The G-I of Cyber Security

Karen Renaud, University of Strathclyde, Scotland (www.karenrenaud.com)

I have gained inspiration from the Human Factors in Diving[1] community to start an "***A-Zs of cyber security***". Last month, we did D to F; now let's see what the next three letters teach us.

G: Goal Fixation. It is all too easy to get fixated on your primary goal, to such an extent that you miss clues that would alert you to danger. Consider someone really wanting to process emails as quickly as possible. That goal can easily become so uppermost in their minds that they miss a Phishing email and open a dodgy attachment.

Organisations can unwittingly incentivise goal fixation. For example, if they make a promise to customers that all emails will be responded to in a certain number of hours, employees are pressured and miss cues. This could also lead to a reticence to point out security issues because of pressure to be productive above all else.

The primary goal of all employees ought to be security, and this means giving employees the time, space and permission to carefully consider what they are doing.

H: Helping Others: Cyber security is so bound up with authentication, given that every single computer user authenticates themselves, mostly with a password, multiple times a day. One of the core pieces of advice related to passwords is that they ought not to be shared with anyone. This might instil a sense of "going solo" in people's minds. However, other aspects of cyber security have different characteristics, and asking for or giving help is highly desirable. Consider, for example, when someone receives an email that they're concerned about: to click, or not to click, that is the question. Asking someone else is eminently better than winging it.

I wrote, in one of my previous columns, about cybersecurity being a team sport. Organisations ought to consider allowing people to volunteer to be the local "cyber champion": one in each department and division. This might be someone who has a particular interest in cyber security, or someone who wants to upskill in this area. Their role is to support other employees in a non-blaming, non-shaming way. Mistakes are merely evidence of our humanity. Imperfections should be tolerated with empathy, not condemned.

Cyber security is challenging, and organisations should ensure that employees have all the support they need to resist the efforts of cyber criminals.

[1] https://www.hf-in-diving-conference.com/

I: Imagine: There are two dimensions to imagining: (1) how could someone be trying to deceive me? and (2) what example am I setting to others in the organisation?

The first relates to putting yourself in an attacker's shoes to anticipate how they might be trying to persuade you to take an insecure action.

The second is illustrated by a personal anecdote. Yesterday, I was waiting for the green light to cross the road. There were only a few cars and I realised I could cross quite safely even though the red man was still showing. Then, I noticed a young girl next to me waiting patiently for the green man. I realised that crossing on the red man could impact her future safety if she followed my lead and disregarded the safety signal. How much more can our behaviours be observed by our colleagues at work? Each and every employee should be **seen** to behave securely, so that the norm becomes "Here, we behave securely in the cyber domain".

Join me next month as I continue my meander down alphabet lane, with J to L.