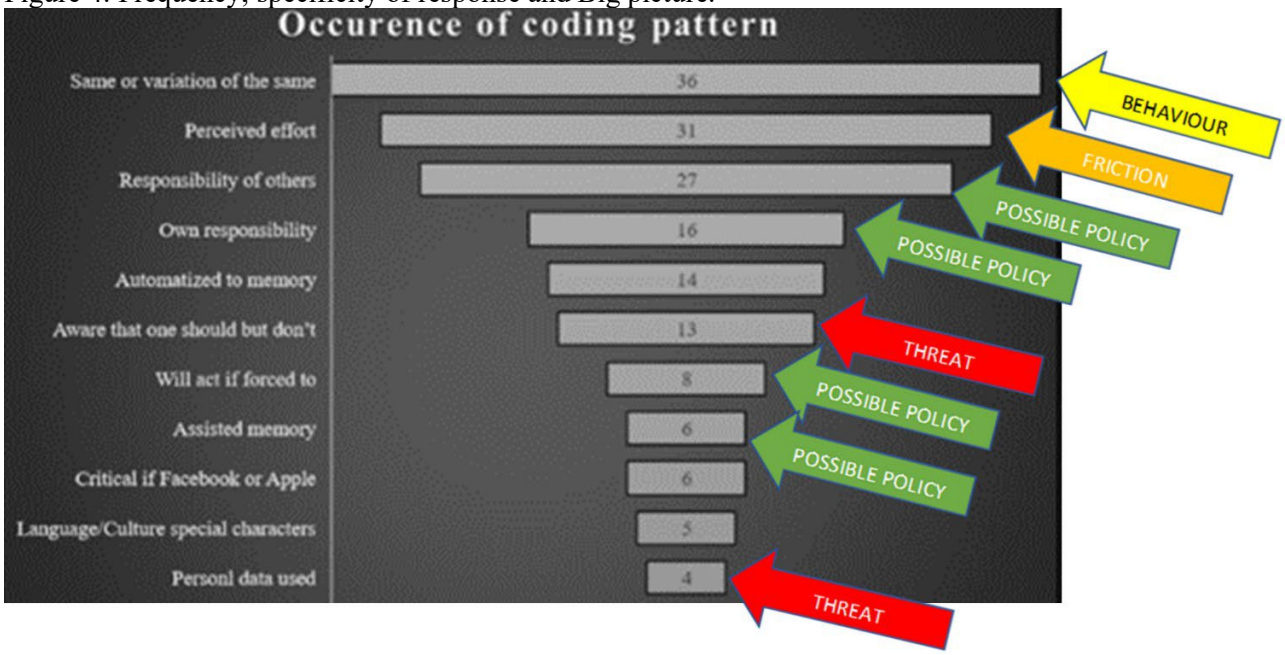
The following section presents the results of the analysis of the data collected during the focus groups. The analysis is based specifically on the framework approach to thematization as suggested by Krueger [35], Rabiee [37] and Krueger and Casey [70]. The presentation of results is divided into two parts, both of which focus specifically on stage three.

The second part of the presentation of results focuses specifically on making comparisons of words, context, internal consistency, frequency, intensity of comments and specificity of response in order to gain the bigger picture across the focus groups. The results here are presented in a qualitative discourse and form the main part of the analysis.

Part one: (See supplementary data one)

The first part focuses on and includes the sifting of data, highlighting and sorting quotes. The results are presented in a quantitative visual manner, this provides a quick overview of the results as demonstrated in figure four below.

Figure 4. Frequency, specificity of response and Big picture.



Source: own working

Part two[6]: (See supplementary data two)

Across the seven focus groups, the average number of passwords that future employees of the financial sector hold are 5,57 passwords. The limited number of passwords is the first indication that attitudes towards Cybersecurity and specifically password creation and use are insecure.

Closer analysis of specificity of response to the question "how many passwords do you have?" indicates that attitudes towards Cybersecurity and specifically password creation and use is highly insecure. This is apparent in statements "one private, same in seven years"(fg2), "two to three variations of the same"(fg2), "I have 15-10 codes in my head that are a variation"(fg3), "four change between. I don't even have one on my mobile phone"(fg3), "many of them I use a handful of times"(fg3), "I have many, but three that I use the most"(fg4), "I have a mass but, four that I primarily use"(fg4), "I have one"(fg4), "one uses classically ones surname"(fg6), "it is the same we use everywhere"(fg6), "those I have created myself are similar to each other"(fg6), "four to five that I change"(fg7), "I have never been hacked"(fg7). This last statement is an indication of perceived necessity. This could indicate that if companies within the financial sector create a strong enough perception of necessity that this could stimulate a change of attitude that could result in changed behaviour.

[6] For analysis and discussion purposes focus groups have been numbered in chronological order of occurrence and referred to as follows; focus group one is (fg1), focus group two is (fg2) and so forth.

In response to a fellow participant's answer to the question on number of passwords "eight to ten change a little"(fg1) a second participant states "crazy that you can remember that"(fg1) demonstrating effort of memory. Together with a third response "sometimes I forget it when there are three guesses"(fg1).

The statement 'I change my password(s) often', demonstrated a similar tendency of unsecure attitude and behaviour. With a close to unanimous agreement on the frequency of changing passwords ranging from not at all by the majority of participants, to a single respondent across the seven focus groups stating that they change their password every three months, though this is limited to a single account, being their email. Surprisingly, on sifting the data and sorting the quotes intensity of comments and specificity of response to this statement clearly demonstrate that future financial sector employees are aware that they should but don't. While one specific statement indicates otherwise "it is a f@#!ing good idea"(fg3). The analysis of the specificity of response demonstrates that this is not due to a lack of knowledge but rather, the perceived effort. Seen in statements across the seven focus groups including "No, I should"(fg1), "a lot of work, one has innumerable places"(fg3), "one must remember"(fg5), "it's easier not to"(fg5), "the more you have, the more difficult it is to remember. I don't want to"(fg7).

As with the results of the first question on number of passwords, there is an indication in further statements that it must be perceived as necessary "if I am forced to"(fg2) and "there needs to be a trigger"(fg3). Once again there is evidence of insecure behaviour to changing passwords "six, seven, ten years since (changing password(s)"(fg2), and "I just 'decorate' the existing"(fg7).

75% of future financial sector employees do not use special characters when creating passwords. Reasons given again include the necessity of effort as demonstrated in statements "It's a habit to use letters and numbers"(fg1), "it's not natural"(fg1), "another thing one has to add"(fg1), "it's irritating if I must"(fg7), "it is easier not to"(fg7). It was clear across the participants in focus group three, four and five that perceived effort and difficulties in remembering are reasons for why future financial sector employees, the digital natives, do not use special characters within their passwords.

Interestingly there appears, once again, evidence on necessity being an effective trigger "only if forced to"(fg2), "perhaps people should be forced to"(fg2), "yes if I have to"(fg7), though the word iterated here is 'forced' indicating that pressure needs to be applied as such, an indication that mere communication will not suffice.

In answer to the explicit question on how participants remember their password(s), the majority of participants remember their password via non-secure methods. Of the 32 future employees within the financial sector, only three 3 demonstrated explicitly through their verbal response that they use a secure method to remember their passwords. It is important to note that this is not a cross analysis of context based on the number of passwords that these individuals use.

Table six below indicates the emerging pattern and thus big picture based on words from the sifting of data and highlighting and sorting of quotes. A traffic light colour coding system based on (un)secure behaviour with the colour red indicating least secure and the colour green indicating most secure behaviour has been used for illustration purposes.

Table 6. How future financial employees remember their passwords.

Group 1	Group 2	Group 3	Group 4	Group 5	Group 6	Group 7
Habit	Only 1	Automatised	Unique life experiences	Personal info.	Same for a long time	It means something to them
Fingers	App	By heart	Used to write them down, now creates codes that mean something	Unchanged password	Had them for a long time	Used the same over a long period (10 years)
Patterns in head	Fewer passwords	Memory	Experiences and letters for each family memeber	The same as my family members	Same code from the government (uni-longin)	1 respondent writes them in notes on their iphone
Personal data		Finger memory	From school intra (uni-login)		They are the same	Random letters and numbers that can be memorised after few repetitions (1-2 times)
It must be easy to remember		Can just				

Source: own working based on analysis of data collected from focus groups.

The comments “fingers”(fg1 and 3) and “by heart”(fg3) and “can just”(fg3) are coded in red as the specificity of response and use of words strongly indicate reuse of few or the same password(s).

In order to dig deeper into attitudes and behaviour it was necessary to establish existing knowledge. This was established through the statement “some passwords are stronger than others.” There is an overall agreement by all groups in response to this statement. Specific responses across the groups further demonstrated understanding of some elements that characterise a strong password. Two groups were overall sceptical as to whether a stronger password would in fact increase security. Some mentioned the use of random, unrelated words and special characters demonstrating further knowledge of security. However, not all group discussions demonstrated knowledge of characteristics of secure passwords. Overall, the result from this statement is that future financial employees are aware that there is a difference between weak and strong passwords however, the knowledge of what characterises this is lacking.

In answer to the question on whether respondents ever consider NOT sharing personal information online, Overall, there exist mixed attitudes towards sharing personal information online. Through specific, explicit utterances the indifference of individuals within the groups towards sharing their personal information online

stems from the knowledge that much a wealth of personal information exists online in the first place, "it's available on 'Krak[7]' anyway" (fg4).

The financial sector's future employees, the digital native Generation Z, are aware that their data is available to those who really want to access it; in fact, they accept that having a digital footprint made up of personal information is part of daily life - "it is practically a demand that people can find one" (fg3), "you have to give permission anyway"(fg5).

Specific utterances demonstrate that they are aware of yet critical to the fluid boundaries of security "one looks for the approval (e.g., https) mark"(fg3), "it makes a difference as to whether is trustworthy or not"(fg3). Yet, when effort of not sharing is deemed high, their attitude changes to becoming more complacent, e.g., when being presented with several pages of Terms and Conditions (Ts&Cs), "I consider some things, not everything. Especially when there are numerous pages of Ts&Cs one has to read"(fg5).

Focus group seven though presents an exception to this submissive, accepting attitude towards sharing personal data, specifically stating the reasoning as the introduction of General Data Protection Regulation (GDPR). This group appears to be more concerned with making an effort "almost everything is made private"(fg7), "after GDPR now I opt out"(fg7), "before GDPR I opted into everything"(fg7). Whilst this group as a whole displays more of an effort towards securing their personal data, at the same time, they too demonstrate scepticism and a lack of trust from the results of secure behaviour "It feels more secure using NemID[8]" (fg7) Specifically in the word "feels".

The statement "It is okay to use a work computer for personal use" was used to establish whether future financial sector employees would exercise more caution specifically within the context of the financial sector. This was to move the focus away from general to more specific contextual behaviour.
The question of using company hardware for private use, thereby inexplicably and unconsciously exposing the company to higher probability of exposure to malicious adversaries gains an almost equal mix of responses from the seven focus groups. Three groups explicitly state that it is not acceptable to use company hardware for personal use, two groups explicitly state that this is acceptable, and 2 groups are not in consensus within the group participants. However, on analysing the specificity of response, the groups that explicitly state that this is an unacceptable scenario (group two, three and seven) demonstrate behaviour to the contrary. Statements include: "Depends on what you want to use it for, banking"(fg2), this statement indicates that this participant would self-select sites that they consider acceptable to access using a computer provided by their

[7] Established in 1996, and taken over by Eniro Danmark, the digital online version of Krak.dk is a database of over 750,000 Danish company and individual contact details including names, address, and telephone numbers, similar to the well-known Yellow Pages. The database is built upon an opt-in/opt-out basis.
[8] NemID: Stands for easy identification, this is a 2factor code system issued by the state and directly connected to Danish citizens' social security number.

employer. "it depends on how your security system at home is"(fg2) This statement indicates that this participant may well use a computer provided by their employer if they considered their security system to be secure enough, this allows for multiple interpretation as to what this participant would base the level of security on. "it depends on the amount of confidential data there is"(fg2) All three participants in group two make specific use of the word 'depend' therefore explicitly contradicting their statement that it is not acceptable to use work issued computer for personal use.

When analysing group three's responses more closely, a similar pattern of contradiction emerges, however not quite as explicit. One participant in group three states "personal emails"(fg3). Like with group two, this suggests a wavering grey area of conscious consideration and judgement as to the circumstance the individual considers acceptable or not. Another participant in this group states "I believe there are many who use company (computers) for private (use)"(fg3) implying that this is acceptable.

A final statement from this group indicating contradiction is "Workplace can protect so much. They can easily set something (security) up" (fg3), this puts specific onus on the company to monitor and guarantee the security of their systems.

Group four appears to be the most complacent. When analysing the specificity of response in this group, one considers it to be "fair" (fg4) implying an expectance. While another responds incredulously "Why should one not use a work computer for personal use?"(fg4). Group five once again demonstrates a wavering consensus with some critical consideration "depending"(fg5) on what is being accessed, this holds well with the emphasis that group 3 holds regarding the circumstances or situation based upon the specificity of response, and in particular the word "depend(ing)(s)" Yet at the same time in self-monitoring and decision making the critical considerations weaken as one participant considers Facebook a no go yet e-commerce acceptable. Another participant indicates that it is the company's responsibility "it depends on the company's surveillance"(fg5), although it is not sure from this statement whether this participant is considering security or getting caught! Two participants consider self-discipline to be an influential and important consideration.

A specific response from group six mirrors the incredulance of the one response from group 4 "why should one not use a work computer for personal use?"(fg4), The response from group 6 is "One should be allowed to, we are people"(fg6) indicating that this is expected, much the same as the word "fair"(fg4) indicates. Participants from focus group 6 iterate the onus on the company that is observed in participant response is group 3 through the following statements "They can ask about everything and one must be prepared for that"(fg6) and "They can lock it if they want"(fg6).

Group seven contradicts the no consensus with the statements "as a starting point, no"(fg7) indicating that there is flexibility. The statement "it depends on what you will use it for"(fg7) reiterates the focus on the word "depend(ing)(s)" observed in focus groups three and five.

To establish attitudes towards responsibility the question of whether responsibility lies with the employer or employee was asked. Across the groups the majority consider responsibility for password creation to be shared. This attitude is heavily weighted towards the main responsibility leaning towards the employees, as observed in group four, five and six. Several specific statements demonstrate that future financial sector employees expect guidelines from their employers both for creating and for remembering their passwords. Key themes observed in the responses to this question include the employer's responsibility for creating guidelines, "The employer is responsible for reminding employees to change their password"(fg1), "The employer should create them, but the employee must remember it"(fg1), "Employer - how and when"(fg2), "Signed for with hardware etc. Policy"(fg2), "The majority, small and large, have guidelines if employees can generate them(fg3), "Employer issued and thereafter hands-off"(fg3), "You can be in a situation where the boss does it (creates password), so it is primarily employers"(fg4), "They say that they reset it. Company can make demands, number of letters, numbers etc"(fg6), "Employer can make demands, that are easier to remember"(fg6), "They set the demands"(fg7), "Employers have responsibility for demands and security"(fg7).

There is an iteration of concern about memory, "The employer should create them, but the employee must remember it"(fg1), "If one must remember it, if one forgets it"(fg6) however, this is not a pronounced theme. In conclusion, the observation across focus groups suggests that acceptance and even expectation that employers, at a minimum, set guidelines for creating passwords and at a maximum issue passwords. Interestingly, one participant states that once the password is issued, the employee takes over full responsibility "Employer issued and thereafter 'hands-off'"(fg3) this statement together with "it is not necessary for the employer to know your password as they can take over the screen"(f4), "primarily with the employee"(fg6) and "whether it is the company themself, it is you that has responsibility for it"(fg7) suggests a sense of ownership and responsibility weighted towards the individual employee.

When analysing the less specific responses there is evidence of contradiction of responsibility weighted towards the individual employee, observed in the following statements "Higher risk if they give responsibility to employees" (fg3) and "The employer can safeguard themselves. They must also safeguard themselves from the human part of it. They carry the most responsibility" (fg3), "Employer-who is the bigger looser"(fg2). Thus, it is clear that future employees of the financial sector have differing opinions as to who is responsible for creating passwords within the workplace.

Most participants across the seven focus groups consider there to be a difference between private passwords and passwords used in the workplace. As with the question on who's responsibility it is, group one iterates that there should be "rules"(regler) with the employer setting a password that employees can change. A concern exists within group 1, in the statements "own creation, it must happen faster"(fg1) and "It should be memorable"(fg1), together with "not too complicated"(fg1) this indicates a higher risk attitude based on convenience and ease of memory. Add the statements "Private is more important than work"(fg3) and "when it is works, then one is a bit looser with it"(fg3), "what do I have that others could be interested in?"(fg6) and "... there are many safety nets"(fg6) and the higher risk attitude increases. In analysing specificity of response and words, the statement "you are forced to"(fg2) indicates an attitude of disdain by using the word "forced". In conclusion, the analysis of specificity of response and words, demonstrates knowledge of the initial, explicit attitude, and brings to light some worrying facts of attitude towards passwords for use in the workplace.

Discussion

The average number of passwords that future employees of the financial sector hold are 5,57 passwords. The limited number of passwords together with responses to the number of passwords held indicates highly insecure behaviour.

Not all future financial employees are aware of characteristics of secure passwords. Furthermore, three quarters of respondents do not use special characters when creating passwords stating that doing so necessitates a shift from habit. The main reasoning, perceived effort and memory limitations can be linked directly to Qureshi, et al.'s [41] studies on memory load, decision trade-off.
Future financial sector employees are aware that they should but do not change their passwords regularly, if at all. This result confirms the studies by [22], [21] and [15] with a close to unanimous agreement on the frequency of changing passwords as not at all by the majority of participants stating blatantly that they should, but do not want to as it is easier not to.

The memory load decision trade-off of effort and easy of memory versus secure password use and creation is confirmed by participants' intensity of comments and specificity of response [49], [44], [41] and [29] across all seven focus groups as demonstrated in table five.

Future financial sector employees display a low Consideration of Future Consequences (CFC) [49]. The Financial sector must emphasise the importance and urgency of applied effort in creating and renewing passwords, as many have not themselves experienced a cyber threat. This can be done via specific examples of actual cyber breaches and the consequential effects, preferably by a trusted individual knowledgeable in security as suggested by [29].

Results of the focus groups suggest that the low CFC is due to future financial employees' knowledge of ease of access to the wealth of their personal information that exists online. This adds to the challenge of changing the behaviour and attitudes to being more secure as they perceive high effort for low return creating a complacent attitude towards secure password creation and use.

There is a significant difference in attitude of necessity between respondents connected to individuals who have experienced a cyber breach and respondents who have no experience of a cyber breach either personally or within their groups. Together with the explicit responses that if they are forced to then they would and that there "needs" to be a trigger. This could indicate that if companies within the financial sector create a strong enough perception of necessity that this could tap into system one decision making and specifically the theory of expert intuition, thus stimulate a change of attitude by means of a personal cue (expert intuition) that could result in changed behaviour, moving heuristic intuition based upon Consideration of Future Consequence towards system two. Companies could further stimulate the change of attitude by exploiting the underlying system two theory of availability heuristic by increasing relative importance through producing regular and easily visible "media" coverage internally within the company in order to encourage ease of retrieval of sense of urgency from memory. This proposed policy could also be implemented to stimulate change based on the unsecure attitude and behaviour towards password renewal.
The financial sector must create clear guidelines as to whether company hardware can be used for private use or not, and to what extent as multiple interpretations and levels of acceptance are evident. A great consideration for companies here is the contradiction of explicit response versus further utterances and explanations by individual respondents, indicating that action differs from intention, emphasizing the necessity for companies to monitor and guarantee the security of their systems.

Future financial employees expect guidelines for creating and remembering passwords, however, there is clear evidence that even with specific policies in place, a small yet significant percentage of individuals will ignore these [44]. Financial companies must consider and include the management of failure to adhere proactively here as non-compliance can lead to severe consequences of data access by malicious adversaries.
An important consideration for financial sector companies here is the evidence of acceptance of shared responsibility by some but not all. This creates a double sword dilemma for ensuring compliance, in that some financial sector employees would expect companies to take a more authoritative, dictatorship role which could in turn motivate compliance, whilst demotivating those future employees who expect a partnership role when it comes to creating and using secure passwords.

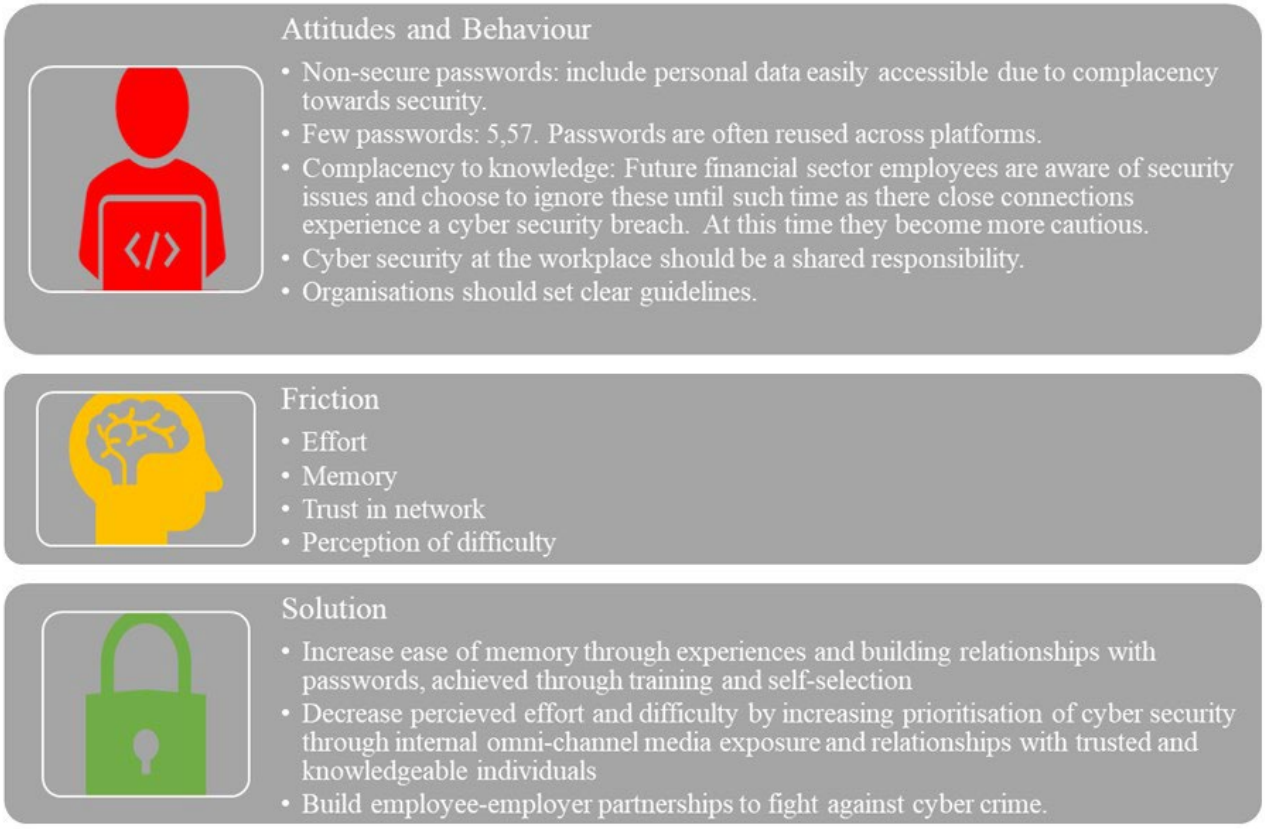
To sum up, future financial sector employees indicate a higher risk attitude based on convenience and ease of memory.

Conclusion

The aim of the research was to explore attitudes and behaviours of Danish future financial sector employees to understand and discover whether their human behaviour is a vulnerability and a weak link exposing this most sensitive sector of society to cyber-attack. The approach was to scan theoretical literature on behaviour, password creation and use by the future workforce, the digital natives also known as Generation Z. Specific, current attitudes and behaviours of Danish future financial sector employees were then explored, resulting in an ensuing discussion coupling the theoretical findings to the current empirical findings.

Figure five below provides an overview of the findings based on a simplified process of behavioural design; namely understanding Behaviour, discovering the Friction, designing the Solution. Where behaviour is observed, the friction causing the behaviour is then sought and from the friction possible solutions are proposed, the focus of which is to modify the original behaviour to a more desired state.

Figure 5. overview of findings.

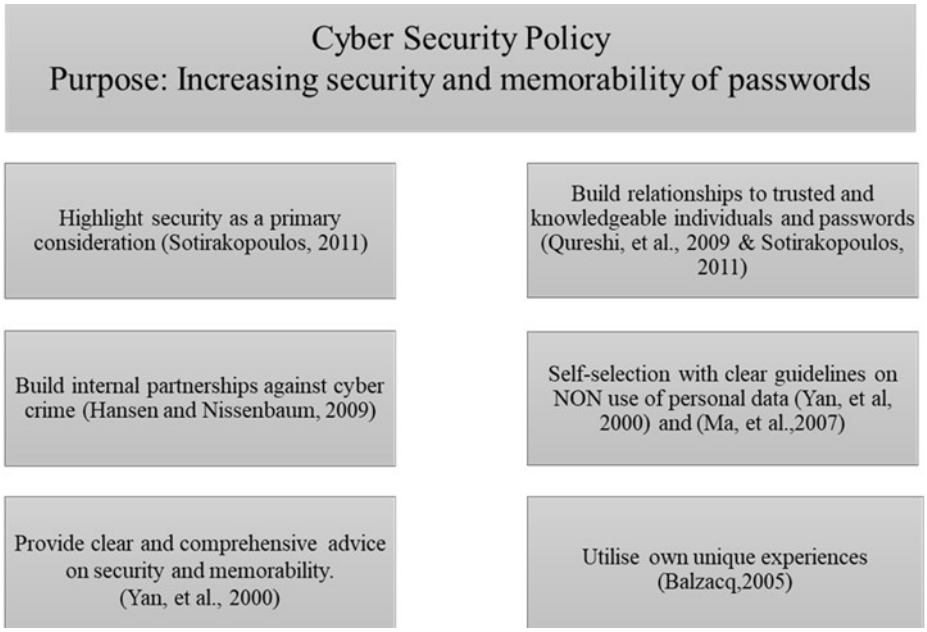


Source: own working

Focusing on the theoretical framework and the empirical findings, the following section is a suggestion of corporate policy for organisations in the financial sector that can be included under IT security policies as a sub policy, and which should form an integral part of compliance and data protection. The policy covers both

the creation and renewal of secure passwords and should be adhered to by all financial sector employees, regardless of rank or longevity of service. A summary of key areas from the theoretical framework for the purpose of policy creation is illustrated in figure six below.

Figure 6. Theoretical framework informing Cyber Security Policy



Source: own working

Policy for business

The results of both the theoretical framework informing the study and the empirical findings can be drawn upon to create a password policy for business as outlined below.

The findings demand a shift from system one to system two decision making and an increase in concentration and effort of mental activity when creating passwords. Essential when considering necessity for self-selected passwords as evident from research demonstrating increased memorability and security over assigned passwords [53]. Allowing self-selected passwords, business tap into sense of agency as individuals experience a greater feeling of controlling their actions by being the initiator and source of action, increasing the feeling of control over actions and subsequent effects in the outside world [76]. However, caution is needed, and practitioners must bear in mind that password composition rules enforced on individuals do not necessarily discourage the use of personal data [54]. Reiterating the necessity of shift from system one to system two decision making.

Shifting behaviour from system one to system two can be achieved for example, by drawing on expert intuition to counteract the memory load effort trade-off between ease and security. To discourage use of

personal data in password creation, employees must be encouraged to build passwords based on memories and past experiences [59]. This will give the added benefit to employees of the feeling and sense of intentionally acting on the experience, a sense of agency, and thus the feeling of being the initiator of the action.
Business must set Cybersecurity as a top priority not to be perceived as an effortful obstacle [29]. By building internal partnerships against cybercrime [59]. Provide continual training setting clear and comprehensive, simplified guidelines [44], [23], [24] using influencers within the organisation. It is essential here that influencers are trusted individuals knowledgeable on security [41], [29]. Regular training including password creation simulations that increase exposure to error, highly informative for future action [60], drawing on sense of agency by encouraging openness and adjustment that will increase perception immediacy of consequence and increase consideration of future consequences (CFC) [49].
Alleviate memory overload of multiple necessary passwords, drawing on availability heuristic, by continual reiteration through increased exposure via internal omni-channel media and training, focusing on sense of agency by inspiring interactions with surroundings to increase the perceived relative importance of secure password creation through the causal-effect of easing retrieval from memory.
Finally, business must be on the side of caution in setting specific and serious consequences, within the current legal framework, to deal with the expected 10% non-compliance to using personal data [44] and [54].

Areas for further study

This study explores a specific segment, digital natives known as generation Z, within a specific sector, the most highly threatened financial sector. The background of the study and the existing literature explored highlight cybersecurity breaches as a societal challenge. It is therefore suggested that the approach to this study be carried out on several segments of society as well as other sectors. In so doing, the suggested policy for business can be tested and, where necessary adjusted and targeted accordingly.

Acknowledgements

The author would like to thank the participating university and especially the participating students for contributing to data collection. A special thanks to Ingo Winkler and Jens Demandt Mourtisen for their help with reviewing the paper, Signe Krause Vilstrup and Connie Kjærgaard for their assistance with referencing and Inga Beckmann for her assistance in preparing the paper for journal submission.

1. Howarth F. The Role of Human Error in Successful Security Attacks. *Security Intelligence* 2014.

2. Deloitte. *The Future Market for Cybersecurity in Denmark.* Innovation Fund Denmark, 2018:4–38.

3. Hadnagy C. *Social Engineering: The Art of Human Hacking*. Indianapolis, IN: Wiley, 2011.

4. IBM Security. *Cost of a Data Breach Report*. IBM Security, 2019:76.

5. Center for Cybersikkerhed. *Trusselsvurdering. Cybertruslen Mod Danmark*., 2019.

6. Turban E, King D, Lee JK *et al. Electronic Commerce: A Managerial and Social Networks Perspective*. 8th ed. New York, NY: Springer International Publishing, 2015.

7. National Research Council (U.S.) ed. *Computers at Risk: Safe Computing in the Information Age*. Washington, D.C: National Academy Press, 1991.

8. Mitnick KD, Simon WL. *The Art of Deception: Controlling the Human Element of Security*. Indianapolis, Ind: Wiley, 2002.

9. Hansen D, Forsvarsakademiet, Dansk Brand- og Sikringsteknisk Institut. *Save: Social Vulnerability & Assessement Framework : A Study in Social Engineering 2.0*. Kbh.: Forsvarsakademiet, 2017.

10. Pieters W, Hadžiosmanović D, Dechesne F. Security-by-Experiment: Lessons from Responsible Deployment in Cyberspace. *Sci Eng Ethics* 2016;**22**:831–50.

11. The Economist. Regulating the internet giants - The world's most valuable resource is no longer oil, but data. *The Economist* 2017;**2017**.

12. National Rsearch Council. *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*. Washington, D.C.: National Academies Press, 2002:10274.

13. Danmarks statistik. *It-anvendelse i befolkningen 2019*. København: Danmarks statistik, 2020.

14. Finanstilsynet/Financial Services Authority. Note Systematic risk- research questionaire survey (Systemisk risiko - spørgeskemaundersøgelse). *innovationsfonden.dk* 2020.

15. Bladt S, Gabrielsen LC. The potential of P2P lending on the Danish market. 2016.

16. Council of the European Unio. Council of the European Union. 9565/15, 11 June 2015. 2015.

17. Danmarks statistik. Statistikbanken FOLK1A: Folketal den 1. i kvartalet efter område, køn, alder og civilstand. *statistikbanken.dk* 2020.

18. Schultz Hansen S. *Digitale indfødte på job*. København: Gyldendal Business, 2015.

19. Prensky M. Digital Natives, Digital Immigrants. *Horiz* 2001;**9**:6.

20. Turkle S. *Alone Together: Why We Expect More from Technology and Less from Each Other*. New York: Basic Books, 2011.

21. Dourish P, Grinter RE, Delgado de la Flor J *et al.* Security in the wild: user strategies for managing security as an everyday, practical problem. *Pers Ubiquit Comput* 2004;**8**:391–401.

22. Whitten A, Tygar JD. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. Vol 223-26th August 1999. Washington, D.C.: Proceedings of the 8th USENIX Security Symposium, 169–84.

23. Gross JB, Rosson MB. Looking for trouble: understanding end-user security management. *Proceedings of the 2007 Symposium on Computer Human Interaction for the Management of Information Technology*. New York, NY, USA: Association for Computing Machinery, 2007, 10-es.

24. Schneier B. *Secrets and Lies: Digital Security in a Networked World*. Indianapolis: Wiley, 2000.

25. Benhamou L. Everything you need to know about Generation Z. *Business Insider* 2015.

26. Human Resource and Development Consultant for Frøs Sparekasse. 2016.

27. Boyd D. *It's Complicated: The Social Lives of Networked Teens*. New Haven: Yale University Press, 2014.

28. Chia PH, Heiner A, N. A. *The Wisdom of Cliques: Use of Personalized Social Rating for Trustworthy Application Installation*. Nokia Research Center, 2010.

29. Sotirakopoulos A. Influencing user password choice through peer pressure. 2011.

30. Carrasco J-A, Lucas K. Workshop Synthesis: Measuring Attitudes; Quantitative and Qualitative Methods. *Transp Res Proc* 2015;**11**:165–71.

31. Stinger P. The social psychologist's perspective. *Transport and Public Policy Planning*. London: Mansell, 1981.

32. Baron RA, Byrne DE. *Social Psychology*. 10th ed. Boston: Allyn and Bacon, 2002.

33. Draper AK. The principles and application of qualitative research. *Proc Nutr Soc* 2004;**63**:641–6.

34. Fade S. Using interpretative phenomenological analysis for public health nutrition and dietetic research: a practical guide. *Proc Nutr Soc* 2004;**63**:647–53.

35. Krueger RA. *Focus Groups: A Practical Guide for Applied Research*. 3rd ed. Thousand Oaks, CA: Sage Publications, 2000.

36. Morgan DL. *Focus Groups as Qualitative Research*. 1 ed. Beverly Hills: Sage Publications, 1988.

37. Rabiee F. Focus-group interview and data analysis. *Proc Nutr Soc* 2004;**63**:655–60.

38. Green J, Draper A, Dowler E. Short cuts to safety: Risk and "rules of thumb" in accounts of food choice. *Health Risk Soc* 2003;**5**:33–52.

39. Morgan DL. *Focus Groups as Qualitative Research / David L. Morgan*. 2nd ed. Thousand Oaks, Calif: SAGE Publications, 1997.

40. Nordlund AM, Garvill J. Effects of values, problem awareness, and personal norm on willingness to reduce personal car use. *Journal of Environmental Psychology* 2003;**23**:339–47.

41. Qureshi MA, Younus A, Khan AA. Philosophical Survey of Passwords. *IJCSI* 2009;**1**:8–12.

42. Zhang L, McDowell WC, Schultz T. Individual differences on inventions to use strong passwords. *IIS* 2010:6.

43. Kahneman D. *Thinking, Fast and Slow*. 1st pbk. ed. New York: Farrar, Straus and Giroux, 2013.

44. Yan J, Blackwell A, Anderson R *et al.* The memorability and security of passwords -- some empirical results. *University of Cambridge - Computer Laboratory* **2000**:13.

45. Han S, Northoff G. Understanding the self: a cultural neuroscience approach. *Progress in Brain Research*. Vol 178. Elsevier, 2009, 203–12.

46. Carstens DS, McCauley-Bell PR, Malone LC *et al.* Evaluation of the Human Impact of Password Authentication Practices on Information Security. *Inf Sci J* 2004;**2004**:67–85.

47. Cazier JA, Medlin BD. Password Security: An Empirical Investigation into E-Commerce Passwords and Their Crack Times. *JISSec* 2006;**15**:45–55.

48. Symantec. *Internet Security Theat Report*. Mountain View, CA: Symantec Corporation, 2019:61.

49. Strathman A, Gleicher F, Boninger DS *et al.* The consideration of future consequences: Weighing immediate and distant outcomes of behavior. *J Pers Soc Psychol* 1994;**66**:742–52.

50. Adams A, Sasse A. Users Are Not the Enemy. *Commun ACM* 1999;**42**:40–6.

51. Andrews LW. Passwords Reveal Your Personality | Psychology Today. 2016.

52. Weinshall D, Kirkpatrick S. Passwords you'll never forget, but can't recall. 2004.

53. Zviran M, Haga, W.J. A Comparison of Password Techniques for Multilevel Authentication Mechanisms. *The Computer Journal* 1993;**36**:11.

54. Ma W, Campbell J, Tran D *et al.* A Conceptual Framework for Assessing Password Quality. *Int j comput sci netw* 2007;**2007**:179–85.

55. Kahneman D. *Thinking, Fast and Slow*. 1st pbk. ed. New York: Farrar, Straus and Giroux, 2013.

56. Kennedy WG. The Roots of Trust: Cognition Beyond Rationa. *Poceedings of the Second Annual Meeting of the BICA Society*. Vol 2011. Amsterdam: IOS Press, 188–93.

57. Dhamija R, Perrig A. *Déjà Vu: A User Study Using Images for Authentication*. University of California Berkeley, 2000.

58. Balzacq T. The Three Faces of Securitization: Political Agency, Audience and Context. *Eur J Int Relat* 2005;**11**:171–201.

59. Hansen L, Nissenbaum H. Digital Disaster, Cyber Security, and the Copenhagen School. *Int Stud Q* 2009;**53**:1155–75.

60. Di Costa S, Théro H, Chambon V *et al.* Try and try again: Post-error boost of an implicit measure of agency. *Q J Exp Psychol* 2018;**71**:1584–95.

61. Oppenheim AN. *Questionnaire Design, Interviewing, and Attitude Measurement*. New York: St. Martin's Press, 1992.

62. Freitas H, Oliveira M, Jenkins M *et al.* The Focus Group, a qualitative research method.Reviewing The theory, and Providing Guidelines to Its Planning. 1998.

63. Ahrengot N, Olsson JR, Lindegaard MA. *Power i projekter og portefølje*. 4. Kbh.: Djøf, 2019.

64. Wrzus C. Similarity in personal relationships : associations with relationship regulation between and within individuals. 2008.

65. Launay J, Dunbar RIM. Playing with Strangers: Which Shared Traits Attract Us Most to New People? Pavlova MA (ed.). *PLoS ONE* 2015;**10**:1–17.

66. Sanz de Acedo Lizárraga ML, Sanz de Acedo Baquedano MT, Cardelle-Elawar M. Factors that affect decision making: gende rand age differences. *Rev Int Psicol Ter Psicol* 2007;**7**:381–91.

67. Gonzalez R, Berggren J. Gender difference in financial decision making. 2010.

68. Robson C. *Real World Research: A Resource for Social Scientists and Practitioner-Researchers*. 2nd ed. Oxford: Blackwell Publishers, 2002.

69. Yin RK. *Case Study Research: Design and Methods*. 2nd ed. London: Sage Publications, 1989.

70. Krueger RA, Casey MA. *Focus Groups: A Practical Guide for Applied Research*. 5th ed. SAGE Publications, 2015.

71. Corbin JM, Strauss AL, Strauss AL. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. 3rd ed. Los Angeles, Calif: SAGE Publications, 2008.

72. Guba EG, Lincoln YS. *Fourth Generation Evaluation*. Newbury Park, Calif: SAGE Publications, 1989.

73. Secker J, Wimbush E, Watson J *et al.* Qualitative methods in health promotion research: some criteria for quality. *Health Educ J* 1995;**54**:74–87.

74. Ritchie J, Spencer L. Qualitative data analysis for applied policy research. *The Qualitative Researcher's Companion*. Thousand Oaks, CA: SAGE Publications, 2002.

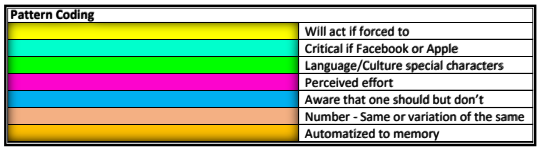
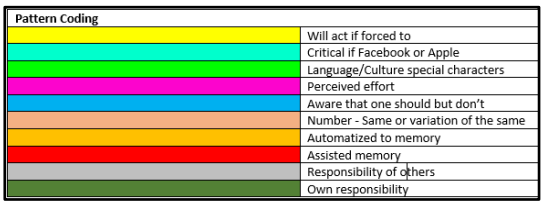
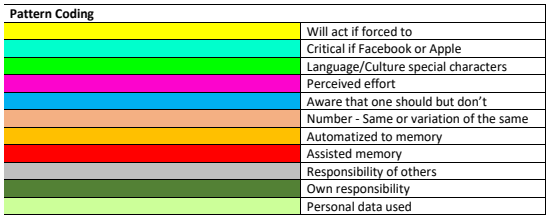
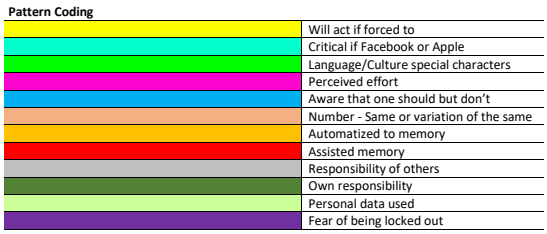
75. Smithson J. Using and analysing focus groups: Limitations and possibilities. *Int J Soc Res Methodol* 2000;**3**:103–19.

76. Haggard P, Chambon V. Sense of agency. *Curr Biol* 2012;**22**:R390–2.

Appendix 1

Supplementary data 1:

The approach to the final analysis design. Stage 3: Emerging patterns and stage 4: Conceptualising, based on (Raibiee, 2004)

Figure 1: Pattern coding. Start day 2  	
Figure 2: Pattern coding. Mid-day 2  	Complete 3rd focus group data analysis with further three additions to pattern coding, resulting in a total of 10 emergent patterns, as demonstrated in figure 2.
Figure 3: Pattern coding. End day 2  	On completing the typing and patern coding of the 4th focus group, a further single addition was made to the patern coding; namely, personal data used, as demonstrated in figure 3.
Figure 4: Patten coding. Start day 3  	With the start of the analysis of focus group 4 on day 3, a final theme emerged. Participants in this focus group referred not only directly to memory of passwords and perceived effort in their discussions on changing passwords but, more interestingly the fear of being locked out of access to their "ting" (things). Thus, the pattern coding was further developed to include a 12th theme as illustrated in figure 4.
Figure 5: Patten coding. End day 3  	During the analysis, on scrolling up and down each question, a further recurring commonality was noticed, that of the mention of the word NEMID, a Danish 2 factor (also known as 2F) log-in. At the end of day 3 a further dimension code was added. Thus a 13th code was added, that of NEMID, taken to represent the broader 2F log-in. As such, the pattern coding was developed as illustrated in figure 5. This Pattern coding remained relevant and was utilised for the subsequent duration of the analysis.