Exploring Human and environmental factors that make organisations resilient to social engineering attacks

Michelle Ancher
m.ancher@hhs.nl

Researcher, lecturer
Lectorate Cybercrime
and Cyber resilience
The Hague University
of Applied Sciences

WHY research on social engineering?

Most common modus operandi of cybercriminals

Social engineering

= Convincing people to give unauthorized persons access to sensitive data through manipulation.

Consequences e.g. data leakage, resulting in reputational or financial damage.

Focusgroup: Small and medium sized enterprises (sme's)

THE HAGUE UNIVERSITY OF APPLIED SCIENCES

Often focus on technical measures

This research: measures aimed at increasing the resilience of people

Research question:
‘Which human and environmental factors play a role in cyber safe behaviour when a social engineering attack takes place?’

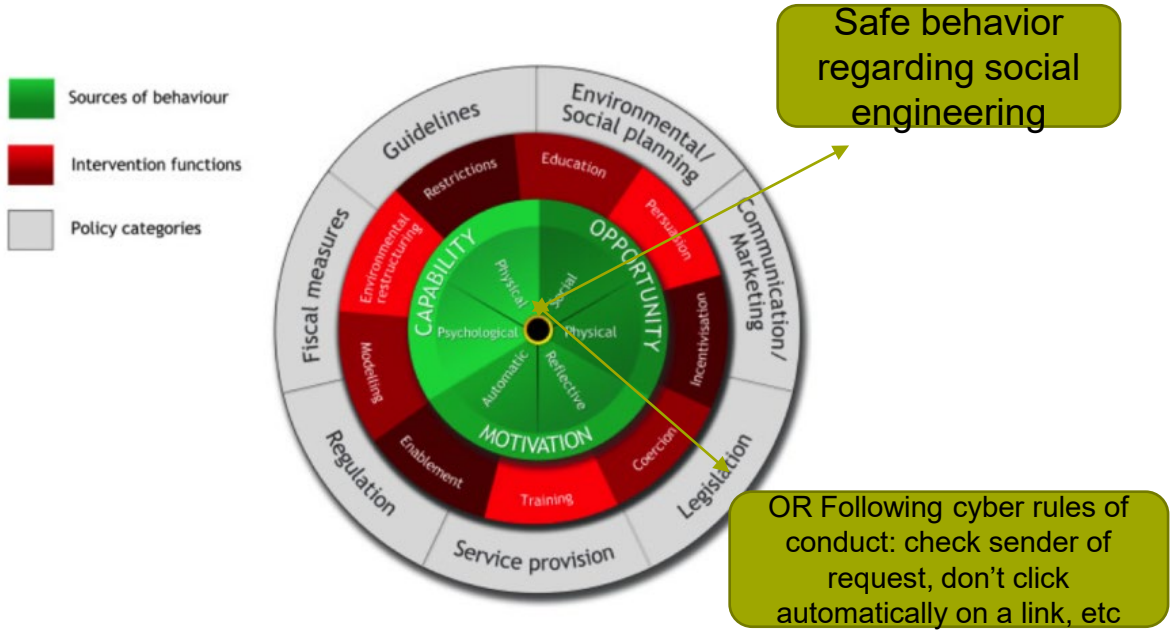
Cyber safe behaviour = not giving sensitive data or access to this data to unauthorized persons when manipulated.

THE HAGUE UNIVERSITY OF APPLIED SCIENCES

Human and environmental factors of behaviour in relation to social engineering

Capability Opportunity Motivation-Behaviour (COM-B) model for behaviour change (Michie, 2011)

Crime Prevention Through Environmental Design (Crowe, 2014)



COM-B model:
The BCW maps out which type of intervention function is likely to initiate behaviour change in each associated COM-B component, and following this, which policy categories should be addressed. By using this framework you are more likely to produce effective, theory-driven interventions, grounded in evidence-based principles.

THE HAGUE UNIVERSITY OF APPLIED SCIENCES

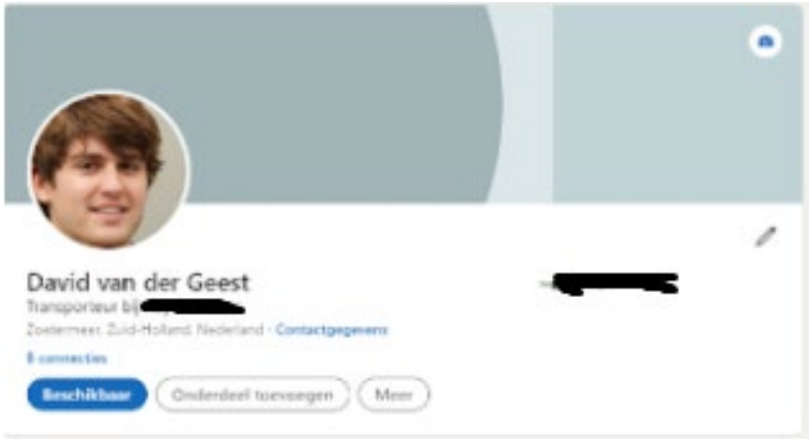
HOW: Method 1
Social engineering attacks

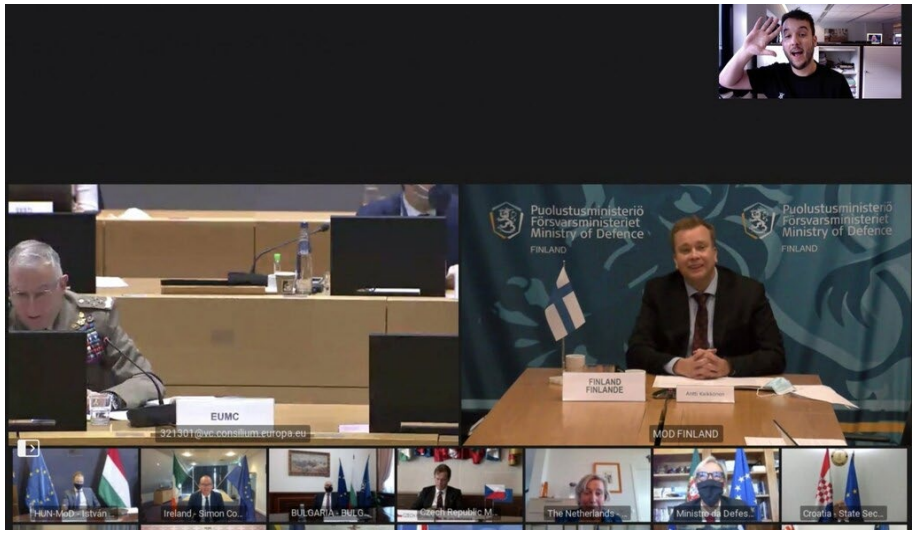
Types of social engineering

By telephone

Physical

Digital





THE HAGUE UNIVERSITY OF APPLIED SCIENCES

Social engineering attacks

Structured checklist:

Social engineeringcycle
Type of attack
Target
Provoked behaviour
Aimed data
Manipulation techniques (Cialdini, 2007) e.g. authority, social norm, scarcity

HOW: Methods

Qualitative explorative research

1. Social engineering attacks (digital, physical, by telephone)
   Analysis reports (observations)

2. Interview contact person social engineering organisations (11)
   7 <250 employees
   Grounded theory analysis of interview transcripts

THE HAGUE UNIVERSITY OF APPLIED SCIENCES

WHAT: Results

P = Physical attack
T = Attack by telephone
D = Digital attack

Organisations	Attack NOT successful	Attack successful
A		D, P
B		D, P
C	D, P	
D	T, D	P
E	T	D, P
F	T	P
G	D	T, P
H	T, P	D
I	D	
J	T, D	P
K		D

Table 1. Organisations and type of attacks that (not) succeeded

- Physical attacks are more successful (7 of 9)
- Nearly all attacks by telephone failed (5 of 6)
- Failed digital attacks (5 of 10)
- Small sized enterprises (<50 employees) Social control

THE HAGUE UNIVERSITY OF APPLIED SCIENCES

Results

"People know it and find it important, but do they behave like it..?"

- **Capability**: present differs per department.
- **Motivation:** present but no relation
- **Opportunity**:

Environmental context & resources

+ budget and involvement of other departments

- clear security policy and IT staff

Social influence

+ **Conversation protocol** how to interact with outsiders:

All failed T (5)

6 succesfull P no protocols

"Employees pick it up faster than management."

THE HAGUE UNIVERSITY OF APPLIED SCIENCES

WHAT: Results

- **Characteristics of leaders**: limited security knowledge, lack of role models
- Sensible information by Open source intelligence **(OSINT):** issues reported (7) but no relation
- All **awareness/security measures** like awareness training, red team assignments

- **Attacks direct influence** safe behaviour: Incident reports more often (3) and banners in emails

Exemplary role is very important to us because we are all young'.

THE HAGUE UNIVERSITY OF APPLIED SCIENCES

Conclusion and discussion

Social control important factor in countering social engineering attacks. All small sized enterprises **(<50 employees**).
Creating a **cyber-safe norm** (attacks are intervention), role model

Conversation protocol

Continue observational research on SMEs
Design of the work environmental context: email banners and report button

THE HAGUE UNIVERSITY OF APPLIED SCIENCES

Michelle Ancher
m.ancher@hhs.nl
The Hague University of Applied Sciences

Published:
Ancher, M., Aslan, E., Kleij, R. (2022). Exploring Human and Environmental Factors that Make Organizations Resilient to Social Engineering Attacks In: Tareq Ahram and Waldemar Karwowski (eds) Human Factors in Cybersecurity. AHFE (2022) International Conference. AHFE Open Access, vol 53. AHFE International, USA.

doi.org/10.54941/ahfe1002203

let’s change
YOU. US. THE WORLD.

Example questions that appear in the interviews

- Which statements apply to your employees/colleagues when it comes to social engineering attacks (COMb):
  C: employees do have the knowledge, skills, are capable
  M: employees think its important, important to take measures, considers to pay attention
  O:
- How do people deal with mistakes? Can they openly talk about them
- What can you say about the physical layout of the work environment
- Which characteristics suit the managers within the organization?
  O monitoring the different processes
  O the main individual who is responsible
  O Are they an example for other employees
  O authentic leader.

30

Welke uitspraken gelden bij uw medewerkers/ collega's wanneer het over social engineeringsaanvallen gaat. (motivation)

- [ ] Medewerkers vinden het belangrijk om maatregelen te treffen tegen malware, virussen, ransomware etc.
- [ ] Overweegt te letten op cyberveilig handelen
- [ ] Vindt cyberveiligheid belangrijk, ook al zijn er andere prioriteiten
- [ ] Handelt automatisch, niet zo alert
- [ ] Krijgt erkenning, wordt beloond bij cyberveilig gedrag

33

De volgende voorzieningen zijn aanwezig. Kruis aan. En zo ja wil je een toelichting geven: (Opportunity)

- [ ] Is er in uw ogen voldoende budget voor IB?
- [ ] Is er voldoende mankracht voor cybersecurity. (Een verantwoordelijke?)
- [ ] Zijn er andere afdelingen betrokken bijv. communicatie
- [ ] Is er een beleid met duidelijke concrete stappen.
- [ ] Andere

31

Welke uitspraken gelden bij uw medewerkers/ collega's wanneer het over social engineeringsaanvallen gaat. (Capability)

- [ ] Medewerkers hebben de benodigde kennis
- [ ] Medewerkers hebben de benodigde vaardigheden
- [ ] Medewerkers zijn in staat om adequaat te handelen
- [ ] Informatiebeveiliging staat regelmatig op de agenda