Password security and game-based learning

Lucy Caroline Gabrielsen, Associate Professor, IBA- Kolding
Laila Nadine Villadsen Kjær, Adjunct, IBA-Kolding
30th June 2022

Abstract

Focusing on financial sector employees in Denmark. The study explores gender and private versus company differences in password creation behaviour and the effect of serious game-based learning. The game, an interactive digital user interface, is custom designed using social design to address previous gaps in research around three areas highlighted in an initial study namely: Shared responsibility, Consideration of Future Consequence and Assisting memory. Conclusions are draw on differences between intended and actual behaviour, and whether password behaviour becomes more secure after the digital interface interaction, resulting in specific practical recommendations for organisations to include in their IT security policies

Key words

Serious games, Passwords, Consideration of Consequence, Memory

Words used interchangeably:

Respondents – participants, Passwords – password, Cyber threat, cyber breach.

Background Relevance

Despite advancements in user authentication methods, the username-password combination still forms part of most multi-factor authentication security systems. Over 60% of us use the same passwords for work and personal accounts, self-selected passwords creation is a major factor affecting password strength (Jayakrishnan et al. 2020). Previous studies show that organisations choosing to assign secure random passwords increase insecure behaviour by the effort necessary for remembering; as individuals more often make written recordings of assigned compared to self-selected passwords (Zviran and Haga, W.J. 1993, Tschakert and Ngamsuriyaroj 2019). Either way, with the increasing risk of identity theft, and the ensuing vulnerability to companies, it is fundamental for companies to encourage the use of highly secure passwords (van Schaik et al. 2017).

Strathman et al. propose that insecure password behaviour is a causal effect of low CFCs (CFC) (Strathman et al. 1994). The trade-off of security versus ease of memory caused by low CFC where individuals continually default towards insecure passwords can be directly linked to the psychology of human decision making. Kahneman offers insight into attitudes and behaviours towards password selection, providing a notion of two systems of mental activity; System 1 and System 2. System 1 operating automatically, quickly, with little or no

effort and no sense of voluntary control whereby individuals tend to assess the relative importance of issues by the ease with which they are retrieved from memory. (Kahneman 2013) The opposite of which is true for the System 2; used for effortful mental activities that are demanded by complex computations, characterised by concentration, choice, and subjective experience.

Jayakrishnan et al.'s study into whether game-based password awareness training could be used to teach participants about the various password heuristics focused specifically on whether game-based password awareness training improved organisational password diversity, concluding that game-based learning can be used to raise awareness, as game-based training resulted in a positive impact with the added advantage of being immersive, successful, engaging resulting in a flow experience (Jayakrishnan et al. 2020) (Nakamura and Csikszentmihalyi 2014). Van Schaik (2017) concludes that when the in-game reward is conceived as great enough, individuals are willing to take a risk. Additionally, Alotaibi et al. found mobile gaming applications to be effective in creating cyber security awareness (Alotaibi et al. 2016). Existing serious games in cyber security include amongst others, Anti Phishing Phil, CyberCIEGE, Phishy, GAP, Cyberaware, PASDJO, Control-Alt-Hack, and Passworld. (Jayakrishnan et al. 2020)

Awareness Programs

Research into password creation behaviour suggests that users fail to understand how and why they need to create strong passwords (Furnell et al. 2018), that users may know the answers to questions regarding cyber security but fail to put them into action either because they are perceived as hard to follow or because the perceived risk of not following the advice is low to non-existing and many cyber security awareness programs have failed to change behaviour as they did not take the recipient into account (Bada, Sasse, and Nurse 2019).

Gaps in research

While these studies provide informative and useful results, the data collected is from outside of Europe, and though literature may be found on the use of user interfaces for raising cyber security awareness, the target group of the studies is mostly the younger generations, with not many studies into professionals within an organisational setting.

In 2020 the Centre for Cyber Security (CFCS), a subsidiary of the Danish Ministry of Defence, published an update on their recommendations for password creation and use. (Center for cyber security 2020). The original report of 2016 included guidelines for businesses, the one of which has been changed from "Awareness, awareness, awareness" (Center for Cybersikkerhed, 2016) to "Awareness and training" (Center for cyber security 2020).

Background study

To determine the relevance and necessity of conducting a study in Denmark, an initial study on behaviour and attitudes to password creation and use was conducted on Danish finance students. These individuals, belonging to Generation Z, the Digital Natives, aim for a career within one of the top 5 sectors most vulnerable to cyber-attack, the financial sector (PricewaterhouseCoopers LLP 2021)

Several findings came from initial studies (Gabrielsen 2022).Firstly, future financial sector employees show non-secure behaviour, in general, when creating and using password authentication. Secondly, they are aware that they should be more vigilant in creating secure passwords, yet there exists a causal friction of perceived effort and weakness of memory based on low CFC and high System 1 decision making resulting in the perceived unlimited choice of password combinations being a mere illusion (Strathman et al. 1994, Kahneman 2013)

Findings from the initial study confirmed the CFCS's guidelines; to minimise the threat of cyber breaches it is necessary to increase the focus on training. In addition, the combination of literature review, theory, and data collection, resulted in highlighting three areas that organisations should focus on when creating their IT security policy, namely:

- Shared responsibility
- Consideration of Future Consequence (CFC)
- Assisting memory[1]

Aims

This study seeks to establish the effectiveness, if any, of game-based awareness and training for password security, with specific focus on CFC, shared responsibility and assisting memory for professional adults in Denmark, within their daily organisational context. The purpose of which is to determine specific practical recommendations for organisations to include in their compliance and IT security policies. The study aims to answer the question: What is the effect of online game-based training, in increasing awareness and changing the behaviour of employees, within the financial sector when it comes to the creation of passwords?

Due to the data exposure that employees in the financial sector are privy to, coupled with the sector's vulnerability to cyber-attack, the study seeks to determine whether there is a difference in financial sector employee's behaviour when comparing private password creation and use to company password creation and use.

The initial study focused on attitudes and behaviour in a general setting and was based on students studying for a career in the financial sector but not yet privy to highly sensitive company data. In addressing previous studies' shortcoming, i.e., focus on end user, informing them within the game of why and how they need to create strong

[1] Note that there is no intended significant relevance to the order in which these three are presented here.

passwords concentrating on increasing the desired behavioural effect of stronger passwords, and by designing a user-focused digital training game, this study seeks to highlight differences, if any, in intended versus actual behaviour, using game-based learning.

Limitations

A weakness to passwords and thus vulnerability to cyberattack is social engineering, for example, where individuals' digital footprints are monitored by adversaries and used to predict their passwords, thus gaining access to otherwise secure internal systems. Data access and the protection thereof via authentication access mechanisms, such as passwords is the main area of study.

Literature has paid considerable attention to how individuals' attitudes can be influenced through awareness-raising using social marketing and other interventions with intentions to change behaviour. (Nordlund and Garvill 2003, Scheiner and Holz-Rau 2007, Ory and Mokhtarian 2009, Carrasco and Lucas 2015). The authors do not deny these causal affects. However, these areas of research do not form a primary role in this study.

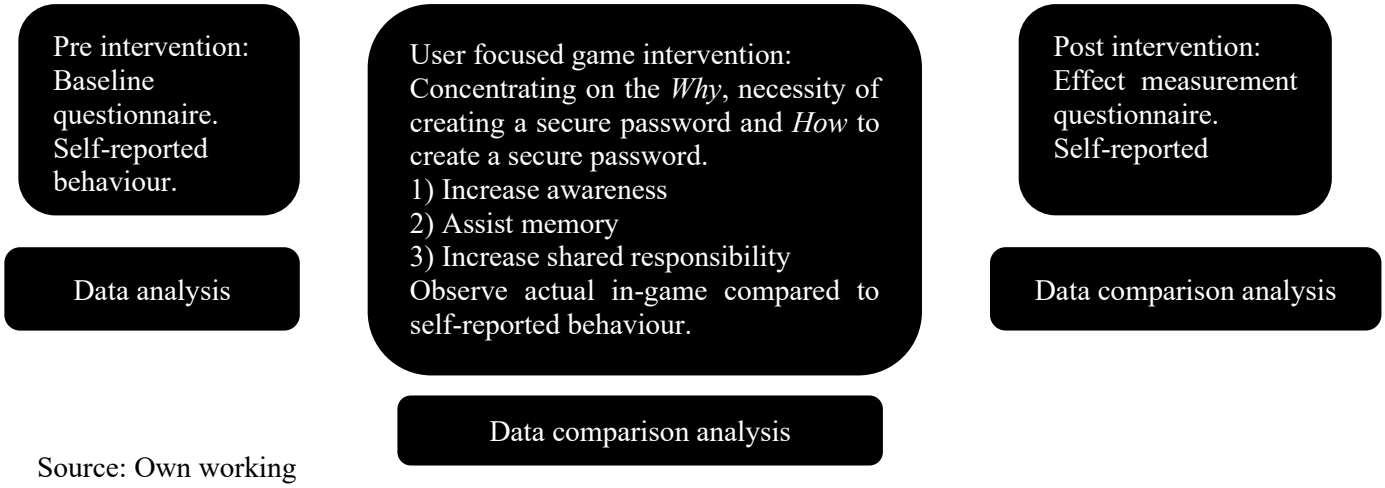
Method

This study makes use of contextual effect evaluation using a semi-controlled experiment by means of a quasi-experimental design (Alkin, Christie, and Vo 2012). According to (Arend et al. 2020) self-reported measures are a unique predictor of cybersecurity-behaviour intention and are significantly correlated to strengthening passwords with any resulting change in condition can lead to the conclusion of the game intervention being the cause of the change in behaviour (Burch and Heinrich 2016). Prior to the serious game intervention, and to address reliability of the post intervention measured effect, an attribution analysis is carried out via a questionnaire used for pre and post intervention testing with the intention of capturing the extent to which the observed results are owed to the role played by the intervention, as suggested by (Krogstrup 2016).

The quasi-experiment is via a user-focused, custom-built training game that focuses on increasing awareness of why and how password security is necessary. The specific intention is to capture actual behaviours toward password creation, compared to actual behaviours from the pre-experiment, self-reporting questionnaire. The purpose-built training features concentrate on assisting memory, increasing CFC, and increasing a sense of shared responsibility.

The objective being to observe how employees within the financial sector act within their daily workplace context. This quasi-experimental study is based on a single non-comparative open case field study following the case observations (Yin 1989), with the single case focus demonstrating results of what is possible rather than what is typical (Tsoukas 1989).

Figure 1: Structure of the study



Source: Own working

To measure the effectiveness of the intervention a clear set of criteria is needed for the evaluation (Krogstrup 2016). Predetermining measurement criteria strengthens validity of the results. The game intervention was designed with inbuilt measurement criteria; assisting memory, CFC, shared responsibility, focus on users via visual identity and professional presentation, addressed previous research shortcomings of why and how.

Case company profile and population size

The case company was established in 2007, and is an independent, privately, family-owned Danish insurance company. Their product offering is primarily on the Danish market and includes both private and business insurances. The company is a simple organisational form, with a flat hierarchy and few layers between the operational core and top management, with processes and communication organised using the functional principle (Mintzberg and Waters 1985). As with all financial sector organisations in Denmark, the company must adhere to the Financial Services Authority's, (Finanstilsynet), regulations including GDPR principles (Hvidvasklovens § 30, stk. 1, nr. 2 2021). Access to personal information is restricted to employees on a need's basis. Those employees' privy to sensitive data are subject to contractual confidentiality requirements, and where not compliant, those is breach are subject to sanctions including dismissal.

Awareness and training at the case company

Prior to the study, during a short informal interview with the company's Compliance Officer (Gabrielsen 2021) the following was established:

1. All employees had previously undergone password training. Password training was carried out via means of a one-off, one-way dissemination by the Head of Compliance, using PowerPoint as visual teaching aid.
2. Whilst internal IT systems can ensure that passwords created are secure, in their formation, i.e., length, digits – upper case, lower case, numbers and special characters, there is no way to ensure that employees

do not use personal information about themselves, that is available on the internet and vulnerable to social engineering.

3. Employees have received training and may have the intention to act in a compliant manner, yet there is no way to ensure the intention is acted upon, specifically when it comes to not using personal information such as family birthdays and names, in the creation of passwords.
4. The company use a two-factor- authorization access to internal IT systems. Employees can choose to have the authorization code sent to them via one of three channels: a phone call via a landline or SMS, or app via their private mobile smartphone.

Data collection design

Phase 1: Pre-intervention, self-reporting, baseline questionnaire

The questionnaire consisted of 18 questions. The first three determine gender, financial sector experience and current department to ensure a broad range across the various functions to strengthen representativeness and therefore validity of the end results. Subsequent questions focused on password behaviour included number of private passwords; same passwords used for private and work purposes; when last a private or work password was changed; when last the password(s) used for authentication access at the company was changed; reason for changing passwords; length and characters used when creating passwords for private use or for authentication access at the company; preferred method when using the company's 2F verification system, and finally as employees can choose to use the 2F verification system sent to their private mobile phone, whether their mobile phone is password protected, digits and information used when creating memorable passwords.

Phase 2: Game intervention

Phase 2 of the data collection was designed around a user focused interactive, visually appealing user interface to appear motivating this approach from previous studies has shown good results in raising awareness of and changing behaviour toward password creation and use (Jayakrishnan et al. 2020).

Reliability and validity of data collected during phase 1

41 respondents from a population size of 62 responded to the pre intervention questionnaire, a 66% response rate. Of those, 46% were female and 54% male. A slight variation from the financial sector most dominated by male gender, being closes rather than further from 50% difference, the data collected is deemed valid. To assess any differences in shared responsibility, CFC, and security awareness, the number of years' experience within the financial sector was measured between a range of under 3 years' to over 24 years' work experience. Most respondents, 32% have worked within the financial sector for less than 3 years, with 3-8 years and over 24 years financial sector experience equally at 22% of respondents. This indicates that respondents of the study represent a wide range of work experience within the financial sector, representative of the sector.

Reliability and validity of the user interface design for phase 2

Drawing on oversights of previous research, lack of purpose, "Why", instruction "How", and attention to end user focus, the digital user interface was designed specifically with the target group in mind, resulting in a purpose-built game made available on a custom-built website. The design focused on the three resulting recommendations from the initial study.

Student involvement

Multimedia Design students were given a briefing and designed separate user interfaces for the purpose of this study, based on the task briefing in figure 2 and 3 below. This resulted in 16 user interfaces.

Figure 2: Task briefing

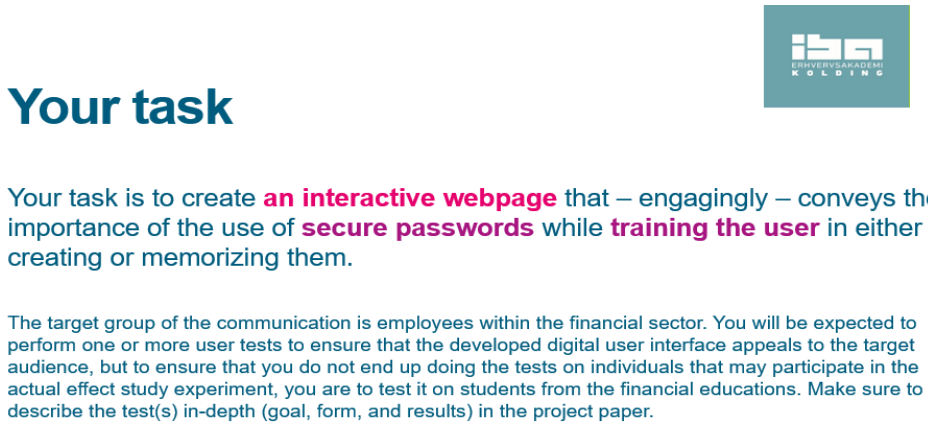
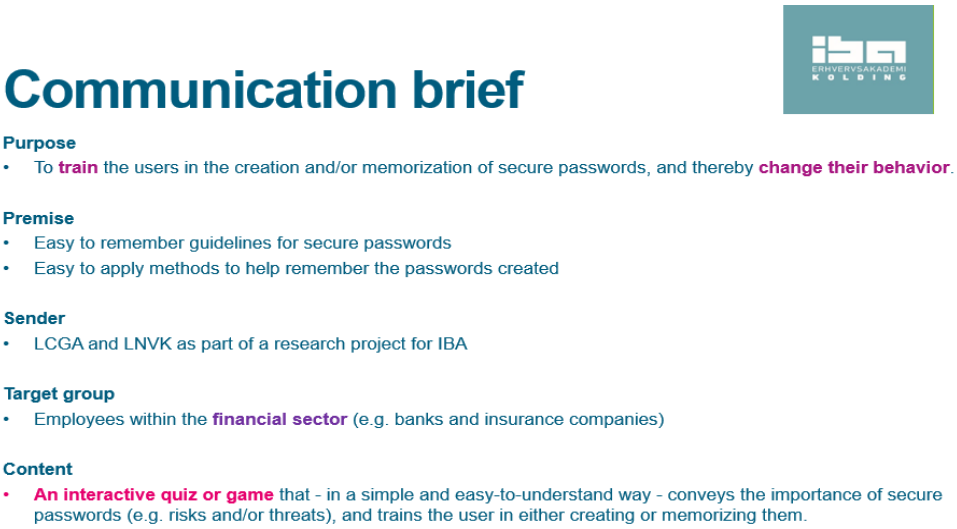


Figure 3: Communication brief



Media

- An **interactive** 1-page website

Situation

- The employees are asked to complete the quiz/game by their compliance officer as part of a cyber security training program within the company

Effect

- The users **create more secure passwords**, and **remember the guidelines** months after their first encounter with the interactive digital user interface.

THE ULTIMATIVE GOAL

- The users strengthen their current passwords after interacting with the program
- The users use the guidelines when creating new passwords in the future
- The users help remind colleagues to strengthen their passwords (creating a security culture within the company)

Pilot Testing the interface

To strengthen reliability data validity, the user interface design included 3 rounds of pilot testing as follows:

Test 1: Students – future financial sector employees

Prior to submission to the research team, interfaces were user tested on finance students, and adjusted according to their comments on usability, design, and appeal.

Test 2: Academics

Following submission, the user interfaces were narrowed down to 6 possible user interfaces matching either one or all the criteria. A broad spectrum of professionals included 6 senior lecturers, 4 Adjunct, 2 program managers, 3 support function employees, 1 Strategic management consisting of 7 females and 9 males, using a Likert scale based on questions on the evaluation criteria with additional qualitative comments available, received a brief on the areas of the study, after which they tested the pre-selected 6 game user interfaces. These 6 digital user interfaces when then merged via reprogramming by the research team. The result of which can be seen in figures 4.1-4.4 below:

Figure 4.1: Game welcoming screen

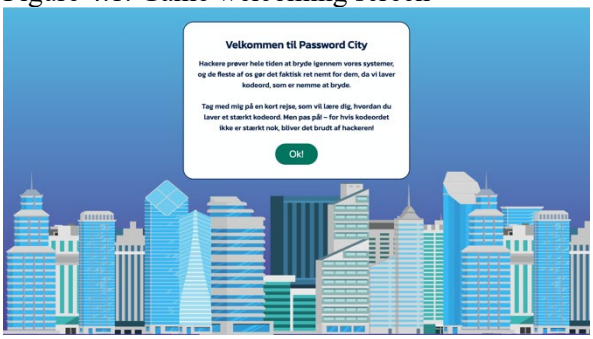


Figure 4.2: In-game awareness signs

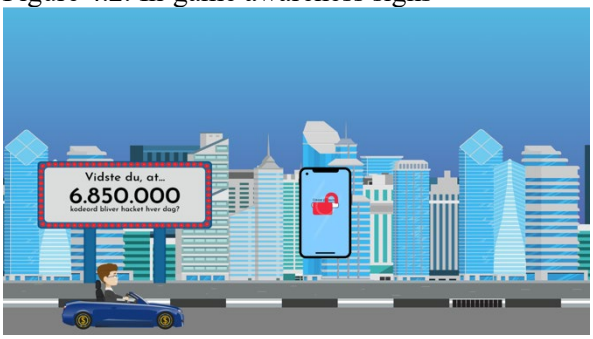


Figure 4.3: Memory helper

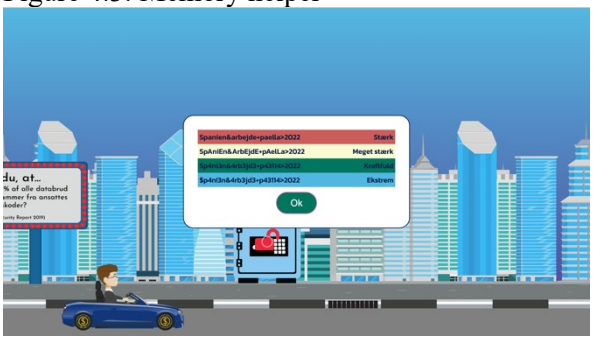
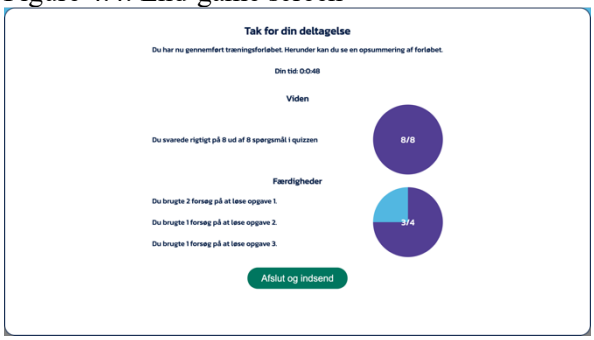


Figure 4.4: End-game screen



Test 3: Practitioner

Finally, the director of a large Danish consultancy company that focuses on optimising and digitalising business processes for industry. The purpose was to gain a pragmatic digitalisation expert opinion on design based on the predetermined criteria Why, how, end user focus. The expert informant was given access to the final merged outcome user interface and tested this under observation, assessing user functionality, instinct, command placement, information, and instruction usability.

Part 3: Post intervention, self-reporting, effect measurement questionnaire

The post intervention, self -reporting, effect measurement questionnaire directly mirrors the pre intervention questionnaire. The questionnaire was sent to respondents via the same channel and in the same manner as with the pre intervention questionnaire.

Reliability and validity of data collected

Pre-intervention questionnaire

41 respondents from a population size of 62 responded to the pre intervention questionnaire, a 66% response rate. Of those, 46% were female and 54% male. A sector dominated by males, respondents' participating somewhat mirrors the gender distribution of the financial sector. The gender distribution for data collected is deemed valid. Previous studies conclude gender to have a unique effect on password-generation. Females are less likely to adhere to behaviours aimed at creating safer passwords. Yet, compared to males, females have higher cyber-security-compliance intentions, and report higher levels of privacy concerns than males (Arend et al. 2020). The data presented below comprises summations and reflection of gender differences.

Password city game intervention

27% of respondents completed and submitted all 5 tasks of the purpose-built game.

Post-intervention questionnaire

46% of respondents completed all sections of the post experiment questionnaire. The analysis and comparison that follows are based on these 46%. 10% partially completed and 44% did not complete any part of the post

implementation questionnaire. 66% of respondents participating in the post questionnaire analysis completed the Password city game. All data from incomplete respondence are deemed invalid and not included in the data presentation below.

Presentation of the data

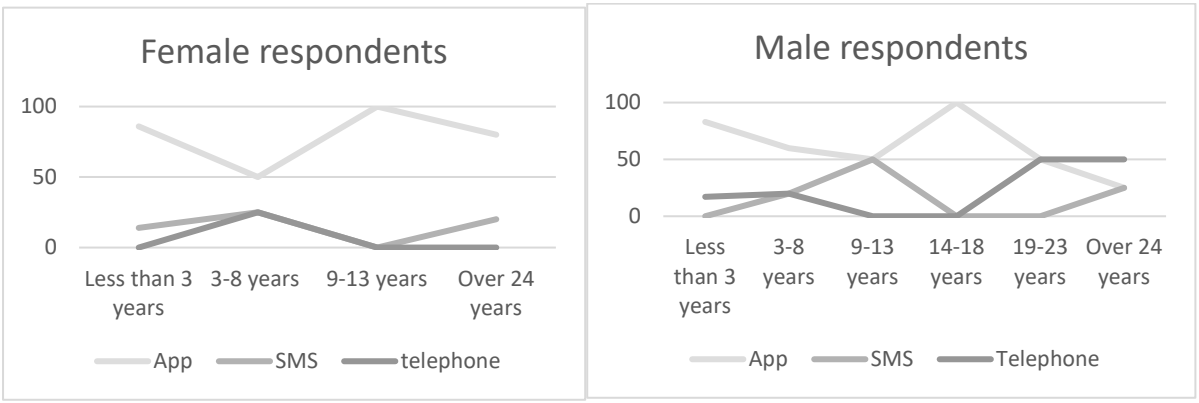
Comparison of Phase 1 and 3 Findings from self-reporting pre and post intervention questionnaires.

The company's password training prior to the experiment does not appear to have had a significant effect on respondent's password creation and use behaviour. This can be seen both for private and company passwords, with 2% changing their private passwords after training and 7% changing their company passwords after training.

An insignificant number of respondents, 2% state that they share their private passwords. No respondents reported sharing their company passwords with others prior to receiving the training, indicating focus of training necessity. 2% reportedly changed their passwords, both private and company, shortly after the training session. Again, indicating that training holds an insignificant motivation to change password regardless of whether for private or company use.

The majority of respondents, 71% of females and 64% of males use the company's 2 factor verification APP. Males are more likely to utilise the phone call system 23% as appose to 15% of females. While the SMS method is the least used by both genders, 15% females and 14% males. Results indicate that, the use of a two-factor verification app is the most attractive, regardless of gender and experience.

Figure 5: Gender and experience differences in 2F verification choices.



Source: Own working from pre-intervention questionnaire.

The APP is installed by employees, on their private smartphone. The SMS system sends the one-time code to employees' private mobile phone, 78% of respondents report using the biometrics option to unlock their private smartphones to access the one-time verification code sent. 39% reported using a 6-digit code and 34% reported using a 4-digit unlocking code on their smartphone. One respondent commented that they use no code to open

their phone. This could lead to a potential high cyber security risk and should be addressed in future training by encouraging employees to log-out of the App each time they use it.

The number of passwords an individual has is a strong indication of use, across systems, specifically reuse (or not) 46% of respondents state that they have between four and six private passwords while 37% have only one-to-three passwords, regardless of span of experience. 78% state that they use different passwords for private and company accounts, more concerning is the number of respondents 17%, that reuse at least one password for both private and company access.

10% of respondents forget their private passwords often and 59% forget on occasion. Respondents appear more likely to remember passwords used for company authentication with only 5% stating that they often forget their company password and 27% stating that they forget their company password on occasion. Suggesting that encouraging using separate passwords should not affect memory to a large extent.

Respondents reported a significant difference of 41% in effort of remembering between private and company passwords with 46% of respondents reporting they forget their private password and 5% of respondents reporting they forget their company password. Table 1 below shows the significant difference in pre-and post-intervention results, both for private and company passwords. The difference can be due to two reasons; firstly, the game had an effect having trained in CFC and ease of memory. Secondly, respondents had changed their password during the game and thus, had no need to change again prior to post-intervention.

Table 1: Changed password because they had forgotten their password

	PRE-INTERVENTION	POST-INTERVENTION	PRE-INTERVENTION	POST-INTERVENTION
Financial sector experience	Number of respondents in %. Private		Number of respondents in %. Company	
less than 3 years	46	17	8	0
3-8 years	67	50	0	0
9-13 years	40	100	0	0
14-18 years	67	0	0	0
19-23 years	0	50	0	0
24+ years	33	33	11	0

Source: Own working from pre and post intervention questionnaires

A significant 88% responded that they changed company password when forced to by the system. On changing private passwords, 46% respond that this is due to having forgotten their password. Indicating a system force is the most significant reason for changing a password, more so than forgetfulness.

Table 2: Changed password due to forgetfulness and system force

Financial sector experience	POST- INTERVENTION	
	Number of respondents in %. Private Due to forgetfulness	Number of respondents in %. Company Due to system forced change
less than 3 years	17	100
3-8 years	25	100
9-13 years	0	100
14-18 years	100	100
19-23 years	50	100
24+ years	33	67

Source: Own working from post intervention questionnaire

Table 2 above demonstrates the post-intervention effect on password change by experience range. The majority of respondents changed their private passwords because they had forgotten, 38%. Compared to respondents' company password, where 95% state that they changed their password due to the system forcing them to do so and a single outlier, with over 24years experience, stating that they change their password every month. Overall, the data suggests a higher CFC (Strathman et al. 1994), indicating shared responsibility toward company policies.

Likewise, password combinations, created and used for company systems authentication too indicate a higher CFC. 24% of respondents create completely unique passwords for company use, that they do not need to write down to remember, compared to 17% for private use. 76% respond that the complexity of their password is more important than easy access to company systems compared to 51% for private system access, indicating higher CFC, shared responsibility (Strathman et al. 1994) (Hansen and Nissenbaum 2009) and heightened awareness of company, compared to private security, considerations. Furthermore, respondents are less likely to share company passwords with others, 95% than they are their private passwords, 63%. Interestingly, female behaviour is more secure when changing company compared to private password and male behaviour becomes less secure when changing company compared to private password.

Table 3: Frequency of forgetting passwords

Financial sector experience	Private passwords changed due to forgetting		Company passwords changed due to forgetting	
	Often	On occasion	Often	On occasion
less than 3 years	15	62	8	23
3-8 years	11	67	0	44
9-13 years	20	60	20	20
14-18 years	0	67	0	33
19-23 years	0	50	0	0
24+ years	0	44	0	22

Source: Own working from pre intervention questionnaire

Table 3 above, demonstrates that forgetting or occasionally forgetting company passwords occurred to a lesser extent with company than with private passwords, across the experience range. While at first, this may appear a positive occurrence for companies, it could too be a causal effect of password reuse, where access to company systems occurs repetitively on a daily basis, thus tuning into system 1 thinking (Kahneman 2013) and therefore less cognitive, memorable effort. It is unclear to conclude as to whether a stronger CFC (Strathman et al. 1994) and shared responsibility (Qureshi, Younus, and Khan 2009, Hansen and Nissenbaum 2009) are the causal effect of this occurrence.

Gender differences

Females

When forced to change their company passwords on a regular basis, 71% of females having worked for less than 3 years in the financial sector state that they often remember their new company passwords. For those with 3-8 years' experience the number falls to 50% and with 9-13 years the number drops further to 33%. This indicates a negative correlation of experience within the financial sector versus memory of company password created. Yet 80% of respondents with over 24 years of experience answer that they too often remember their new company password. 11% of female respondents in total often forget their company password versus 0% of male respondents. This would indicate that employees with between 3-13 year and over 24 years' experience within the financial sector have developed a good system for creating and remembering their company password. There were no female respondents with financial sector experience between 13 and 24 years, which could be an area for further research.

Males

67% of male respondents with less than 3 years and 14-18 years of experience state that they often remember their new company passwords. With males 3-8 years of experience the number falls to 60%. The percentage of male respondents who never forget their passwords does not drop below 60%. Like private passwords this indicates a higher cognitive overload for female employees. This result is a contradiction to Jayakrishnan et al.'s study which concluded remembering strong passwords is more difficult for men than women (Jayakrishnan et al. 2020).

Changing passwords

The reason given, for both genders, for changing their company password was not due to any specific consideration other than that the system had forced them to. Equally only 5% of both genders changed their company password because they had forgotten their password. This would indicate that the interval of system forced change of password occurs at an effective rate with 84% of females and 91% of males changing their company password due to a system forced change. Overall, occurrence of changing is highly dependent on system force.

Table 4: Sharing passwords

Financial sector experience	Last shared their private password (s)			Last shared their company password (s)		
	Before corporate training	Within the last 6 months	Can't remember	Before corporate training	Within the last 6 months	Can't remember
less than 3 years	8	15	23	0	0	0
3-8 years	0	33	22	0	11	11
9-13 years	0	0	0	0	0	0
14-18 years	0	33	0	0	0	0
19-23 years	0	50	50	0	0	0
24+ years	0	0	11	0	0	0

Source: Own working from pre intervention questionnaire

The majority of respondents changed their password within the last 6 months. With almost none changing passwords, private or company, prior to the traditional one-way pre study corporate training. Most changed company password as they could not remember. When it comes to sharing passwords, a higher percentage of participants have never shared their company password, compared to private passwords, indicating a higher CFC and sense of responsibility aimed toward the company (Strathman et al. 1994, Hansen and Nissenbaum 2009).

Ease versus complexity

82% of males and 68% of female respondents find password complexity to be more important than ease of access. Across the experience range, complexity is considered more important than ease of access for company passwords, 21%, suggesting a higher consideration of importance of complexity compared to ease of access. Indicating a sense of shared responsibility towards the company and a higher CFC. The data suggests gender difference in ease of memory versus complexity of password(s).

Table 5: Easy access is considered more important than passwords complexity

Financial sector experience	Private	Company
less than 3 years	38	23
3-8 years	56	22
9-13 years	40	40
14-18 years	100	33
19-23 years	100	0
24+ years	33	22

Source: Own working from pre intervention questionnaire

Gender differences

Females

100% of females working for more than 24 years prefer complexity over ease of access. Those working in the financial sector for less than 3 years 43% prefer easy access. 3-8 years the number falls to 25% meaning that

they are more considerate of consequence. However, 9-13 years the number increases again to 67%. From this we cannot conclude that consideration of consequence increases or decreases over time, rather the group who have been in the financial sector between 9 and 13 years show a lower CFC.

Males

100% of males with less than 3 year and 9-13 years and 19-23 years of financial sector experience consider complexity of passwords to be more important than ease of accessing company systems. Yet those with 3-8 years of financial sector experience are more likely to prefer ease of company systems access over password complexity. 33% 14-18 years prefer ease of access over password complexity. Interestingly, an equal number. 50% of males with over 24 years of financial sector experience choose ease of access over password complexity and vice versa.

There is a higher number of females with 24 years of experience that choose password complexity over ease of access when compared to their male counterparts. While several groups across the ranges of experience respond with a higher choice of password complexity over ease of access, there exists an equal number of groups that do not.

DISCUSSION

Memory

The data shows that respondents admit to having less secure password behaviour when accessing their private accounts. The most common reason for changing private account passwords is due to having forgotten their password. Regardless of experience, most respondents can't remember having changed, or have never changed their private password. A resounding majority of respondents, across seniority state that when they do change their private password it is a consequence of having forgotten their password. 50% of male versus 42% of female respondents state that they forgot their passwords. Indicating that it is more common for male respondents to change their password due to memory constraints.

69% of respondents overall experience a memory relapse when it comes to passwords. With 16% of women, compared with 5% of men often forgetting their password. This in contradiction to previous findings leading to an inconclusive conclusion. 26% of females versus 9% of males stated that they can't remember when last they shared their password. This indicates that they have shared but cannot remember the lapsed time period, further indicating memory constraints, additionally this indicates a low CFC of repercussions from sharing their passwords.

Consideration of consequence

68% male and 58% females report never having shared their private password with anyone. 18% male and 16% females have shared their password with others within the last half year. In the instance of sharing their

passwords, gender differences are negligible. Indicating a similar level of CFC and (in)secure behaviour. Answering this question in the survey and being able to put a time stamp on suggests that respondents are consciously aware of sharing their password and thus consciously choose high risk behaviour, this furthermore indicates a CFC that does not necessarily lead to a lower security risk for themselves.

DATA COLLECTION PHASE 2

Implementation of the serious game

The game was developed with five tasks for participants to complete, an overview of which is demonstrated in table 6 below. The game was developed so that respondents had the possibility of going straight to task 5, this was a conscious decision to collect data on any respondents who did not complete the previous tasks, an indicative measure of low CFC.

Table 6: Game tasks and connection to theory

Task	Description	Link to theory
1	Type in a password that consists of 16 or more characters.	Current behaviour Awareness
2	Type in a password that consists of 16 or more characters and includes lower and upper case, special characters, and numbers.	Awareness
3	Type in a password that consists of 16 or more characters and includes lower and upper case, special characters and numbers and retype that password.	Awareness Memory
4	Training easy of effort and memory.	Memory
5	Quiz	Awareness CFC.

Source: own working

Respondents

17 out of 62 respondents completed the game. 1 respondent only completed task 5. Each task was developed so that respondents had to complete the task correctly before they could continue. Meaning that some had multiple attempts before moving onto the next task.

Task 1

77% of respondents completed the task on the first try by creating a password of 16 or more characters. These passwords were the instructed length only, with no indication of awareness of the importance of password complexity expected by including upper, lower case, numbers and/or special characters. 53% of respondents used lower, upper case, numbers, and special characters on task 1, without instruction to do so, this indicates that their awareness of necessity of password complexity is strong which is also an indication of CFC however, the length of their passwords did not necessarily meet the criteria. 67% completed the task on the first try, by meeting both the complexity criteria and the correct number of characters (16 or more). The maximum number of attempts by any one respondent was three. Three respondents used multiple attempts (two-three).

Results from task 1 data indicate that 35% of respondents are aware and behave in a secure manner and 65% would need more prompting at the point of password creation, even after corporate training.

Task 2

77% completed the task on the first try, creating a complex password with the instructed number of characters. Of these, from the 67% who completed task 1 meeting both complexity and length, of 66% completed task 2 on the first attempt. Given more instructions in task 2 (length and complexity) resulted in 17% of these respondents decreasing the length of their password from 22 -18 characters. Although a small sample size, and thus an outlier of the data set, this could be an indication of perceived effort causing lowered CFC, focusing more on the instruction given. A warning that companies need to consider setting requirements and prompting at time of password creation.

Overall, 24% of respondents decreased their password length when instructed to create a complex and lengthy password. 18% of respondents who completed task 1 on the first attempt, used three or more attempts when completing task 2. 2 of these 3 are the same respondents that were able to complete task 1 on the first attempt and who included complexity and length without instruction for both in task 1.

24% use the same length and complexity in both task 1 and task 2. This indicates reuse of password in the in-game situation. 30% of respondents completed task 2 by merely adding an additional single character compared to task 1. The maximum number of attempts for completion of this task was ten attempts. Three respondents (different respondents to those in task 1) used multiple attempts (three-ten) to complete task 2.

Most respondents have the same length and mix, or a more complex password mix that meet the requirements of task 2, compared to task 1 indicating reuse of same password with a more complex mix. 12% increased password length by three or more characters and used three attempts to do so. 6% of whom increased length from 27 (with no-uppercase) to 33 characters meeting all complexity requirements. The in-game behaviour of this respondent suggests password reuse on the first attempt, and by the third attempt a more secure behaviour that required more effort. The remaining 6% increased length from 18-21, also met all requirements of complexity and the instructed number of characters. They could have reused the same password as in task 1 but didn't and took three attempts to recreate as lengthy and complex password as in task 1. A clear indication that a higher effort was required by the 12% of respondents when not reusing a complex password.

Task 2 results

The data indicates a positive correlation between increased demands for complexity and the perceived effort, to meet password criteria and subsequently remember the password created. CFC is lower when employees focus more on complying with the increased demands to gain system access, and a more conscious system 2 effort is required.

Compliance officers must be aware that as the number of requirements increases, so too does the cognitive strain. The findings from task 2 suggest that companies must consider both establishing specific requirements and prompting at the time of password creation, as prompting alone is not enough to ensure the creation and use of secure passwords. Whilst it is questionable as to whether this would be the same behaviour for company systems, the data suggests that companies should be aware of the high probability of password reuse, especially when considering the indications from the questionnaire data, that several employees have hybrid passwords, across private and company systems.

Task 3

65% of respondents completed task 3 on the first attempt. 35% used multiple attempts (two-six). 18% decreased the number of characters compared to previous from task 1 and 2, as follows 18 characters used in task 1, increased to 21 characters used in task 2, reduced to 16 characters in task 3.

Table 7 below presents the data collected from task 3, illustrating difference in length, complexity and attempts with between task 1 and 3, with task 1 as a benchmark. The colour coding of task 2 compared to task 1 is as follows: Complexity increased for all. Those marked with red performed worse in length when required to increase complexity. Marked in yellow, are those who have increased the complexity to the requirement with minimal effort, by increasing the length with 1 additional character, the length is increased to meet necessary requirements, indicating reuse of the password from task 1. Overall, the majority performed better in task 2 than in task 1 indicating a conscious effort to comply when forced to by the system.

Table 7: Task 1-3 data presentation

	Task 1			Task 2			Task 3		
R*	L	C	A	L	C	A	L	C	A
1	16	4/4	1	17	4/4	10	17	4/4	1
2	17	4/4	2	17	4/4	1	17	4/4	1
3	27	¾	1	33	4/4	3	23	4/4	1
4	23	3/4	1	18	4/4	1	18	4/4	1
5	24	3/4	1	22	4/4	1	22	4/4	1
6	16	4/4	1	16	4/4	1	16	4/4	1
7	18	4/4	2	18	4/4	1	18	4/4	1
8	22	4/4	1	18	4/4	1	18	4/4	2
9	21	4/4	1	22	4/4	1	22	4/4	3
10	16	4/4	1	16	4/4	1	19	4/4	1
11	18	4/4	1	21	4/4	3	16	4/4	6
12	23	¾	1	19	4/4	1	16	4/4	2
13	17	¾	1	18	4/4	1	18	4/4	1
14	-	-	-	-	-	-	-	-	-
15	17	4/4	3	19	4/4	1	19	4/4	1
16	20	3/4	1	21	4/4	1	21	4/4	2
17	17	2/4	1	18	4/4	1	18	4/4	1

*R (Respondent), C (Complexity), A (Attempts), L (Length)

Compared to task 2, in task 3 the majority have the same complexity and length as in task 2. 12% decreased the length of password using additional attempts. This clearly demonstrates a higher effort when given further instructions. As instruction and requirement complexity increases so too does effort. With number of attempts increasing when having to remember more complex passwords, leading to a clear decrease in length of password. The authors are aware that due to the limited population size, it is possible that this could also be a result of typing errors.

Overall, the data strongly indicates that awareness increases with respondents taking the tasks seriously from the beginning of the game. The amount of effort increased as the instructions increased with the number of attempts indicating participants had to increase efforts to complete the task and coped with the effortful cognitive strain when moving from system 1 to system 2 thinking (Kahneman 2013) by minimising the length of the password.

Task 4

Task 1-3 of the game, guided participants from length to complexity of password, primarily focusing on the effect, if any, of complexity on length. Task 4 was purely training as demonstrated in figure 4.3. The purpose, not only to increases awareness of secure password creation, but more so to assist memory. (Yan et al. 2004, Sotirakopoulos 2011, Alotaibi et al. 2016, Furnell et al. 2018). The intention was to not collect data from this task but rather, to test – in the task 5 quiz and post-intervention questionnaire – any causal effect.

Task 5: The quiz – testing awareness and CFC

Unlike the previous tasks, the quiz questions were purposefully structured in a random order with no build-up of progression. Questions were kept to a minimal, to minimize fatigue. No participants answered all the quiz questions correctly. All participants answered question 1 correctly. The questions that most respondents didn't get correct were 2 and 7, both of which focused on password reuse. 6% answered all but question 7 correctly. Question 5, focusing on best practices of length or complexity, resulted in many incorrect answers. In game behaviour passwords became shorter as requirements became more complex. The passwords became more complex as a result of the complexity of requirements, i.e., special characters. The pre-quiz, in-game behaviour appears atypical to participants, seen in the number of attempts and decrease in length as the game progressed. This concentration on effort to create a more complex password within the game, prior to the quiz could be a causal effect resulting in most respondents considering complexity as more important than length of password, as demonstrated in the number of incorrect answers for question 5. Most participants answered questions 3, 4 6 and 8 correctly, indicating a high awareness of CFC, Best practices, Multi Factor Authorisation, and shared responsibility. Table 8 below presents the data collected from task 5:

Table 8: Awareness training quiz results

	Quiz questions							
R*	1	2	3	4	**5**	6	7	8
1	✓	X	X	✓	✓	✓	X	✓
2	✓	X	✓	✓	✓	✓	✓	✓
3	✓	X	✓	✓	**X**	✓	✓	✓
4	✓	X	✓	✓	✓	✓	X	✓
5	✓	X	X	✓	✓	✓	✓	✓
6	✓	X	✓	✓	✓	✓	X	✓
7	✓	X	✓	✓	**X**	✓	X	✓
8	✓	X	✓	✓	**X**	✓	X	✓
9	✓	X	✓	✓	✓	✓	X	✓
10	✓	X	✓	✓	**X**	✓	X	✓
11	✓	X	✓	✓	**X**	✓	X	✓
12	✓	✓	✓	✓	✓	✓	X	✓
13	✓	X	X	✓	**X**	✓	X	✓
14	✓	X	✓	✓	**X**	✓	X	X
15	✓	X	✓	✓	✓	X	X	✓
16	✓	X	✓	X	**X**	✓	X	✓
17	✓	X	✓	✓	**X**	✓	X	✓

Source: own working from in-game data collection

Conclusion

Cybercrime is rising and organisations often address the risk by focusing on system technology, directing less attention to employee behaviour. Modern technological developments for authentication access include biometrics and multifactor authentication systems yet many company systems rely solely on single password authentication access. An initial study on password behaviour highlighted three areas organisations should address: CFC, shared responsibility and assisting memory. Based on the initial study findings a purpose built online-game explored password behaviour of employees within the setting of a financial sector company, employing a quasi-experiment methodology. The purpose, to investigate whether online game-based training increases awareness and changes employee behaviour when it comes to the creation of secure passwords.

Findings

Prior to the experiment, the number of employees changing their company password in connection with training they have received is low across genders. Two questions were asked to collect the data on the effect, if any, of pre-experiment training. The one question is a time related question with the option for selecting "I changed my password in connection with or shortly after receiving password training from the company", 5% of female respondents and 9% of male respondents changed their company password in connection with or shortly after training. Yet, the second question, asked for the purpose of increasing validity of response, forms a contradictory picture. When asked about the reason for changing company password 0% of females and 5% of males respond they did so after having received training. This response is the complete opposite for reasons for

changing private passwords with 5% females and 0% males responding they did so after having received training. Overall, the date indicates that training in a less interactive physical classroom setting using PowerPoint, teaching with facts and examples has a minor, almost negligible effect on whether respondents change their passwords or not.

The results of the study find that most respondents across all seniority groups change their company password when forced to by the system. A little over half as many change their private password because they have forgotten them. Respondents are less likely to share company passwords than they are their private passwords. Altogether indicating that CFC, shared responsibility, heightened awareness, and effortful memory are higher for company than private passwords.

In contradiction to (Arend et al. 2020), the data from the introductory questionnaire compared to the data collected from the game shows a significant difference between self-reported and actual behaviour. Previous research suggests that guidance and feedback help generate stronger passwords. The data from this study does not support this significantly. Worryingly, length of password decreases as password complexity increases.

Gender differences

Results indicate that male respondents create more complex passwords, are more likely to remember these – thus indicating a better process for remembering their passwords - and do not share their company passwords. Furthermore, they do not use the same passwords for private and company accounts, and they change their passwords more often than female respondents. Overall, males are more risk averse and less likely to be vulnerable to cyber-attack, this is seen in both their behaviour when considering their company and private password behaviour, where they have more private passwords than their female counterparts.

Consideration of consequence

Male respondents are unanimous in their reply, with no respondents using the same password for access to both private and company systems. Less experience among female employees within the financial sector, increases the likelihood of high-risk behaviour due to using hybrid passwords, indicating a lower of CFC among female respondents with less experience in the financial sector. Companies should be aware of the hybrid use of passwords, as this opens vulnerability to cyber breach, especially when considering that the data indicates employees having a lower CFC for private passwords. Assuming less experience within the financial sector as an indicator of a younger age and the probability of female employees being part of the digital generation, compliance officers must not be complacent to their oblivion and lack of consideration towards security, which is evident of both male and female future financial sector employees. A high percentage, 84% female and 91% male, responded that the reason for changing their company password was due to a system forced change. An indication that users expect a reminder from the company before considering the necessity to update their

password. When considering the results of system forced password changes from the pre-and post-questionnaires, together with the data from task 1 of the training game, prompting at the point of password creation when developing and implementing system forced changes could positively increase compliance.

CFC appears to be higher in a company context compared to a private context and ease of access appears to be considered more important when it comes to accessing private systems than when accessing company systems. These findings suggest a feeling of shared responsibility.

Financial sector employees create long (16+ characters) and complex passwords when only presented with a minimum length requirement. A little over half use special characters when length of password is the only explicit requirement however, as additional demands for password complexity are increased, password length is reduced. Users are not necessarily conscious that they meet requirements of password length and complexity in the password creation process when confronted with additional requirements. This suggests that organisations should make a more conscious effort in finding methods to assist memory. Complexity requirements limit CFC and shared responsibility as individuals make more conscious effortful system 2 decisions, requiring organisations to increase memory assistance methods.

Online game-based learning helped highlight problem areas but had little to no measurable effect on the employees' password creation behaviour. Awareness and training programs via game-based learning do not appear to be a motivational factor. Out of the 65% of participants who completed the pre-experiment questionnaire, only 27% completed the game and submitted their results. In contradiction with (Jayakrishnan et al. 2020) suggestion that game-based training shows positive impact. Overall, the findings of the study suggest that, when compared to existing traditional one-way teaching methods, the use of game-based learning method does not have a significant positive effect on employees within the financial sector.

The probability of transferability from this single case lies within the universality of the contextual parameters. Each industry within the financial sector is made up of a broad spread of specialists, ages, seniority, experience within the industry etc. Together with broad spread of employees as types of individuals attracted to employment within the financial sector.

Recommendations

Organisations should be cautious about prompting for password complexity as this can lead to a decrease in password length. The decreased CFC and shared responsibility when accessing private

systems suggests that special attention be paid when access to organisational systems, in one way or the other, goes through an employee's private account for example where password resets or verification codes are sent to an employee's private telephone or email. The number of passwords overall was reported as low for logging in to private accounts. This could be the perception that when logging in to private accounts, e.g., social media, users do not log out and thus stay logged on to privately used websites and apps on their private mobile devices. With the popularity, among the respondents, of the 2-factor authentication App access, that is on their private mobile device, further research should be conducted in this area, for example frequency of log-in and out of private accounts.

A single case study, the population is very specific and could be deemed by some academics and practitioners alike as having a lower rate of transferability. Further research carried out on additional organisations within the financial sector could show different results and is encouraged by the authors.

The purpose designed game was in two-dimensional format. The authors suggest further studies, including focus on motivational theory, based on further development of the purpose-built game to a three-dimensional format.

There were no female respondents with between 13- and 24-years financial sector experience which, to increase representativity, could be an area for further research.
It is clear when comparing private password behaviour with company password behaviour that individuals display a more secure password behaviour and thus a higher CFC at the workplace. An area of further study would be the motivation behind the higher CFC at the workplace. The partial response of the 10% who started yet did not complete the questionnarie could indicate a lower sense of shared responsibility, perhaps equally so this could also be an indication of experiment fatigue. The same can be said for the 44% choosing not to participate in the post questionnarie. It would be interesting to carry out qualitative data collection on these 54% to determine which is the case.

Forgetting or occasionally forgetting company passwords occurs to a lesser extent than with private passwords, across the experience range. It would be interesting to discover whether this is due to a system 2 thinking where individuals are in a more conscious and effortful state when accessing company systems of whether this is on the contrary, a causal effect of password reuse, where access to company systems occurs repetitively daily, thus tuning into system 1 thinking and therefore a less cognitive, memorable effort.

As the study moved from phase 1 to phase 3, the response rate decreased. This could be due to experiment fatigue, communication prior and during the experiment, or both. Either way, the results of this study present significant implications and useful considerations for compliance officers, as the study is grounded in, and findings linked to existing research.

Bilbliography

Alkin, M., Christie, C., and Vo, A.T. (n.d.) *Evaluation Roots A Wider Perspective of Theorists' Views and Influences*. vol. 2012. Cambridge, Massachusetts: SAGE Publications

Alotaibi, F., Furnell, S., Stengel, I., and Papadaki, M. (2016) 'A Review of Using Gaming Technology for Cyber-Security Awareness'. *International Journal for Information Security Research* [online] 2016 (2). available from <http://infonomics-society.org/wp-content/uploads/ijisr/published-papers/volume-6-2016/A-Review-of-Using-Gaming-Technology-for-Cyber-Security-Awareness.pdf> [1 February 2021]

Arend, I., Shabtai, A., Idan, T., Keinan, R., and Bereby-Meyer, Y. (2020) 'Passive- and Not Active-Risk Tendencies Predict Cyber Security Behavior.' *Computers & Security* 97, N.PAG-N.PAG

Bada, M., Sasse, A.M., and Nurse, J.R.C. (2019) 'Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?' *ArXiv:1901.02672 [Cs]* [online] available from <http://arxiv.org/abs/1901.02672> [1 February 2021]

Bladt, S. and Gabrielsen, L.C. (2016) *The Potential of P2P Lending on the Danish Market*. International Business Academy

Burch, P. and Heinrich, C.J. (2016) *Mixed Methods for Policy Research and Program Evaluation*. 2016th edn. vol. 2016. Thousand Oaks, CA: SAGE Publications

Carrasco, J.-A. and Lucas, K. (2015) 'Workshop Synthesis: Measuring Attitudes; Quantitative and Qualitative Methods'. *Transportation Research Procedia* 11, 165–171

Center for cyber security (2020) *-vejledning-passwordsikkerhed-(2020).pdf*. Ministry og defence. available from <https://cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/-vejledning-passwordsikkerhed-2020.pdf> [16 February 2021]

Forsvarets Efterretningstjeneste (2018) *Center for Cybersikkerhed indvier i dag nyt Cybersituationscenter* [online] available from </da/nyheder/2018/center-for-cybersikkerhed-indvier-i-dag-nyt-cybersituationscenter/> [28 April 2020]

Furnell, S., Khern-am-nuai, W., Esmael, R., Yang, W., and Li, N. (2018) 'Enhancing Security Behaviour by Supporting the User.' *Computers & Security* 75, 1–9

Gabrielsen, H.M. (2021) *Current Password Training Process*, 30 September 2021

Gabrielsen, L.C. (2022) *Password Behaviour: A Threat to Cyber Security* [online] Kolding, Denmark: IBA Kolding. available from <https://www.eaviden.dk/project/password-behaviour-a-threat-to-cyber-security-a-study-of-future-financial-sector-employees-in-denmark/>

Hansen, L. and Nissenbaum, H. (2009) 'Digital Disaster, Cyber Security, and the Copenhagen School'. *International Studies Quarterly* 53 (4), 1155–1175

Hvidvasklovens § 30, stk. 1, nr. 2 (2021, Hvidvask) [online] 1417. available from <https://www.finanstilsynet.dk/tilsyn/information-om-udvalgte-tilsynsomraader/hvidvask/meddelelser/opbevaring-af-oplysninger-om-en-kundes-transaktioner>

Jayakrishnan, G.C., Sirigireddy, G.R., Vaddepalli, S., Banahatti, V., Lodha, S.P., and Pandit, S.S. (2020) *Passworld: A Serious Game to Promote Password*. 19

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

Krogstrup, H.K. (2016) *Evalueringsmodeller*. 3rd edn. vol. 2016. 1 vols. Hans Reitzels Forlag

Mintzberg, H. and Waters, J.A. (1985) 'Of Strategies, Deliberate and Emergent'. *Strategic Management Journal* 6 (3), 257–272

Nakamura, J. and Csikszentmihalyi, M. (2014) 'The Concept of Flow'. in *Flow and the Foundations of Positive Psychology* [online] Csikszentmihalyi, M. Dordrecht: Springer Netherlands, 239–263. available from <http://link.springer.com/10.1007/978-94-017-9088-8_16> [24 May 2022]

Nordlund, A.M. and Garvill, J. (2003) 'Effects of Values, Problem Awareness, and Personal Norm on Willingness to Reduce Personal Car Use'. *Journal of Environmental Psychology* 23 (4), 339–347

Ory, D.T. and Mokhtarian, P.L. (2009) 'Modeling the Structural Relationships among Short-Distance Travel Amounts, Perceptions, Affections, and Desires'. *Transportation Research Part A: Policy and Practice* 43 (1), 26–43

PricewaterhouseCoopers LLP (2021) *Cyber Threats 2020: A Year in Retrospect* [online] Industry report. UK: PricewaterhouseCoopers LLP. available from <https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf>

Qureshi, M.A., Younus, A., and Khan, A.A. (2009) 'Philosophical Survey of Passwords'. *International Journal of Computer Science Issues* 1, 8–12

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., and Kusev, P. (2017) *Risk Perceptions of Cyber-Security and Precautionary Behaviour*. 50

Scheiner, J. and Holz-Rau, C. (2007) 'Travel Mode Choice: Affected by Objective or Subjective Determinants?' *Transportation* 34 (4), 487–511

Sotirakopoulos, A. (2011) *Influencing User Password Choice through Peer Pressure* [online] M Sc Thesis. Vancouver: The University of British Columbia. available from <https://doi.library.ubc.ca/10.14288/1.0072416> [23 October 2020]

Strathman, A., Gleicher, F., Boninger, D.S., and Edwards, C.S. (1994) 'The Consideration of Future Consequences: Weighing Immediate and Distant Outcomes of Behavior.' *Journal of Personality and Social Psychology* 66 (4), 742–752

Tschakert, K.F. and Ngamsuriyaroj, S. (2019) 'Effectiveness of and User Preferences for Security Awareness Training Methodologies'. *Heliyon* 5 (6), e02010

Tsoukas, H. (1989) 'The Validity of Idiographic Research Explanations'. *Academy of Managment Review* 14/1989 (4), 551–561

Yan, J., Blackwell, A., Anderson, R., and Grant, A. (2004) 'Password Memorability and Security: Empirical Results'. *IEEE Security & Privacy Magazine* 2004 (5), 25–31

Yin, R.K. (1989) *Case Study Research: Design and Methods*. 2nd ed. Applied social research methods series. London: Sage Publications

Zviran, M. and Haga, W.J. (1993) 'A Comparison of Password Techniques for Multilevel Authentication Mechanisms'. *The Computer Journal* 36 (3), 11