The human threat to cyber security:

Attitudes and behaviours of future financial sector employees towards password creation and use

Lucy Gabrielsen lcga@iba.dk

THE WORLD'S MOST VALUABLE RESOURCE IS DATA

Cyber security breaches are assessed as one of the highest ranking of national security threats in Denmark, with the financial sector considered the most vulnerable.

Both public and private organisations are constantly investing in and improving software as a precautionary measure yet **the weakest link, the human factor**, is often neglected.

Increased digitalization results in a significant increase in shared data, across several platforms. Causing individuals to leave a data rich trail of digital footprints behind. Using social engineering, the data shared by individuals across platforms is easily accessible and open to cyber-attack.

Password authentication serves as a direct line of defence against cyber-attacks. Individuals **creating insecure passwords and reusing the same password** across several platforms reduces and weakens their very purpose.

LIMITATIONS OF HUMAN MEMORY

95% HUMAN ERROR

95% of cyber attacks are caused by human error.

(Howarth, 2014) and (IBM Security, 2019)

EMPLOYEES CAUSE 50%

Approximately 50% of cyber security breaches are caused by employees.

(Turban, et al., 2018)

Individuals continually produce insecure passwords.

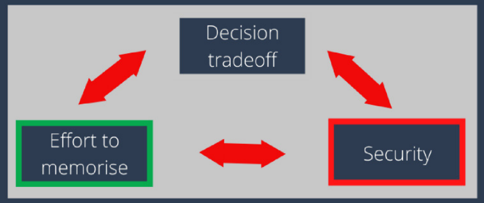
>50% ONLY use alphabetical characters

33% use both letters and numbers

<2% use random strings of letters, numbers and special characters

Based on study of Gazier and Medlin (2006)

The unlimited possibility of secure combinations of random strings of alphabetical characters, letters and special characters is **limited by human memory** and effort perception. Creating a causal effect of individuals focusing on short term needs, **neglecting long term consequences**. This results in the **creation of insecure passwords and the insecure behavior of reusing these across several platforms**. (Kahnemann, 2011)



Own working

CREATING SECURE PASSWORDS

- Minimum 16 characters long
- Random combination letters, numbers, special characters
- Lower and upper case letters
- Appears random to others
- No dictionary words

- Easy to remember
- Not written down
- Changed at frequent intervals
- Hard to guess
- Not used or reused across several platforms

NEVER shared with ANYONE

AIMS OF STUDY

Focusing on the most vulnerable financial sector, the study explores the friction behind individuals' complacency towards secure password creation and reuse. Future financial employees, identified as Generation Z financial students, attitudes and behaviours towards cyber security and specifically password creation and use, and personal data sharing in the cybersphere are explored. The study combines theoretical insight together with empirical the study directly to result in practical implications for business.

The study asks the question:

Are future financial sector employees' online attitudes and behaviours towards password creation and re-use putting the sector at risk of cyber-attacks?

METHODOLOGY

A post positivistic approach to the exploratory research was taken. Using qualitative methods of data collection by means of focus groups with the aim of capturing attitudes and decision making, while simultaneously highlighting different perspectives, both between participants within an individual group and between each of the focus groups. Data was captured through both the dialogue and actual utterances between participants as well as the interaction between group members.

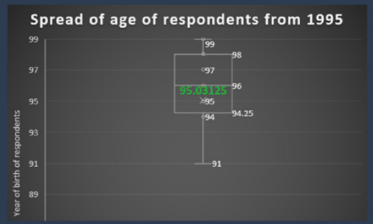
VALIDIFYING DATA

Generation Z

Born mid-1990's, these digital natives grew up with the internet. They are aware of personal data mining yet are mostly indifferent to securing their data. Data collection targeted Generation Z.

Age distribution

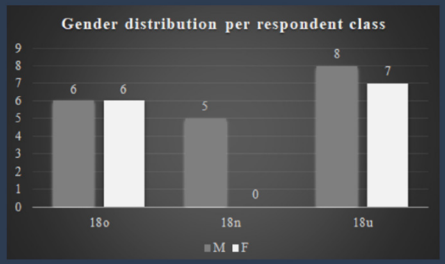
Data collection is centered on respondents' year of birth measured as 1995 with no significant outliers.



Own working

Gender distribution

Gender ratio 19:13 males to females. Extremes are equidistant and closely grouped to the median of 16 indicating less variety and higher reliability.



Own working

THEMATICAL FRAMEWORK ANALYSIS APPROACH

A thematical framework approach adapted form Krueger (1994), Raibiee (2004) and Krueger and Casey (2015) was used to analyse the data collected.

RESULTS

FUTURE FINANCIAL SECTOR EMPLOYEES' BEHAVIOUR AND ATTITUDE TOWARDS PASSWORD CREATION AND USE IS A HIGH-RISK FACTOR FOR SOCIETY.

Future financial sector employees have on average **ONLY 5.6** passwords

75% of future financial sector employees **DO NOT** use special characters in their passwords

ONLY 4 IN 32 Of future financial sector employees use a secure method to remember their passwords

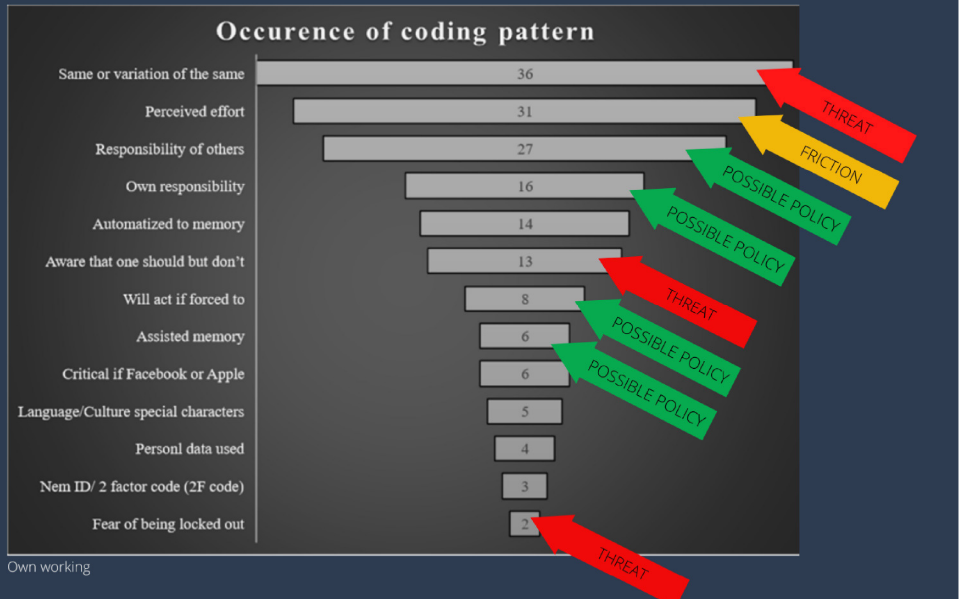
>50% of future financial sector employees **NEVER** change their passwords

Future financial employees' methods of remembering passwords

🟥 Habit	🟥 Only 1	🟥 Automatised	🟩 Unique life experiences	🟥 Perosnal 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 member	🟥 The same as my family members	🟥 Same code from the government (uni-login)	🟥 1 respondent writes them in notes on their iPhone
🟥 Perosnal data		🟥 Finger memory	🟥 From shcool 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				

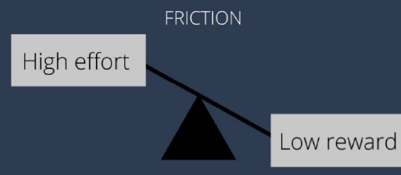
🔴 Insecure behavior
🟡 Moderately secure behavior
🟢 Secure behavior

Future financial sector employees display insecure password behaviour. The causal effect is due to perceived effort and memory constraints NOT the lack of knowledge of secure good practices.



Own working

Future financial sector employees are aware that there is a difference between weak and strong passwords. Yet all participants display a low Consideration of Consequences (CFC – the measure of consideration of potential future outcomes). Low CFC appears a causal effect of Generation Z's knowledge that personal data left in digital footprints is easily accessible by malicious adversaries regardless of secure behaviour. Changing habits to more secure password behaviour is perceived as high effort for low return.



Effort-reward imbalance model according to Siegrist

RECOMMENDATIONS FOR CYBER SECURITY POLICY

✓ **Shared responsibility**

✓ **Consideration of consequence**

✓ **Assisting memory**

Both business and employees must increase proactive efforts towards secure password behaviour. Results demonstrate that future financial sector employees are positively inclined to business setting guidelines for creating and remembering secure passwords. Business must increase the Consideration of Consequence and lower perceived effort by assisting memory. Business must move future financial sector employees from system 1 to system 2 thinking and behaviour.

Password creation and use MUST be given HIGHER PRIORITY and NOT be perceived by future financial sector employees as an effortful obstacle.

Highlighting security as a primary consideration (Sotirakopoulos, 2011)

Build relationships to trusted and knowledgeable individuals and passwords (Qureshi, et al., 2009 & Sotirakopoulos, 2011)

Building internal partnerships against cybercrime (Hansen and Nissenbaum, 2009)

Self-selection with clear guidelines on NON use of personal data (Yan, et al., 2000) and (Ma, et al., 2007)

Provide clear and comprehensive advice on security and memorability (Yan, et al., 2000)

Utilise own unique experiences (Balzaq, 2005)