Familiarity with Internet threats: Beyond awareness

Debora Jeske,

University College Cork, Ireland

Paul van Schaik

Teesside University, United Kingdom

Accepted manuscript. Published in Computers & Security 2017. Please cite as follows:

Jeske, D., & van Schaik, P. (2017). Familiarity with Internet threats: Beyond awareness. Computers & Security, 66, 129-141. doi: 10.1016/j.cose.2017.01.010

Corresponding author:

Debora Jeske, PhD, FHEA

School of Applied Psychology

University College Cork

Enterprise Centre, North Mall Campus

Cork City

Republic of Ireland

Email: d.jeske@ucc.ie

Familiarity with Internet threats: Beyond awareness

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 labelled experts (n = 92). Cluster 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 an important mediator between Internet use and security behaviors – making this an important 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.

Keywords

Internet experience; familiarity; Internet threats; computer behavior; cluster analysis; mediation

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; Camp and Garg, 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). An example of a very familiar occurrence are cookies which 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 towards 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 (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 as 'two faces' of the same phenomenon (Latour, 1999). In other words, actor-network theory (or ANT) 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 may also influence which activities the user pursues and which precautionary behaviors they adopt.

Second, as ANT suggests, entities and understanding emerge and gain meaning as the result of their interaction and relations with each other. Arnaboldi and Spiller (2011, pg. 645) note the following, in reference to Latour (2005) and Law (1992): "The increasing popularity of ANT arises from a pivotal, though controversial, feature: the symmetrical treatment of human and non-human actors, and of social and technical elements." This might indeed be particularly relevant to cybersecurity behaviors. The creation of threats and the effect of certain cybersecurity threats relies on the interactions of numerous technical and human aspects. For example, in the absence of precautionary tools and the users' unwillingness to engage with threats, negative outcomes due to

email harvesting or identity theft are also much more likely. This outcome may not be repeated if the precautionary behavior is prompted or prevention tools are automatically triggered, reducing the reliance on the user. However, such settings also reduce their control over their devices, which is why such mechanisms are not always readily adopted by the user. Familiarity with threats, either by direct exposure or experience, is likely to emerge as the result of an interplay between the users' technical experience (e.g., Internet use), their personal characteristics (such as Internet attitudes), and their behavior to date, especially when this is reinforced by social or technical means (such as the adoption of pre-cautionary behavior, which may be achieved through nudges or social norms).

Finally, ANT considers the importance of translation in terms of how various, potentially contradictory interests, are captured (Hassard and Alcadipani, 2010, pg. 10). This process further recognizes the role of stakeholders, the need for information sharing and evolution in terms of the roles that actors inherit (see also Arnaboldi and Spiller, 2011). Users are often, by default and unintentionally, designated as recipients of data security training – but not necessarily viewed as active participants. This set-up may ensure that training aims at raising threat awareness, but not necessarily foster actual familiarity with threats by involving users directly.

Nevertheless, ANT as an explanatory method to understand cybersecurity is still limited. For example, many will argue that the assumption of symmetry between human and non-technical elements is misplaced – and that in the context of cybersecurity, it may not be feasible to aim for such symmetry due to the challenges associated with keeping up one's knowledge of emerging and existing threats.

1.2 Rationale and Research Questions

A particularly relevant target group for interventions are university students as many are soon entering the workforce – and with that their lack of knowledge or awareness of online threats may represent an important knowledge gap that needs to be addressed in company inductions and training schemes. Learning what students know about threats is the first step to understand why and when they adopt computer security behaviors. In line with current knowledge and knowledge gaps, the present paper poses three questions.

The questions are as follows: how familiar are students with the various online threats and is this similar for UK and US samples (RQ1)? Dinev et al. (2009) noted that awareness of the threats posed by spyware predicted favorable attitudes towards protective information technology, but

that this relationship was more pronounced for the US than the South Korean sample in their research. This suggests that familiarity and thus awareness of threats may vary across countries. However, in this study we focus on similar cultures to assess the robustness of findings in the UK and a comparative sample from the USA. We propose that the two samples are unlikely to vary significantly in terms of their familiarity with threats. By extension of these findings, we ask if we can identify groups that are more or less familiar with certain new vs. well-known (established) threats (RQ2). We are particularly interested to learn how familiarity clusters relate to Internet attitudes and computer security (e.g., differences between the two subsamples or group clusters).

Third and finally, we consider a mediation hypothesis (see Figure 1). That is, to what extent is past Internet experience and familiarity with threats overall related to security measures being implemented by individuals (RQ3)? Previous research on risk and technology has found evidence in favor of the 'familiarity hypothesis' (Lee and Ho, 2015; Satterfield et al., 2009; Wogalter et al., 1991). Accordingly, the perception that the benefits associated with a particular technology outweigh its risks is positively related to people's extent of familiarity with the technology. This means prior experience, if linked to familiarity may also have implications for the security measures that are being implemented by individuals – in support of a mediation model.

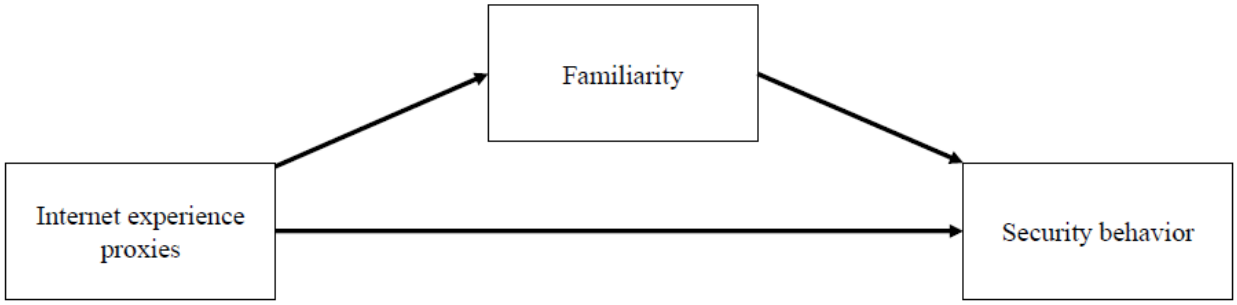

Figure 1: Proposed mediation model

2. Method

2.1 Recruitment and Participants

The data for the current paper were based on a previous dataset collected over the course of 2015 and 2016. Participants were recruited by mailing list in the UK and via their instructors in the USA. Participation was voluntary. As only 323 participants responded to the familiarity items, the

current study focuses on this subset. The participations included 169 participants taking social science programs in the Midwest of the USA and 154 participants completing various social science and other programs at several universities in the UK. The age ranged from 18 to 60 (M = 22.78; SD = 5.89). As the purpose of the analysis is to compare samples, we also investigated potential differences between samples prior to the main analysis. Overall, 74.9% of the participants were female (n = 242) and 25.1% were male (n = 81). The two groups did not differ ($F(1, 321)$ = .21, p = 648) in terms of their age characteristics (UK M = 22.92; US M = 22.64) and gender distribution (Pearson's $\chi^2(1) = .025$, $p = .874$). Over half of the sample were employed (n = 191, 59.5%), with the remainder being either unemployed or looking for work (n = 90, 27.9%), with a small minority selecting the option of 'other' (n = 41, 12.7%; with one missing value). Students in the USA were more likely to be employed than students in the UK (Pearson's $\chi^2(3) = 12.37$, p = .006). In terms of education, 26.6% had a high school diploma or similar, 31% had already obtained an associate degree (at community college), 29.1% had already obtained an undergraduate degree (e.g., BA or BSc), 5.6% had already obtained a postgraduate degree, while 7.7% had obtained other unspecified qualifications). The main difference in education (Pearson's $\chi^2(4) = 56.70$, $p < .001$) arose in terms of the greater number of students in the USA having already completed an associate degree (two-year degree, e.g. at community colleges), a qualification that is less common in the UK. In addition, more participants in the UK were working towards a postgraduate qualification at the time of the survey than in the USA. Participants had used the Internet for around 12 years (M = 11.72, SD = 3.44), although Internet use ranged from 2 to 24 years. Students in the USA had used the Internet on average one more year (M = 12.29, SD = 3.22) than students in the UK (M = 11.10, SD = 3.57), ($F(1, 320) = 9.792$, p = .002).

2.2 Procedure

As soon as participants had read the study information and completed the consent form, they were asked to complete items on their attitude towards their personal use of Internet, their use of security measures, and their general Internet experience. They were then presented with 18 different threats and Internet behaviors. Each of these 16 threats were also defined for the participants to ensure they all knew the characteristics of each threat (see Appendix). All participants were asked to indicate their familiarity with each of the threats individually. The survey ended with questions about their demographics and the debrief statement. All participants were eligible for course

credits when completing the survey and were also given the option to enter a prize draw (£50 or $50). In order to separate their anonymous responses to the survey from the registration page and thus identify user details, a separate link was presented in the debrief statement that redirected participants to a separate registration form not connected to the survey.

2.3 Measures

A number of single item measures were used to assess familiarity, use of computer security, and participant's attitude towards the Internet, Internet experience, and demographics.

2.3.1 Familiarity with online threats

Familiarity with 16 threats was examined in line with previous work (Garg and Camp, 2012; see additional work on familiarity and information security perceptions by Huang et al., 2007). The list consisted of the following threats: cat-fishing, social engineering, e-mail harvesting, zero-day attack, rogueware, botnet, trojan, keylogger, spyware, virus, cyber-bullying, virtual stalking, Internet surveillance, identity theft, phishing, cookie. Answering options ranged from 1 = *fully unfamiliar* to 7 = *fully familiar*.

2.3.2 Use of security measures

The degree to which participants used certain precautions was assessed using the Computer Security Usage scale (by Claar and Johnson, 2012). The scale involved five items with a response scale from 1 = *never* to 7 = *always*. The items asked participants whether or not they used anti-virus software, firewall software, anti-spyware software, software updates and security updates. The items were used individually and combined in one composite.

2.3.3 Internet attitude

This was measured using five items starting with "All things considered, my use of the Internet is…" followed by a 7-point response scale (e.g., 1 = *good*, 7 = *bad*). An example item is "All things considered, my use of the Internet is good-bad." The items were used individually.

2.3.4 Internet experience

All participants were asked three questions about their Internet experience. The first question asked participants how long they have been using the Internet (in years). The second question required participants to share how often they log onto the Internet. Answering options ranged from 1 = *weekly* to 6 = *more than 3 times a day*. The third question asked participants how much time they

spend on the Internet per day. The response options ranged from 1 = *1-5 minutes* to 7 = *several hours*.

2.3.5 Internet use

We also asked participants what they used the Internet for. Participants used the Internet for various purposes, specifically, e-mail (96.9%), social networking (90.4%), searching for work-related or study-related information (85.8%) as well as education/training (82.7%), shopping (81.4%) and banking (75.9%).

2.3.6 Demographics

Demographics included age, gender, education and employment status.

3. Results

This part of our paper is organized in four sections in line with research questions.

3.1 Threat familiarity (RQ1)

We had proposed that given the rather homogenous nature of our two samples from the UK, it was unlikely that these two groups of students would differ in their familiarity with threats (RQ1). The analysis of covariance (ANCOVA, where we considered potential control variables such as gender, age, education, and employment status) revealed that the UK and US sample was relatively similar in terms of their familiarity overall (composite score) with threats ($p > .05$). This was largely confirmed in 16 threats when we teste group difference in familiarity (for each individual threat). Table 1 presents all descriptives. In two cases, the two samples did differ in terms of their familiarity scores for individual threats. The UK sample appeared to be more familiar ($M = 4.34$, $SD = 1.91$) with social engineering ($F(1, 315) = 3.86$, $p = .050$, $\eta_p^2 = .01$) then the USA sample ($M = 3.86$, $SD = 1.79$), also controlling for gender and employment status ($p < .05$). In addition, the UK sample was more familiar ($F(1, 319) = 13.49$, $p < .001$, $\eta_p^2 = .04$) with phishing ($M = 5.30$, $SD = 1.79$) than their US counterparts ($M = 4.53$, $SD = 1.94$), also controlling for age ($p < .05$). It is not entirely clear which factors may explain these differences.

Table 1: Familiarity descriptives across samples and clusters

	UK	USA

Online threats	(*n* = 154)		(*n* = 169)	
	M	SD	M	SD
More recent (newer):				
Cat-fishing	6.09	1.33	5.97	1.41
Social engineering *	4.34	1.91	3.86	1.79
E-mail-harvesting	4.82	1.93	4.65	1.90
Zero-day attack	2.69	1.73	2.93	1.95
Rogueware	3.41	1.91	3.55	2.02
Botnet	2.87	1.88	2.98	1.84
Trojan	4.80	2.07	4.55	1.92
Keylogger	3.56	2.05	3.49	1.94
Phishing *	5.30	1.79	4.53	1.94
Well-known (established):				
Spyware	4.95	1.75	5.26	1.47
Virus	5.96	1.45	6.07	1.25
Cyber-bullying	6.26	1.26	6.25	1.19
Virtual stalking	5.62	1.46	5.78	1.27
Internet surveillance	4.90	1.77	5.14	1.57
Identity theft	5.80	1.22	5.72	1.36
Cookie	5.60	1.64	5.37	1.56

Note. The two samples (UK and USA) do not differ in terms of familiarity except in two instances identified with a * ($p \leq .050$).

3.2 Familiarity differences across all clusters (RQ2)

As we obtained very limited evidence that the two national samples differed significantly in their familiarity of threats (with the exception of two threats), we investigated the possibility that the sample may be differentiated in terms of their familiarity with threats (RQ2). We conducted hierarchical cluster analysis applying Ward's linkage method and squared Euclidian distance. The resulting dendrogram was then examined to identify potential solutions. The visualization of the clusters suggested that the participants could be allocated to three main groups of similar size. Analysis of variance suggested that the three clusters did differ significantly from one another in almost all cases, as assessed in a post-hoc comparison, in terms of their familiarity with different threats and online behaviors ($p < .001$). Table 2 summarizes the descriptives for each of the three clusters ($N = 296$).

Table 2: Familiarity descriptives across clusters

Online threats	Cluster 1 *Experts: higher familiarity overall* (*n* = 92)		Cluster 2 *Unfamiliar with well-known threats* (*n* = 112)		Cluster 3 *Unfamiliar with newer threats* (*n* = 92)	
	M	SD	M	SD	M	SD
More recent (newer):						
Cat-fishing	6.45	0.91	*5.11*	1.63	6.75	0.57
Social engineering *	5.22	1.47	4.06	1.59	*2.82*	1.74
E-mail-harvesting	5.67	1.47	*4.17*	1.78	4.42	2.19
Zero-day attack	3.51	1.94	2.87	1.75	*1.68*	1.22
Rogueware	4.87	1.79	3.30	1.73	*2.05*	1.29
Botnet	3.72	1.84	3.24	1.88	*1.51*	0.81
Trojan	6.09	1.26	*3.55*	1.71	4.59	2.07
Keylogger	4.84	1.73	3.24	1.74	*2.36*	1.74
Phishing *	5.86	1.35	4.24	1.72	4.74	2.25
Well-known threats:						
Spyware	5.98	1.03	*3.81*	1.58	5.92	0.95
Virus	6.59	0.65	*5.21*	1.61	6.60	0.74
Cyber-bullying	6.72	0.58	*5.40*	1.52	6.88	0.33
Virtual stalking	6.07	1.22	*5.12*	1.45	6.13	1.11
Internet surveillance	5.84	1.25	*4.42*	1.63	4.89	1.85
Identity theft	6.24	0.87	*5.04*	1.45	6.29	0.90
Cookie	6.43	0.98	*4.53*	1.70	5.58	1.43

Note. Three main clusters were identified based on familiarity scores ($p < .001$). Values in italics are lowest familiarity score across the three clusters.

Having identified three clusters, we next decided to explore the characteristics across the three clusters. Significant differences in overall familiarity with threats (using the composite measure) were observed ($F(2, 293) = 11.29$, $p <. 001$, $\eta_p^2 = .43$). We also considered a number of covariates. The difference in familiarity between clusters was still significant ($F(2, 291) = 112.83$, $p <. 001$, $\eta_p^2 = .44$) after we controlled for gender and age ($p < .05$).

Post-hoc analysis further showed that the Cluster 1 differed significantly from both Cluster 2 ($n = 92$) and 3 ($p < .001$), while Cluster 2 and 3 also differed marginally from one another ($p = .001$). Participants in Cluster 1 appeared to be highly familiar with threats (scored a mean score of 5.63 out of 7), so we labelled them the *experts* ($n = 92$). Individuals in Cluster 2 ($n = 112$) appeared to have slightly lower familiarity scores (4.21 out of 7). They also tended to have better awareness of new threats. As a result, this cluster captured those who were *unfamiliar with well-known threats*. Participants in Cluster 3 had a slightly above average familiarity with most threats (4.58

out of 7), but it was on average lower than the familiarity of the experts. The participants in Cluster 3 appeared to less familiar with more recent threats, but they tended to be more familiar with established threats (see Table 2). Cluster 3 therefore captured those who were *unfamiliar with new threats (n = 92).*

In order to visualize the findings, we also produced two figures (Figure 2a and 2b) that outline the differences between the three clusters: the experts, those unfamiliar with well-known threats and those unfamiliar with new threats. Figure 1a outlines the familiarity with specific threats. Figure 2b summarizes the descriptives for threats that are likely to be a function of the user's online engagement (frequency, social engagement, and information sharing). Generally, familiarity scores seem to be higher with the threats outlined in Figure 2b than Figure 2a. Overall, we can conclude that the level of familiarity across all three clusters was lowest for specific threats such as zero-day attack, rogueware, botnets, and keyloggers (newer threats).

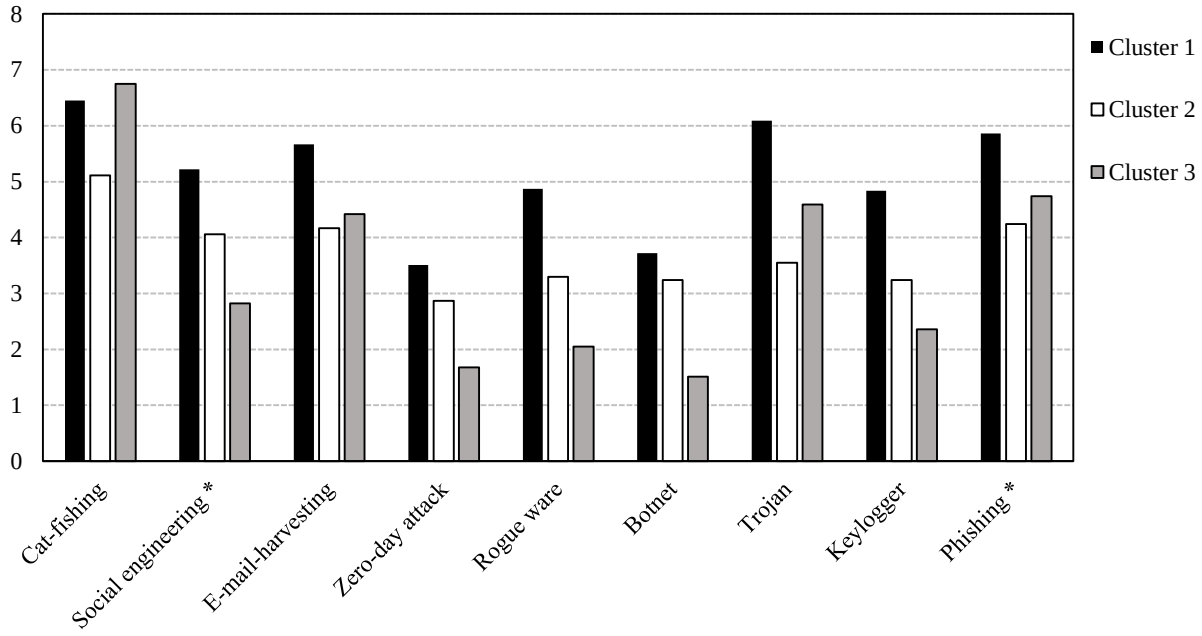

Figure 2a: Cluster differences in familiarity (for new threats)

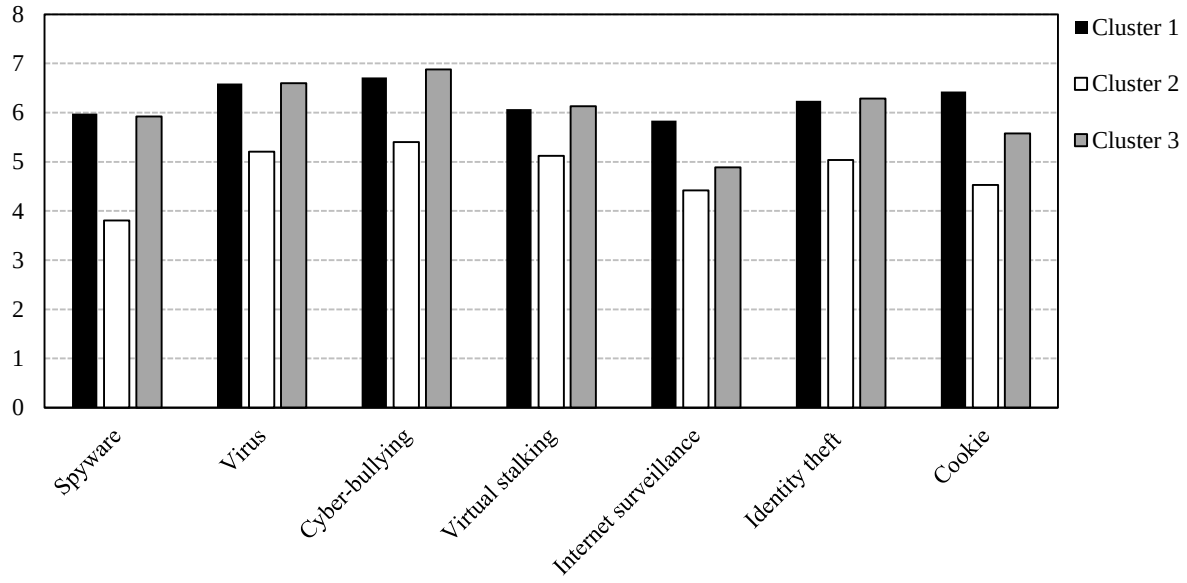

Figure 2b: Cluster differences in familiarity (for established threats)

3.2.1 Self-evaluation of Internet activities/behaviors

Having identified the three familiarity clusters, we wanted to assess how the degree of familiarity also related to self-reported Internet use. We summarize the descriptives in Figure 3. As expected, we observed significant differences across all three clusters ($p < .001$; see Table 3). By and large, the experts ranked their Internet use as more positive than negative (as in advantageous compared to disadvantageous to user's security), more beneficial than harmful, and so on. Participants who self-identified as less familiar about well-known threats were more likely to report more problematic behavior (Cluster 2) than those who were less familiar with new threats (Cluster 3).

These findings further suggest that participant's general self-awareness of their own potentially problematic Internet use as indicated across all five attitude measures (see Table 3) may be linked to the degree to which participants are (un)familiar with threats – at the same time it is maybe a question as to whether or not familiarity is the result of more online engagement. However, we only noted a marginally significant difference in terms of the frequency with which participants in the three clusters used the Internet ($F(2, 292) = 2.49$, $p = .085$). Internet use was high amongst the experts (Cluster 1, $M = 5.38$, $SD = 0.87$) and those unfamiliar about newer threats (Cluster 3, $M = 5.29$, $SD = 0.96$) compared to those more unfamiliar with well-known threats (Cluster 2, $M = 5.09$, $SD = 1.06$).

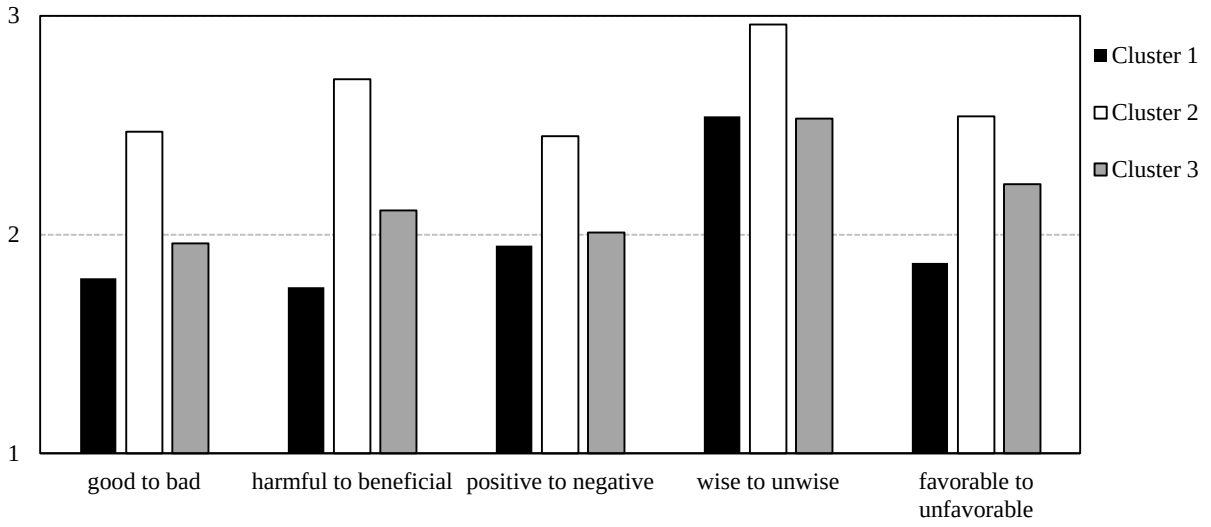

Figure 3: Self-reported Internet use in relation to familiarity

Table 3: Self-evaluation of activities/behaviors

Attitudes towards Internet use	Cluster 1 Expert (n = 92)		Cluster 2 Unfam. (w) (n = 112)		Cluster 3 Unfam. (n) (n = 92)		AN(C)OVA
	M	SD	M	SD	M	SD	
Good to bad	1.80	1.05	2.47	1.30	1.96	1.18	$F(2,293) = 9.03$, $p < .001$[a]
Beneficial to harmful	1.76	0.94	2.71	1.45	2.11	1.18	$F(2,292) = 17.88$, $p < .001$ [b]
Positive to negative	1.95	1.03	2.45	1.18	2.01	0.96	$F(2,291) = 7.83$, $p < .001$ [c]
Wise to unwise	2.54	1.29	2.96	1.38	2.53	1.39	$F(2,291) = 4.17$, $p = .016$ [d]
Favorable to unfav.	1.87	1.07	2.54	1.27	2.23	1.08	$F(2,289) = 10.10$, $p < .001$[e]

Note. Cluster 1 (experts), Cluster 2 (unfamiliar: well-known threats), Cluster 3 (unfamiliar: new threats). Covariates: [a] no significant covariates, [b] age ($p < .05$), [c] employment status ($p < .05$), [d] employment status ($p = .006$), [e] employment status ($p < .05$).

3.2.2 Computer security use

Having obtained evidence that familiarity is also linked to self-evaluations of one's Internet use (Internet attitude) as well as differences in terms of the frequency with which the participants in

different clusters use the Internet, the question arose if familiarity is therefore also linked to whether or not participants used different security features. In line with previous findings and as outlined in Table 4 (and Figure 4), experts (Cluster 1) were more likely to use security features than participants who were less familiar with threats (in Cluster 2 and Cluster 3).

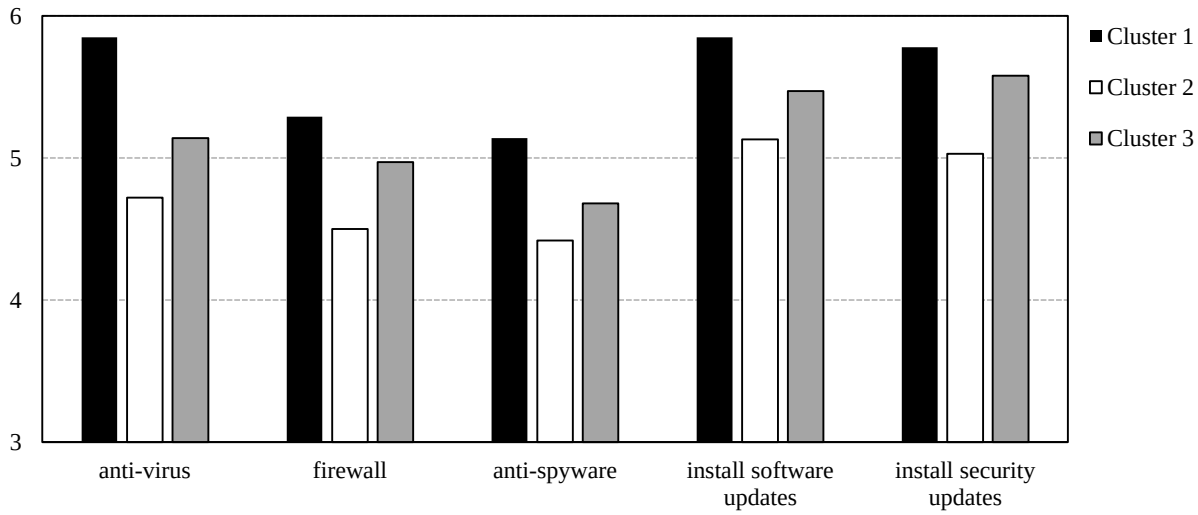

Figure 4: Computer security in relation to familiarity

Table 4: Computer security use

Security actions	Cluster 1 Expert (n = 92)		Cluster 2 Unfam. (w) (n = 112)		Cluster 3 Unfam. (n) (n = 92)		AN(C)OVA
	M	SD	M	M	SD	M	
Anti-virus software	5.85	1.48	4.72	1.96	5.14	1.91	$F(2,291) = 7.96$, $p < .001$ [a]
Firewall software	5.29	1.89	4.50	1.87	4.97	1.89	$F(2,291) = 3.56$, $p = .030$ [b]
Anti-spyware	5.14	1.96	4.42	1.92	4.68	1.99	$F(2,293) = 3.48$, $p = .032$ [c]
Run software updates	5.85	1.30	5.13	1.57	5.47	1.66	$F(2,293) = 5.71$, $p = .004$ [d]
Run security updates	5.78	1.56	5.03	1.77	5.58	1.76	$F(2,291) = 4.53$, $p = .012$ [e]

Note. Cluster 1 (experts), Cluster 2 (unfamiliar: well-known threats), Cluster 3 (unfamiliar: new threats). Covariates: [a] employment status ($p < .05$), [b] employment status ($p < .05$), [c] no significant covariates, [d] no significant covariates, [e] employment status ($p < .05$).

3.3 Familiarity as Mediator between Internet Use and Security Behaviors (RQ3)

We considered the role of previous experience as a precursor to familiarity of threats and behaviors. And only when threats were known are participants likely to engage in computer security behavior. This mediation hypothesis was tested using the three questions related to Internet experience as predictors, overall familiarity as mediator (composite score), and the composite based on all computer security responses. The mediation was assessed using the PROCESS macro from Hayes (2013). We ran three mediation models, one for each of the three Internet experience variables that we predicted were direct predictors of familiarity and potentially indirect predictors (via familiarity) of computer security use. We also considered potential covariates. Gender and employment status were significant covariates but their inclusion did not significantly change the results. As a result, we report the outcomes of the mediation without these covariates.

Two out of three questions (see Figure 5 and 6) were significant predictors of familiarity (composite score) as hypothesized. The frequency with which they used the Internet was not a significant predictor of overall familiarity with risks (although the frequency of Internet use differed across the three clusters, see previous analysis). The average time spent online was a positive predictor of familiarity (β = .079, p = .013) as was the length of Internet use over several years (β = .055, p < .001). Familiarity was a significant predictor of computer security behavior (β = .433, p < .001). However, time online on average (β = .020, p = .708) and length of Internet use (β = .028, p = .246) were not significant direct predictors of computer security behavior, with familiarity held constant. However, we did obtain a significant indirect effect, demonstrating full mediation, for time online (β = .034, p = .032; LLCI = .0078 and ULCI = .0746) and length of Internet use (β = .024, p = .004; LLCI = .0095 and ULCI = .0449).

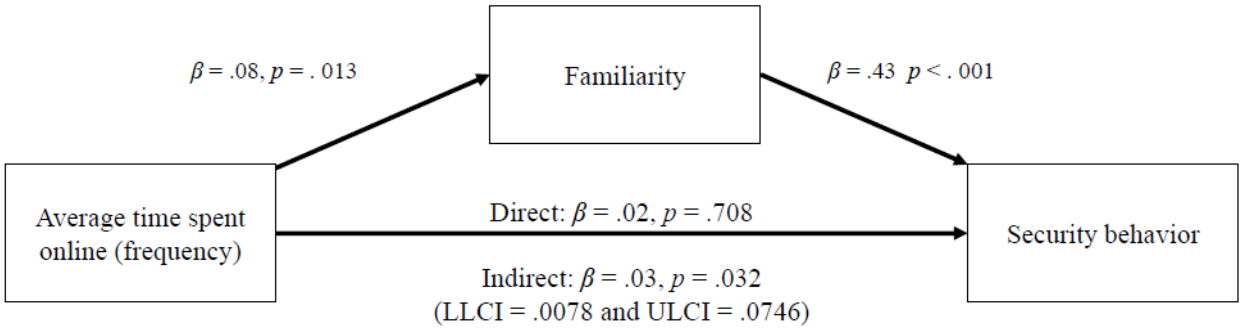

Figure 5: Mediation results for average time spend online

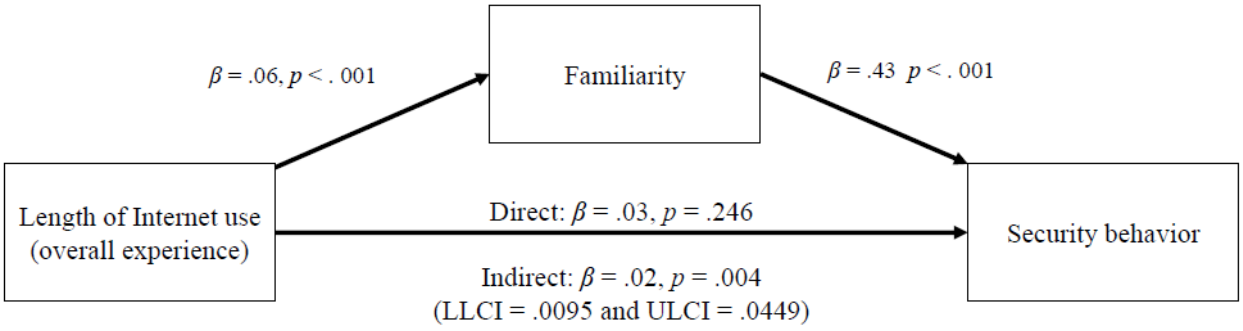

Figure 6: Mediation results for overall Internet experience, familiarity and security behavior

4. Discussion

The purpose of the current paper was to examine the role of familiarity with threats, in computer security use. In the following section, we briefly summarize our findings and connect these to practical implications.

The first question of interest considered how familiar students were with the various online threats (RQ1). We had assumed that students in the UK and USA would show similar degrees of familiarity. This hypothesis was largely confirmed – except in terms of social engineering and phishing. In each of these two cases, the UK sample appeared to be more familiar with these threats then their counterparts in the USA. Two explanations may be offered. First, the sample in the UK was potentially more diverse in terms of their educational goals than the US sample. That is, the participants from the USA were largely recruited from social science courses, while the participants in the UK were recruited as part of a university-wide research call. While we do not have the means to assess degree-specific differences in our dataset, it is possible that familiarity with certain risks is associated with different background and educational experience. In addition, the universities may have differed slightly in terms of the content of their educational outreach activities. Many universities realize the value in educating their students about Internet threats as their risky or problematic online behavior is likely to also threaten the university's network and Internet infrastructure.

The second question of interest looked at differences in our dataset due to different degrees of familiarity with threats (RQ2). Using cluster analysis, we identified three main clusters. The three clusters were differentiated along with their general familiarity with threats and labelled the experts (Cluster 1), or those unfamiliar with well-known threats (Cluster 2) vs. newer threats (Cluster 3). All three clusters were less familiar with four particular threats. These were threats such as the zero-day attacks, rogueware, botnets, and keyloggers. This identifies a clear area for future training and awareness campaigns in these university settings.

While we found no evidence of significant as well as consistent differences between the two national samples (except for the two exceptions noted above), the three clusters had clearly very distinct Internet attitudes and computer security behaviors. Specifically, participants (Cluster 2) who were less familiar with well-known threats overall also reported more negative (personally problematic or disadvantageous) compared to positive (and unproblematic) self-evaluated Internet use (Internet attitude). Participants in Cluster 2, together with the group less informed about newer threats (Cluster 3), were also less likely to use specific computer security features than the experts (Cluster 1). The three features more likely to be used by the experts were firewalls, software and security updates. However, it is noteworthy that all these features are default features that can be readily enabled on most computers these days. The fact that no significant differences ($p < .05$) were obtained for anti-spyware and anti-virus software is rather disheartening. However, we should note that since the familiarity questions were located at the end of the survey, it is possible that self-evaluation of one's Internet use may have influenced the familiarity ratings. This is a possible limitation of the study.

Despite these limitations, our results allow us to draw two tentative conclusions. First, greater familiarity with threats does not necessarily go hand in hand with better computer security. What is more, familiarity with threats and different online behavior may also depend on how recent/new or well-known threats and behaviors are. This is in line with related evidence that suggests that users often do not understand all the functions of the tools they use (Clark et al., 2015), and thus may not understand the threats that exist. Participants (particularly those in Cluster 2 and 3, see Table 4) did not use readily available computer security features and programs to the same degree that experts did (Cluster 1). It is unclear if this reflects an overreliance on the university's (or home environment's) infrastructure (e.g., convenience versus security driven decision-making, see Jeske et al., 2014). This lack of alignment between what participants know and do may also be

attributable to some other factor such as inability to grasp the implications of one's behavior for one's computer security (suggesting low risk awareness; see Coventry et al., 2014). And second, further exploration showed that regular Internet experience and use may be particularly relevant for fostering familiarity with threats – in line with the notion of situated learning (Lave and Wenger, 1990).

The mediation (RQ3) provided further evidence that time spent on the Internet and the length of Internet experience (but not daily or weekly frequency) were significant predictors of familiarity with threats and online behaviors. Similarly, these variables were also significant indirect predictors of computer security use (a relationship fully mediated by familiarity). Again, this is a finding in support of situated learning (Lave and Wenger, 1990). Although the effects were quite small overall, the practical implication may be that computer security behavior is an outcome of familiarity, which is not accomplished without significant time investment. This also means that the time spent to familiarize oneself with threats and learn about online options is a time spent learning – but also a period of greater vulnerability until some degree of familiarity with threats is achieved that triggers security behavior. However, again a limitation of this analysis is the use of single-item measures (e.g., in relation to Internet use) as this might introduce bias due to unreliability (e.g., Petrescu, 2013). As a result, our conclusions need to be interpreted with caution.

The results suggest that numerous factors come into play, both human and technical, in line with the ANT approach (Hassard and Alcadipani, 2010). This was evidenced by age and employment status, both of which were important covariates. Simultaneously, precautionary behaviors requires access to but also familiarity with both threats and technical tools to combat them. Internet experience is particularly shaped by both human (user) and technical characteristics and tools available to the users. The starting points for interventions as well as practical implications are outlined in the next two sections.

4.1 Starting points for interventions

A number of starting points for interventions exist. Work on nudging individuals and research on evidence-based practice (see Michie and West, 2013) focuses on helping online users to make better security-related decisions on social media, mobile devices and in relation to wireless options – and thus enable them to overcome lack of knowledge and awareness of security threats on the part of the users (e.g., Choe et al., 2013; Kruger et al., 2010; Turland et al., 2015). In addition, the

research on user perceptions has frequently utilized some of the premises of the Health Belief Model by Rosenstock (1974). This includes studies to learn more about email-related security behavior (e.g., Ng et al., 2009), to explore how safe and secure online users felt about using technology to complete financial transactions (Davinson and Sillence, 2014), to educate users about phishing (Davinson and Sillence, 2010) and how to increase the use of computer security software (Claar and Johnson, 2012). As a result, this model may also provide a general explanatory framework for understanding a number of additional threat perceptions, which may also help IT departments in universities and private businesses to identify starting points for interventions and awareness campaigns.

The main purpose of the Health Belief Model is to understand why individuals engage in preventive actions or behaviors (Rosenstock, 1974). The model includes several concepts: Self-efficacy (the degree to which individuals feel capable to tackle certain challenges), perceived susceptibility (opinion that one will contract health issues), perceived severity of the condition and consequences, and the perceived benefits and barriers to taking action. The model also considers the influence of triggers within the individual and environment. These serve as 'cues to action' (Siepmann, 2008). The model may also provide insight into understanding online users' threat perceptions. It further captures the complexity of individual or situational antecedents to these perceptions – and thus the precautions that users may take. Taking a similar approach as Davinson and Sillence (2014), we outline each of the five concepts of the Health Belief Model as they could be applied in future research and interventions (Table 5). The threats may also influence perceptions of susceptibility, severity, costs, benefits, cues to action and perceived control.

Table 5: Concepts of the Health Belief Model as applied to the security context

Concept	Cybersecurity context
Perceived susceptibility	How likely is the threat for the user? This might be reflected in *perceptions of risk* and the users' *information-sharing attitude.*
Perceived severity	How serious are the consequences (*perceived risks*) for the user?
Perceived costs	What are the costs (*balance between risks and benefits*) that the user might incur as a result of the threat?
Perceived benefits	What are the benefits of precautions (*perceived benefits*) to a threat?
Self-efficacy	How capable does the users feel about facing these threats? This may be subject to the users' actual *familiarity with risks* and *computer security use*.
Cues to action	What triggers (antecedents) lead to more secure user behavior? These triggers may also influence as and when online users take *precautions*.

If this model is applied in combination with concepts such as situated learning (Lave and Wenger, 1990) and learning from failure (see Fortune and Peters, 1995; see also Dalcher and Drevin, 2003), individuals as well as trainers may become more well-rounded in their understanding of threats (and how they are perceived). Such training may also enable students and other less security-experienced trainees to gain a better understanding of how threats, if not prevented, impact on their data security and system operability. In addition, groupware and online collaborative tools as well as social networks exist – all of which can enable social interaction, access and support across time and location (Harr et al., 2011). For those tasked with teaching cybersecurity to employees and students, various e-mentoring and e-coaching schemes exist as well as guidance on online tutoring (e.g., Perren, 2003). Furthermore, new platforms allow individuals to interact face-to-face in real time using video chats. Customized configurations of technologies and settings (e.g., Shanks et al., 2003) enables organizations to not only engage others, monitor trainees' progress but also provide means to provide feedback (e.g., by using analytics and discussion forms).

System-specific interventions may also be an option. Cues to action may be designed with system nudges and similar system interventions to flag issues (see Acquisti, 2009; Coventry et al., 2014; Grossklags et al., 2010). While many cues to action (e.g., warning messages upon installation of unknown or third-party software) are used already, it is clear that many interventions fail – and we suggest that the lack of familiarity with the threats or issues can be a major determinant of individual's disregard or disengagement with such interventions. Relying on user expertise and understanding of nudges may disregard the first step: ensuring that the users are sufficiently familiar with potential threats so that those who seek to improve their security behavior can be successful.

4.2 Expanding knowledge base: Final comments for practitioners and researchers

Past evidence suggests that while information campaigns may change attitudes, behavior will not necessarily change in line with attitudes (McKenzie-Mohr, 2000). This may be due to various reasons, including the difficulty of changing a behavior (e.g., Constanzo et al., 1986) given environmental constraints and habits. However, when behavioral change would be of personal or even financial benefit, behavioral change is more likely to follow (McKenzie-Mohr, 2000).

However, it will be more difficult to change a behavior that is perceived as a low priority rather than a high priority (see example in Sadalla et al., 2014). If lack of familiarity is high, it is unlikely that users will change their security behavior. That said, familiarity is again a self-reported and subjective variable to consider in this context. Finding means to assess subjective as well as objective familiarity may be an important way forward to optimize computer security training. Some support for the importance of clarifying what users actually think they know versus what they actually know comes from work on domain knowledge (see Hadar et al., 2014). When individuals lack domain knowledge, they may rely on the information available to them, although they cannot know if this is all the information they need. And in the context of security, they may even rely on mere recognition of the threat that can be attributed to repeated exposure to warnings – but it may not be based on any substantial knowledge. Finding ways to differentiate between degrees of awareness versus actual knowledge may contribute significantly to the effectiveness of computer security awareness campaigns and training initiatives.

Future work in the design of training that builds on familiarity may also benefit from threat research conducted by Huang et al. (2010) on perceptions of information security. These authors examined 20 factors that shape threat perceptions to a variety of information security threats. They identified several factors that influenced information security perceptions, such as knowledge (including familiarity), perception of risks, severity of consequences, controllability, possibility of being exposed to threats, and awareness of threats (Huang et al., 2010). If we increase users' attention to, and accurate self-evaluation of these facets, they may also adopt more secure behaviors. This suggests that familiarity and threat perceptions are important antecedents which shape the likelihood with which precautions are taken.

Finally, while many interventions are focused on increasing employees' awareness of risks (Stewart and Lacey, 2012), improving information-sensitive managerial operations and supporting security service providers (e.g., Ulltveit-Moe, 2014), the education of students is often left to cash-strapped IT departments in university settings. However, students are an important target group as they represent future employees and managers. It is unlikely that their lack of precautions and knowledge gaps will disappear upon graduation and entry into the labor market. Thankfully, some recommendations have already been developed for students on how to raise their information security awareness in different contexts (see Kim, 2014; Park et al., 2017) and how to create

engaging, motivating and practically focused information security lessons (e.g., Ahmad and Maynard, 2014). We would direct practitioners and graduate recruiters towards these resources.

5. Acknowledgements

We gratefully acknowledge the support of our colleagues at the UK and US institutions who supported the data collection and design (anonymized for review).

6. Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

Acquisti, A. (2009). Nudging privacy. The behavioral economics of personal information. *Security & Privacy Economics,* Nov/Dec., 82-85.

Acquisti, A., & Grossklags, J. (2004). Privacy attitudes and privacy behavior. Losses, gains, and hyperbolic discounting. In L. J. Camp and R. Lewis (Eds.), *The Economics of Information Security. Advances in Information Security,* Vol. 12 (pp. 165-178). Norwell, MA; Dordrecht, Netherlands: Kluwer Academic Publishers Group.

Ahmad, A., & Maynard, S. (2014). Teaching information security management: reflections and experiences. *Information Management & Computer Security, 22,* 513-536. doi: 10.1108/IMCS-08-2013-0058

Arnaboldi, M., & Spiller, N. (2011). Actor-network theory and stakeholder collaboration: The case of Cultural Districts. *Tourism Management, 32,* 641-654. doi:10.1016/j.tourman.2010.05.016

BBC (2011). New net rules set to make cookies crumble. BBC News Technology, March 8. Available at: http://www.bbc.co.uk/news/technology-12668552 (accessed August 24, 2016).

Bonneau, J., Herley, C., van Oorschot, P.C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proceedings of The IEEE Symposium on Security and Privacy* (SP '12), pg. 553-567. doi: 10.1109/SP.2012.44

Brinton Anderson, B., Vance, A., Kirwan, C. B., Eargle, D., & Jenkins, J. L. (2016). How users perceive and respond to security messages: a NeuroIS research agenda and empirical study. *European Journal of Information Systems, 25*, 364–390. doi: 10.1057/ejis.2015.21

Choe, E. K., Jung, J., Lee, B., & Fisher, K. (2013) Nudging people away from privacy-invasive mobile apps through visual framing. In *Proceedings of INTERACT*, Sep 2-6, Cape Town, ZA. doi: 10.1007/978-3-642-40477-1_5

Claar, C. L., & Johnson, J. (2012). Analyzing home PC security adoption behavior. *Journal of Computer Information Systems*, Summer, 20-29. doi:

Clark, J. W., Snyder, P., McCoy, D., & Kanich, C. (2015). "I Saw Images I Didn't Even Know I Had" Understanding User Perceptions of Cloud Storage Privacy. In Proceedings of *CHI 2015*, April 18–23, Seoul, Republic of Korea. doi: 10.1145/2702123.2702535

Clarke, R. (2014). Vignettes of corporate privacy disasters. Available at: http://www.rogerclarke.com/DV/PrivCorp.html (accessed August 24, 2016)

Constanzo, M., Archer, D., Aronson, E., & Pettigrew, T. (1986). Energy conservation behavior: The difficult path from information to action. *American Psychologist, 41*, 521-528. doi: 10.1037/0003-066X.41.5.521

Coventry, L., Briggs, P., Jeske, D., & van Moorsel, A. (2014). SCENE: A Structured Means for Creating and Evaluating Behavioral Nudges in a Cybersecurity Environment. In A. Marcus (Ed.), *Design, User Experience, and Usability. Theories, Methods, and Tools for Designing the User Experience*. Lecture Notes in Computer Science. Vol. 8517. Springer International Publishing. doi: 10.1007/978-3-319-07668-3_23.

Coventry, L., Jeske, D., & Briggs, P. (2014). Perceptions and actions: Combining privacy and risk perceptions to better understand user behavior. Workshop paper presented at the *Symposium on Usable Privacy and Security* (SOUPS), July 9-11, 2014, Menlo Park, CA.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*, 79-98. doi: 10.1287/isre.1070.0160

Dalcher, D., & Drevin, L. (2003). Learning from Information Systems failures by using narrative and ante-narrative methods. *Proceedings of the 2003 Annual conference of the SAICSIT*. (South African Institute of Computer Scientists and Information Technologists), pp. 137-142.

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behavior among internet users. *Computers in Human Behavior, 26*, 1739-1747. doi: 10.1016/j.chb.2010.06.023

Davinson, N., & Sillence, E. (2014). Using the health belief model to explore users' perception of 'being safe and secure' in the world of technology mediated financial transactions. *International Journal of Human-Computer Studies, 72*, 154-168. doi: 10.1016/j.ijhcs.2013.10.003

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behavior towards protective information technologies: The role of national cultural differences. *Information Systems Journal, 19*, 391-412. doi: 10.1111/j.1365-2575.2007.00289.x

Finneran, C.M., & Zhang, P. (2003). Person-Artifact-Task (PAT) Model of Flow Antecedents in Computer-Mediated Environments. *International Journal of Human-Computer Studies, 59*, 475-496.

Fortune, J., & Peters, G. (1995). *Learning from Failure*. John Wiley & Sons.

Garg, V., & Camp, L. J. (2012). End user perception of online risk under uncertainty. In Proceedings of *The 45th Hawaii International Conference on System Sciences* (HICSS), Manoa, HI, 4-7 January 2012. doi: 10.1109/HICSS.2012.245

Grossklags, J., Radosavac, S., Cárdenas, A. A., & Chuang, J. (2010). Nudge: Intermediaries' role in interdependent network security. In *Proceedings of the International Conference on Trust and Trustworthy Computing*, June, pp. 323-336. doi: 10.1007/978-3-642-13869-0_24

Hadar, I., Soffer, P., & Kenzi, K. (2014). The role of domain knowledge in requirements elicitation via interviews: an exploratory study. *Requirements Engineering*, *19*, 143–159. doi: 10.1007/s00766-012-0163-2

Harr, R., Wiberg, M. and Whittaker, S. (2011). Understanding interaction search behavior in professional social networks. *Human Technology: An Interdisciplinary Journal on Humans in ICT Environments, 7,* 194-215.

Hassard, J., & Alcadipani, R. (2010). Actor-Network Theory. In Albert J. Mills & Gabrielle Durepos & Eiden Wiebe (Eds), *Encyclopedia of Case Study Research* (pp. 9-13). Thousand Oaks: SAGE Publications.

Hayes, A. F. (2013). *Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach.* New York: Guilford Press.

Huang, D.-L., Rau, P.-L, P., & Salvendy, G. (2010). Perceptions of information security. *Behaviour & Information Technology, 29*(3), 221–232. doi: 10.1080/01449290701679361

Jeske, D., Coventry, L., & Briggs, P. (2014). Decision justifications for wireless network selection. In *Proceedings of the 2014 Workshop on Socio-Technical Aspects in Security and Trust* (STAST), Vienna, Austria, pp. 1-7. doi: 10.1109/STAST.2014.9

Kim, E. B. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security, 22*, 115-126. doi: 10.1108/IMCS-01-2013-0005

Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security, 18*, 316-327. doi: 10.1108/09685221011095236

Kurkovsky, S., & Syta, E. (2010). Digital natives and mobile phones: A survey of practices and attitudes about privacy and security. In *Proceedings of ISTAS* (International Symposium of the Technology and Society), 7-9 June, pp. 441-449. doi: 10.1109/ISTAS.2010.5514610

Latour, B. (1987). *Science in action: How to follow scientists and engineers through society*. Milton Keynes, UK: Open University Press.

Latour, B. (1999). On recalling ANT". In Law, J., & Hassard, J. (Eds). *Actor Network Theory and after*. Oxford: Blackwell Publishers (pg. 15-25).

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford: Clarendon.

Lave, J., & Wenger, E. (1990). *Situated Learning: Legitimate Peripheral Participation*. Cambridge, UK: Cambridge University Press.

Law, J. (1992). Notes on the theory of the actor network: Ordering, strategy and heterogeneity. *Systems Practice, 5*, 379-393. doi: 10.1007/BF01059830

Lee, E. W. J., & Ho, S. S. (2015). The perceived familiarity gap hypothesis: examining how media attention and reflective integration relate to perceived familiarity with nanotechnology in Singapore. *Journal of Nanoparticle Research, 17*, 1-15. doi: 10.1007/s11051-015-3036-z

McKenzie-Mohr, D. (2000). Fostering sustainable behavior through community-based social marketing. *American Psychologist, 55*, 531-537. doi: 10.1037/0003-066X.55.5.531

Michie, S. & West, R. (2013). Behaviour change theory and evidence: a presentation to Government. *Health Psychology Review, 7*, 1-22. doi: 10.1080/17437199.2011.649445

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*, 815-825. doi: 10.1016/j.dss.2008.11.010

Opentracker (2014). Third-party cookies vs first-party cookies. Available at: http://www.opentracker.net/article/third-party-cookies-vs-first-party-cookies (accessed August 24, 2016).

Park, E.H., Jongwoo Kim, J., & Park, Y.S. (2017). The role of information security learning and individual factors in disclosing patients' health information. *Computers & Security, 65*, 64-76. 10.1016/j.cose.2016.10.011

Perren, L. (2003). The role of e-mentoring in entrepreneurial education and support: A meta-review of academic literature. *Education + Training, 45*, 517-525. doi: 10.1108/00400910310508900

Petrescu, M. (2013). Marketing research using single-item indicators in structural equation models. *Journal of Marketing Analytics, 1*, 99-117. doi: 10.1057/jma.2013.7

Rocha Flores, W., Holm, H., Svensson, G., & Ericsson, G. (2014). Using phishing experiments and scenario-based surveys to understand security behaviors in practice. *Information Management & Computer Security, 22*(4), 393-406. doi: 10.1108/IMCS-11-2013-0083

Rosenstock, I. (1974). Historical origins of the Health Belief Model. *Health Education Monographs, 2*, 328-335. doi: 10.1177/109019817400200403

Sadalla, E., Berlin, A., Neel, R., & Ledlow, S. (2014). Priorities in residential water use: A trade-off analysis. *Environment and Behavior, 46*, 303-328. doi: 10.1177/0013916512456286

Satterfield, T., Kandlikar, M., Beaudrie, C. E. H., Conti, J., & Herr Harthorn, B. (2009). Anticipating the perceived risk of nanotechnologies. *Nature Nanotechnology, 4*, 752-758. doi:10.1038/nnano.2009.265

Shanks, G., Seddon, P. and Willcocks, L. (Eds) (2003), *Second-Wave Enterprise Resource Planning Systems.* Cambridge: Cambridge University Press.

Siepmann, M. (2008). Health behavior. In *Encyclopedia of Public Health* (pp. 515-521). Springer.

Stewart, G., & Lacey, D. (2012). Death by a thousand facts. Criticising the technocratic approach to information security awareness. *Information Management & Computer Security, 20*, 29-38. doi: 10.1108/09685221211219182

Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: A tradeoff between security and convenience. *Behaviour & Information Technology, 29*, 233-244. doi: 10.1080/01449290903121386

Turland, J., Coventry, L., Jeske, D., Briggs, P., & van Moorsel, A. (2015). Nudging towards security: Developing an application for wireless network selection for android phones. In *Proceedings of the 2015 British HCI conference*, ACM, pp. 193-201. doi: 10.1145/2783446.2783588

Ulltveit-Moe, N. (2014). A roadmap towards improving managed security services from a privacy perspective. *Ethics of Information Technology, 16*, 227-240. doi: 10.1007/s10676-014-9348-3

Wogalter, M. S., Brelsford, J. W., Desaulniers, D. R., & Laughery, K. R. (1991). Consumer product warnings: The role of hazard perception. *Journal of Safety Research, 22*, 71-82. doi: 10.1016/0022-4375(91)90015-N

Appendix

Definitions of threats used in this study

Cat-fishing: The act of building a fake relationship online by pretending to be someone else, creating an online romance through a false persona or fake social media profile.

Social engineering: The act of manipulating individuals to divulge confidential information. Criminals usually try to trick their victims into breaking normal security procedures and releasing valuable information such as passwords and bank details.

E-mail-harvesting: The process of obtaining a large list of email addresses though various means for purposes such as bulk spamming without the authority or the persons involved.

Zero-day attack: An attack that exploits previously unknown software vulnerabilities before security researchers and software developers become aware of them to create a fix or patch.

Rogueware: Malicious software that restricts access to the computer system that it infects. Either demands a ransom to lift the restriction or frightens people into purchasing and installing additional malicious software by alerting a user to a false problem.

Botnet: A collection of private computers that have been set up to forward transmissions (including spam or viruses) to other computers on the Internet, even though the computers' owners are unaware of this.

Trojan: Tracking software that attempts to infiltrate a computer without the user's knowledge or consent. This software often presents itself as one form while it is actually another.

Keylogger: A computer program that records every keystroke made by a computer user to gain fraudulent access to passwords and other confidential information.

Phishing: The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise. The aim is to scam the user into surrendering private information that will be used to steal the user's identity.

Spyware: A program that runs on a user's computer and tracks their browsing habits or captures information such as email messages, usernames, passwords, and credit card information.

Virus: Harmful computer program or script that attempts to spread from one file to another on a single computer and/or from one computer to another, using a variety of methods, without the knowledge and consent of the computer user.
Cyber-bullying: The use of information technology, in particular through the Internet, to harm or harass other people in a deliberate, repeated, and hostile manner.
Virtual stalking: Use of the Internet, e-mail or other electronic communication devices to stalk or repeatedly follow and harass another person.
Internet surveillance: The monitoring of online behavior, activities or other changing information, often in secret and without authorization. This is usually carried out on individuals or groups observed by governmental organizations.
Identity theft: Any kind of fraud on the Internet that results in the loss of personal data, such as passwords, user names, banking information, or credit card numbers
Cookie: A small piece of text or file that is stored in a user's computer.

Highlights

Different groups of student users present different patterns of familiarity with threats.

Threat familiarity may vary depending on whether threat novelty.

Threat familiarity impacts tendency to adopt precautionary behaviors.

Familiarity mediates the link between Internet experience and precautionary behavior.