12-11-2016

Familiarity with threats, Internet experience and user behaviors

Debora Jeske
University College Cork, d.jeske@ucc.ie

Paul van Schaik
Teesside University,, p.van-schaik@tees.ac.uk

Familiarity with threats, Internet experience and user behaviors

Debora Jeske
University College Cork
d.jeske@ucc.ie

Paul van Schaik
Teesside University, UK
P.Van-Schaik@tees.ac.uk

ABSTRACT

The degree of familiarity with threats is considered as a predictor of Internet attitudes and security behaviors. Cross-sectional data were collected from 323 student participants using an online survey, with 169 participants located in the USA and 154 in the UK. Several analyses were conducted. Cluster analysis to examine familiarity with threats and everyday Internet behaviors. This was followed by mediation analysis to examine the link between time spend on the Internet and Internet experience as indirect predictors of the security precautions taken. This relationship was predicted to be mediated by familiarity with threats and Internet behaviors.

The results showed the following. First, we found significant differences in familiarity between the national samples in relation to social engineering and phishing. Cluster analysis identified three distinct groups: the experts (cluster 1; n = 103) who were very familiar with the 16 threats and 2 everyday Internet behaviors, clusters 2 and 3 (n = 90) who were less familiar with recent threats, and others who were less familiar with established threats (n = 98). The two clusters composed of participants who were less familiar with threats, were also significantly less likely to use security features on their computer to protect themselves from threats in comparison to experts. Security actions included the use of anti-virus, firewall, anti-spyware, and the use of software and security updates.

Second, time spent on the Internet and the length of Internet experience were significant predictors of familiarity and significant indirect predictors of security behaviors behaviours (suggesting a relationship fully mediated by familiarity). This means that experience influences threat familiarity – and via familiarity – predicts subsequent use of security actions. The results suggest two insights. Based on the cluster analysis, we note that familiarity may vary depending on the type of threat. This may be due to a lack of familiarity with threats because these are novel and users have not been exposed to them. In other words, while users may report they are aware and have knowledge of threats – this does mean they are equally familiar with different threats and online behaviors. In addition, familiarity may account for the relationship between past time and experience and subsequent adoption of security.

On a practical level, the findings have two implications. First, awareness may not be as informative as threat-specific familiarity. Second, since familiarity is an important predictor of security action, it may be important to consider how familiarity may be increased. Users need to know about threats as soon as they emerge in order to reduce the initial period of heightened vulnerability.

Where does this leave IT and those responsible for training? We propose that situated learning – learning by doing and learning about new threats and tools – may be essential. This kind of approach would require users to not only learn about threats in an abstract manner (e.g., news bulletins from IT), but also through learning-by-doing approaches (such as simulated learning exercises). This may allow them to see and experience the outcomes of the threat (which often stay very abstract) and help them understand the role of certain security measures to fight them (in scenarios such as simulations). This approach may foster a better understanding of how this threat relates to them, supporting familiarity and increasing subsequent use of security options.

The columns on the one page abstract should be of approximately equal length.