Bruce Schneier popularised the concept in 1999: cyber security is about people, process and technology. Yet almost two decades later, the industry still focuses so much more on technology than the other two dimensions of our discipline. For a long time, when the cyber security community has considered the human nature of cyber security, it has been within the context of a narrative that ‘humans are the weakest link’. However, it might be more accurate to say that understanding humans is the weakest link in cyber security. Looking to behavioural economics, psychology and sociology, we can understand cognitive biases and how we can better engage people to improve cyber security awareness, behaviour and culture.

Social Proof

*When people don’t know how to act, they assume the behaviour of others.*

- Messaging in cyber security is usually how bad everyone is at cyber security, which essentially psychologically drives the message “everyone else is terrible at this stuff, so it’s ok for you to be terrible at it too!”
- If we want to encourage people to practice more secure behaviours online, we need to start highlighting the positive behaviours of others
- E.g. if you run a phishing exercise, it will be more effective to promote the number of people who *did not* click the link than the number who *did*

**Lesson 1: Get social proof on side**

The Optimism Bias

*People underestimate the likelihood of bad things happening in their future and overestimate the likelihood of good things happening.*

- “We’ll never get hacked”
- When faced with a non-technical person who displays this kind of stubborn optimism, many cyber security professionals respond by trying to use facts
- Psychologically, optimism is more powerful than facts

**Lesson 2: Harness optimism**

The Psychology of Fear

- Fear does not motivate people to take action
- Research shows that anticipation of pleasure is much more powerful in changing behaviour than anticipation of pain, and so rewards are more effective than punishments at influencing people (Sharot, T., 2017)

**Lesson 3: Spread hope not fear**
The Human Nature of Cyber Security  
Dr Jessica Barker, Co-Founder, Redacted Firm  

The Stereotype Threat  

*The burden of a stereotype makes people unintentionally confirm it.*

- If people enter a situation in which they know they are the subject of a stereotype, knowledge of that stereotype will be such a burden and distraction that they are likely to unintentionally end up confirming it
- Actively challenging the stereotype removes the burden and frees the subject to concentrate on the task in front of them
- A stereotype that ferociously dominates this industry is that “users are stupid”; instead of undermining people, let’s start spreading a more empowering message.

**Lesson 4: Resist stereotypes**

**Self-efficacy**

*A person’s belief in their ability to succeed in specific situations or accomplish a task.*

- Empowerment drives self-efficacy, and self-efficacy drives better behaviours
- Give people the encouragement and the tools they need to practice more secure behaviours
- For example, if you haven’t already, implement a ‘report a phish’ button in your corporate emails so that people have a quick and easy way to report suspected phishing emails. We are trained to click, we don’t like emails sitting in our inbox, we want simple tools to support us.

**Lesson 5: Raise self-efficacy**

**References**


Oliveira, D et al (2008) 'It’s the Psychology Stupid: how heuristics explain software vulnerabilities and how priming can illuminate developer’s blind spots’ ACSAC pp. 296-205


