BIZCOMMUNITY

Do our personality traits matter when it comes to cybersecurity?

By Anna Collard

6 Jun 2019

In the digital era, cybercrime is a high-stakes business, with criminals constantly upping the ante in a bid to gain access to valuable data. Criminals know it's easier to hack a human than trying to break through sophisticated security technology and have consequently become very good at it. The art of "people hacking", or social engineering, uses psychological techniques to trick people into revealing information, installing malicious software or participate in scams.

Anna Collard, managing director and founder of Popcorn Training

Certain personality traits seem to make us more or less likely to fall prey to specific attacks or scams. According to “Scam Compliance and the Psychology of Persuasion” people who are more likely to fall for scams do not seem to be in general poor decision-makers, for example, they may have a successful business or professional careers. It also has nothing to do with age or sex.

However, their personality makes up does determine why some people simply seem to be unduly open to persuasion and are easier prey than others. Research recently conducted confirms this.

Through the support of the Sanlam Group, Popcorn Training - a KnowBe4 company, developed a personality traits assessment combined with security general knowledge and behaviour questions called the “Cyber Strengths Test”.

This test was delivered via an online questionnaire rolled out to the Sanlam Group companies as well as some of Popcorn Training's South African enterprise customers and their users, with over 12,000 responses to date. We analysed a total of 12,459 unique and anonymised responses and compared how the “bad” and “good” security scorers fared by personality traits in the hope of finding a correlation between personality profiles and their security scores.

Three personality traits out of the Big 5, were particularly interesting, as they were linked to security behaviour in various other research papers. These are:

- **Conscientiousness** - describes a person's tendency to be organised and goal-oriented and shows awareness of the impact that their own behaviour has on those around them
- **Neuroticism** – emotional sensitivity and self control
- **Openness** – reflects the degree of intellectual curiosity and creativity

For example, highly conscientious people may be more vulnerable to scams impersonating authority figures. And people with a high degree of sensitivity may be more likely to react to scams that play on their anger or fear.

We set out with the hypothesis that a strong security profile is someone with a high degree of conscientiousness, a low degree of neuroticism and high openness. And a weak security profile is the inverse, i.e. someone with a low level of consciousness, high degree of neuroticism, and low openness. The results were fascinating, in that the percentage of bad security scorers was significantly higher amongst the risky personality profile.

In turn, stronger personality profiles had significantly better average security scores. Significance testing showed a definite dependency between the personality profiles and their security scores. For security awareness professionals, this provides an indication of higher risk users which can feed into a prioritised training and awareness plan.

We have to keep in mind that context influences how people react, and someone with what may be considered a “low risk” personality profile may be just as likely to fall victim to scams when put under pressure, when in a rush or when faced with a cleverly crafted targeted attack that is very convincing.

Using security assessments that check a user’s current level of cybersecurity understanding, as well as mock phishing results, are a powerful way to identify gaps in security awareness behaviour. Ensuring subtle continuous awareness messages are spread throughout the company on at least a quarterly basis, as well as creating targeted training interventions for the more vulnerable groups is an effective way in changing behaviour in the long run.

Take action

Other actions that can be taken include:

- Increase security awareness on social engineering scams by making use of phishing simulation and training platforms.
- Make it easy for your users – allow them to report phishing emails easily and provide quick feedback loops
- Help change user behaviour: awareness is a bit like flossing, it's a continuous communication project
- Targeted training - Use pre-assessments to determine risk profiles and remediate/conduct more intense training for

repeat offenders

ABOUT THE AUTHOR

Anna Collard is the managing director and founder of Popcorn Training