School of

Engineering and Computer Science

Te Kura Mātai Pūkaha, Pūrorohiko

CYBR 171 T1 2023

Ngā whakapūtanga o Te Haumaru rorohiko

Cybersecurity Fundamentals

Week 9 - Social engineering: The *whys*

Problem

THE NEW PAPER/Wednesday, October 6, 2004

SINGA

Hacker's polite approach works like a charm

By Abiz Jory

reveal computer system passwords during happy hours.

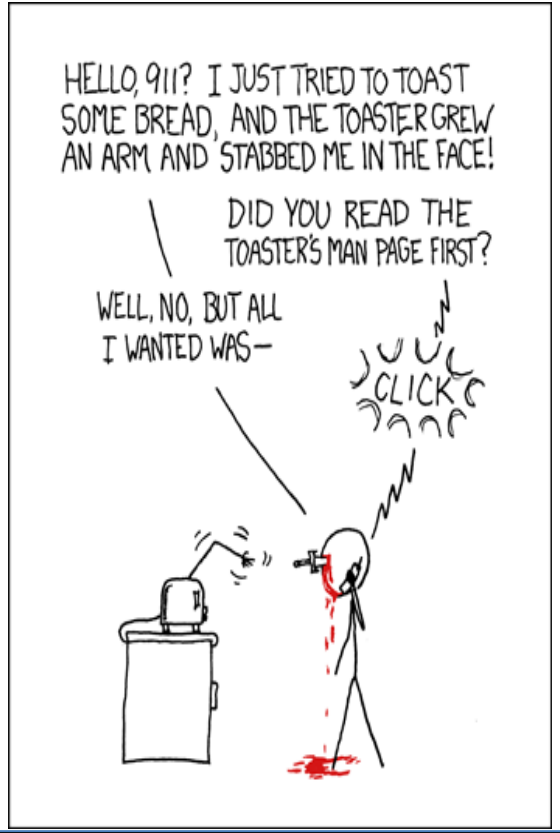
Last year, he said computer fraud.

We build systems that are <u>vulnerable</u> to *social engineering attacks*.

WHY IS SOCIAL ENGINEERING SO SUCCESSFUL?

Why is social engineering successful?

Social engineering doesn't work because people are stupid or just follow the instructions.



Why is social engineering successful? (cont.)

Attackers exploit cognitive and social biases that are part of human nature.

How can we mitigate the problem?

- Understanding the biases can help us design mechanisms to protect the system.
- People are trusting requiring the need for:
  Operational security controls.
  i.e. how do you counter natural human impulses to be helpful?
- Variant on idea of educating users, works in highly structured organisations.
- Design of controls – insights from decision science and social psychology

How can we mitigate the problem? (cont.)

Idea originated with the military.

Operational security … minimise risk (limiting who knows) and control access (via training about the rules and explaining the reasons for the rules).

Some measures:

1. limit access to information.
2. controls on who I discuss things with.
3. controls that specify that they have to prove who they are.
4. controls on how I can talk to them (means of communication)
5. controls on the protocol for responding to queries.
6. control the flow/disposal of information.

COGNITIVE PSYCHOLOGY

Cognitive psychology

- Cognitive psychology = experimentally based and field based insights into how individuals think, remember, make decisions and daydream

- “To err is human”

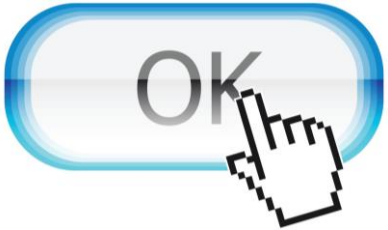
Three main types of errors

Insights from studies of machine operators:

1. Slips and lapses at the level of skills.
2. Mistakes at the level of rules (just a set of rules that you apply).
3. Mistakes at the cognitive level (related to view of understanding the world).

Class 1 error

Class 1 errors when we don't need to **think about practiced skills**. *Handy!* (e.g. riding a bike)



The OK button for example.

Downside. Inattention leads to a practiced action to be performed instead of the intended one.

We get are prone to **capture errors** and **post-completion** errors (e.g. ATMs).

Class 2 error

Class 2 errors when operator has to follow rules (e.g. phishing emails and the different indicators).

Downside. When overlapping rules and under pressure, may not choose ***best*** rule.

Class 3 error

Class 3 errors when an operator has to **apply a mental model** to choose what to do (e.g. they do not understand the technology).

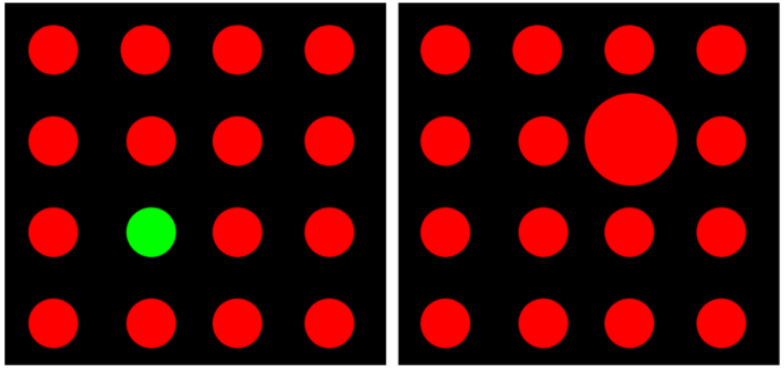
Downside. When the mental model is wrong!

Security warnings

Why do we ignore security warnings?

One aspect might be selective inattention.

https://video.link/w/2C9d



DECISION SCIENCE

Decision science

Behavioural economics/decision science =
investigates decision making

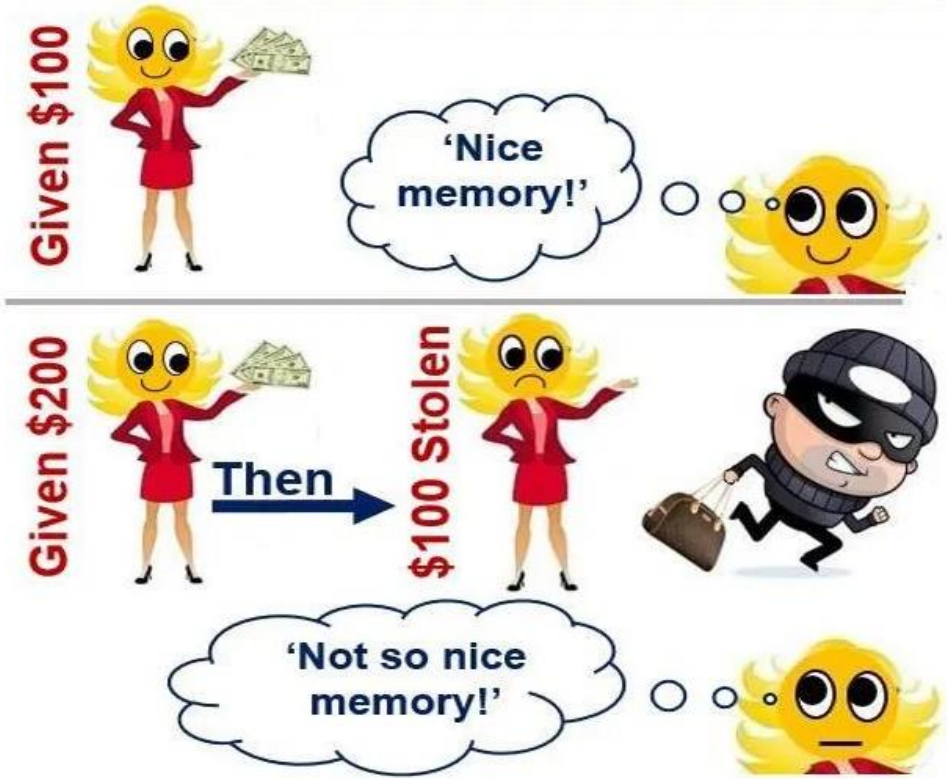
We use heuristics, **not completely rational beings**

Prospect Theory

X avoids losing $100, Y wins $100.

X is twice as happy as Y.

(Kahneman and Tversky)

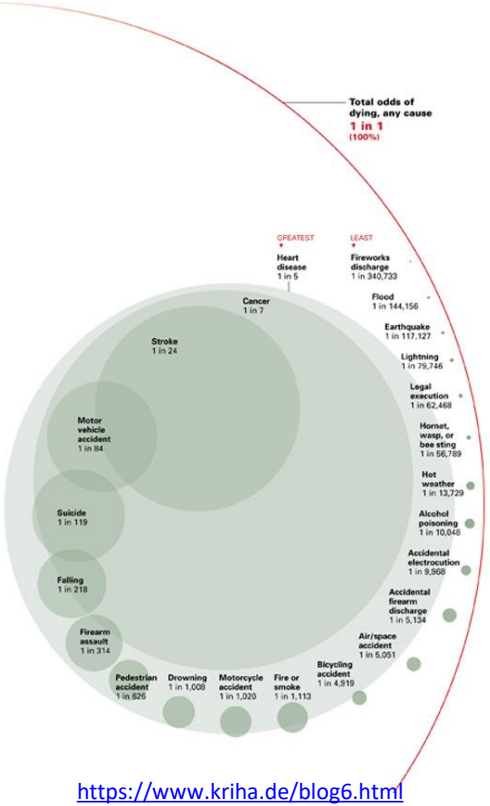


Prospect theory (cont.)

- More likely to take an action if it is *framed* as a gain rather than a loss.
- *Don't tell me how much it costs, tell me how much I save!*

Risk Assessment

Attackers want us to **misjudge** potential risks and also misjudging potential risks can stop us from doing “sensible” things.



https://www.kriha.de/blog6.html

Satisficing

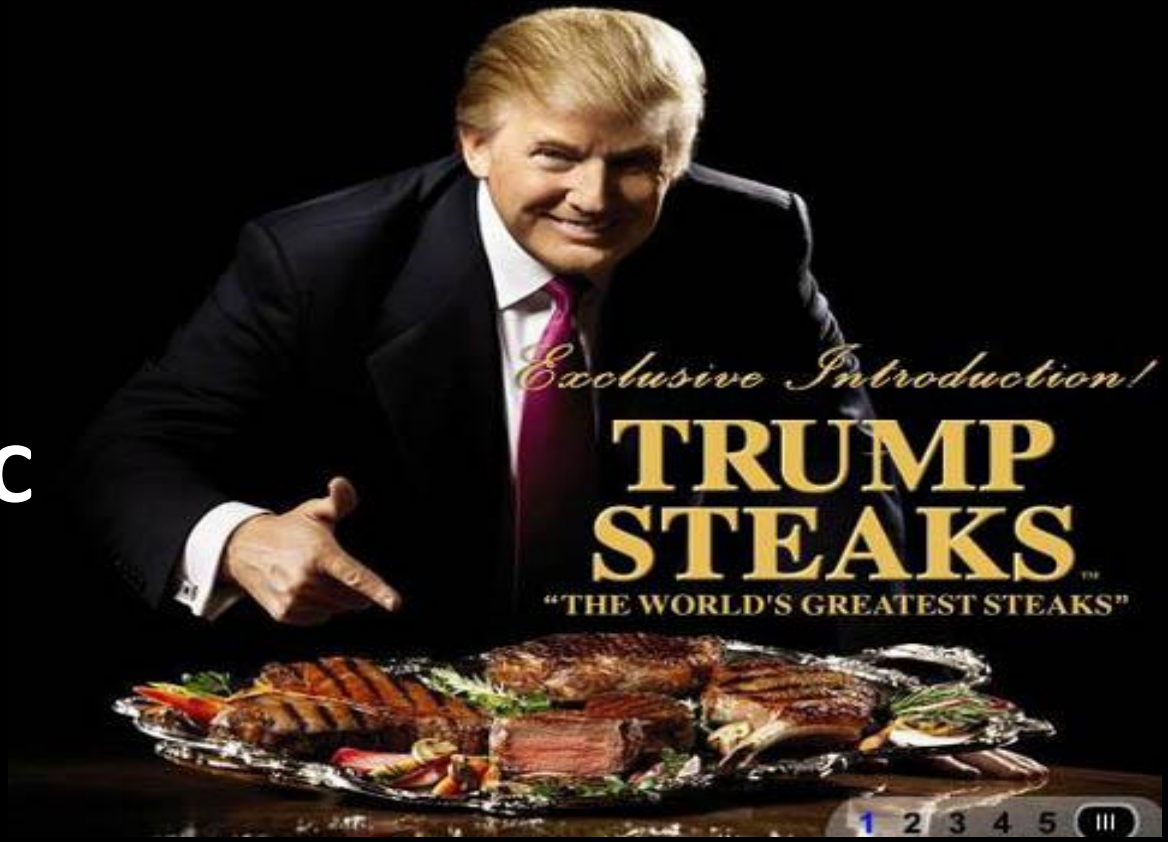
- When we are faced with a choice where the **risks** are hard to assess accurately we tend to go for the "good enough".

- Keep those default security settings.

Different aspects of mental processing

- Minds composed of affective (“heart”) and cognitive (“head”) components.
- Social decision making uses heart and other decision making uses head.

AFFECT HEURISTIC



Affect heuristic

- Paul Slovic (emotion as an influencer).
- What matters more, your heart or your head when making decisions?
- Mental shortcut based upon fear, pleasure, surprise, etc.
- "How many dates did you have last month?" + "How happy are you with your life?"
- .66 correlation when dates question comes first.
- Indicates response shaped by emotion.
- Use by attackers who **include images of celebrities** in phishing emails or have them purport to come from someone you know and trust.

Fundamental Attribution Error

- People try to explain things by intentionality rather than by situation.

- Jones & Harris (1967)

Fundamental Attribution Error (cont.)

- Subjects read pro- and anti- Fidel essays.
- Rate writers on positive attitude to Castro.

Fundamental Attribution Error (cont.)

- BUT … then told people assigned on a coin toss.
- Did it change ratings?
- NO!

Fundamental Attribution Error (cont.)

- Subjects ignore the situation.
- X would never send me a virus because their intentions are pure.
- Bit of a problem if they have been infected, suspend some vigilance.

The “just world” hypothesis

“just world” hypothesis – it cannot happen to me because I am a good person

SOCIAL PSYCHOLOGY

Social psychology

Social psychology =

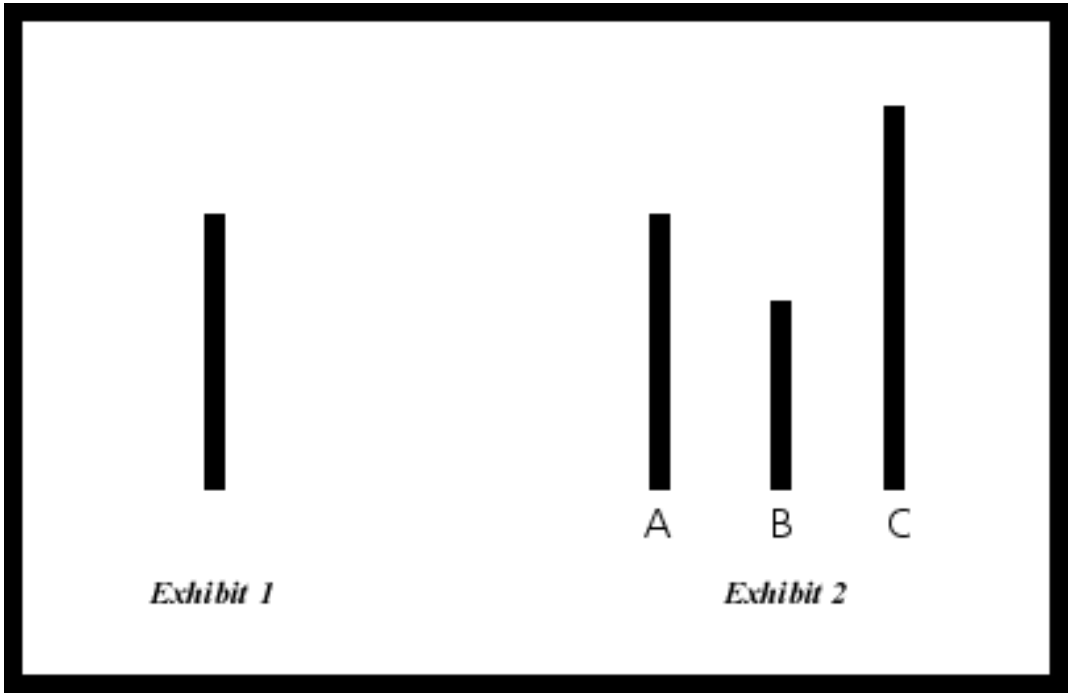
explains the thoughts, feelings and behaviours influenced by the actual, imagined, or implied presence of **others**.

Persuasion, prejudice, conformity!

With rise of social systems, attack vector.

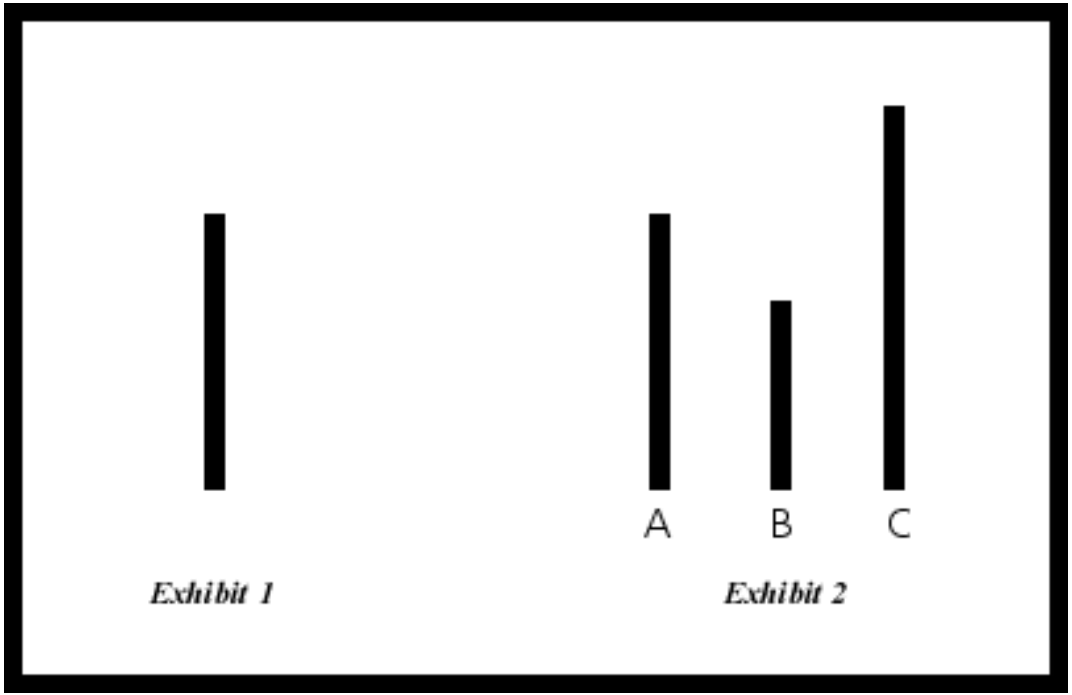
Solomon Asch (1951)

- People can be induced to deny the evidence of their senses in order to conform to a group.
- Choose closest matching length of the right.



Solomon Asch (1951)

- People can be induced to deny the evidence of their senses in order to conform to a group.
- **71% chose the closest matching length of the right**.



Stanley Milgram (1960s)

People will do immoral things and obey authority rather than their conscience.

Basic of pre-texting attacks

Stanley Milgram (1960s)

- Milgram polled fourteen Yale University senior-year psychology majors.
- Only 1.2 percent would inflict the maximum voltage.
- Also checked with his colleagues.

Stanley Milgram (1960s)

- When the experiment was run in the first test participants were given to option of opting out at any point.
- 26 out of 40 or 65% inflicted 450-volt shock.
- This relates to the Authority hack.

Philip Zimbardo (1971)

Normal people can behave wickedly in the absence of orders.

Experiment halted after **six days**.

Cognitive dissonance

- Once started why don't people stop?
- ***Cognitive dissonance theory***.
- Basically hoaxers know no-one wants to look like a dupe, most people are optimistic and most people follow social norms.
- Might explain why people who have made contact with fraudsters like the Bank Advance or Nigerian scams continue to get further into debt.

Social engineering is so powerful!

- Perhaps you can see now why social engineering is so powerful!
- Ross Anderson book ***Security Engineering*** has an unsettling example involving McDonalds.
- Combatting these problems could rely upon creating strong social norms amongst security professionals.

What we covered

- Why do people fall for social engineering?
- Cognitive psychology
- Decision science
- Social psychology

Excellent book – Ross Anderson, Security Engineering 2nd Edition

Thursday

Guest Lecture – Sam Leggett (CERT)