Detecting and preventing cyber-scams

Monica Whitty
University of Melbourne

Cyber-scams are any type of fraud that exploits mass communication technologies to trick people out of money. Examples include: foreign lotteries, '419' scams and romance scams. In the UK in 2016, it was reported in the England and Wales Crime Survey that citizens are 10 times more likely to be robbed while at their computer by a criminal based overseas than to fall victim of traditional theft. These scams cause both financial as well as psychological harms. This paper provides a theoretical framework to explain why some individuals are tricked out of their money. The framework accounts for the profile of the victim, including: psychological characteristics (e.g., impulsivity), belief systems (e.g., romantic beliefs, beliefs about invulnerability) and routine activity behaviours (e.g., online behaviours). It also takes into account the persuasive and deceptive techniques employed by criminals (e.g., creation of false identities, norm activation, sales techniques, etc.). Furthermore, the affordances of the space are considered. Importantly, the framework is not a one size fits all approach, but also considers the qualitative and quantitative differences between cyber-scams. Based on the research projects I have been leading on I will also be proposing some strategies and recommendations to prevent and detect cyber-scams.