Univerza *v Ljubljani*
Fakulteta *za računalništvo in informatiko*

Human Attack Vectors I.

dr. David Modic

25/11/20

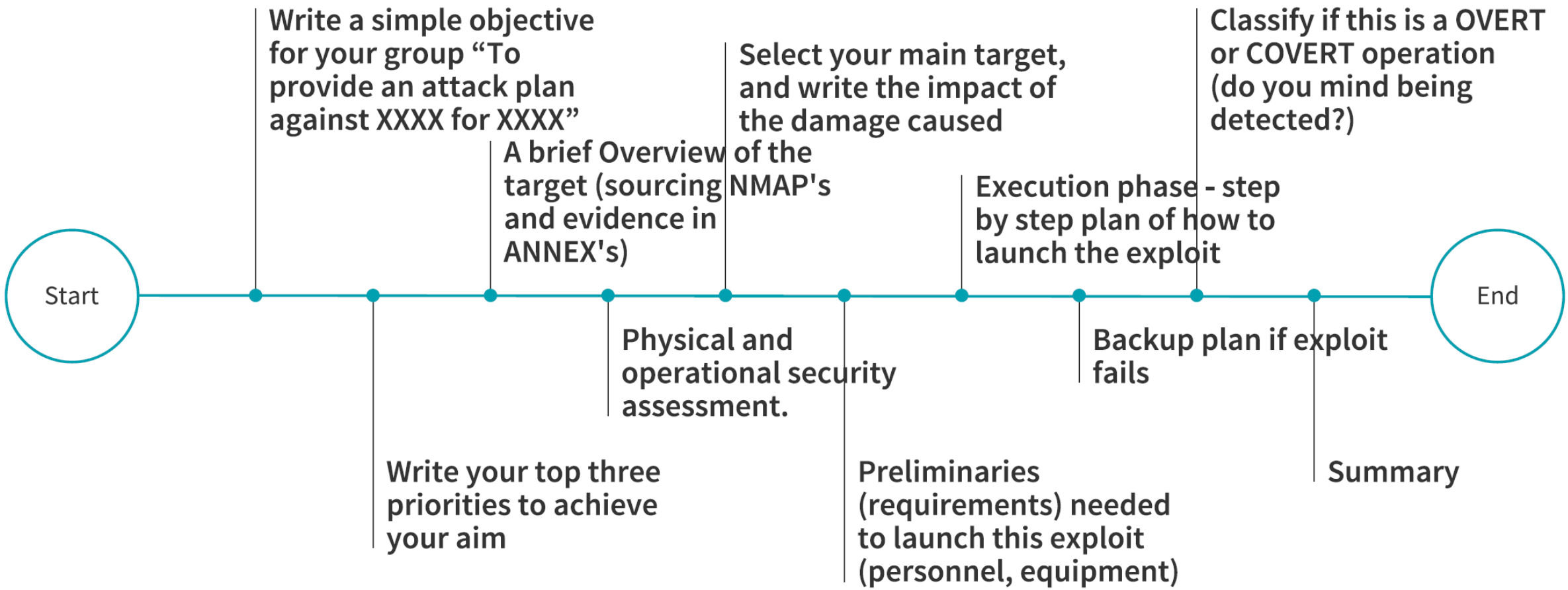
The story so far…

- We talked about Ethics and how they pertain to hacking.
- We talked about penetration testing process and is required to do it.
- We explored Open Source Intelligence gathering and you started dabbling in it.
- We then looked at Shodan, a tool used for OSINT and metasploit.
- Therefore, we will be talking about human attack vectors.

Before we start. Homework 3 - OSINT

- Generally speaking, you all did a decent job. Some invested more, some less effort. But overall, it was good.
- I have not yet marked it all. There are some with **a lot** of content.
- High points:
  - Some of you looked at the breach database. Well done.
  - Some of you looked at haveibeenwned. Not as good, but still good.
  - Some of you explained the process in detail and made suggestions on which tools to use.
  - Some of you looked at hobbies of individuals you were gathering information on.

OSINT Brief Summary



ON WITH THE SHOW!

david.modic@fri.uni-lj.si

Summary of findings from previous talks

- Attacking people instead of machines is:
  - Simpler.
  - Cheaper.
  - Yields higher success rate.
  - Requires less prior knowledge and less prep work.
- Cambridge Netflow logs show that practically all successful exploits use social engineering (as an addition or the only attack vector).

If that is true, then we should focus on people

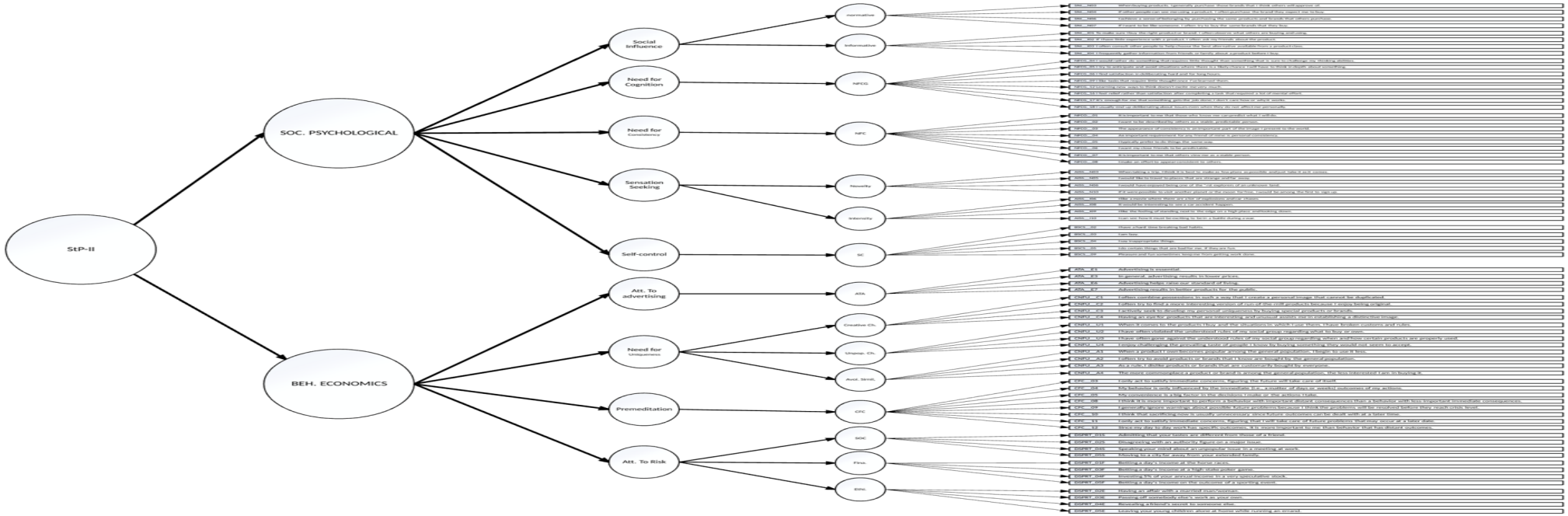
- In order to do that, we'll need to discuss them.
  - What makes them tick?
  - Why do they behave the way they behave?
  - How do hackers influence their behavior?
- How to use this in the present module.

Human behaviour

- We do not operate in vacuum.
- See for example the **Machiavellian brain hypothesis** (Humphrey, 1976)
- We do whatever it is we do, because we react to others and our environment.
- We are persuaded to behave in certain ways.
- But what is the point of persuasion?
- To get someone to do something they did not plan on doing initially (i.e. behavior modification).
- Why should security behavior be any different?

Susceptibility to persuasion

- At the Cambridge Computer Lab, we developed a scale that measures susceptibility to persuasion - the StP-II.



david.modic@fri.uni-lj.si

The Story of StP-II

- In order to understand the reasoning behind the scale, we need to briefly talk about Internet Fraud.
- *Scam compliance* == To comply with fraudulent requests.
- Staged process. Plausibility => Response => Loss.
- Marketing theory. *Scam as an illegal marketing offer.*
- Compliance across different categories of Internet fraud is influenced by different mechanisms of persuasion.

But why psychology in security and in fraud?

- Why would it make sense to look at people?
- Because of victim facilitation.
- Online fraud is well suited to victim facilitation.
- It would thus be logical that some people are more likely to comply with requests of scammers or hackers, depending on what kind of person they are.
- AHA! Psychology.

I said that there are three stages of compliance (Plausible, Respond, Loss).

- One predicts another (logitp, n=479):
- P predicts R: Odds r. = 1.78, Wald t = 3.47, $p < 0.1$ (logitp).
- R predict L: Odds r. = 16.15, Wald t = 54.68, $p < 0.001$ (logitp).
- Other theories specify other stages:
  - Either not granular at all (a Boolean variable)
  - Or more elaborate (4 stages - taking re-victimisation into account – Shadel & Pak, 2007).

Low probability event

- Falling for any kind of scam (or being hacked/phished) is a low probability event. Also cf. Herley (2009).
- Victimisation
  - Theory: 1% of 419 Scams get answered, 1% of that yields results. Effectiveness is one hundredth of one percent; Dyrud (2005)
  - Shadel & Pak (2007) - ~ 2-3% (several studies in that report)
  - OFT (2009) – guesstimate at 4.86% of UK population.
  - Modic and Lea (2011) – 12.8% responded, <1% lost.
  - **Modic and Anderson (2015) – 22% lost.**

Re-victimization

- Repeat Victimization – becoming a victim again.
- Re-victimization is fairly common –
  - Titus and Dover (2001) - occurs in ~50% of the cases.
  - Modic and Lea (2011); n = 429; ~ 33% of cases.
  - Modic and Anderson (2015); n = 6609; ~ 20% cases.

Secondary victimization

- Secondary victimization – being victimized, because a person was victimized in the first place.
- Secondary Victimization is also probably common.
- Only ~ 25% of fraud is reported (Copes, Kerley, Mason & van Wyk, 2001) -> due to fear of 2nd victimization.
- This is also an argument for why you do not phish your own employees!

Illegal marketing offers

- Scams are like illegal marketing offers:
- Fischer, Lea and Evans (2009) Office of Fair Trade Report on psychology of Fraud come up with it.
- Modic and Lea (2013) show it again (with StP-I).
- Modic, Anderson and Palomaki (2018) build on it.
- Why is this good for us? Lots of existing research on persuasion.

Persuasion

- *People who like adverts and buy stuff when they see them, should be more compliant with scams and social engineering.*
- How is this helpful?
- We can develop a scale that measures Susceptibility to Persuasion (based on what makes adverts persuasive).

The basis for StP-II

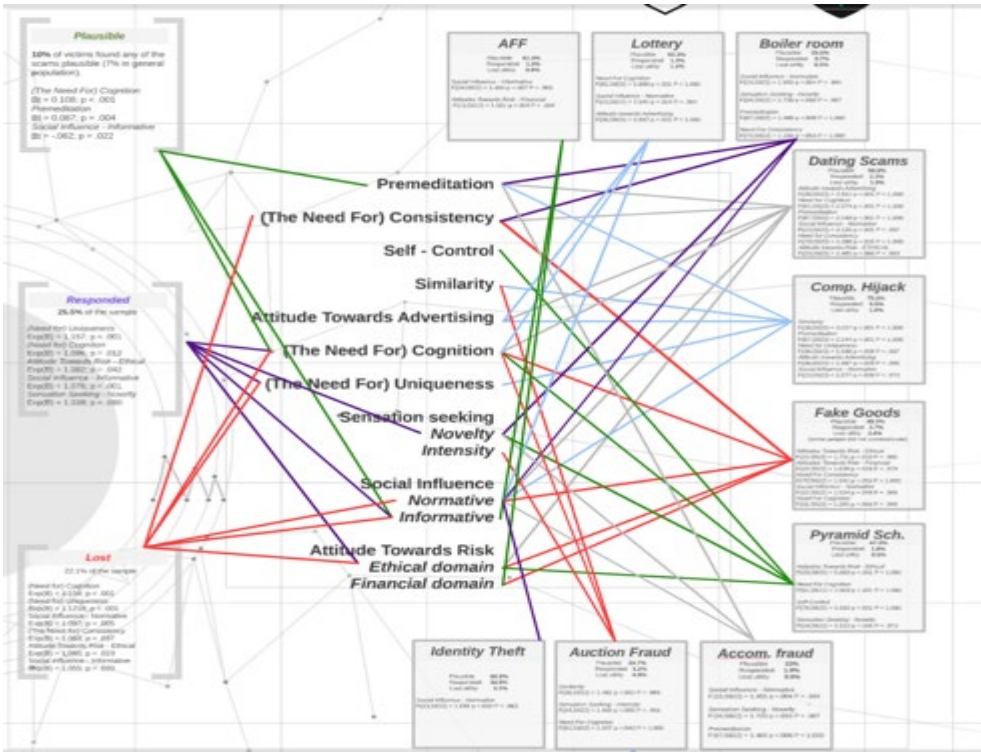
- Marketing psychology, *nudges*, behavioural economics.
- We developed a scale in 2011 (StP-I). It was reliable and had good results. Not publishable. Long rejection letters.
- All reject comments have been taken into account with the next version of the scale.
- **~ 1000 people; 137 questions; 9 existing psychometric tools; high reliability -> Cronbach Alpha > .9**

Measured mechanisms

- StP-II measures:
  - Premeditation (Consideration of Future Consequences)
  - Need for Consistency (Things to stay the way they are)
  - Sensation Seeking (both Novelty and Intensity)
  - Self-Control (as a trait)
  - Social Influence (both Normative and Informative)
  - Similarity (we expect people to be like us)
  - Risk Preferences (DOSPERT-R; Ethical and Financial)
  - Attitudes towards Advertising
  - Need For Cognition (things need to make sense)
  - Need for Uniqueness (We like unique things)

Experimental outline

- n = 6609
- StP-II and 9 different types of most frequent types of Internet fraud **x** scam compliance (plausible, responded, lost).
- We will focus on Computer Hijack and Phishing (victims of).



Partial Results - hijack

Salient StP-II mechanisms in Scam Compliance (Computer Hijack) (n = 6609)

Mechanism	F	p	Observed Power
Self-Control	9.627	.002	.873
Sensation Seeking (Novelty)	9.170	.002	.857
Sensation Seeking (Intensity)	2.942	.086	.403
Social Influence (Informative)	13.413	.000	.956

Note. The lighter the color, the bigger the effect size.

david.modic@fri.uni-lj.si

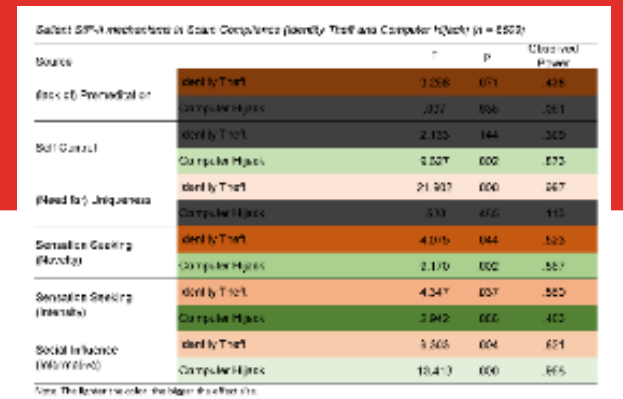
Partial Results – Identity theft

Salient StP-II Mechanisms in Scam Compliance (Identity Theft) (n = 6609)

Source	F	p	Observed Power
(lack of) Premeditation	3.258	.071	.438
(Need for) Uniqueness	21.902	.000	.997
Sensation Seeking (Novelty)	4.075	.044	.523
Sensation Seeking (Intensity)	4.347	.037	.550
Social Influence (Informative)	8.303	.004	.821

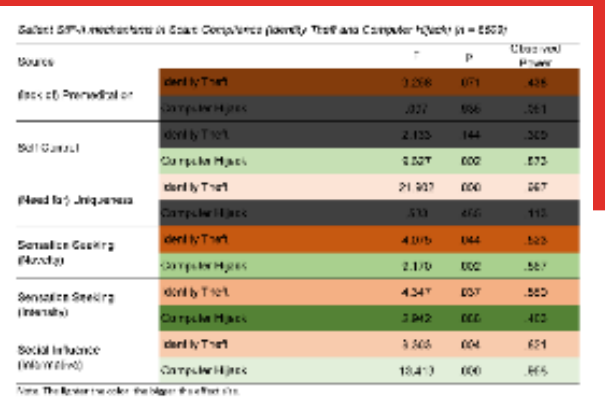
Note . The lighter the color, the bigger the effect size.

david.modic@fri.uni-lj.si



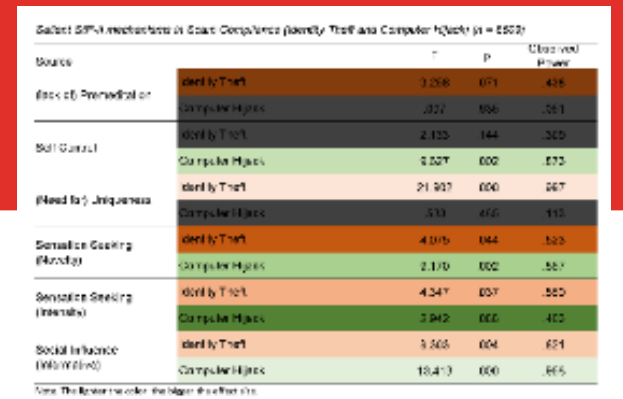
(Lack of) Premeditation

- Lack of Premeditation; or Consideration of Future Consequences is an intrinsic part of impulsivity (Whiteside & Lynam, 2001) and a significant predictor of scam compliance (Modic & Lea, 2011).
- Simply put – how good are we at predicting what is going to happen if we do something.



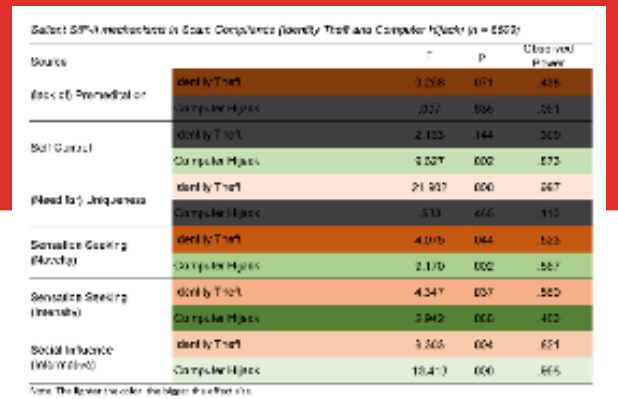
(Lack of) Premeditation

- Unsurprisingly, people with low impulse control are more likely to jump without checking the landing site first.
- Important predictor for successful phishing, because it is easier to get personal data from people, when they share it without thought.
- Salient in two ways: (a) make the messages appear so routine that no one considers them in depth, and (b) expect the mark to lack premeditation.



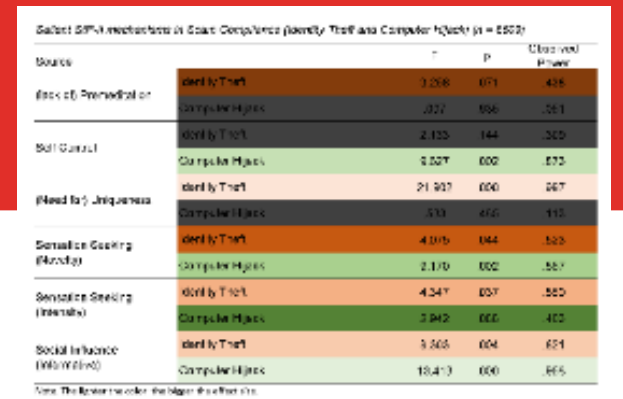
Self-control I.

- Self-control (SC) can be defined as the ability to exert will over, and shape your behaviour (Kanfer & Karoly, 1972; Muraven & Baumeister, 2000; Nadel, 1953).
- From this definition we can infer the concept of willpower (Gailliot et al., 2007).
- Let's define will as a building block of self-control (i.e. you need willpower to control yourself).



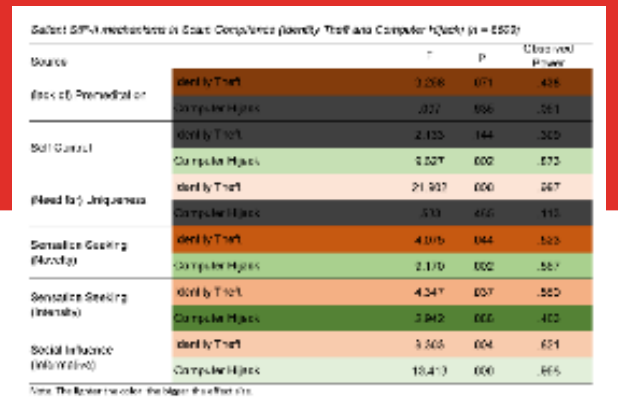
Self-control II.

- Willpower - one of the three pillars of personality (cognition, affect, conation/will; James, 1890).
- Conation / willpower is defined clearly by William James (1890a, 1890b) in The Principles of Psychology.
- James (1890) says that willpower is one of the mechanisms that make behaviour (You need willpower to behave in a certain way. Will-less person is inert).



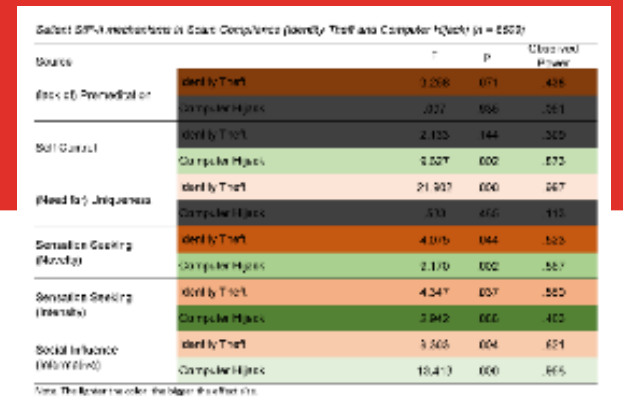
Self-control III.

- Self-control has proven to be an important predictor across contexts.
- Wegner, Schneider, Carter and White (1987) - Suppression of unwanted thoughts (White bear experiment).
- Logue (1988) and Metcalfe & Mischel (1999) - resisting the desire for instant gratification.
- Predictor of physical fitness (Muraven, Tice and Baumeister, 1998).
- and body weight (Kuijer, de Ridder, Ouwehand, Houx and van den Bos, 2008).



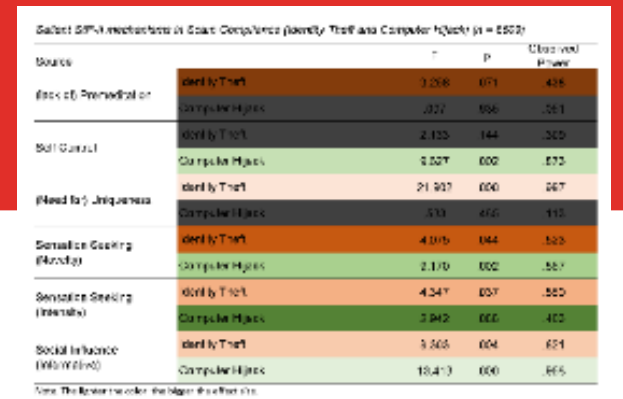
Self-control IV.

- Self-control can be construed as a personality trait, captured through the Big Five (FFM) (Self-control as a subdomain of Conscientiousness; or Impulsivity as a subdomain of Neuroticism; Costa and McCrae, 1987);
- or it could be measured with a stand-alone scale (Tangney, Baumeister and Boone, 2004).
- In that model SC is a relatively static trait. You either have it or not. The amount is a constant.



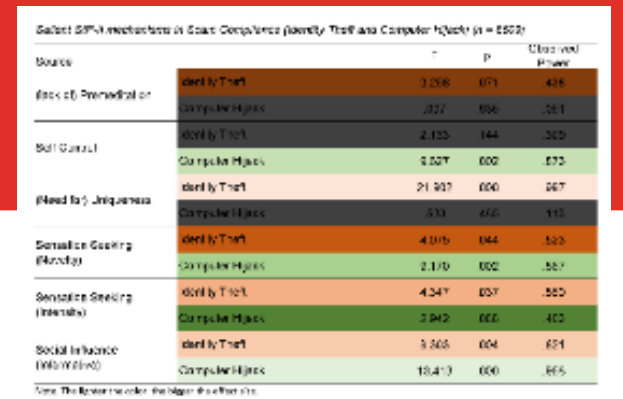
Self-control V.

- Self-Control can be construed as a cognitive state (Baumeister and Heatherton, 1996; Baumeister, Bratslavsky, Muraven and Tice, 1998) .
- In that model SC is a changeable state, likened to a muscle - it tires with exertion and replenishes itself with rest.
- Baumeister also shows that SC can be exercised and trained to be more durable as in the case of other muscles.
- StP-II looks at SC as a trait, not a state (because of the experimental model).



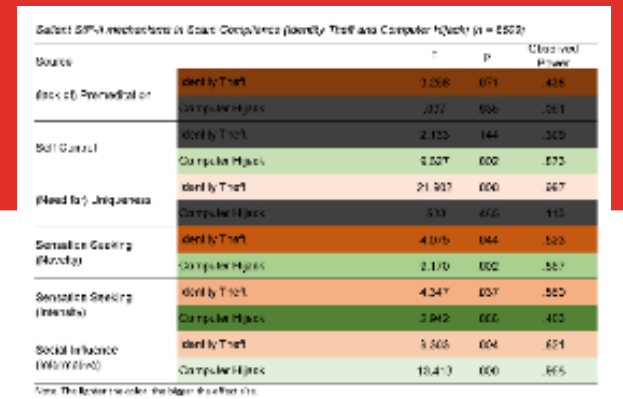
Self-control - applicability

- In our case, much like with impulsivity, those who have a harder time controlling themselves become more likely to lose personal information.
- We can either look to deplete self-control or attack those with already lowered self-control.



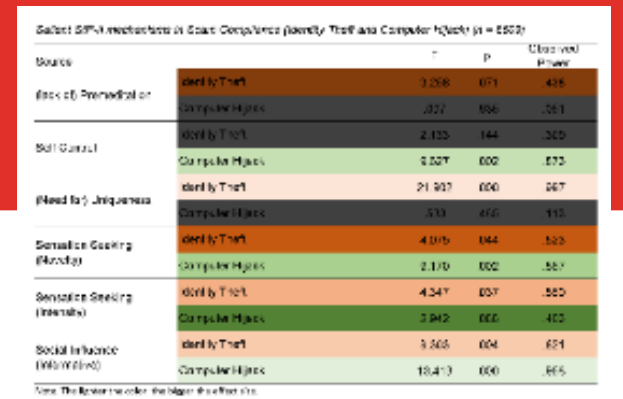
Need for Uniqueness

- Need for Uniqueness drives certain aspects of consumer behaviour.
- Research has shown consumers to be likely to respond positively to marketing offers when they believed that the goods on offer to be unique or scarce (Folkes, Martin, & Gupta, 1993; Kramer & Carroll, 2009; Suri, Kohli, & Monroe, 2007).
- In scam research, Langenderfer and Shimp (2001) have shown that many scam offers utilize that phenomenon to great effect.



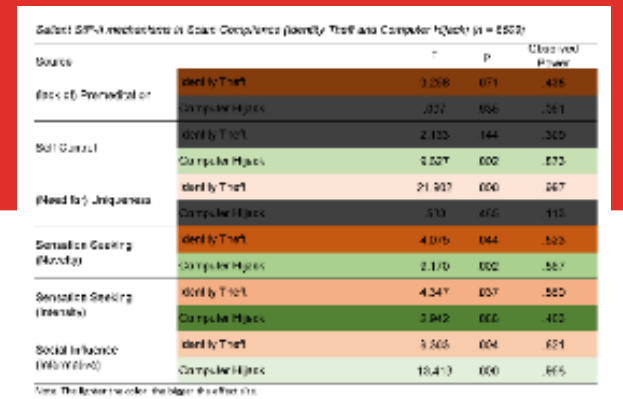
Sensation Seeking

- Sensation Seeking has been shown to influence impulsive behaviour (Whiteside, Lynam, Miller, & Reynolds, 2005), which in turn has an impact on compliance (Modic & Lea, 2011).
- There are two subscales: Intensity (how much this thing gets your blood pumping), and Novelty (have you ever experienced this before).
- Both play a role in falling for phishing and malware installation.
- The logic is that one likes living on the edge by installing this new fangled anti-virus.



Social Influence

- Human susceptibility to group pressure or social influence is well supported empirically, from early line experiments by Asch (1956) to newer work.
- Markus and Kitayama (1991) showed that individuals in different cultures construct their self-worth through comparison with other in-group members.
- Criminologists have found that individuals are more likely to comply with formal norms if they believe other members of their community also comply with them, while on the other hand visible disorder is a self-reinforcing cue for criminal activity (Kahan, 1997).



Social Influence II

- Consumers susceptible to social influence may buy products a seller favors even if their preferences are different (Bearden, Netemeyer, & Teel, 1989).
- There are two types of social Influence – Normative and Informative.
- StP-II measures both of them, but only Informative is salient in our use case.

Trust

- A prerequisite of being persuasive is trust. That is, a person needs to trust us to:
  - have their best interests at heart, and
  - fulfil our part of the transaction.
- We have shown in previous talks, that trust plays an important part in security (and perception of hackers).

No homework this time!