

Security Awareness is Dead! Long Live Security Awareness!

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 runs 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 Stereotype Threat

The burden of a stereotype makes people unintentionally confirm it.

- If I enter a situation in which I know I am the subject of a stereotype, knowledge of that stereotype will be such a burden and distraction that I 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

- Bargh JA, Chen M, Burrows L (1996) ‘Automaticity of social behavior: direct effects of trait construct and stereotype-activation on action’ *Journal of Personality and Social Psychology* 71 pp. 230–244
- Goldstein, N. J. et al (2008) ‘A room with a viewpoint: Using social norms to motivate environmental conservation in hotels’ *Journal of Consumer Research* 35 pp. 472-482
- 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
- Rhee, S-K et al (2009) ‘Self-Efficacy in Information Security: its influence on end users’ information security practice behavior’ *Computers and Security XXX I-II*
- Sharot, T. (2012) *The Optimism Bias* [video file] retrieved from https://www.ted.com/talks/tali_sharot_the_optimism_bias
- Sharot, T (2017) *The Influential Mind* (Little, Brown, London)
- Spencer, S. J et al (1999) ‘Stereotype Threat and Women’s Math Performance’ *Journal of Experimental Social Psychology* 35 pp. 4–28