Seminar 3: Developing Positive Security Culture in an Organisation

During this week's seminar, we will be working through an example of applying a social marketing approach and mental models to develop a security awareness programme. It would involve students working in groups for 15 minutes and regrouping to present a communication strategy.

To prepare for the seminar, ensure you have:

- Reviewed all the lecturecasts in this module.
- Read the articles provided in the reading list for this unit.
- Read the article by Ashenden, D. & Lawrence, D., (2013) Can we sell security like soap? A new approach to behaviour change. In *Proceedings of the 2013 new security paradigms workshop*. 87-94.

Then **reflect** on:

- The methods employed in this article.
- Are the methods transferable?
- How can the methods be adapted to suit our context?

---

1. The methods employed in this article

The article strives to:

- define clear targets for behavioural change
- understand self-reported end-user behviour
- develop an exchange proposition satisfying both of the above to chance behaviour
- develop an effective intervention
- evaluate its success in changing behaviour.

2. Are the methods transferrable?

Yes, especially if the transtheoretical model is applied. Understanding the psychological motivators or deterrents of end users is critical for passing on information. We cannot assume what people should need to hear in order to change behaviour. If we define what we would like to change in workforce bahviour, and then understand the self-projected behaviour of the individuals which make up that work force, we could design a campaign which encompasses " pre-contemplation of the need to change, to contemplation of behaviour change, and then from preparation for chance to taking action" (90).

The training should see the 'product' of the social marketing campaign as the benefit derived from the behaviour change – that is the exchange proposition. It is true that rewards and consequences which do not outweigh the benefits of non-compliance and ineffective, so fostering motivation through marketing tactics could be very successful.

The design of this 'product' will determine its efficacy. It should include education to create awareness, clear expectations of the environment and processes for change, clear demonstrations of sanctions for non-compliance, services that support new behaviour, and messages that communicate and the new behaviour.

Evaluation should be robust but ethical, without crossing privacy boundaries or putting undue pressure on individuals to perform in overtly controlled manners.

3. How can the methods be adapted to suit our context?

One example of how this could work in an anti-phishing campaign comprises the following:

1. define the diminutive goal: we want people to check sender addresses and ask supervisors if the sender if unknown to the recipient.

2. conduct a survey of reported behaviours and expectations surrounding phishing

3. The exchange proposition could tap into the need to look competent at work, the desire to help, and the desire to be liked – if double checking unknown senders leads to an actual case of phishing, there could be a reward there – maybe extra vacation time, a project veto vote, or something else that would be desirable.

4. The intervention would be comprehensive training about phishing techniques and prevention, and then unveiling the diminutive goal: if you see something phishy tell your boss, and if it’s real you get a reward. The slogan could be “Catch a Phish, get a wish” or something like that. Signs could be put up in the office to reinforce the benefits of the behaviour.

5. Based on the number of reports vs the number of actual caught fish along with report rates of actual phishing successes over time would reveal if the campaign was successful or not.