Risk perceptions of cyber-security and precautionary behaviour

Abstract

A quantitative empirical online study examined a set of 16 security hazards on the Internet and two comparisons in 436 UK- and US students, measuring perceptions of risk and other risk dimensions. First, perceived risk was highest for identity theft, keylogger, cyber-bullying and social engineering. Second, consistent with existing theory, significant predictors of perceived risk were voluntariness, immediacy, catastrophic potential, dread, severity of consequences and control, as well as Internet experience and frequency of Internet use. Moreover, control was a significant predictor of precautionary behaviour. Methodological implications emphasise the need for non-aggregated analysis and practical implications emphasise risk communication to Internet users.

Keywords

risk perception; precautionary behaviour; information security; cyber-security; non-aggregate data analysis

Highlights

We studied students' responses to security hazards on the Internet

Students perceived identity theft as the riskiest hazard

Perceived risk was predicted by specific risk dimensions and use habits

Precautionary behaviour was predicted by students' perceived control

This work has implications for data analysis and risk communication to students

1 Introduction

Citizens are using the Internet (e.g., e-mail and the World Wide Web) more and more[1]. This Internet use[2] can increasingly lead to violations of security by criminals (Schneier, 2015). In particular, cyber-security is the protection of cyberspace as well as individuals and organizations that function within cyberspace and their assets in that space (Von Solms & Van Niekerk, 2013). Various hazards (i.e., situations with the potential to do harm) exist to computer users' information and pose risks to cyber-security. These include user surveillance, identity theft, phishing, viruses, spyware, trojans, and keyloggers (for details, see Appendix 1). As a result of extensive press coverage regarding corporate privacy and security disasters (Clarke, 2016; Garg, 2016), many users are exposed to information about these hazards. However, some hazards may be newer, less known and receive less coverage.

When we consider means to improve cyber-security, the nature of the hazards and the requisite countermeasures are one aspect that requires deliberation. Another aspect that needs attention is users' engagement with these and their perceptions of risk (Johnson & Tversky, 1983; Slovic, 1987; Johnston & Warkentin, 2010; Jansen & Van Schaik, 2016). Moreover, people adapt their behaviour based on how much risk they are willing to take (Workman, Bommer & Straub, 2008). Risk perceptions play a fundamental role in models as predictors of precautionary behaviour (Huang, Rau, Salvendy, Gao & Zhou, 2011; Boss, Galletta, Lowry, Moody & Polak, 2015). Precautions include the use of computer security software (e.g., anti-virus software, firewall software and anti-spyware software).

Research has demonstrated that students are lax about security, particularly in terms of mobile devices (Jones & Heinrichs, 2012; Tan & Aguilar, 2012). It is unlikely that their lack of precautions and knowledge gaps will disappear when graduates enter into the labour market. Therefore, the aim of this research is to study students'risk perceptions in Internet use, in relation to security. Our goals are to (1) determine how different potential security-related hazards on the Internet are perceived, (2) establish to what extent students take precautions (Kusev, Van Schaik, Ayton, Dent & Chater, 2009; Van Schaik, Kusev & Juliusson, 2011) against different potential security-related hazards, and (3) ascertain the antecedents of risk perception and precautionary security behaviour. Various approaches to studying risk have been developed and are reviewed next.

2 Theoretical approaches to studying risk perception

A number of theoretical approaches are available to understand how risk perceptions may be shaped by the context related to risk.

---

[1] *http://www.internetlivestats.com/internet-users/*

[2] Internet use describes the use of interconnected computerized networks, including the commercial and social platforms and applications that are running on these appliances.

Risk compensation model. Adams' (1988, 2012) conceptual risk compensation aims to explain human risk-taking behaviour as balancing between (non-monetary) costs and benefits. On the one hand, propensity to risk-taking is influenced by baseline propensity to risk-taking (individual 'risk thermostat'), which differs between individuals, and by potential rewards of a particular risk-taking behaviour. On the other hand, risk perception is influenced by the direct or indirect experience of losses from risk as a result of a particular risk-taking behaviour and voluntariness of risk (with greater perceived voluntariness resulting in lower perceived risk). Actual risk-taking behaviour is then influenced by both propensity to risk-taking and risk perception. Interventions that do not change risk propensity cannot reduce risk-taking behaviour because individuals will strive to restore the balance according to their risk thermostat. Several aspects play a role when studying risk perception.

The presentation of risk information. According to Gigerenzer, Todd et al. (1999), human decision-making is constrained by people's cognitive limitations and the structure of the environment, and a risk is an uncertainty that can be expressed as a number (e.g., probability or frequency) derived from empirical data. In particular, the aim has been to change the structure and experience of the environment by presenting information so that people's risk perception (more) closely matches empirical frequency. However, Gigerenzer et al.'s (1999) approach cannot be readily applied to the domain of online security and privacy risks, as empirical data of security breaches are usually non-existent or unreliable (Schneier, 2015).

Availability of risk information. Kahneman (2011, p. 129) stresses the essential role of availability of information ("the ease with which instances come to mind"), which influences an individual's risk perception. Availability, and thereby risk perception based on this, can be enhanced by saliency (the extent to which an event attracts attention), the dramatic nature of an event (e.g., a plane crash) and source of experience (personal experiences result in increased availability).

Affect in risk perception. According to the affect heuristic, the more technologies or activities that are associated with positive feelings, the less they are judged to be risky and the more they are judged to be beneficial (Finucane, Alhakami, Slovic & Johnson, 2000). Therefore, if people associate an activity (e.g., smoking or fracking) with positive feelings then they will judge the activity to be harmless and beneficial.

Revealed risk-related preferences. Starr (1969) used population statistics of human behaviour to infer people's (revealed) risk preferences regarding particular technologies and human activities. He analysed the relationship between risk (the statistical expectation of death per hour of exposure) and benefit (the average amount of money spent per individual participant or the average contribution made to a participant's annual income) for some common activities. However, the approach of revealed preferences suffers from several shortcomings. First, preferences may not be stable over time and aggregate data do not take into account the variability among hazards (Fischhoff, Slovic, Lichtenstein, & Combs, 1978). Second, the underlying assumption that people have both full information and use that information optimally has been refuted (Simon, 1956). Third, different measures of risk and benefit lead to different conclusions (Fischhoff et al., 1978).

Expressed risk preferences. Psychometric methods have been used to study (expressed) preferences regarding particular technologies and human activities (Slovic, 1987). This has the advantage of eliciting perceptions (thoughts and judgments) of risk from people who are (potentially) exposed to particular risks that are studied, and can provide information about the causes of behaviour and potential ways to influence this. Applications of the results of research using these methods include risk communication (Fife-Schaw & Rowe, 1996; Garg & Camp, 2012; 2015; Young, Kuo & Chiang, 2014; Kim, Choi, Lee, Cho, & Ahn, 2015) and risk policy (Slovic, Fischhoff & Lichtenstein, 1982; Huang, Ban, Sun, Han, Yuan & Bi, 2013).

Prediction equations of risk perception from a set of risk dimensions (e.g., voluntariness, controllability and newness; see Online Supplementary Material OSM1) have been developed (Fischhoff et al., 1978). A limitation is that data are usually averaged over hazards. Therefore, the effect of or variability in hazards cannot be analysed, with (other) predictors held constant, and the analysis may not predict risk perceptions for individual hazards. Moreover, there is an apparent lack of research showing how risk perceptions 'translate' into behaviour.

The current research combines the study of expressed preferences and revealed preferences. This enables us to pursue our goals: to quantify variation among hazards, and to predict risk perception and precautionary behaviour.

3 Background to the current study

Risk perception and precautionary behaviour in relation to cyber-security. As highlighted in Section 1, students are an important user group to study in terms of cyber-security. It is important to improve the awareness of one's susceptibility and fallibility to risk, and thereby increase the likelihood of online users consulting appropriate information sources to make better information security decisions. Therefore, we need to study students' risk perceptions in relation to cyber-security in order to understand where the knowledge gaps are that employers may need to tackle upon recruitment of recent graduates. Thus,

Research Question 1: how do university students perceive different online information security-related hazards in terms of risk, benefit, and other risk dimensions (cf., Fischhoff et al., 1978)?

According to Öğütçü, Testik and Chouseinoglou's (2016) results, students, academics and administrators differ in terms of online activities (such as using social media), which may expose users to cyber-security hazards. Öğütçü et al. (2016) noted that exposure to hazards was highest in students although they also engaged in more precautionary behaviour (for instance, using anti-virus software) while risk perception tended to be lowest among administrators. Therefore,

Research Question 2: to what extent do university students take precautions against online information security-related hazards?

Predicting risk perception. Previous research has proposed various risk dimensions (see Online Supplementary Material OSM1) as predictors of perceived risk that are also relevant to the current study. In particular, voluntary activities are perceived as less risky[3] (Starr, 1969). Therefore, for example, the more voluntary people believe exposure to the risks associated with phishing (the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise) is, the less risky they perceive phishing to be. When positive effects are immediate and negative consequences of an activity are delayed perceived risk is reduced (Kahneman, 2011). For example, the effect of a 'dormant' computer virus on the integrity of a computer system may only become apparent in the longer term. Knowledge by population affected is also a potential predictor, as people's risk perception is reduced when they believe they understand the underlying risks (e.g., in social-media use; Garg & Camp, 2015). In addition, the perceived knowledge by experts, or the effectiveness of systems that are seen as expert, also influences non-experts' risk perception and their behaviours (e.g., in social-media use; Garg & Camp, 2015). According to Adams (2012), when people believe they are in control, their perception of risk is reduced. Therefore, when people's perceived control over potential information security breaches is increased, their perceived risk is reduced (Rhee, Ryu & Kim, 2012). Because of the newness of some risks, people may exaggerate these (e.g., genetically modified foods). In particular, various pieces of information shared online may be combined; this may substantially increase risks to security (Schneier, 2015) and such new risks may not be acceptable to the public (Malin & Sweeney, 2001).

Moreover, people's perceptions of more common risks are normally reduced, while uncommon risks evoke dread (Fishhoff et al., 1978). In modern society, Internet use is a common activity, for example because of its efficiency; however, reliable data on risks to security are not readily available (Garg & Camp, 2015; Schneier, 2015). Activities or technologies with greater catastrophic potential, where many people are affected in a single event, are perceived as riskier, even though other activities that affect fewer people per event may overall impact more people per year (Adams, 2012; Mumpower, Shi, Stoutenborough & Vedlitz, 2013). For example, people overestimate the risk of terrorist attacks, but underestimate the risk of traffic accidents (Adams, 2012) and exposure to cyber-security hazards (LaRose, Rifon &

[3] Behaviours may be considered risky when engaging in a behaviour may increase the exposure to danger, harm or loss that may impact the individual user, their immediate network, or all users regardless of their personal connection to the individual user engaging in this behaviour. The hazards in our study each represent such sources of danger, harm or precursors of loss (e.g., in terms of personal data, finances, identity).

Enbody, 2008). Risks that are perceived to have more severe consequences are perceived to be riskier. For example, severity of consequences predicted perceived risk of water poisoning, nuclear device, airline attack and bomb (Mumpower et al., 2013). Moreover, perceptions of the severity of a security breach through hacking predicted perceived risk of online shopping in younger and older adults (Chakraborty, Lee, Bagchi-Sen, Upadhyaya & Raghav Rao, 2016).

According to the affect heuristic (Finucane et al., 2000), technologies that are perceived to be more beneficial are also perceived to be less risky and vice versa either because both are consequents of affect or because affect is a mediator. Therefore, perceived benefit is a potential predictor of perceived risk after taking into account the effect of affect. In cyber-security, insider threats can be explained by the affect heuristic (Farahmand & Spafford, 2013). In addition, demographic variables have previously been found to be predictors of risk perceptions (Bronfman, Cifuentes & Gutiérrez, 2008) and were therefore considered here for inclusion as candidate predictors (age, gender, education level, work status, years of experience in Internet use, and duration per Internet session).

Applying risk perception prediction to cyber-security. Furthermore, research in cyber-security has empirically studied risk dimensions (e.g., perceived control) as predictors of perceived risk. Huang, Rau and Salvendy (2010) and Garg and Camp (2012) conducted work in relation to the current study by analysing the perception of risk in cyber-security. Both studies analysed a set of hazards (21 and 15 respectively in the two respective studies) on the Internet in terms of perceived risk and other risk dimensions. They then used these risk dimensions to predict perceived risk. In Huang et al.'s (2010) results statistically significant predictors of risk were severity of consequences, scope of impacts, accident history, voluntariness, duration of impacts, understanding and possibility of exposure. According to Garg and Camp's results (2012), statistically significant predictors of risk were voluntariness, knowledge to science, controllability, newness, dread and severity. However, in both studies the data were collapsed over hazards in the regression analysis. Therefore, these studies could not establish the degree of variance between hazards in risk perception (e.g., specific risk differences). However, this is important as people's perceptions may differ depending on the information item that is at stake. Our study thus builds on a number of different pieces of literature, but also attempts to address certain analytical limitations. Therefore,

Research Question 3: what are the antecedents of risk perception in cyber-security in university students? Potential antecedents include voluntariness of activity, immediacy of consequences and others discussed above.

Predicting precautionary behaviour. Pattinson and Anderson (2005) noted the role of risk perception as a mediator in the relationship between risk communication and risk-taking behaviour in information security. Vance, Eargle, Anderson and Brock

Kirwan (2014) tested the strength of risk perception as a predictor of information security behaviour. Self-reported perceived risk was predictive of security behaviours only when security information was salient (through a simulated malware incident). Furthermore, self-competence was a positive predictor of precautionary behaviour against attacks from a computer virus, in employees in different sectors (Mariani & Zappalà, 2014), although there was no evidence for the role of perceived risk.

Moreover, the risk dimensions that predict perceived risk (discussed in relation to Research Question 3) are also potential predictors of precautionary behaviour. Previous research on risk perception supports this idea (Slovic, MacGregor & Kraus, 1987; Sjöberg, 2000) and the role of demographics as predictors (Layte, McGee, Rundle & Leigh, 2007). Thus,

Research Question 4: what are the antecedents of precautions taken against risk in cyber-security in university students?

Knowledge gaps. In response to gaps in previous research (see above), first, the current study considers the degree to which hazards vary in terms of individuals' (specifically, students') cyber-security-related risk perceptions and precautionary behaviour. Second, we research and identify several predictors of perceived security-related risks and precautionary behaviour online, linking our findings to the existing research in risk perception and cyber-security. Third, we demonstrate the benefits of using non-aggregated data analysis to avoid methodological fallacies and derived recommendations for educating Internet users such as students in relation to cyber-security.

4 Method

4.1 Design and material

An online-survey design was used. The independent variable was cyber-security hazard, with 16 levels. In addition, two further comparisons were included (browsing the Internet for information and information sharing on social media). Previous research has predominantly recruited USA students; therefore, in order to establish the generality of the findings, we included both UK and USA students. The dependent variables were perceived risk, perceived benefit, risk balance (risk score subtracted from benefit score; Bronfman & Cifuentes, 2003), perceptions of nine risk dimensions (see Section 3, Table 4 and Online Supplementary Material OSM1) and computer security use.

4.2 Participants

Respondents were 436 UK and USA university students (336 female, 100 male; mean age = 23, *SD* = 7; UK: *n* = 267 [students recruited from social-science and other courses at four universities]; USA: *n* = 169 [students recruited from social-science courses at a Midwestern university]). Participants received course credits or were eligible to enter a prize draw (£50 or $50) as a reimbursement. They were experienced Internet users (mean = 12 years, *SD* = 3) and used the Internet for various purposes, most notably e-mail (96.1%), social networking (91.3%), searching for work-related or study-related information (87.2%), and buying products or services (83.3%). In terms of demographics, universities did not differ on gender, frequency of Internet use or average length of Internet session ($p > .05$), but differed on age and Internet experience ($p < .001$).

4.3 Measures

A set of 16 hazards and two comparisons (Table 1 and Appendix 1 for details) was compiled based on previous research (Garg & Camp, 2012). For this research, the hazards were categorized and some hazards were added, such as zero-day attacks and cyber bullying and others deleted, such as spam and malware, to improve coverage and specificity. The first 16 items were selected because they were considered to be important potential cyber-security hazards and were categorized as identity-related (2), monitoring (1), online social (4) and software (9). In contrast, the last two were considered as relatively low-risk online activities and were included as comparisons. The definition of each of the 18 hazards/comparisons was presented to participants in the questionnaire that was used for data collection (see Appendix 1 for definitions; see Online Supplementary Material OSM1 for questionnaire). This was to ensure that they would consider the intended meaning in their response to the questionnaire items.

Perceived risk, benefit and nine risk dimensions were based on Fischhoff et al. (1978), and Bronfman, Cifuentes, Dekay and Willis (2007). These dimensions were voluntariness, immediacy of effect, knowledge about risk by affected population, knowledge about risk by science, control over risk, newness, (chronic-)catastrophic potential, dread, and severity of consequences (see Online Supplementary Material OSM1 for details). In response to each item (from the set of 16 hazards and 2 comparisons [Table 1]), participants had to give a rating on 11 dimensions of risk perception, using a 7-point semantic-differential.

We used and expanded the Computer Security Usage scale (CSU; Claar & Johnson, 2012) to five items, with a 7-point Likert scale to measure precautionary behaviour against specific potential Internet security hazards. In particular, these were taking protective measures through add-on anti-virus software, firewall software, antispyware software, software updates and security updates. By engaging in this behaviour, computer users can reduce the likelihood of breaches due to software hazards such as virus infection from occurring. Therefore, risk perceptions of specific software hazards may be predictive of computer security use.

A principal component analysis with varimax rotation of the CSU produced a one-component solution, and explained 65% of variance, with loadings ranging from 0.67 to 0.82 (average = 0.80). Internal-consistency reliability was good (Cronbach’s alpha

= 0.87). On the scale, mean scores were calculated per participant and used in subsequent data analysis.

4.4 Procedure

Research ethics approval was obtained from the local research ethics committee at two universities. The ethics approval at these two institutions was subsequently accepted by the additional institutions involved in data collection. Students were recruited by e-mail, with a link to the online questionnaire. Questions on demographics were presented first. The next section included each of the 18 hazards/comparisons. Each hazard was presented individually and in randomized order to all participants. For each hazard, participants answered 11 perception-related questions on perceived risk, benefit, and nine additional risk dimensions (see above) in random order. Finally, the CSU items were presented in random order.

5 Results

5.1 Analysis of hazards and precautionary behaviour

In relation to *Research Question 1*, we analysed how different online information security-related hazards are perceived. Confidence intervals of the mean (see Table 2) for 16 hazards and 2 comparisons indicate that perceived risk was highest for identity theft, keylogger, cyber-bullying and social engineering, and lowest for browsing Internet sites for information and cookie. The converse was true for risk balance (Table 3). Preliminary mixed-measures analysis of covariance (ANCOVA) of the four UK samples was conducted. Hazard was the within-subject independent variable, nation was the between-subjects variable and other demographics were covariates (age, gender, frequency of Internet use, average length of Internet session and years of Internet experience). The results show that the sample did not have a significant main effect or interaction effect on perceived risk ($p > .05$). The following analysis therefore combined the UK samples.

With the same covariates, mixed-measures ANCOVA for the 16 hazards showed a small significant effect of hazard on risk perception (F (15, 6480) = 10.04, $p < .001$, partial eta squared = .02), a non-significant effect of nation (UK vs US) (F (1, 427) = 2.58, $p > .05$, partial eta squared < .01) and a small significant interaction effect (F (15, 6480) = 6.14, $p < .001$, partial eta squared = .01). The remaining covariates were not significant ($p > .05$). Follow-up pairwise comparisons with Bonferroni correction and the same covariates showed the following significant differences: US-students' perceptions of risk were higher than UK-students' perceptions for surveillance (partial eta squared = .03, small to moderate effect size, $p < .001$) and cookie (.05/moderate/< .001), but lower for social engineering (.03/small to moderate/< .001). Although the interaction effect was significant, the main finding regarding the comparison of the two nations is that overall the pattern of mean scores across hazards in both was clearly similar (see Figure 1); this is despite the small interaction effect that was inevitably statistically significant due to the large sample size (Field, 2013).

Analysis by nation showed that the effect of hazard on risk perception was small to moderate and significant in UK students (F (15, 3960) = 10.49, p < .001, partial eta squared = .04), but small and approaching significance in US students (F (15, 2520) = 1.43, p = .06, partial eta squared = .01). None of the covariates were significant. Pairwise comparisons with Bonferroni correction over the pooled samples showed that *identity theft* was generally perceived as riskiest (significantly riskier than 12 other hazards in US students and nine other hazards in UK students). Two hazards were generally perceived as the least risky: *cookie* (less risky than 15 other hazards in UK students and 14 other hazards in US students) and *e-mail-harvesting* (less risky than 13 other hazards in UK students and 12 other hazards in US students). Additional analysis showed that the comparison item *browsing Internet sites* was generally perceived as least risky in both UK and US students (but equally risky as cookie) and the comparison item *information-sharing on social media* was perceived as the second least risky (less risky than 12 other hazards in UK students and 8 other the hazards in US students).

Risk profiles were analysed per hazard, showing the mean for perceptions of risk, benefit, and the nine risk dimensions (Table 4). Differences among hazards were greatest on perceived risk, perceived benefit, and severity of consequences (all partial eta squared = .02). Mixed-measures ANCOVA showed that the effect of hazard was significant for all perceived-risk dimensions. Again, the pattern of mean scores across the hazards was clearly similar, and the main effect of nation and its interaction with hazard were small (average partial eta squared = .01).

In relation to *Research Question 2*, we analysed to what extent people take precautions against different online information security-related hazards. The level of precautionary behaviour (computer security use over the five behaviours) was relatively high (in comparison to the neutral scale value of 4, mean = 5.29, $CI_{.95}$ = [5.13; 5.39]). Computer security use was not significantly correlated (all p > .05) with average time per Internet session(r = -.02), Internet experience in years (r = .05), frequency of logging on to the Internet (r = .00), age (r = .04), gender (r = .01) or sample (UK vs US, r = .05).

In an analysis of individual scale items, repeated-measures ANOVA showed a significant effect of individual computer security behaviour (F (4, 1740) = 27.11, p < .001, partial eta squared = .06). Follow-up pairwise comparisons with Bonferroni correction showed that security behaviour was more frequent in terms of using anti-virus software (mean = 5.35, SD = 1.84), installing operating-system software updates (mean = 5.52, SD = 1.52) and installing security-software updates (mean = 5.53, SD = 1.70) than in terms of using add-on firewall software (mean = 5.04, SD = 1.87) and anti-spyware software (mean = 4.88, SD = 1.94) (all six comparisons: p < .001).

5.2 Predicting perceived risk and precautionary behaviour

In relation to *Research Question 3*, we analysed the antecedents of risk perception in online information security. In the analysis of perceived risk, two levels can be distinguished: hazard (at Level 1, 16 hazards, corresponding with Internet security hazards, existed) and subject (or participant; at Level 2, 436 participants existed). In relation to different analysis levels (non-aggregated [e.g., individual respondent] and aggregated [e.g., group]), Pedhazur (1997) points out that *cross-level* inferences (interpreting the results obtained at one level [e.g., group] to apply to another [e.g., individual]) “may be, and most often are, fallacious and grossly misleading” (p. 677). Similarly, Tabachnick and Fidell (2013) discuss the *ecological fallacy*: analysing only aggregated data (at a higher level) and then interpreting the results at a higher level to apply to a lower level. In order to avoid cross-level inferences and the ecological fallacy, multi-level analysis was performed, with perceived risk as the dependent variable and the remaining variables as predictors[4]. For comparison with previous research (Garg & Camp, 2012), who tested their model of perceived risk with multiple-regression analysis, Online Supplementary Material OSM2 presents corresponding results of multiple-regression analysis. The difference in the results with those of our multi-level analysis (presented below) clearly demonstrates the fallacy of cross-level inferences and the benefit of conducting non-aggregated analysis.

In staged model testing (recommended by Tabachnick & Fidell, 2013), the difference between subsequent models was tested (Table 5). A model with hazard-related Level-1 predictors (Model 2) explained more variance than the null model (without predictors) (Model 1). Model 3 (Model 2 augmented with established subject-related Level-2 predictors) explained significantly more variance than Model 2. Model 4 (Model 3 augmented with interaction effects of hazard with the Level-1 predictors) explained significantly more variance than Model 3. Model 5 (Model 4 augmented with exploratory Level-2 predictors) explained significantly more variance than Model 3 and Model 4. Therefore, Model 5 was retained as the final model. The following results are those observed in this final model (Table 6). Significant Level-2 (subject-related) predictors of perceived risk were voluntariness (over all hazards), immediacy (over all hazards), catastrophic potential (over all hazards), dread (over all hazards), severity (over all hazards), length of Internet experience, and frequency of Internet logon. Specifically, the results show that perceived risk was higher the longer Internet experience, the less frequent Internet use, the greater involuntariness (over all hazards), the greater immediacy/the less delay (over all hazards), the greater catastrophic potential (over all hazards), the less dread (over all hazards) and the greater perceived severity (over all hazards) were.

Significant Level-1 (hazard-specific) predictors were voluntariness, control, catastrophic potential, severity, knowledge to science by hazard, dread by hazard

[4] The analysis did not include subject (participant) as a random effect. This is because the finding of a significant random effect of subject is expected and not of interest.

and severity potential by hazard. The greater involuntariness (hazard-specific), the greater lack of control (hazard-specific), the greater catastrophic potential (hazard-specific) and the greater perceived severity (hazard-specific) were, the higher perceived risk was.

Some further observations are worth noting here. The contribution to predicting perceived risk by hazard-specific knowledge to population, dread and severity was moderated by, and therefore varied with, hazard. Because of these three moderated effects, follow-up regression analyses per hazard were conducted (Online Supplementary Material OSM2). Most consistent were the effects of severity of consequences, catastrophic potential, dread and benefit. Furthermore, where the correlation between dread (over all hazards) and perceived risk was positive, the regression coefficient was negative. This result may be interpreted as effect reversal, a type of suppressive recast mediation (Koeske & Koeske, 2006). Results from additional analysis indicate that, together, the predictors severity (hazard-specific and over all hazards) and catastrophic potential severity (hazard-specific and over all hazards) were responsible for the effect reversal; with both these predictors removed the regression co-efficient changed from negative (-.09) to positive (.03). As in previous analyses (see Section 5.1), in our multi-level analysis hazards also differed in perceived risk, but here we show that this is the case even with length of Internet experience, frequency of Internet use and perceptions of other risk dimensions, both over all hazards and hazard-specific, held constant. Moreover, the effect of risk dimension varied depending on level of aggregation (over all hazards or hazard-specific). In particular, control was a positive predictor of perceived risk at the level of hazard, but not at the level of participant. There was also evidence of a composition effect of voluntariness, catastrophic potential and severity[5]. For example, perceived risk decreased as voluntariness for specific hazards increased; this was in addition to the decrease in perceived risk with an increase in voluntariness over all hazards.

In relation to *Research Question 4*, we analysed the antecedents of precautionary behaviour against risk in cyber-security. Precautionary behaviour was analysed for those behaviours for which risk perceptions of hazards were also measured. These were using anti-virus software and using anti-spyware software. Overall, the amount of variance that we were able to explain in computer security use was low (e.g., around 3 to 4% in the use of anti-spyware and anti-virus software respectively). For the behaviour of using anti-virus software, control was a significant positive predictor (beta = 0.12, $p < 0.05$), so the more participants perceived themselves to be in control over the risk computer viruses posed, the more frequently they used anti-virus software.

[5] A composition effect is the extent to which the relationship at a higher level adds to or differs from the relationship at a lower level (Heck, Thomas & Tabata, 2010).

5.3 Summary of results

The analysis of hazards showed significant variation among security hazards in perceived risk, benefit and other risk dimensions (voluntariness, immediacy of effect, knowledge about risk by affected population, knowledge about risk by science, control over risk, newness, (chronic-)catastrophic potential, dread, and severity of consequences). Students perceived identity theft as the riskiest hazard, and cookie and e-mail harvesting as the least risky. The self-reported level of precautionary behaviour taken by students was relatively high and highest for using anti-virus software, and installing operating-system software updates and security software.

Significant positive predictors of students' risk perceptions were Internet experience, involuntariness, lack of control, immediacy of consequences, catastrophic potential and severity. Significant negative predictors were frequency of Internet use and dread. A significant positive predictor of the precautionary behaviour of using anti-virus software was perceived control.

6 General discussion

The specific aim of this research is to study risk perceptions on the Internet, in particular in relation to security. Our goals were to (1) determine how different security-related hazards on the Internet are perceived, (2) establish to the extent to which students take precautions against different potential security-related hazards, and (3) ascertain the antecedents of risk perception and precautionary behaviours. In this section, we review our results in relation to each of the three goals. We also discuss the implications of our work, make recommendations, and discuss limitations of our work and ideas for future work.

6.1 Risk perceptions and precautions for individual hazards

Although previous research (Garg & Camp, 2012) analysed students' risk perceptions of Internet hazards, differences among hazards were not statistically tested. Our results are novel as we statistically test differences, not only in terms of perceived risk, but also on other risk dimensions. In the next section, we discuss our results in relation to hazard-specific risk perception and precautionary behaviour.

Risk perception. The results for risk perception suggest that among our participants, perceptions of risk, dread and severity were highest for identity theft and keylogger on the Internet – the former finding in line with the results by Garg and Camp (2012). Both keyloggers and identity theft suggest immediate and personal consequences for users, which may therefore also have increased our respondents' perceptions of risk. In addition, press coverage about identity theft may have increased awareness by increasing availability, "the ease with which instances" of identity theft come to mind (Kahneman, 2011, p. 129). Perceptions of risk and severity were also among the highest for cyber-bullying and social engineering. This may be because both these hazards were described in terms of their adverse consequences (harming or harassing a victim for cyber-bullying and releasing a victim's valuable information for social engineering). Both news reports in the media of cyber-bullying may lead to higher availability of episodes related to these risks. In addition, students may be more aware of cyber-bullying due to their use of social media, thereby raising concerns (Finucane et al., 2000). These circumstances may both increase the perceived risk of being targeted by a social-engineering attack as well.

There was also significant variance in terms of the degree to which hazards did or did not raise risk perceptions. For example, perceptions of risk were among the lowest for catfishing (a type of social engineering; see Appendix 1). This may be because genuine potential adverse consequences for the individual are not immediately obvious and in contrast to cyber-bullying or identity theft, it is less likely for most students to come across the real-world equivalent in their daily interactions.

Precautionary behaviour. Our participants' ratings of their precautionary behaviour in terms of computer security usage were relatively high but not correlated with demographics. Furthermore, some computer security behaviours (e.g., relating to anti-virus software) were used more frequently than others (e.g., relating to anti-spyware software), perhaps because the former are more familiar. This self-reported behaviour is only related to software hazards; in particular, virus and spyware were included in the scale items. However, these tools may not be effective against identity-related and online social hazards. Moreover, users may make trade-offs between security and convenience. Herley (2009), for example, argues that security behaviour may protect users against direct costs of potential security breaches, but at the same time burdens them with indirect costs in terms of effort. This means adopting security measures is also associated with additional costs, reducing users' intention to adopt and implement security measures (e.g., Lee, 2011; Liang & Xue, 2010).

6.2 Antecedents of perceived risk and precautionary behaviour

Previous research tested the predictive power of risk dimensions for perceived risk in cyber-security (Huang et al., 2010; Garg & Camp, 2012, 2015). However, this previous work used aggregated data analysis and therefore suffered from the ecological fallacy. Moreover, there seems to be a lack of research testing a comprehensive set of risk perception predictors.

Risk perception. Antecedents of risk perception were differentiated in terms of those that were hazard-specific (Level-1) and subject-specific predictors (Level-2). Together, these were analysed using multi-level analysis (Heck et al., 2010). Perceived risk was positively predicted by immediacy (over all hazards), catastrophic potential (over all hazards) and perceived severity (over all hazards), catastrophic potential (hazard-specific) and perceived severity (hazard-specific), as well as Internet experience. These findings lead us to conclude the following. First, the greater the perceived *immediacy* of security hazards overall, the higher the perceived risk of cyber-security hazards. This is consistent with previous work that indicates that when negative consequences are likely to be delayed, perceived risk is reduced (Kahneman, 2011).

Second, perceived risk was higher with greater perceived *catastrophic potential* of hazards overall and of individual hazards. This finding is consistent with the idea that hazards with a larger impact on a single occasion are perceived as more risky (Adams, 2012) and with research findings showing that this applies to a range of hazards in the domain of terrorism (Mumpower et al., 2013). Third, the greater the *severity* of consequences of hazards overall and of individual hazards was, the higher the perceived risk. Previous research has also demonstrated that risks that are perceived to have more severe consequences are perceived to be riskier. For example, perceptions of the severity of a security breach through hacking predicted perceived risk of online shopping (Chakraborty et al., 2016). Fourth, *Internet experience* was a significant positive predictor of perceived risk. This finding is consistent with previous research that has demonstrated that personal experience positively predicts perceived risk (Van der Linden, 2014; Lujala, Lein & Rød, 2015).

A number of variables operated as negative predictors of risk perceptions. These were voluntariness (over all hazards), voluntariness (hazard-specific) and control (hazard-specific), as well as frequency of Internet use. The prediction of risk perception by (hazard-specific) knowledge by population, dread and severity, was moderated by hazard. These results also indicate, first, that the less *voluntary* an Internet user perceives exposure to security hazards overall and to individual hazards, the riskier they perceive specific hazards to be. These findings provide support for the idea that the more voluntary risks are perceived to be, the less risky they are perceived to be (Starr, 1969). This can lead to optimism bias (underestimation) regarding security risk (Rhee et al., 2012) and consequently less safe online behaviour on the network (Huang et al., 2011). Second, when people feel more in *control,* their perception of risk is reduced (see also Rhee et al., 2012). Our results support this idea, as perceived control over individual hazards was a significant negative predictor of perceived risk. Third, students who more frequently *used the Internet* (more than three times a day) perceived cyber-security hazards as less risky. This may be because students who are more frequent Internet users are also more prone to impulsivity and sensation-seeking, which have been linked to reduced risk perception (Hosker-Field, Molnar & Book, 2016).

Precautionary behaviour. Our analyses revealed that the predictive power of our antecedents of precautionary behaviour was considerably less (they only explained 3 to 4% of the variance compared to more than 40% of variance in terms of risk perception). This may be due to a number of reasons. First, measurements of precautionary behaviour were available for only two hazards, while risk perception was measured for 16 hazards. Second, a comprehensive multi-level analysis with each hazard measured in terms of risk dimensions and precautionary behaviour was not an option here. Our results show that control was a significant positive predictor of computer security use, in terms of using add-on anti-virus software. Therefore, and consistent with previous research (e.g., Anderson & Agarwal, 2010), students who felt more in control of their computer security used anti-virus software more frequently.

6.3 Methodological implications

The specific aim of this research is to study university students' risk perceptions and precautionary behaviour in Internet use, in relation to security. As part of this research, we expand on and contribute to the existing theory and research in a number of ways. First, and at a more general level, we introduced readers to different approaches that may be used in the study of risk and outline the pros and cons of these in terms of their merit or use to inform empirical research. We expand on existing work on risk perception by studying a broad range of both technical and social hazards. The research design is inspired by and builds on the previous studies conducted in China and the USA with students (Huang, 2011; Garg & Camp, 2012, 2015), older adults (Garg, Lorenzen-Huber, Camp & Connelly, 2012) and others (Huang et al., 2010) as participants, but is novel in the following respects.

In terms of the theoretical as well as methodological level, we use a multi-level analysis and provide an example of how the expressed risk-related preference approach (see Slovic, 1987) may support a more refined analysis of risk perceptions. We essentially demonstrate the benefit of psychometric methods. Our study thus provides insight that may contribute to the improvements in research design and data analysis, most notably through multi-level analysis on non-aggregated data. This is important because existing research that has developed prediction equations of perceived risk has usually averaged data over hazards (Fischhoff et al., 1978), thereby potentially suffering from the fallacy of cross-level inferences (Pedhazur, 1997) and the ecological fallacy (Tabachnick & Fidell, 2013). At a methodological level alone, we analysed both risk perception and precautionary behaviour separately and in relation to each other, rather than only risk perception (Slovic, Kraus, Lappe, Letzel & Malmfors, 1989). Our approach to studying risk perception and precautionary behaviour can be summarised as follows. We compared the results of our non-aggregated linear multi-level analysis (Section 5.2) with those of aggregated multiple-regression analyses (Online Supplementary Material OSM2). We found that the latter analysis failed to identify immediacy and control as significant predictors of perceived risk (although these predictors were significant in the former analysis) and incorrectly identified benefit as a significant predictor. These results empirically demonstrate the loss of information (Tabachnick & Fidell, 2013) that aggregated analysis entails. As a comparison, Garg and Camp's (2012) regression analysis of perceived risk was conducted at the aggregate level and therefore could not identify the moderation of predictors by hazard, as in our study.

The implication of the results of multi-level analysis is that in statistical inference non-aggregated data should be analysed to avoid fallacies of inference and a loss of information that are associated with the analysis of aggregated data. In particular, in prediction equations, multi-level analysis needs to include two levels: hazard (Level

1) and subject (over hazards, Level 2). Level 1 predictors are those that have been measured per hazard (e.g., perceived control to avoid potential harm from a particular hazard). Level 2 predictors are those that have not been measured per hazard (e.g., length of Internet experience) and aggregates of Level 1 predictors (e.g., perceived control to avoid potential harm from the combined set of hazards that is presented). The analysis of the predictive power of these Level 2 aggregates and their Level 1 counterparts allows us to assess which predictors are significant at each level, and whether a compositional effect exists (Heck et al., 2010).

6.4 Practical implications and recommendations

Organisations have several options available to them to teach students and other computer users about risks and educate them about the merit of precautionary behaviours. *Education*-based interventions (Caputo, Pfleeger, Freeman & Johnson, 2014) will typically involve developing knowledge and skills of learners, with potential 'refresher' education from time to time; the aim is that the application of knowledge and skills 'transfers' to the real-world, so that computer users are more likely to engage in safe behaviour. *Marketing*-linked interventions (Reid & Van Niekerk, 2016) will typically employ one-off awareness campaigns or continual campaigns presenting persuasive messages, with changing content and/or delivery to keep the audience's attention; the aim is that computer users' raised awareness will make them act safely in the real world. Some interventions may focus on the use of specific *design* features (e.g., Coventry, Briggs, Jeske & Van Moorsel, 2014) such as human-computer interaction 'nudges' to improve people's precautionary decisions. The advantage of these types of intervention is that nudges direct people's choices, without coercion, towards safer behaviour by helping them to engage in precautionary decision-making behaviour that is also less effortful (or by making less safe behaviour more effortful). Based on our prediction results regarding precautionary behaviour (discussed in Section 6.2), education and marketing interventions should consider emphasising computer users' control in relation to software hazards.

We can identify a number of practical recommendations, many of which build on existing recommendations to raise their information security awareness (see also Ahmad & Maynard, 2014; Kim, 2014). Based on our results regarding the variability of risk perception and precautionary behaviour among hazards, universities' education and marketing interventions should consider the following. First, although some security-related hazards (e.g., catfishing) are perceived by students as less risky than others, they do pose potential danger. Consequently, students – and future new hires – may be particularly vulnerable to security breaches emanating from a lack of awareness of these hazards. Therefore, if the aim is to raise risk perception for specific hazards among students then target hazards that can have substantial negative consequences for students, but that are perceived as less risky (technical hazards such as trojans and online social hazards such as catfishing). Second, if the aim is to increase precautionary behaviour among students then target technical hazards of using add-on firewall software and anti-spyware software (relative to other technical hazards).

Based on our results on the prediction of risk perception and precautionary behaviour, universities' education- and marketing interventions should consider the following. First, if the aim is to raise risk perception then (1) target students who have less experience with using the Internet and students who use the Internet more frequently; and (2) emphasise to students the knowledge to population, dread and severity associated with particular hazards[6]. More generally, interventions should ideally be considering the baseline knowledge of individuals about hazards to tackle gaps in risk knowledge strategically. Second, if the aim is to increase precautionary behaviour then emphasise students' control in relation to software hazards.

We illustrate potential specific interventions with the hazard of catfishing. In an education intervention (Caputo et al., 2014), students (or members of other target populations) may develop knowledge about the nature of catfishing in terms of its defining features and skills in detecting catfishing through realistic exercises. In a marketing intervention (Reid & Van Niekerk, 2016), members of the target population (e.g., university students) may receive persuasive messages, warning of the potential negative consequences of falling victim to and/or the benefits of avoiding catfishing. After all, when risks are underestimated it can encourage people to demonstrate unsafe behaviour (Huang et al., 2011). In a design intervention (Coventry et al., 2014), the e-mail client program may be enhanced with an automated catfishing detector that analyses individual messages sent to a student-user, and e-mail threads between the user and the perpetrator; when the program detects a potential instance of catfishing, the user is notified and urged not to (further) respond.

6.5 Limitations and future research

This study has some methodological and substance-related limitations. In terms of *method*, for example, a limitation of the current study is its cross-sectional design. Longitudinal research may be better suited to testing and assessing the stability of risk perceptions. Additionally, this paper deals with conduct-related risk. People's behaviour often changes when they become more familiar with risks. In other words, a potential difficulty of studying such risk is that perceptions change once risks are identified as such (see also Garland, 2003). Hence, risk is reactive, meaning that respondents' perceptions might be influenced by filling out a risk questionnaire.

In addition, our sample consisted of (mainly social-science) students, so the results may not generalise to other populations; however, students are an important group to study in their own right in relation to cyber-security (see Section 3). Furthermore,

[6] phishing, cookie for knowledge to population; and phishing, identity theft, Internet surveillance, cookie, trojans, botnet, e-mail harvesting, virtual stalking, cyber-bullying and social engineering for dread.

we did not rely on participants' risk perception only, but also measured computer security behaviours with the CSU measure (Claar & Johnson, 2012).

We also ought to acknowledge that the antecedents we reviewed above are unlikely to be a 'complete list'. Rather, we set out to determine how useful predictors are that appear in the risk perception literature using psychometric methods, but now in the context of security in online social networks. Furthermore, future work may use a more comprehensive measurement of security measurement (Egelman & Peer, 2015; Egelman, Harbach & Peer, 2016) that includes a precautionary behaviour for each hazard[7]. In addition, the focus of our paper was on threat appraisal, rather than coping appraisal. Future research may build on the detailed insights regarding perceived threat appraisal from our study by exploring both threat appraisal and coping appraisal together and how they influence behaviour.

In terms of *substance*, in our results, the effect of control on perceived risk differed from its effect on precautionary behaviour. This can be understood as follows. On the one hand, recent studies have demonstrated the positive effect on precautionary behaviour of personal responsibility to take control of one's own security (Anderson & Agarwal, 2010; Boehmer, LaRose, Rifon, Alhabash & Cotten, 2015; Shillair, Cotten, Tsai, Alhabash, Larose & Rifon, 2015; Jansen & Van Schaik, 2016; Jansen, Veenstra, Zuurveen & Stol, 2016). On the other hand, more control results in a reduction in perceived risk (Rhee et al., 2012), which (in turn) leads to less precautionary behaviour. Future longitudinal research may be able to give a better insight into how different antecedents interact, inhibit or enable each other.

A focus on and blame of 'the human factor' as the 'weakest link' to explain security breaches ignores the limitation of other layers of the security control system (e.g., anti-virus software, host intrusion protection system, network protection and firewall) (Garg, 2016). In Garg's argument, if security is breached because of human error, a host of other controls have failed as well; for example, anti-virus software might only block 70% of computer viruses, but anti-virus is still considered useful and is purchased. Therefore, why do we expect human computer users to make correct cyber-security decisions 100% of the time, but not expect technical controls (e.g., security software) to work correctly 100% of the time? "If anything, technical controls should perform better" (Garg, 2016). Interdisciplinary future research may therefore examine the security control system as a whole. A comprehensive analysis may identify alternative security plans from which to choose to achieve a target level of security that is deemed acceptable.

7 Conclusion

Using psychometric methods in a quantitative empirical online study, we analysed students' security-related risk perceptions and precautionary behaviour in their use

[7] Egelman and Peer's (2015) inventory was not available at the time the current study was designed.

of the Internet. The main contributions of our work lie in demonstrating variation between hazards in people's risk perceptions related to cyber-security; and identifying predictors of perceived security-related risks and precautionary behaviour online in relation to existing research in risk perception and cyber-security. The main implications are the empirical demonstration that non-aggregated data analysis can help avoid methodological fallacies and derived recommendations for behavioural interventions with regard to cyber-security. We encourage future research to build on our insights, as part of a larger effort to better understand the determinants of people's propensity to protect themselves from potential cyber-security hazards.

References

Adams, J. G. U. (1988). Risk homeostasis and the purpose of safety regulation. *Ergonomics, 31*(4), 407-428. doi:10.1080/00140138808966688

Adams, J. (2012). Managing transport risks: what works? In R. Hillerbrand, P. Sandin & M. Peterson (Eds.), *Handbook of risk theory, epistemology, decision theory. ethics, and social implications of risk* (pp. 239-264). Berlin: Springer Science Business Media.

Ahmad, A., & Maynard, S. (2014). Teaching information security management: Reflections and experiences. *Information Management and Computer Security, 22*(5), 513-536. doi:10.1108/IMCS-08-2013-0058

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly: Management Information Systems, 34*(SPEC. ISSUE 3), 613-643.

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behaviour: Towards an intervention strategy for college students. *Behaviour and Information Technology,34*(10), 1022-1035. doi:10.1080/0144929X.2015.1028448

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly: Management Information Systems, 39*(4), 837-864.

Bronfman, N. C., & Cifuentes, L. A. (2003). Risk perception in a developing country: The case of Chile. *Risk Analysis, 23*(6), 1271-1285. doi:10.1111/j.0272-4332.2003.00400.x

Bronfman, N. C., Cifuentes, L. A., Dekay, M. L., & Willis, H. H. (2007). Accounting for variation in the explanatory power of the psychometric paradigm: The effects of aggregation and focus. *Journal of Risk Research, 10*(4), 527-554. doi: 10.1080/13669870701315872

Bronfman, N. C., Cifuentes, L. A., & Gutiérrez, V. V. (2008). Participant-focused analysis: Explanatory power of the classic psychometric paradigm in risk perception. *Journal of Risk Research, 11*(6), 735-753. doi:10.1080/13669870801967143

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going spear phishing: Exploring embedded training and awareness. *IEEE Security and Privacy, 12*(1), 28-38. doi:10.1109/MSP.2013.106

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Raghav Rao, H. (2016). Online shopping intention in the context of data breach in online retail stores: an examination of older and younger adults. *Decision Support Systems, 83*, 47-56. doi:10.1016/j.dss.2015.12.007

Claar, C. L., & Johnson, J. (2012). Analyzing home pc security adoption behavior. *Journal of Computer Information Systems, 52*(4), 20-29. doi: 10.1080/08874417.2012.11645573

Clarke, R. (2016). Vignettes of corporate privacy disasters. Retrieved from *http://www.rogerclarke.com/DV/PrivCorp.html*

Coventry, L., Briggs, P., Jeske, D., & van Moorsel, A. (2014). SCENE: a structured means for creating and evaluating behavioral nudges in a cyber security environment. *International Conference of Design, User Experience, and Usability* (pp. 229-239). Springer.

Egelman, S., Harbach, M., & Peer, E. (2016). Behavior ever follows intention?: A validation of the security behavior intentions scale (SeBIS). *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems,* 5257-5261. doi: 10.1145/2858036.2858265

Egelman, S., & Peer, E. (2015). Scaling the security wall : Developing a security behavior intentions scale (SeBIS). *33rd Annual CHI Conference on Human Factors in Computing Systems, CHI 2015, 2015-April* 2873-2882. doi:10.1145/2702123.2702249

Farahmand, F., & Spafford, E. H. (2013). Understanding insiders: an analysis of risk-taking behavior. *Information Systems Frontiers, 15*(1), 5-15. Doi:10.1007/s10796-010-9265-x

Field, A. P. (2013). *Discovering statistics using IBM SPSS statistics*. London: Sage.

Fife-Schaw, C., & Rowe, G. (1996). Public perceptions of everyday food hazards: A psychometric study. *Risk Analysis, 16*(4), 487-500. doi: 10.1111/j.1539-6924.1996.tb01095.x

Finucane, M. L., Alhakami, A., Slovic, P., & Johnson, S. M. (2000). The affect heuristic in judgments of risks and benefits. *Journal of Behavioral Decision Making, 13*(1), 1-17. doi: 10.1002/(SICI)1099-0771(200001/03)13:1<1::AID-BDM333>3.0.CO;2-S

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., & Combs, B. (1978). How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy Sciences, 9*(2), 127-152. doi:10.1007/BF00143739

Garg, V. (2016). *Threats, facts, bribery, and beyond: All we do to stop a click. Presentation delivered at the CITP luncheon speaker series, Princeton university, 12 April 2016*. Princeton, NJ, USA.

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

Garg, V., & Camp, L. J. (2015). Cars, condoms, and Facebook. In Y. Desmedt (Ed.), *Information security* (pp. 280-289) Springer International Publishing. Doi: 10.1007/978-3-319-27659-5_20

Garg, V., Lorenzen-Huber, L., Camp, L. J., & Connelly, K. (2012). Risk communication design for older adults. *29th International Symposium of Automation and Robotics in Construction, ISARC 2012,* Eindhoven.

Garland, D. (2003). The rise of risk. In R. V. Ericson, & A. Doyle (Eds.), *Risk and morality* (pp. 48-86) University of Toronto Press Toronto.

Gigerenzer, G., & Todd, P. et al. (1999). *Simple heuristics that make us smart*. Oxford: Oxford University Press.

Heck, R. H., Thomas, S. L., & Tabata, L. N. (2010). *Multilevel and longitudinal modeling with IBM SPSS*. London: Routledge Academic.

Herley, C. (2009). So long, and no thanks for the externalities: The rational rejection of security advice by users. *New Security Paradigms Workshop 2009, NSPW 2009,* Oxford. 133-144. doi:10.1145/1719030.1719050

Hosker-Field, A. M., Molnar, D. S., & Book, A. S. (2016). Psychopathy and risk taking: Examining the role of risk perception. *Personality and Individual Differences, 91*, 123-132. doi:10.1016/j.paid.2015.11.059

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

Huang, D., Rau, P., Salvendy, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human Computer Studies, 69*(12), 870-883. doi: 10.1016/j.ijhcs.2011.07.007

Huang, L., Ban, J., Sun, K., Han, Y., Yuan, Z., & Bi, J. (2013). The influence of public perception on risk acceptance of the chemical industry and the assistance for risk communication. *Safety Science, 51*(1), 232-240. doi:10.1016/j.ssci.2012.05.018

Jansen, J., & Schaik, P. van (2016). Understanding precautionary online behavioural intentions: A comparison of three models. In N. Clarke, & S. Furnell (Eds.), *Tenth international symposium on the human aspects of information security & assurance (HAISA 2016)* (pp. 1-10)

Jansen, J., Veenstra, S., Zuurveen, R. & Stol, W. (2016). Guarding against online threats: why entrepreneurs take protective measures. *Behaviour & Information Technology*, *35*(5), 368-379. doi: 10.1080/0144929X.2016.1160287

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

Jones, B. H., & Heinrichs, L. R. (2012). Do business students practice smartphone security? *Journal of Computer Information Systems, 53*(2), 22-30. doi: 10.1080/08874417.2012.11645611

Johnson, E. J., & Tversky, A. (1983). Affect, generalization, and the perception of risk. *Journal of Personality and Social Psychology, 45*(1), 20-31. doi:10.1037/0022-3514.45.1.20

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*, 549-566.

Kahneman, D. (2011). *Thinking, fast and slow*. London: Penguin.

Kim, E. B. (2014). Recommendations for information security awareness training for college students. *Information Management and Computer Security, 22*(1), 115-126. doi:10.1108/IMCS-01-2013-0005

Kim, K. H., Choi, J. W., Lee, E., Cho, Y. M., & Ahn, H. R. (2015). A study on the risk perception of light pollution and the process of social amplification of risk in Korea. *Environmental Science and Pollution Research,* doi:10.1007/s11356-015-4107-5

Koeske, G. F., & Koeske, R. (2006). A typology of outcome patterns in three-variable models: The pervasive role of mediation in causal systems. *Journal of Social Service Research, 33*(1), 1-14. doi:10.1300/J079v33n01_01

Kusev, P., van Schaik, P., Ayton, P., Dent, J., & Chater, N. (2009). Exaggerated risk: Prospect theory and probability weighting in risky choice. *Journal of Experimental Psychology: Learning Memory and Cognition, 35*(6), 1487-1505. doi:10.1037/a0017039

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM, 51*(3), 71-76. doi:10.1145/1325555.1325569

Layte, R., McGee, H., Rundle, K., & Leigh, C. (2007). Does ambivalence about becoming pregnant explain social class differentials in use of contraception? *European Journal of Public Health, 17*(5), 477-482. doi:10.1093/eurpub/ckl263

Lee, Y. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems, 50*(2), 361-369. doi:10.1016/j.dss.2010.07.009

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association of Information Systems, 11*(7), 394-413. Available at: http://aisel.aisnet.org/jais/vol11/iss7/1

Linden, S. van der (2014). On the relationship between personal experience, affect and risk perception: The case of climate change. *European Journal of Social Psychology, 44*(5), 430-440. doi:10.1002/ejsp.2008

Lujala, P., Lein, H., & Rød, J. K. (2015). Climate change, natural hazards, and risk perception: The role of proximity and personal experience. *Local Environment, 20*(4), 489-509. doi:10.1080/13549839.2014.887666

Malin, B., & Sweeney, L. (2001). Re-identification of DNA through an automated linkage process. *Proceedings. AMIA Symposium,* 423-427. doi:D010001685

Mariani, M. G., & Zappalà, S. (2014). PC virus attacks in small firms: Effects of risk perceptions and information technology competence on preventive behaviors.

TPM - Testing, Psychometrics, Methodology in Applied Psychology, 21(1), 51-65. doi:10.4473/TPM21.1.4

Mumpower, J. L., Shi, L., Stoutenborough, J. W., & Vedlitz, A. (2013). Psychometric and demographic predictors of the perceived risk of terrorist threats and the willingness to pay for terrorism risk management programs. *Risk Analysis, 33*(10), 1802-1811. doi:10.1111/risa.12033

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers and Security, 56*, 83-93. doi:10.1016/j.cose.2015.10.002

Pattinson, M., & Anderson, G. (2005). Risk communication, risk perception and information security. *Security management, integrity, and internal control in information systems* (pp. 175-184) Springer. doi: 10.1007/0-387-31167-X_11

Pedhazur, E. (1997). *Multiple regression in behavioral research: Explanation and prediction* (3rd ed.). London: Harcourt Brace.

Reid, R., & Van Niekerk, J. (2016). Decoding audience interpretations of awareness campaign messages. *Information and Computer Security, 24*(2), 177-193. doi:10.1108/ICS-01-2016-0003

Rhee, H., Ryu, Y. U., & Kim, C. (2012). Unrealistic optimism on information security management. *Computers and Security, 31*(2), 221-232. doi:10.1016/j.cose.2011.12.001

Schaik, P. van, Kusev, P., & Juliusson, A. (2011). Human preferences and risky choices. *Frontiers in Psychology, 2*(NOV) doi:10.3389/fpsyg.2011.00333

Schneier, B. (2015). *Secrets and lies: Digital security in a networked world (15th-anniversary edition)*. Hoboken, New Jersey: John Wiley & Sons.

Shillair, R., Cotten, S.R., Tsai, H.-S., Alhabash, S., Larose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing internet users to protect themselves. *Computers in Human Behavior, 48*, 199-207. doi:10.1016/j.chb.2015.01.046

Simon, H. A. (1956). Rational choice and the structure of the environment. *Psychological Review, 63*(2), 129-138. doi:10.1037/h0042769

Sjöberg, L. (2000). Factors in risk perception. *Risk Analysis, 20*(1), 1-11. doi:10.1111/0272-4332.00001

Slovic, P. (1987). Perception of risk. *Science, 236*(4799), 280-285.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1982). Why study risk perception? *Risk Analysis, 2*(2), 83-93. doi:10.1111/j.1539-6924.1982.tb01369.x

Slovic, P., Kraus, N. N., Lappe, H., Letzel, H., & Malmfors, T. (1989). Risk perception of prescription drugs: Report on a survey in Sweden. *Pharmaceutical Medicine, 4*(1), 43-65. doi:10.1007/978-3-642-74272-9_12

Slovic, P., MacGregor, D., & Kraus, N. N. (1987). Perception of risk from automobile safety defects. *Accident Analysis and Prevention, 19*(5), 359-373. doi: 10.1016/0001-4575(87)90022-4

Starr, C. (1969). Social benefit versus technological risk. *Science, 165*(3899), 1232-1238.

Tabachnick, B. G., & Fidell, L. S. (2013). *Using multivariate statistics* (6th ed.). Boston, MA; London: Pearson.

Tan, M., & Aguilar, K. S. (2012). An investigation of students' perception of bluetooth security. *Information Management and Computer Security, 20*(5), 364-381. doi:10.1108/09685221211286539

Vance, A., Eargle, D., Anderson, B. B., & Brock Kirwan, C. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association of Information Systems, 15*, 679-722. Available at: http://aisel.aisnet.org/jais/vol15/iss10/2

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security, 38*, 97-102. doi:10.1016/j.cose.2013.04.004

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816. doi:10.1016/j.chb.2008.04.005

Young, L., Kuo, H., & Chiang, C. (2014). Environmental health risk perception of a nationwide sample of Taiwan college students majoring in engineering and health sciences. *Human and Ecological Risk Assessment,* doi:10.1080/10807039.2014.913443

Table 1
Hazards and comparison activities

Activity/artefact	Current study	Garg and Camp (2012)	Type	Category
Identity theft on the Internet	√	√	Hazard	Identity-related
Phishing	√	√	Hazard	Identity-related
Internet surveillance	√	√	Hazard	Monitoring
Virtual stalking	√	√	Hazard	Online social
Cyber-bullying	√		Hazard	Online social
Social engineering	√		Hazard	Online social
Catfishing	√		Hazard	Online social
Virus	√	√	Hazard	Software
Spyware	√	√	Hazard	Software
Trojan	√	√	Hazard	Software
Worms		√	Hazard	Software
Keylogger	√	√	Hazard	Software
Malware		√	Hazard	Software
Spam		√	Hazard	Software
Botnet	√	√	Hazard	Software
Zombies		√	Hazard	Software
Cookie	√	√	Hazard	Software
Spoofing		√	Hazard	Software
Rogueware	√		Hazard	Software
Zero-day attack	√		Hazard	Software
E-mail-harvesting	√		Hazard	Software
Browsing Internet sites for information	√		Comparison	NA
Information-sharing on social media	√		Comparison	NA

Table 2

Means for risk

Hazard/comparison	Mean	CI.95 Lower	CI.95 Upper
Identity theft on the Internet	5.94	5.83	6.06
Keylogger	5.73	5.61	5.85
Cyber-bullying	5.67	5.54	5.79
Social engineering	5.63	5.50	5.75
Virus	5.54	5.41	5.66
Phishing	5.51	5.38	5.63
Virtual stalking	5.50	5.37	5.63
Botnet	5.45	5.32	5.57
Spyware	5.44	5.29	5.58
Rogueware	5.41	5.28	5.54
Trojan	5.40	5.27	5.53
Zero-day attack	5.27	5.14	5.41
Catfishing	4.98	4.84	5.12
Information-sharing on social media	4.61	4.48	4.76
Internet surveillance	4.38	4.22	4.54
E-mail-harvesting	4.21	4.04	4.38
Cookie	3.39	3.24	3.54
Browsing Internet sites for information	2.87	2.74	3.02

Note . Responses on a 7-point semantic-differential.

Table 3

Means for risk balance

Hazard/comparison	Mean	CI.95 Lower	CI.95 Upper
Browsing Internet sites for information	2.79	2.55	3.03
Cookie	0.74	0.52	0.96
Internet surveillance	0.00	-0.26	0.26
Information-sharing on social media	-0.65	-0.88	-0.44
E-mail-harvesting	-1.73	-1.96	-1.51
Zero-day attack	-2.51	-2.75	-2.24
Spyware	-2.66	-2.91	-2.42
Catfishing	-2.72	-2.94	-2.52
Trojan	-2.95	-3.17	-2.72
Botnet	-3.04	-3.25	-2.81
Rogueware	-3.17	-3.38	-2.97
Keylogger	-3.28	-3.50	-3.07
Virtual stalking	-3.30	-3.50	-3.07
Virus	-3.33	-3.56	-3.09
Phishing	-3.35	-3.57	-3.12
Social engineering	-3.42	-3.64	-3.21
Identity theft on the Internet	-3.69	-3.90	-3.48
Cyber-bullying	-3.69	-3.90	-3.48

Note . Responses on a 7-point semantic-differential.

Table 4

Mean ratings of perceived risk and other risk dimensions

Hazard/comparison	Risk	Benefit	Voluntariness	Immediacy	Knowledge (population)	Knowledge (science)	Control	Newness	Catastrophic potential	Dread	Severity
Identity theft on the Internet	5.94	2.25	5.29	3.58	3.86	2.95	3.76	4.46	4.14	5.22	5.72
Keylogger	5.73	2.45	5.54	3.96	4.97	3.47	3.00	3.30	4.34	5.20	5.60
Cyber-bullying	5.67	1.98	5.22	3.17	3.29	2.88	3.71	4.22	3.30	4.85	5.45
Social engineering	5.63	2.22	4.57	3.69	4.56	3.31	4.33	4.01	4.12	4.98	5.60
Virus	5.54	2.22	5.16	3.36	3.98	2.96	3.92	5.11	4.66	4.47	5.31
Phishing	5.51	2.16	4.69	3.89	4.30	3.02	4.57	4.54	4.42	4.48	5.44
Virtual stalking	5.50	2.20	5.31	4.03	4.13	3.36	3.49	4.03	2.88	4.99	5.19
Botnet	5.45	2.41	5.54	3.65	5.28	3.67	3.23	3.53	5.26	4.78	5.14
Spyware	5.44	2.78	5.15	3.90	4.38	3.02	3.68	4.24	4.46	4.68	5.20
Rogueware	5.41	2.24	5.17	3.10	4.70	3.47	3.53	3.62	4.26	5.01	5.25
Trojan	5.40	2.45	5.44	3.65	4.62	3.24	3.63	4.33	4.36	4.76	5.29
Zero-day attack	5.27	2.76	5.51	3.20	5.19	4.28	2.98	2.99	5.14	4.90	5.09
Catfishing	4.98	2.26	3.95	4.78	4.18	3.41	4.43	3.50	2.89	4.20	4.97
Information-sharing on social media	4.61	3.96	2.33	4.01	3.14	2.74	5.66	4.02	3.62	2.91	4.34
Internet surveillance	4.38	4.38	5.61	4.53	4.87	3.01	3.03	3.82	4.74	4.14	4.34
E-mail-harvesting	4.21	2.48	5.44	3.80	4.10	3.14	3.64	4.63	5.12	3.34	3.95
Cookie	3.39	4.13	3.87	4.06	3.87	2.78	4.61	4.41	3.63	2.76	3.34
Browsing Internet sites for information	2.87	5.67	2.46	3.42	3.22	2.66	5.58	5.04	3.42	2.38	2.90

Table 5

Model testing, dependent variable perceived risk

	Model	df	-2LL	*r* (pv, risk)	Test of model difference				
					Model difference	chi square	*df*	*p*	Δ*r* (pv, risk)
1	Null model	2	26158.15	0.00	M1 - M2	3918.62	25	0.000	0.66
2	Level-1 predictors[a]	27	22239.53	0.66	M1 - M3	4038.62	35	0.000	0.67
3	Level-1 predictors; established Level-2 predictors[b]	37	22119.53	0.66	M1 - M4	4374.52	185	0.000	0.66
4	Level-1 predictors; established Level-2 predictors[b]; interactions with hazard	187	21855.72	0.68	M1 - M5	4374.52	187	0.000	0.68
5	Level-1 predictors; established Level-2 predictors[b]; interactions with hazard; exploratory Level-2 predictors[c]	189	21783.63	0.68	M2 - M3	120.00	10	0.000	0.01
					M3 - M4	263.81	150	0.000	0.02
					M4 - M5	72.09	2	0.000	<0.01

Note . pv: predicted value. Null model: intercept only. Level 1: hazard. Level 2: subject (participant).

[a]hazard, benefit, voluntariness, immediacy, knowledge by population, knowledge by science, control, newness, catastrophic potential, dread, and severity

[b]averaged over hazards, benefit, voluntariness, immediacy, knowledge by population, knowledge by science, control, newness, catastrophic potential, dread, and severity

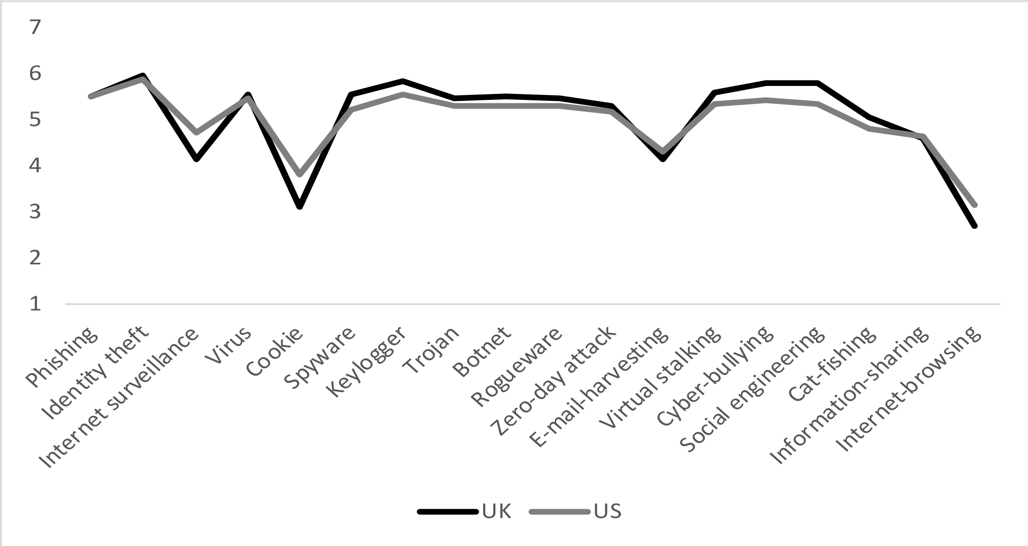
[c]length of Internet experience; frequency of Internet logon

Table 6

Parameter estimates and tests of effects, dependent variable perceived risk

Parameter	*b*	*CI* 95%		*df*	*df2*	*F*	*p*
		LL	*UL*				
Intercept				1	6960	4108.81	.000
Length of Internet experience	0.01	0.00	0.02	1	6960	8.29	.004
Frequency of Internet logon	-0.06	-0.12	-0.01	1	6960	4.85	.028
Benefit (subject)	-0.01	-0.06	0.03	1	6960	0.53	.468
Voluntariness (subject)	0.09	0.04	0.13	1	6960	14.58	.000
Immediacy (subject)	-0.04	-0.09	0.00	1	6960	3.96	.047
Knowledge to population (subject)	-0.01	-0.06	0.03	1	6960	0.26	.613
Knowledge to science (subject)	0.02	-0.02	0.06	1	6960	0.67	.412
Control (subject)	-0.01	-0.06	0.03	1	6960	0.43	.510
Newness (subject)	0.00	-0.04	0.03	1	6960	0.08	.783
Catastrophic potential (subject)	0.05	0.01	0.09	1	6960	5.26	.022
Dread (subject)	-0.09	-0.13	-0.05	1	6960	16.72	.000
Severity (subject)	0.26	0.21	0.32	1	6960	81.60	.000
Hazard				15	6960	8.68	.000
Benefit (hazard)	0.02	-0.06	0.09	1	6960	0.17	.676
Voluntariness (hazard)	0.08	0.01	0.14	1	6960	5.66	.017
Immediacy (hazard)	0.06	-0.01	0.12	1	6960	3.23	.073
Knowledge to population (hazard)	-0.03	-0.09	0.04	1	6960	0.70	.403
Knowledge to science (hazard)	-0.02	-0.09	0.05	1	6960	0.32	.571
Control (hazard)	0.08	0.01	0.14	1	6960	5.35	.021
Newness (hazard)	0.02	-0.04	0.08	1	6960	0.30	.586
Catastrophic potential (hazard)	0.11	0.05	0.17	1	6960	12.28	.000
Dread (hazard)	0.06	-0.01	0.12	1	6960	2.69	.101
Severity (hazard)	0.42	0.34	0.51	1	6960	95.59	.000
Benefit (hazard) by hazard				15	6960	1.65	.053
Voluntariness (hazard) by hazard				15	6960	0.99	.463
Immediacy (hazard) by hazard				15	6960	1.08	.367
Knowledge to population (hazard) by hazard				15	6960	0.94	.524
Knowledge to science (hazard) by hazard				15	6960	2.05	.009
Control (hazard) by hazard				15	6960	0.71	.778
Newness (hazard) by hazard				15	6960	1.03	.416
Catastrophic potential (hazard) by hazard				15	6960	1.18	.278
Dread (hazard) by hazard				15	6960	1.68	.047
Severity (hazard) by hazard				15	6960	3.51	.000

Figure 1 . Mean perceived risk as a function of hazard and nation.



Appendix 1 – cyber-security hazards defined (see Jeske & Van Schaik, 2017)

	Identity-related hazards	
1	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.
2	Identity theft on the Internet	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
	Monitoring	
3	Internet surveillance	The monitoring of online behaviour, activities or other changing information, often in secret and without authorization. This is usually carried out on individuals or groups observed by governmental organizations.
	Software hazards	
4	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.
5	Cookie	A small piece of text or file that is stored in a user's computer. Contains information that identifies the user to a particular Web site, and any information about the user during their visit to the site.
6	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.
7	Keylogger	A computer program that records every keystroke made by a computer user to gain fraudulent access to passwords and other confidential information.
8	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.
9	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.
10	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.
11	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.

12	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.
		Online social hazards
13	Virtual stalking	Use of the Internet, e-mail or other electronic communication devices to stalk or repeatedly follow and harass another person.
14	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
15	Social engineering	The art 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.
16	Catfishing	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.
		Comparison activities
17	Browsing Internet sites for information	Visiting Internet sites to gain information on topics chosen by the user.
18	Information sharing on social media	Making personal information available to other users of social media.