Does simulating a serious information security threat cause a user's self-efficacy to increase, with regards to the fear appeals of Protection Motivation Theory?

Mark Shaw
Newcastle University

1 Structured Abstract

Background. Protection Motivation Theory (PMT) and the Extended Parallel Process Model (EPPM) have been used to demonstrate that fear appeals can perform a dutiful role in motivating users to increase their self-efficacy regarding Information Security (ISec) concerns. Currently, there is very little research into whether having a user be confronted with a threat that they perceive to be real, the realisation that the threat is not threatening should allow for users to increase their perceived susceptibility of ISec threats, thus allowing users to increase their self-efficacy. @Articleâ, author = â, title = â, journal = â, year = â, OPTkey = â, OPTvolume = â, OPTnumber = â, OPTpages = â, OPTmonth = â, OPTnote = â, OPTannote = â

Aim. Does simulating a ransomware attack on a user increase the user's self-efficacy with regards to Information Security?

Method. A blind study was carried out on two groups of N subjects. During the study, one group experienced a simulated ransomware attack, the other did not. A questionnaire was then completed by the groups, and ISec concerns were measured and compared across groups.

Anticipated Results. We anticipate that the users who experience the simulated ransomware attack will show greater concern for information security, compared to the control condition.

Anticipated Conclusions. The Limited Parallel Process Model predicts that users who experience a threat have heightened levels of perceived susceptibility, which should in turn allow for these users to have raised self-efficacy. The study will investigate whether the relief that comes from the realisation that the threat was simulated is enough to positively enforce self-efficacy.