A user by any other name

Karen Renaud
Verena Zimmermann

A User by any other name

Karen Renaud & Verena Zimmermann
Abertay University & Technische Universität Darmstadt

The cyber security field can be characterised by its silos, differing from each other based on levels of cyber security expertise. In many organizations, one silo contains the security specialists, one the IT staff, another the employees and yet another the customers. Members of the last two silos, who generally do not have high levels of expertise, are often collectively called "users" and might be referred to as "the weakest link" or "the enemy of good security" by those in the higher skilled silos.

It is worth considering the impact of these silos on the general state of cyber security.

First, outside the IT context, where else do we use the term "users"? "Illegal drug users"? "Alcohol users"? The negativity of this usage might well be leaching into the term "computer users". Some researchers believe that labels influence people's behaviours. This "labelling theory" is not universally embraced, but some researchers certainly believe that negative labels can cause damage. It might be time to start thinking about replacing the term "users".

Second, the term "user" implies a certain passivity. They are not actively involved in security development and decision processes, nor do they expect to be. Rather, the term denotes a passive acceptance of whatever the "experts" judge to be appropriate. The consequence is that cyber security becomes someone else's problem.

Third, in any situation where people are allocated to groups, between-group animosity becomes likely. The pejorative terms sometimes used to describe the average computer operator, such as "lazy", "blissfully unaware" or "unmotivated", might well be a symptom of this.

Fourth, think about how you feel if someone laughs at you for making an honest mistake, especially when there is a hint of derision or superiority in the laughter. People do not like being humiliated, and could react by putting their head in the sand and refusing to engage with any cyber security activities at all. Others might deliberately subvert security measures.

In summary, by assigning a label, which might be perceived negatively by anyone who lacks expert knowledge, we effectively exclude them from being part of the security solution. In a way, we are treating them as "a problem" whose behaviour needs to be "solved". One can see evidence of this if you look at how some organisations are more focused on compliance, than on commitment and collaboration, when it comes to security.

The first thing we should do is to stop blaming non-experts for honest mistakes. A friend, who knows more a lot about Phishing, fell for a carefully-crafted Phish. She had signed up to be part of a Phishing study, so she was expecting such an email to appear. She was still deceived. It really can happen to anyone. Phishing does not succeed because people are lazy or uninformed – it succeeds because we are human. Such humanity should be accepted and celebrated, not denounced and crushed.

Secondly, we should find a way to break down the silos. We have to encourage experts and non-experts to see each other as team members working together to secure the enterprise's information resources. This new mindset has been applied very successfully in other contexts, and we should find a way to do it in cyber security too. This will recognise the role of every single person in securing an organisation's information assets. A first step might be to call *everyone* interacting with IT technologies something like "netizens" (interNET citIZENS), regardless of their level of expertise.

The aim is better organisational security, something we ALL want.