Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Familiarity with Internet threats: Beyond awareness

Debora Jeske [a,*], *Paul van Schaik* [b]

[a] *University College Cork, Ireland*
[b] *Teesside University, United Kingdom*

ARTICLE INFO

Article history:
Received 11 December 2016
Accepted 29 January 2017
Available online 3 February 2017

Keywords:
Internet experience
Familiarity
Internet threats
Computer behavior
Cluster analysis
Mediation

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 about their familiarity about 16 different Internet threats. All participants were presented with definitions of threats and then asked to state how familiar they were with each. Their responses were then used to identify the extent to which threat familiarity differed among the sample. Three different clusters were identified. One set of participants were relatively knowledgeable about all threats. Cluster 1 was therefore labeled experts ($n = 92$). Clusters 2 ($n = 112$) and 3 ($n = 92$) showed very different patterns as familiarity appeared to depend on the novelty of the threat (with one cluster showing more familiarity with well-known threats and the other more familiarity with new threats). Participants who were experts were more likely to engage in computer security behaviors than the other two groups. Mediation analysis showed that time spent on the Internet and the length of Internet experience were significant predictors of familiarity, and both were significant indirect predictors of computer security use (suggesting a relationship fully mediated by familiarity). Our paper makes several important contribution. First, the research reflects a systematic effort to investigate the relationship between the familiarity and engagement of online security activities. Second, we provide evidence that familiarity is a mediator between Internet use and security behaviors – making this a baseline variable to consider in terms of training on future threat-oriented interventions aimed at changing security behavior. This study also provides implications for practitioners to improve user familiarity of security risks.

© 2017 Elsevier Ltd. All rights reserved.

1. Introduction

The threat landscape of computer security is continuously changing and new threats are emerging all the time. As a result, users are likely to be familiar with certain online threats more than others. In order to anticipate how users will respond to future challenges, it is therefore increasingly important to understand how risk perceptions are formed (Bonneau et al., 2012; Garg and Camp, 2012; Huang et al., 2010). Various threats exist to user information, including public information sharing on social media, user surveillance, identity theft, phishing, viruses, spyware, trojans, and keyloggers (e.g., Rocha Flores et al., 2014). Examples of a very familiar occurrence are cookies which

* *Corresponding author.*
E-mail addresses: d.jeske@ucc.ie (D. Jeske), P.Van-Schaik@tees.ac.uk (P. van Schaik).
http://dx.doi.org/10.1016/j.cose.2017.01.010
0167-4048/© 2017 Elsevier Ltd. All rights reserved.

feature on many sites. These are text files that are designed to track user activity (BBC, 2011). Cookies may also be set by the browser or third-parties not associated with the browser (for more details see Opentracker, 2014). Due to press coverage regarding corporate privacy disasters (see Clarke, 2014), many users are exposed to information about these threats. However, some threats may be more recent and less known – which may also affect familiarity and thus potentially the extent to which security measures are taken by individuals. These include sophisticated spear phishing (targeted emails that include personal user details to convince users to provide specific information), keyloggers and rogueware. In addition to more traditional online security threats, a number of additional threats need to be considered. These include threats such as cat-fishing, cyber-bullying, social engineering and virtual stalking.

A number of researchers have studied the role of attitudes toward the Internet, and information hiding versus information sharing (e.g., Acquisti and Grossklags, 2004). Similarly, precautionary user behavior such as use of computer security features also requires a certain awareness and familiarity of the threats a user faces (see Dinev et al., 2009; Kruger et al., 2010). We differentiate awareness from familiarity as being aware of something may not necessarily indicate more than a fleeting degree of knowledge that a threat of a certain kind exists. Awareness alone may also be subject to repeated exposure, and thus subject to habituation which leads to less and less attention given to warning (Brinton Anderson et al., 2016). However, this does not guarantee that the user becomes knowledgeable or familiar with what the threat entails – they only recognize it. For example, individuals may be aware of email as a communication medium but not realize that it operates as a storage medium – and that even deleted emails may still continue to be accessible via their devices or cloud servers (e.g., Clark et al., 2015). So awareness of one function does not imply that the user really understands all functions – or threats. Threat awareness suggests individuals show realization, perception of knowledge of a threat – but this knowledge is not driven by experience and may not be very in depth. Attitudes and behaviors may be shaped by what users think they know, rather than their actual knowledge. As a result, awareness may be a precursor to familiarity. In contrast, familiarity is linked to knowledge in more concrete ways in that knowledge is knowing something through experience or association implying an understanding of a threat.

Unfortunately, many individuals are not cognizant of how much personally relevant information they share online (Kurkovsky and Syta, 2010), in line with a low familiarity with the threats that may arise. For example, threats may be dismissed if they appear to be unlikely to occur (no immediacy), the user discounts the possibility of being affected, or they feel competent and confident to tackle potential risks and handle the consequences themselves. These aspects have certainly been observed in relation to password management (e.g., Tam et al., 2010). Security countermeasures such as security policies, security education and awareness, and computer monitoring have also been proposed to affect perceived certainty and severity of sanctions and subsequent misuse of information systems (D'Arcy et al., 2009). This suggests that attitudes and user awareness of consequences play a significant role in determining how risks are perceived and responded to.

1.1. *A theoretical perspective to understanding threat familiarity: connecting the human and technical elements*

The difficulties associated with encouraging awareness to progress to actual knowledge and understanding of threats may be best explained using a framework as an explanatory metaphor. It is here that Actor-network theory (ANT; Latour, 1987) may help explain the reactions to, barriers and challenges that arise when we try to understand the many interrelated variables that determine security-related engagement and behavior (e.g., past experience, affordance of technology, and user attributes). A few comments are warranted to define the meaning and relevance of actor-network theory. First, ANT as proposed by Latour (1999, pg. 20) is a "very crude method to learn from actors without imposing on them on a priori definition of their work-building capacities." Second, it is important to avoid misunderstandings about the meaning of actors and networks as Latour conceptualizes these as interlinked, rather than opposites (hence the hyphen). The actor-network element of Latour's theory does not refer to a dichotomy that differentiates between agency and structure. While the actor does not represent a reflection of human agency, nor does the network element reflect society as such. Both are continuously transformed and redefined through the interdependent activities (Hassard and Alcadipani, 2010). Latour (1999, pg. 17) clarifies and states that network element captures all "interactions through various kinds of devices, inscriptions, forms and formulae, into a very local, very practical, very tine locus". Indeed, actors and networks are "two faces" of the same phenomenon (Latour, 1999). In other words, actor-network theory acknowledges and highlights the connections between both macro and micro level influencers of social processes (such as societal norms and culture vs. local and personal norms).

We propose that ANT is a useful approach to understand how threat familiarity relates to online behaviors (e.g., those that shape Internet experience and online engagement) and the adoption of security behaviors. First, ANT clearly rejects the separation of the human, non-human, technical elements and the social elements (Hassard and Alcadipani, 2010) that drive user behavior in various domains. When we focus on the user alone (e.g., his or her attitudinal indicators), the technical (e.g., automatic processes rather than those that have to be started by the user) or the social influencers (e.g., social norms norms), we may only explain some of the variance in behavioral patterns; however, the interaction of these variables may be particularly informative. ANT therefore considers a combination of variables, in a similar fashion (but not exactly the same) as (many) other "models", such as ISO 9241 and the Person-Artifact-Task (PAT) model (see Finneran and Zhang, 2003). Security behavior is essentially the outcome of a combination of all these elements as well. For example, personal characteristics and propensity for risk may shape users' willingness to take risks when online. Technical features may protect a user to different degrees from threats, while social pressures and norms

دریافت فوری ← متن کامل مقاله

ISIArticles
مرجع مقالات تخصصی ایران

✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
✓ امکان دانلود نسخه ترجمه شده مقالات
✓ پذیرش سفارش ترجمه تخصصی
✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
✓ دانلود فوری مقاله پس از پرداخت آنلاین
✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات