
# Information Governance CIS4012

Social Engineering 2

# Recap & introduction

Last time - “Social Engineering” – what it is, problems for businesses
This week looking at “Information Security Awareness and training” -> feeds into:

- LO5 - *Design an appropriately researched data governance implementation plan appropriate for a specified business need that includes business continuity and disaster recovery planning*
- LO7 - “*Demonstrate a complex understanding of the breadth and depth of the physical and environmental security issues for a given scenario and demonstrate a critical awareness of current problems and issues informed by research findings and professional practice.”*
- Assessment Parts 1 & 2 – ed & training forms part of risk management/mitigation (PT1) & you will need to identify some ‘controls’ to combat SE attacks (Pt 2)

# IS policies & compliance

One of the ways that companies try and combat hacking/social engineering threats is to have a series of policies that employees are expected to follow (see my later lectures on ISO27k as well)
The challenge is to get employees to actually follow them!
Reasons for non-compliance have been suggested (see practical exercise)
Orgs need to be creative about how they achieve policy compliance and understand how and especially *why* people 'break the rules'

# Neutralisation Theory

- Neutralization theory claims that both law-abiding citizens and those who commit crimes or rule-breaking actions tend to believe in the norms and values of the community in general (Sykes and Matza 1957)
- **So why do people break the rules?**
- Sykes and Matza suggested that people enable themselves to break the rules by applying techniques of neutralisation
  - i.e. **Rationalise behaviour by minimising the perceived harm of their behaviours**
- **Sykes & Matza's techniques of neutralisation:**
  1. Denial of responsibility (e.g. act due to forces beyond their control)(correlation found to justify bad IS behaviours)
  2. Denial of injury (e.g. no real or lasting damage)(computer crimes often justified on the grounds that it doesn't harm people)
  3. Denial of the victim (e.g. shifts blame from themselves to the victim)
  4. Condemnation of the condemners (e.g. condemners are hypocrites likely to do similar behaviour themselves) (claiming that the law is unjust)
  5. Appeal to higher loyalties (e.g. motivation is to benefit group or family i.e. hacktivists)
  6. "metaphor of the ledger" (i.e. rationalizing that the good done in this life outweighs the bad) (employees could argue that their general adherence to security policies compensates their occasional violation of security policies)
  7. Defence of necessity (i.e. portrayal of act as crucial to survival or as lesser of two evils)(employees claim that they do not have time to comply with policies due to tight deadlines)

# Deterrence theory

- Dates back to Jeremy Bentham (1748-1832)
  - individuals weigh costs and benefits when deciding whether or not to commit a crime, and they choose crime when it pays.
- Sanctions (i.e. getting caught (**certainty of sanctions**), disciplinary action (**severity of sanctions**)) are often used as a way to compel employees to comply with policies. But:
  - Employees can & do use “neutralisation” techniques to by-pass these sanctions
    - Rationalise behaviour by minimising the perceived harm of their behaviours
- However D’Arcy et al (2009) found that “certainty of formal sanctions did not have any effect on intention to misuse IS”
- Shame (informal sanction) (inc disapproval of peers & colleagues) is also used as a deterrence

# Deviant behaviour

- Employee violations of IS security policies are most often due to **negligence** or **ignorance** of IS security policies on the part of employees but some can be down to *deviant behaviour*
- **Deviant** behavior may violate formally-enacted rules or informal social norms. ...**Examples** of *formal* **deviance** include robbery, theft, rape, murder, and assault. *Informal* **deviance** refers to violations of informal social norms, which are norms that have not been codified into law.
  - This also applies to workplace norms and values
- Cyber-deviance – these behaviours facilitated by technology

# "Nudging" - What on earth is it & why is it important?

- We've probably all been subject to it at some point! (especially recently)
- Comes from the work of Richard Thaler (who won an economics Nobel prize in 2017 for his work)
  - See book: "**Nudge: Improving Decisions About Health, Wealth and Happiness**" by Richard Thaler & Cass Sunstein (2009) (in the library)
  - Read "Nudging: A Very Short Guide" by Cass Sunstein (2014) (access thro library)
- A nudge is "a relatively subtle policy shift that encourages people to make decisions that are in their broad self-interest".
  - It's about making it easier for them [population] to make a certain decision
- "if a particular unfortunate behavioral or decision making pattern is the result of cognitive boundaries, biases, or habits, this pattern may be "nudged" toward a better option by integrating insights about the very same kind of boundaries, biases, and habits into the *choice architecture* surrounding the behavior – i.e. the physical, social, and psychological aspects of the contexts that influence and in which our choices take place – in ways that promote a more preferred behavior rather than obstruct it." (ref)

# Behavioural Insights Team (BIT) aka "The Nudge Unit"

- Set up in 2009 by David Cameron (now privatised) led by DR David Halpern & Owain Service
  - See book: "Inside the Nudge Unit" by David Halpern & Owain Service (in library)
  - See the BIT website
- Similar units now set up by other govs around the world
- E.g. of govs use of nudging:
  - UK Pension Policy – not enough people saving for old age – gov made employers establish "automatic enrollment" pension schemes in 2012
  - Meant that employees were automatically put in their company's pension scheme unless they formally requested to be exempted.
  - The "nudge" – theory was that most people *wanted* to save for retirement but perceived that the process was too complicated and/or they didn't have time to sort it out – so the nudge was making it easier to do what they wanted to do anyway
  - Did it work? 2012 – 2.7 million people enrolled in pension schemes. 2016 – 7.7 million!
- Behaviourial science experts have been used a lot to direct behaviour during the Covid crisis - https://www.bi.team/our-work/covid-19/

# Some concerns about nudging

- Criticised as being “paternalistic”
  - people in authority making decisions (usually for the best) for other people rather than letting them take responsibility for their own lives
  - Nudging sometimes known as “soft paternalism”
  - But option to “opt out” is always available
- Worry of science being utilized by potentially biased policy makers to manipulate citizens
- Who “nudges” the “nudgers”?
- Nudges should be transparent & open NOT hidden & covert
- Should *always* be an element of choice in the nudge, if there isn’t its not a nudge!

# Nudging and cybersecurity

- Key paper: Acquisti, A., Adjerid, I., & et al. (2017). Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computer Surveys*, *50*(3), Article 44.
- Link between UX design and potential cybersecurity nudges
- Nudging intervention should be regarded as complimentary to traditional education and training approaches:
  - Providing feedback in a system or app - suggestions for beneficial actions, along with an explanation why those actions were suggested.
  - users can benefit if they are given relevant information to make decisions, including the available options and the expected results.
  - By using "known metaphors," e.g locked doors and bandits, in warnings, users were better informed about risks and made more security-protective decisions

# Nudging and cybersecurity cont

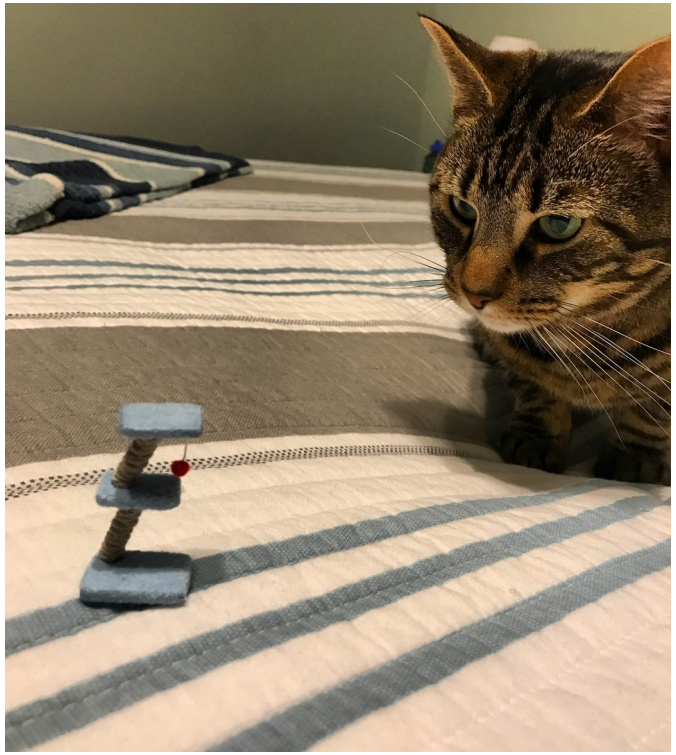
- Permission requests that included an explanation were more likely to be approved
- Password meters, shown as the user creates the password, can be effective nudges in helping users create more secure passwords by providing immediate feedback on password strength
- Ordering – the order in which options are presented impacts users behaviour – i.e. the 1st piece of info affects a user's perception of the other options available
- Status-quo bias – people tend to stick with the default settings – this can be used in nudging users decisions
  - Lack of time and knowledge found to be barriers to customizing software
  - Designers should set defaults that protect information of users
- Rewards & punishments – virtual badges have been found to be a strong incentive for users

# Other useful journal articles

Shelia M. Kennison, Ian T. Jones, Victoria H. Spooner, D. Eric Chan-Tin; ”Who creates strong passwords when nudging fails”, *Computers in Human Behavior Reports*, Volume 4, 2021, 100132, https://doi.org/10.1016/j.chbr.2021.100132.
Zimmermann, Verena; “The Nudge Puzzle Matching Nudge Interventions to Cybersecurity Decisions” *ACM transactions on computer-human interaction* 02.2021 Volume: 28 Issue: 1 Page: 1-45 DOI:10.1145/3429888
A search of “nudging” AND “cybersecurity” on the library website will bring up lots of resources.

# “Negative” nudges (i.e. those used by orgs or cyber-criminals)

- Not changing default settings – have been exploited by some companies to encourage users to make unintended purchases
  - Downloading unwanted anti-virus software or a “default” browser toolbar
- LinkedIn, display progress bars on a user’s profile indicating “profile completion” to nudge users to disclose more information



# Nudges & ISA campaigns

Nudges can be used as part of **Information Security Awareness (ISA)** campaign
Security awareness training is a formal process for educating employees about computer security. Or:
“Systematically planned interventions to continuously transport security information to a target audience”.
Usually part of a more comprehensive training and education programme

- Training – teaching new skills
- Awareness – focussing attention on a specific issue or set of issues

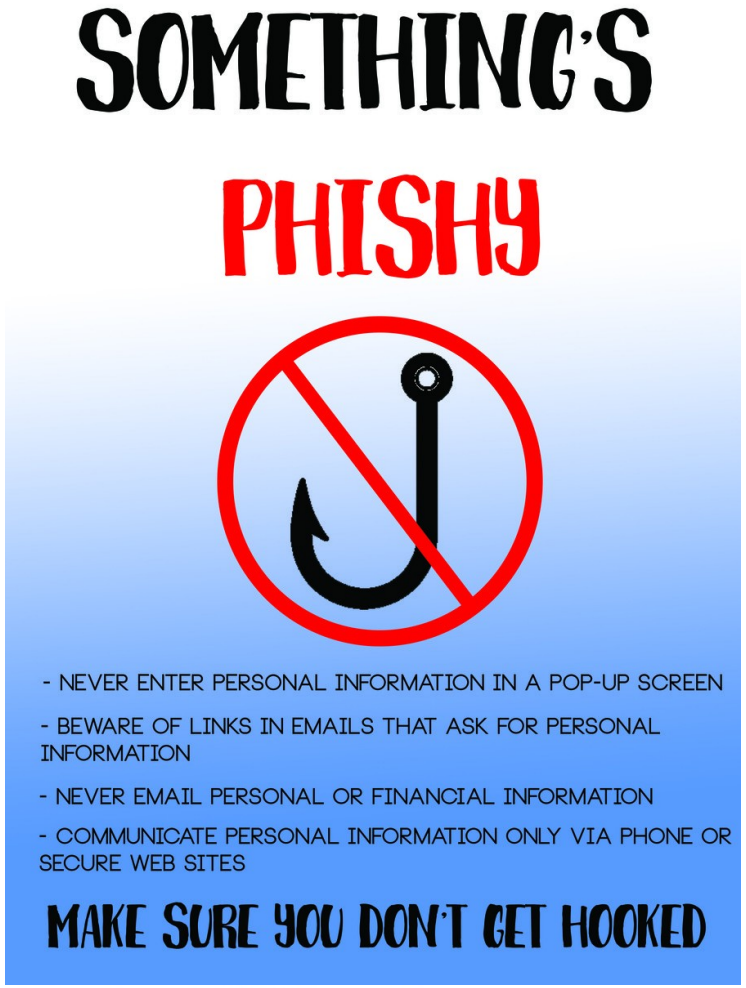
Can involve:

- distribution of messages via, e.g. pamphlets, e-mails, intranet pages, screen savers, posters, mouse pads, and pens to games, formal presentations, lunch meetings etc

# ISA campaigns

- Restricted Intelligence



# What is the difference between ‘education’ & ‘training’?

- **Training**:
  - Learning a specific set of *skills*, usually for employees
  - Tested by observing if they are putting the skills into practice
- **Education**:
  - Usually a plan of specific learning around key concepts, principles etc i.e. *knowledge* about a particular subject
  - Assessed via some sort of approach that requires application of that knowledge e.g. exams, written assignments, oral discussions (viva voce)
- In the workplace this usually involves a combination of the two approaches, e.g. password security
  - Training – *how* to come up with a secure password
  - Education – *why* doing so is important

# Education & training programmes

- Can be bought “off the shelf” e.g.
  - https://www.infosecinstitute.com/skills/skillset-is-now-infosec-skills/
  - https://www.itgovernance.co.uk/shop/product/information-security-staff-awareness-e-learning-course
  - Cheapest option is via e-learning but organisations will also come into the workplace to deliver courses
    - Ethical issue – should an employer give paid time off during the working week or should en employee be expected to undertake the training in their own time?
- Or “do-it-yourself” in-house
  - Requires knowledge in how to construct a program of learning, delivering and assessing it.
- Aka SETA (Security Education Training and Awareness)

# What does the research say?

- Search ("*information security training and education*") on the library database from 2014 onwards revealed:
  - 5,187 results
  - So a *lot* of work has gone into this subject
- Everyone is in agreement that this important, but
- Less so on *how* to do this well for best effect

# Recent research cont

- Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, *34*(4), 757–778
  - Found that education programs based around *theory* (i.e. based on educational theory – constructivist) got positive results and that training should utilize content (i.e. theory about the subject) and methods that activate and motivate learners to systematically process the information they receive during the training.

# Research cont

- Ayyagari, Ramakrishna & Figueroa, N. (2017). Is Seeing Believing? Training Users on Information Security: Evidence from Java Applets: *Journal of Information Systems Education*, *28*(2), 115–122.
  - Interesting study looking at the impact of users deeper understanding of the “why” behind the need to do a particular info sec behaviour

# Research cont

Alyami, A., Sammon, D., Neville, K. and Mahony, C. (2024), "Critical success factors for Security Education, Training and Awareness (SETA) programme effectiveness: an empirical comparison of practitioner perspectives", *Information and Computer Security*, Vol. 32 No. 1, pp. 53-73. https://doi-org.ezproxy.tees.ac.uk/10.1108/ICS-08-2022-0133.
Found:

- SETA can “produce questionable results around effectiveness”
- Identified 5 CSFs for SETA programmes;

1. raise employee IS/cyber security awareness and knowledge to enhance organisational maturity
2. evaluate employee performance at a frequency that aligns with the organisational IS/cyber security strategy
3. secure top management support to encourage all employees to comply with IS/cyber security policy
4. avoid a one size fits all approach to programme content to promote employee engagement
5. appreciate employee cultural differences to shape programme content

# Ideas about learning

- Behaviourism – instruction led, one-way interaction, specific, measurable and observable objectives. (passive)
- Constructivism – interactive, two-way communication, activates learners' own thinking processes, critical reflection of learners' own knowledge, conversational forms of evaluation (active)
- Importance of motivation
  - Extrinsic
  - Intrinsic

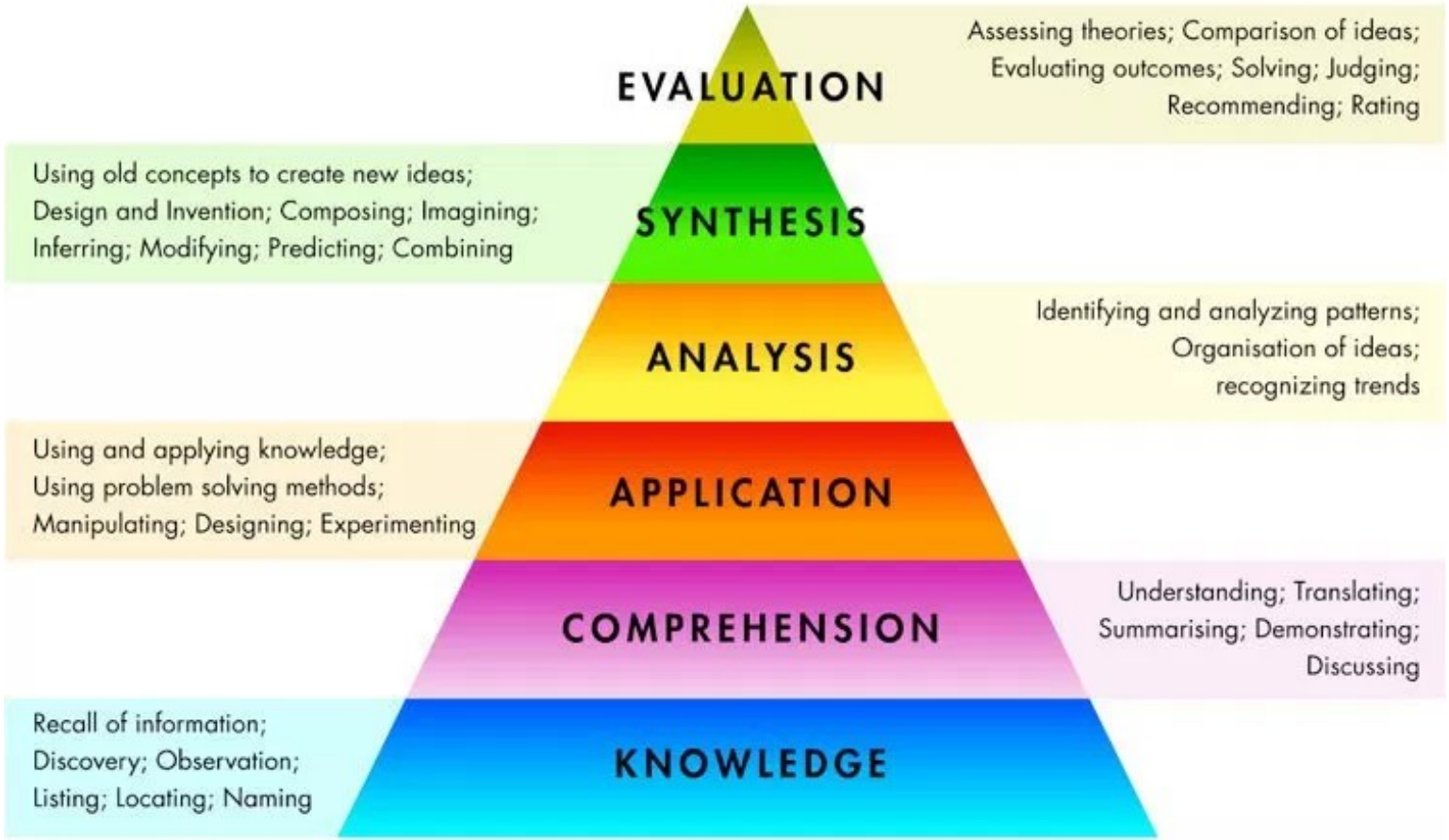
# Designing a training/education programme

1. Decide what behaviour you want to change
   a) Don't try and do too much all at once – prioritise
   b) How many sessions do you think you might need?
2. Determine the Learning Outcomes (LOs) for each session
3. Plan & prepare training:
   a) Behaviourist or constructivist? A bit of both?
   b) How will you appeal to different types of learners?
   c) Prepare materials
4. Deliver training
5. Evaluate learning
   a) how will you determine if the learners have achieved the LOs?
   b) What will you do about learners who don't achieve the LOs? (imp ethical question)

# Writing Learning Outcomes

- Usually written in terms of what the learner will be able to do at the end of the learning session:
  - E.g. see LOs for this module
- The *words* you use are very important
- Bloom's Taxonomy – see next slide

# BLOOMS TAXONOMY



# Using Bloom's Taxonomy to write LOs

- See:
  - https://tips.uark.edu/using-blooms-taxonomy/
  - https://technologyforlearners.com/applying-blooms-taxonomy-to-the-classroom/
  - You also need to think about how you will measure/judge if the LOs have been met or not
  - Think about the verbs you've used:
    - Describe? Evaluate? List? Etc
- How do you *measure* that these have been achieved?

# Conclusion

- A lot covered this week, for part 2 of the ICA think about what types of training or nudges the organisation might need (the "what" should come from your risk assessment)
- Ethically training is very important for an org (also legally but we will cover this in a later lecture) – employees need *appropriate* ***quality*** training to do their jobs
- If you want to read more on this topic, try exploring the articles I have mentioned (available in the module Reading List).
- Next time (with me) – information security systems frameworks, standards & policies – very important!