Red flags™ from ThinkCyber

Science applied: how to motivate users to do security training

Why do 90% of cyber attacks start with a human user? Behavioural Science theories give us a clue to the reasons, and ideas on what we can do about it.

Standard economic theory used to hold sway in its suggestion that we make decisions in a purely rational, selfish, way. It is now well established, however, that the reality is somewhat more complicated than that. The field of Behavioural Economics provides multiple theories that can begin to predict these less-than-rational behavioural choices.

Protection Motivation Theory

At ThinkCyber, we are constantly exploring new approaches to delivering security awareness. In a project supported by Innovate UK, we explored Protection Motivation Theory, one of the most thought-provoking theories.

The theory suggests that we make two assessments when making a decision under threat. The first assesses the threat in terms of perceived severity and our perceived vulnerability to it. The second assesses our capacity to cope with the threat in terms of our ability to respond effectively, and the cost to us of making that response.

While it is interesting to consider security decisions with this threat/coping framing, of far greater relevance is the fact that the most recent research into the application of this theory in the security context suggests the importance of accentuating coping over threat. As Pam Briggs, Professor and Chair of Applied Psychology at Northumbria University puts it, “we shouldn't focus on the threat (scaring people), but instead focus on building up people's confidence and knowledge in knowing what action to take (the 'coping appraisal' part)".

Science Applied: Current approaches to security awareness

Clearly Protection Motivation Theory is just that: a theory. It's a simplification of the complex realities of human cognitive processes. However, that doesn't mean it's not useful, and the idea of placing greater emphasis on the coping component is not only interesting from an academic perspective but can also be directly applied to how we think about influencing people's security behaviour.

Considering the theory against our experience of current approaches to security awareness, we observe that:

- They focus primarily on the threat and do too little to address effective and actionable coping mechanisms.
- Over-complex security instructions may even risk negatively impacting people's perception of their ability to make good decisions, whilst also increasing their perception of the cost (in other words 'effort') of doing the right thing.

In short, getting the approach and emphasis wrong risks removing people's motivation to do the right thing – increasing the likelihood that they just (for example) cross their fingers, click the link and plead ignorance after the fact!

Science Applied: Triggering our protection motivation

So, what does this mean for practitioners developing security awareness training courses? For us the theory suggests the following:

- *Just enough 'threat'.* It's important that people have enough of an appreciation of the threat for coping mechanisms to come into play. After all, if people don't recognise they are under threat, a coping mechanism is irrelevant. But don't overdo it, and make sure people understand how they personally are vulnerable.
- *Make it actionable*. Ensure that information about the threat is accompanied by practical 'coping' information about steps people can take to deal with it. As a basic example in the context of phishing, simply encourage people to, if they're not sure about an email, consult colleagues or those with expert knowledge (if present in the organisation). Alternatively, ask people to take simple steps to verify suspect emails – for example, by picking up the phone, or by logging into relevant accounts without acting on email links.
- *Keep it simple*. Ensure that security instructions are realistic, and perceived as low cost, for the typical user. And make them memorable. Don't expect people to become security experts.

We believe the focus should be on creating an enduring, but appropriate, level of security awareness. We would advocate thinking hard about the degree of expertise we expect people to have and whether it is realistic; and then making sure it goes hand in hand with effective, simple and memorable coping mechanisms.