Information & Computer Security

Factors in an end user security expertise instrument

Prashanth Rajivan, Pablo Moriano, Timothy Kelley, L. Jean Camp,

Received 2 April 2017
Revised 2 April 2017
Accepted 5 April 2017

Factors in an end user security expertise instrument

Prashanth Rajivan
Social and Decision Sciences, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA
Pablo Moriano
School of Computing and Informatics, Indiana University Bloomington, Bloomington, Indiana, USA
Timothy Kelley
Psychological and Brain Sciences, Indiana University Bloomington, Indiana, USA, and
L. Jean Camp
School of Computing and Informatics, Indiana University Bloomington, Bloomington, Indiana, USA

Abstract

Purpose – The purpose of this study is to identify factors that determine computer and security expertise in end users. They can be significant determinants of human behaviour and interactions in the security and privacy context. Standardized, externally valid instruments for measuring end-user security expertise are non-existent.

Design/methodology/approach – A questionnaire encompassing skills and knowledge-based questions was developed to identify critical factors that constitute expertise in end users. Exploratory factor analysis was applied on the results from 898 participants from a wide range of populations. Cluster analysis was applied to characterize the relationship between computer and security expertise. Ordered logistic regression models were applied to measure efficacy of the proposed security and computing factors in predicting user comprehension of security concepts: phishing and certificates.

Findings – There are levels to peoples' computer and security expertise that could be reasonably measured and operationalized. Four factors that constitute computer security-related skills and knowledge are, namely, basic computer skills, advanced computer skills, security knowledge and advanced security skills, and these are identified as determinants of computer expertise.

Practical implications – Findings from this work can be used to guide the design of security interfaces such that it caters to people with different expertise levels and does not force users to exercise more cognitive processes than required.

Originality/value – This work identified four factors that constitute security expertise in end users. Findings from this work were integrated to propose a framework called Security SRK for guiding further research on security expertise. This work posits that security expertise instrument for end user should measure three cognitive dimensions: security skills, rules and knowledge.

Keywords Privacy, Psychometrics, Security, Expertise, Security comprehension

Paper type Research paper

This research was sponsored by the Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF-13-2-0045 (ARL Cyber Security CRA). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the US Government. The US Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon. The authors would also like to acknowledge Dr Cleotilde Gonzalez for her support and guidance.

Information & Computer Security
Vol. 25 No. 2, 2017
pp. 190-205

2056-4961
DOI 10.1108/ICS-04-2017-0020

1. Introduction

Security technologies are increasingly being developed with a user-centric approach. Part of the challenge of user-centred security is that people interacting with security systems possess tremendously different levels of computer and security knowledge and even different levels of basic literacy. This heterogeneity was illustrated by a recent Organisation for Economic Co-operation and Development (OECD) study with 215,942 people from across the globe which tested 14 computer-based skills in adults (Nielsen, 2016; OECD, 2016). More than 95 per cent of participants in the study were unable to perform basic-to-moderate computer tasks, let alone tasks that require interactions with security interfaces. It should be noted that this work did not assess the skills of people beyond the age of 66 years.

Developing security technologies and awareness programmes requires addressing both security expertise and computer expertise. Appropriate design requires identification and operationalization of valid factors that constitute security expertise in end users. This need motivates our goal of creating an instrument. One of Nielsen's widely applied usability heuristic is "accelerators" for systems used by people with different expertise levels, which include quicker interface modes "unseen by the novice user" but included to be useful for the expert user who does not need the additional details or navigation steps to accomplish their goals. This kind of system design is used so that a system "can cater to both expert and novice users". This human–systems gap between end users and security systems needs to be reduced or people will continue to demonstrate wide differences in their response behaviour to security controls and warnings.

Expertise is granular (Reisberg, 1997), and we began with an assumption that this general observation applies to end users with respect to computer security. Disparities in users' expertise could lead to seemingly stochastic user interactions with security- and privacy-enhancing technologies. Security experts and novices have been shown to differ widely in terms of mental models (Asgharpour *et al.*, 2007), security practice (Ion *et al.*, 2015) and security awareness (Stephanou, 2009) and in terms of interactions with security interfaces (Bertenthal, 2015). Expert users can leverage their extensive security knowledge and experience to better use available information to make informed choices. In contrast, novice users must either use their partial knowledge to make decisions or must rely on others' expertise. Both experts and novices can ignore security and make decisions based on convenience and perceived benefits rather than the risk of ignoring security controls. Experts can make informed risk decision; novices just do not know.

Validated instruments for measuring the security (and computer) expertise of end users along the lines of instruments developed for evaluating user privacy concerns on the internet – Internet Users' Information Privacy Concerns (IUIPC) – (Malhotra *et al.*, 2004) are needed. It is widely recognized that security and computing expertise affect security attitudes and behaviours. To address this, three common practices are used in behavioural and usable security research today. A way in which security expertise is addressed is by participant selection; for example, choosing computer science students (Maxion *et al.*, 2005) versus choosing non-technical retirees (Garg *et al.*, 2012) as study participants. In other cases, user expertise is measured in association with other security behavioural research using one-off closed-response questions on security knowledge (Almuhimedi *et al.*, 2014). A third approach involves not addressing expertise in formal analysis but rather including it in discussion as a potential hidden factor.

To address the need for standardized and valid measures of security expertise in end user, we developed a questionnaire containing a combination of skills and knowledge-based questions. This included open-ended validation questions on concepts critical for secure e-commerce transactions. Using a combination of factor analysis and logistic models, we

identified those factors that indicate computer and security expertise of end users. We present our instrument, describe our analysis and posit how this could be leveraged in future research. In closing, we describe how these skills and knowledge factors can be integrated with user's contextual rules for a comprehensive expertise instrument.

2. Related work

Past research on security expertise has predominantly focused on measuring expertise of system administrators and security analysts who, by definition, have background education and experience in computer security (Barrett *et al.*, 2004; Goodall *et al.*, 2004; Ben-Asher *et al.*, 2015). The high-level themes on expertise that emerged from these works include expertise in threat detection, detection of vulnerabilities, contextual awareness and assessments of risk and attack response. These factors are closely tied to the context and vary based on role and organization.

With respect to end users, past security research has placed significant emphasis on identifying security attitudes, awareness and practices. There are field studies done to understand novice users' views about security practices and awareness (Albrechtsen, 2007; Ion *et al.*, 2015). An early field study on security-related employee behaviours, such as backup and file access practices, specifically, indicates knowledge and informal heuristics as better determinants of behaviour than enforced security policies (Frank *et al.*, 1991). Such qualitative investigations (interviews and field observations) enable a deep exploration of a narrow work domain, context or demographics, but results from these may not be generalizable to a larger population.

Early survey-based research explored detrimental behaviours that affect both personal security (Furnell *et al.*, 2006) and the security posture of an organization (Stanton *et al.*, 2005). Later attempts have been made for applying existing models of user behaviours developed for other domains, to study user behaviours indepth in the security context. This includes validation of a health belief model from healthcare to study users' computer security behaviour, while interacting with e-mail attachments (Ng *et al.*, 2009); general deterrence theory from criminology to study employee information-sharing behaviours and security policy compliance (Fan and Zhang, 2011); agency theory or principal–agent theory to study factors that incentivize and dis-incentivize security compliance behaviours (Herath *et al.*, 2009); and knowledge–attitude–behaviour model to study the impact of security awareness programme on employees (Kruger and Kearney, 2006). These are model-driven, survey-based research that use exploratory and confirmatory factor analysis to identify pertinent variables that predict security awareness and behaviours. The drawback of a model driven approach is the bias towards validating variables of the theory under investigation (Parsons *et al.*, 2014). Our work differs in that the primary objective of these works is theory validation and development – not scale development.

Our research is also informed by literature specifically focused on developing instruments for measuring end user security behaviours and security awareness. Egelman and Peer developed the Security Behavior Intentions Scale (SeBIS), which is a 16-item, scale-based instrument to measure the intention of security rules that end users use while interacting with a wide variety of security controls and interfaces (Egelman and Peer, 2015). The authors further refined this work by testing factors identified from the scale against a set of specific security behaviours (Egelman *et al.*, 2016). In another research, Parsons *et al.* (2014) conducted an inductive, exploratory approach to measure employee awareness of security policies and procedures. They developed variables of interest based on interviews with the senior management from three government organizations. The authors took inspiration from the knowledge–attitude–behaviour model (Kruger and Kearney, 2006) in

evaluating the knowledge of security policy and procedures. This work focussed on six areas: password management, email use, social networking, incident reporting, mobile computing and information handling. The authors used correlations to detect a positive relation between knowledge and attitude of security polices and actual security behaviour. They followed up on their previous work to evaluate the test–retest reliability and internal consistency of the questionnaire (McCormac *et al.*, 2016). Related research described here has focussed on a multitude of novice users' security behaviours and interactions but have not addressed measures of security and computer expertise.

Measures of privacy perceptions and the handful of "scaling" work in usable security (Parsons *et al.*, 2014; Egelman and Peer, 2015) have inspired much of this work. The standard we hope to meet is that set for measuring privacy through IUIPC (Malhotra *et al.*, 2004). That work offered a set of questions to enable comparisons across research based on privacy perceptions. While there have been changes in technology since 2008, IUIPC has been widely used, providing a basis for comparisons. Until recently, the most widely used measure of privacy perceptions was the Westin model despite its proven flaws (Cranor *et al.*, 2000; Garg *et al.*, 2014; Butler *et al.*, 2015). When limited to Westin, the lack of robust and consistent measures of privacy perceptions was problematic. Similarly, lack of a robust measure for expertise is problematic in usable security today. Instruments for measuring human aspects of security must be developed and refined iteratively. Ideally, instruments address specific aspects of human behaviour in the context of security and refine these in each iteration. Large-scale data collection addressing a bevy of human behaviours, unless extreme care is taken, could lead to "p-hacking" (Gelman and Loken, 2013) and confounded results.

3. Instrument design

Our goal was to design an instrument that could be used to measure and differentiate end users' computer and security expertise. We used the standard four-step procedure in developing a measurement scale/instrument (Netemeyer *et al.*, 2003; Bernard, 2011). The first step involves identifying and defining the variables intended to be measured using the scale. The second step involves developing the actual items for the scale. When studying human expertise in a complex environment such as security, single indicators that can predict the intended construct are usually not available (Bernard, 2011 on Scales and Scaling). Hence, we need to identify a composition of indicator items conjectured to be strong determinants of the construct being measured. This list of indicator questions is usually developed through an induction exercise that is based on a combination of literature review, personal experience, ethnography and expert opinions (Bernard, 2011). The third step involves exploratory factor analysis to reduce the scale and extract latent factors that summarize the relationship among original variables to build a prediction model. Finally, the fourth step requires confirming the scale fits the intended model.

We began by generating a list of common yet essential computer security skills and knowledge an end user would require to make risk-aware decisions online. We drew primarily on work by Egelman and Sotirakopoulos, Hawkey and Beznosov to develop questions dealing with technical expertise (Egelman, 2009; Sotirakopoulos *et al.*, 2011). For queries based on skills, we were informed by Sheng *et al.*'s (2010) work on demographics and phishing risk. Security expertise classification questions were derived from Arianezhad *et al.*'s (2013) work investigating factors affecting attention to browser-based security cues. Relevant computer security skills and knowledge were operationalized through a questionnaire composed of open-response questions, Boolean-type questions and multiple-choice queries. Table I presents the questions in our instrument. Academic and professional security background can be strong predictors of security expertise. Hence,

Category	Question
Academic and professional background	Do you have a degree in an IT-related field (e.g. information technology, computer science, electrical engineering, etc.)?
	Have you ever taken or taught a course on computer security?
	Is computer security one of your primary job responsibilities?
	Have you attended a computer security conference in the past year?
Computer security skills	Have you ever installed a computer programme?
	Have you ever written a computer programme?
	Have you ever designed a website?
	Have you ever registered a domain name?
	Have you ever created a database?
	Have you ever used SSH?
	Have you ever configured a firewall?
	Have not done any of the above
Everyday computer interactions	Please estimate how many hours you spend on the internet per week?
	I often ask others for help with the computer. On a scale between strong disagree to strongly agree
	Others often ask me for help with the computer. On a scale between strong disagree to strongly agree
Security knowledge	If you know, please describe what is meant by "phishing", otherwise write "Don't know"
	If you know, please describe what a "security certificate" is in the context of the internet, otherwise write "Don't know."

Table I.
Questions in the instrument

questions that queried security-related academic and professional experience were asked. Hands-on computer and security experience can play a vital role in shaping one's expertise, as it would involve active learning. Furthermore, we identified questions that queried the participants' interactions with computing devices in everyday lives. More interactions could be causal for improved expertise. Finally, two open-ended questions were used to assess end users' depth and correctness of knowledge towards two security-related concepts that are used or are exposed daily. For the open-response questions, we describe the qualitative analysis performed along with the coding scheme used for analysis.

4. Experiment methods

We recruited 898 participants for this study from five different populations: MTurk (696 participants), the Bloomington Farmers' Market (27 participants), Dashcon (106 participants), Mini-University (49 participants) and Grace Hopper (23 participants). The questionnaire was distributed among different populations to obtain responses from non-overlapping subject populations. The Farmers' Market population included responses from people visiting their local farmers' market. The Dashcon population included responses from enthusiasts attending the blogging (Tumblr) conference. Mini University included retired University alumni attending a week-long adult learning experience. Finally, the Grace Hopper population included responses largely from woman technologists attending the annual Grace Hopper conference.

4.1. Demographics

The median age of survey participants was 34 years (median age of US population is 36.8 years). The minimum age of participants was 18 years and the maximum age was 68 years. The average age of participants is slightly skewed (younger) than the US population despite the inclusion of the Mini University population. In total, 47 per cent of survey participants were male, whereas 53 per cent were female. The higher number of female participants could be because of Grace Hopper participants. Fewer than 11 per cent of the participants were students, whereas 78 per cent of them were employed. In terms of income, the median income level of the US population shows a peak at the US$25,000-30,000 level, with a median income of US$51,000, per year. That is skewed by the 4 per cent of households making more than US$200,000 a year, itself a subgroup with a highly skewed distribution. For survey participants, the income peak is in the category of more than US$20,000 to less than US$30,000, close to the distribution of US population.

4.2. Qualitative analysis

The instrument also included two open-ended security knowledge questions, which allowed participants to provide descriptive responses. Answers to the two questions were analysed by researchers both independently and collaboratively to develop a classification of answers (codebook). The codebook was used to bin the participants' answers. The coding scheme was re-evaluated through several iterations of analysis until it was possible to classify the vast majority of answers. The researchers then shared their individual classification of responses, and inter-rater reliability was measured using a kappa coefficient. The kappa coefficients calculated for analysis of both questions were close to 0.70, which demonstrated good inter-rater reliability. Finally, researchers independently rated the accuracy level of the classifications for each of the two questions, and later they came together to develop the final order of classification based on consensus as shown in Tables II and III.

Table II provides the list of codes developed to classify the responses to the question about phishing. Phishing is something we expected to be far more common and well-known than certificates. The range of responses indicated that our understanding of non-experts' perceptions towards security was very limited. We did not expect, for example, that behavioural advertising would be one definition of phishing (Code G in Table II). From the rest of the codes, we observed a variance in comprehension on the scope and methods of a phishing attack (e.g. hacking a computer). We observed difficulty in differentiating the subtle, yet important differences between a spam e-mail and a phishing attack. Lack of comprehension about phishing attack methods could lead to careless e-mail behaviours.

Code	Meaning
A	Pretending to be someone or a company to steal users' information
B	Website: Making a fake website that looks legitimate to steal user information (where not mentioned together with email)
C	Emails/links: Sending spam emails and or redirecting links (unsuspecting)
D	Tricking/identity theft: Defrauding someone online; getting, collecting, stealing, seeking information (but only if there is no method mentioned)
E	Other methods for stealing information
F	Hacking: Hacking someone's computer
G	Tracking: Tracking your internet habits to send advertisements
H	Other
I	Do not Know

Table II.
Qualitative codes for phishing ordered by level

Code	Meaning
A	Certifies domain name (DNS)
B	Verification: The certificate confirms that "I am who I say that I am" authentication
C	Encryption/decryption: The certificate encrypts and/or decrypts, https
D	Information access: The certificate makes sure that only certain people get access to the information
E	Website registration/certification: When a website has to register or be certified and the certificate checks this certification/registration
F	Validation: The certificate states the site is valid (fake website) authorization
G	Information access by website: The certificate makes sure that only the website has access to the stored information
H	Protection: The certificate actively protects against malicious stuff, including hackers/unauthorized people/virus, it is competent
I	Agreement of accountability (handshake), guarantee: The certificate expresses that an agreement has been made between the user and website of accountability for information
J	Security/safety: The certificate says that the website is safe/secure (competence)
K	Trustworthiness of website: The website can be trusted to be benevolent (morally/ethically upstanding), not necessarily competent
L	Other
M	Do not know

Table III.
Qualitative codes for certificates ordered by level of accuracy

Table III presents the list of codes developed to classify the user definitions of X.509 certificates. We expected a range of answers addressing privacy and security, yet multiple participants responded that X.509 certificates conveyed legal accountability of the site (Code I in Table III). The next surprising result was the optimism with respect to the scope and the function of a security certificate. The presence of a security certificate was misconstrued as security to personal information (Codes G and D, in Table III), protection against active threats (Codes J and H, in Table III) and validation of "safeness" of the site (Codes J and H, in Table III). Placing such inappropriate optimism on a security certificate could lead to detrimental online behaviours.

It should be noted that few participants responded with irrelevant answers (coded as "other" in Table II and Table III) or "Don't Know" for both questions. To reduce the likelihood of participants selecting, "Don't know", they were required to actually write the phrase. There were no pre-defined options. Finally, we observed that the number of codes generated for the question on security certificates (Table III) was significantly greater than the number of codes generated for the question on phishing (Table II). This difference in response variance between the two questions demonstrates the inconsistency in end-user expertise across different security concepts. Based on our participant demographic distribution and variance observed in responses to the two questions, we operationalized the two open-ended questions as security expertise performance variables. Hence, these two open-ended questions were used as dependent variables in the regression models.

5. Results

5.1. Exploratory factor analysis

Exploratory factor analysis using principal component analysis (PCA) was used for factor extraction. PCA was used to summarize the relationships among the original variables in terms of a smaller set of dimensions. The responses of 898 participants were used to calculate the factor loadings of 15 variables from the instrument. The variable to subject ratio was 1:59.9. This ratio shows that the number of participants per question was adequate to obtain

quality in the factor solution (Kline, 2014). The "psych" package in statistical software R was used to run the factor analysis.

We tested the adequacy of the factor analysis for this data set using the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy and Bartlett's test of Sphericity. The KMO measure of sampling adequacy revealed that the use of factor analysis was adequate, given the data (KMO = 0.83). A commonly accepted measure is that a KMO coefficient greater than 0.80illustrates that factor analysis approach is appropriate. On the other hand, the Barlett's test of sphericity tests the hypothesis that the correlation matrix came from a population of independent variables. A Bartlett's test of sphericity revealed that the correlation matrix came from a population of independent samples ($\chi^2 = 4087.4$, df = 105, $p < 0.001$), and further indicated that the factor analysis was justified by the properties of the correlation matrix. We used oblique rotation with the "oblimin" method, based on the assumption that the factors are correlated. We identified and extracted five factors based on the Kaiser's criterion for eigenvalues (Figure 1).

To characterize the factors, let $F = \{F_1, F_2 [\ldots], F_5\}$ be the set of factors. The five factors identified through factor analysis encompass 14 of the 15 original variables (i.e. $X_1, X_2 [\ldots], X_{14}$). We retained only variables with factor loading greater than 0.3, and therefore the variable "Internet hours per week" was excluded from further analysis. The complete list of factors along with their respective correlations and variables within the factors is shown in Figure 2. The five factors are arranged in a decreasing order of variance, such that $\text{Var}(F_1) \geq$

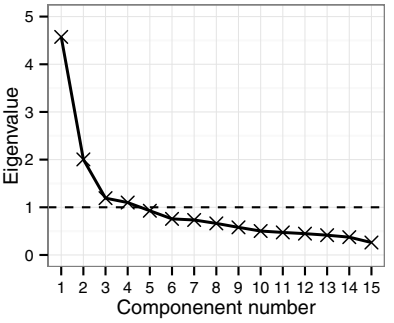

Figure 1.
Scree plot for the correlation matrix

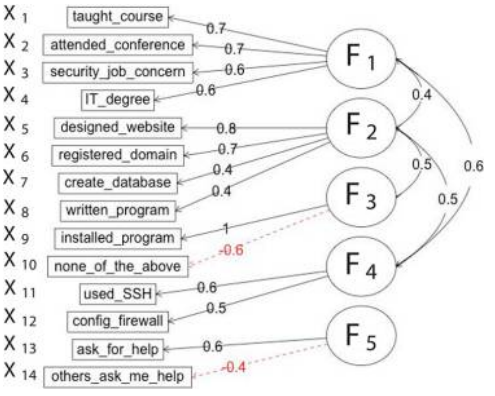

Figure 2.
Factor analysis diagram

$\text{Var}(F_2) \geq [\ldots]. \geq \text{Var}(F_5)$. Similarly, the variables (i.e. X_1, X_2 *[…]*, X_{14}) are arranged in decreasing order of correlation within each factor.

The first four factors (F_1, F_2, F_3 and *F4*) account for 91 per cent of the total variance within the data. Specifically, the first factor consistsof variables that are related to advanced security knowledge and skills. It accounted for 32 per cent of the total variance and had an eigenvalue of 4.574. The second factor contains variables that are related to advanced computer knowledge and skills. It accounted for 27 per cent of the total variance with an eigenvalue of 2.004. The third factor contains variables that are related to basic computer knowledge and skills. It accounted for 19 per cent of the total variance with an eigenvalue of 1.191. The fourth factor contains variables that are related to basic security knowledge and skills and accounts for 13 per cent of the total variance with an eigenvalue of 1.099. We also present a fifth factor with an eigenvalue close to unity, 0.927, and accounts for 9 per cent of the total variance. This factor contains variables on social behaviour, e.g. the queries on helping others or seeking help.

5.2. Cluster analysis

We used results from factor analysis to define a metric to quantify computer and security expertise. Specifically, we merged pairs of correlated factors based on the degree of correlation between them. For example, looking at Figure 2, F_1 is more correlated with F_4 (0.6) than F_2 (0.4). Therefore, we merged the factors F_1 and F_4 into a single factor that encompasses security centric variables. Similarly, the factors F_2 and F_3 were merged and the new unified factor comprises computer skills related variables. The fifth factor F_5 is not correlated at a significant level with other factors. Hence, we excluded the variables (which are questions, as given in Table I, on everyday computer interactions) within this factor as predictors of computer and security knowledge and skills. Therefore, for posterior analysis, we only used the four most representative factors (latent factors), which in turn, contain only 12 of the 15 variables in the original questionnaire.

Based on final factor analysis configuration, we defined two scores: computer and security scores. Specifically, let $\Omega = \{X_5, X_6, X_7, X_8\}$ U $\{X_9, X_{10}\}$ be a set with the characteristic variables that define the computer score. These variables are part of the factors F_2 and F_3 in Figure 2. Similarly, let $\Phi = \{X_1, X_2, X_3, X_4\}$ U $\{X_{11}, X_{12}\}$ be a set with the characteristic variables that define the security score. These variables are part of the factors F_1 and F_4 in Figure 2. The computer score (CS) of a participant is defined as $\Sigma_{X \epsilon \Omega} \{X \times \Lambda_X\}$, where X corresponds to the actual value of the variable in the survey for the participant to the question x, and Λ_X corresponds to the loading for the variable extracted from the factor analysis. Security score for each participant was also calculated using questions in the security score set and their corresponding factor loadings.

We characterized the relationship between computer and security expertise using unsupervised cluster analysis. Figure 3 illustrates a scatter plot between the two scores (i.e. CS and SS) for the participants. Participants with higher SS tend to be confined in the region of higher CS. This relationship shows a positive association between the two scores, which means that security expertise is predicated on computer expertise. This behaviour is illustrated in the right-upper cluster. Those participants with low computer score are less likely to be security experts, as can be seen in the left-bottom cluster (outliers in the upper-left region did not influence the clustering results.) This result provides some validation for the instrument, and validates the merging of factors to create computer and security scores.

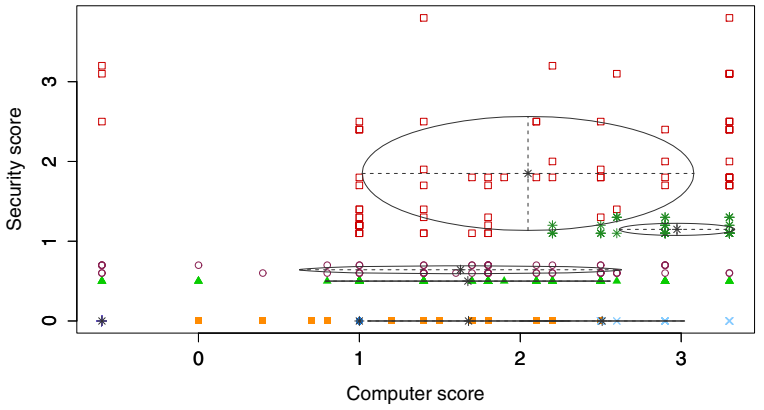

Figure 3.
Unsupervised cluster analysis

5.3. Regression analysis

A set of codes (Tables II and III) is derived to substitute the participants' answers to the two open-ended questions on security concepts based on the qualitative analysis, i.e. phishing and certificates. The two coded security comprehension questions on phishing and certificates were then used as dependent variables for running ordered logistic regression analysis with SS_i and CS_i serving as non-parametric independent variables.

We define the logistic regression models for predicting the phishing variable as follows (similarly defined model applies to predicting certificates response as well). Let Y_Ω^i be an ordinal outcome variable for participant i that has G_Ω categories (i.e. $\forall\, i \in \{1, 2, \ldots, N\}$, $Y_\Omega = 2, \ldots, G_\Omega$). In the case of phishing variable, $G_\Omega = 9$ (Table I). Then, there are $G_\Omega - 1$ ways to dichotomize the outcomes (i.e. $Y_\Omega^i \geq 2$ *vs.* $Y_\Omega^i < 2$, $Y_\Omega^i \geq 3$ *vs.* $Y_\Omega^i < 3$, …, $Y_\Omega^i \geq G_\Omega$ *vs.* $Y_\Omega^i < G_\Omega$). With this categorization of Y_Ω^i, the odds $Y_\Omega^i > y_\Omega$ is equal to the probability of $Y_\Omega^i > y_\Omega$ divided by the probability of $Y_\Omega^i < y_\Omega$, where $y_\Omega = \{2, 3, \ldots, G_\Omega\}$ (Kleinbaum and Klein, 2010). In other words, the ordered logit model assumes that $odds(Y_\Omega^i \geq y_\Omega) = P(Y_\Omega^i \geq y_\Omega)/P(Y_\Omega^i < y_\Omega) = \exp(a_{y_\Omega} + \beta_1 CS_i + \beta_2 SS_i)$, where the intercept a_{y_Ω} is the log odds of $Y_\Omega^i \geq y_\Omega$ when all independent variables are equal to zero. The intercepts satisfy the condition $\alpha_2 > \alpha_3 > \cdots > \alpha_{y_{G_\Omega}}$. In other words, every intercept a_{y_Ω} corresponds to the log odds of a different inequality depending on the value of y_Ω. Similarly, β_2 and β_2 are the regression coefficients for the independent variables CS_i and SS_i, respectively. Finally, to calculate the probability that an individual i is in a specific outcome category, we used $P(Y_\Omega^i = y_\Omega) = P(Y_\Omega^i \geq y_\Omega) - P(Y_\Omega^i \geq y_\Omega + 1)$. The same construct was applied on coded responses to question on certificates but in that case, we denote Y_Φ^i instead of Y_Ω^i and $G_\Phi = 13$ for certificates variable.

As defined, we ran ordered logistic regression to evaluate the predictive ability of CS_i and SS_i, in terms of participants' responses to open-ended questions on phishing and X.509 certificates. In this analysis, we considered only participants who responded to both the questions resulting in 781 responses. The results of logistic regression analysis on phishing responses are shown in Figure 4. To check the proportional odds assumption, we used a test score based on a χ^2 distribution with degrees of freedom equal to the number of independent variables. Thus, under the null hypothesis that the ordinal model fails to explain the data, the score test produced ($\chi^2 = 66.045$, df $= 2$, $p < 0.01$), indicating that the ordinal regression carried out on phishing responses is justified by the properties of the data set. The hypothesis testing on intercepts estimates using the Wald test yielded significant results on all

intercepts. As shown in Figure 4, CS and SS are both statistically significant in predicting phishing responses in this two-predictor model ($p < 0.01$). The CS was found to have a greater impact than SS on phishing responses. We also ran an ordered logistic regression to predict the certificate responses using computer and security score. The results of the regression analysis are shown in Figure 5. The proportional model odds assumption was checked and was found to be satisfied ($\chi^2 = 155.746$, df = 2, $p < 0.01$). In addition, estimates of the intercepts and coefficients were found to be statistical significant. For certificates and for phishing, both predictors (CS and SS) were statistically significant.

Finally, in Figures 6 and 7, we illustrate the accuracy of the regression model in predicting phishing and X.509 certificates. In Figures 6 and 7, for every qualitative code, the dark-coloured bar represents the actual proportion of participants, who were classified in

CS Coef.	0.355***
	(0.059)
	$t = 6.028$
	$p = 0.000$
SS Coef.	0.309***
	(0.103)
	$t = 3.006$
	$p = 0.003$
Observations	781
R^2	0.083
χ^2	66.045*** (df = 2)

Note: *$p < 0.1$; **$p < 0.05$; *** $p < 0.01$

Figure 4.
Ordered logistic regression for phishing

CS Coef.	0.682***
	(0.068)
	$t = 9.249$
	$p = 0.000$
SS Coef.	0.411***
	(0.103)
	$t = 3.991$
	$p = 0.000$
Observations	781
R^2	0.186
χ^2	155.746*** (df = 2)

Note: *$p < 0.1$; **$p < 0.05$; *** $p < 0.01$

Figure 5.
Ordered logistic regression for X.509 certificates

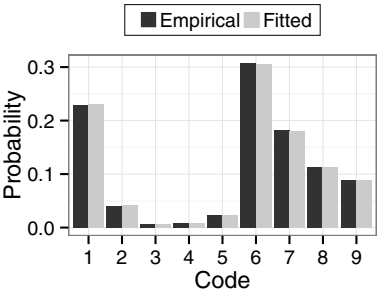

Figure 6.
Predictive probabilities for phishing

that respective code, and the light bar represents the predictive probability using the fit from the ordered logistic model. For both phishing and certificates, the codes derived from qualitative analysis were predicted with good accuracy.

6. Discussion

Qualitative analysis revealed significant variability in terms of participant comprehension of X.509 certificates and phishing. Even though participants are often broadly classified as security novices, we find there are levels to their computer and security expertise that could be reasonably measured. Furthermore, their level of knowledge varied by security concept probably based on individuals' experience and awareness. Hence, we recommend, it is imperative to develop a multi-dimensional security expertise instrument that can assess end users' knowledge on a diverse set of security concepts. This will require development of code books for different security concepts through qualitative analysis, with this research being a first step.

Through exploratory factor analysis, we identified four factors encompassing 12 of the 15 variables (excluding two open-ended questions) from our survey, as shown in Table I. The four factors were operationalized as two predictors (CS and SS) in a logistic regression model. Computer and security expertise variables were found to be strong determinants (Figure 4 and 5) of participant comprehension on two essential security concepts: X.509 certificates and phishing. On further inspection, we found that the four factors can be classified into four categories of computer security-related skills and knowledge: basic computer skills, advanced computer skills, security knowledge (academic and professional) and advanced security skills. We put forward that these "skill-" and "knowledge-" based factors are crucial predictors of computer security expertise in end users.

Cluster analyses showed more diversity in terms of computer skills when compared to security knowledge and skills. These results indicate that computer skills are more common among our participants than security skills, reflecting the state of the world. The regression analysis also revealed that the computer (vs security) score is a better predictor of phishing and certificate knowledge. This implies that advanced computer skills are important predicates for security expertise, possibly more so than security knowledge *per se*. We propose that end-user security expertise instruments should include queries on advanced computer skills and knowledge in addition to queries focussed on security concepts.

In a related but independent work, researchers have developed a scale-based instrument to measure security behavioural rules end users intend to use (Egelman and Peer, 2015). The 16-item in this scale were mapped onto four factors of security behavioural rules: device securement, password generation, proactive awareness and updating. The items on the scale are essentially assessing the behavioural "heuristics or rules" that the end user intends to

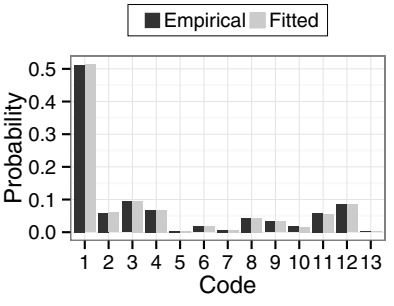

Figure 7.
Predictive probabilities for X.509 certificates

use while interacting with security controls in different devices. The four factors on security rules/heuristics identified through Egelman's and Peer's work and the four factors on security skills and knowledge identified through our work encourage us to propose a high-level theoretical framework for measuring end user security expertise.

6.1. Security skills, rules and knowledge

By combining our results with the skills, rules and knowledge (SRK) taxonomy, widely accepted in the human factors and cognitive engineering community (Rasmussen, 1983; Sanderson and Harwood, 1988), we propose a framework for reproducible evaluation of user expertise. The SRK taxonomy describes the cognitive mechanisms that people use while interacting with a complex system (Vicente and Rasmussen, 1992; Leplat, 1988). Per this taxonomy, depending on complexity of the context, familiarity and expertise level, people use three main levels of cognitive processes (Rasmussen, 1983). Three corresponding cognitive behaviours can result, based on the type of cognitive process used: skill-based behaviour, rule-based behaviour and knowledge-based behaviour. Skill-based behaviour is perceptual processing and is fast because actions are taken automatically (tacit) in response to perceptual features of the environments. Rule-based behaviour is also perceptual, but actions are taken through cue-action mapping (consciously) based on internal rules/heuristics. Knowledge-based behaviour is concerned with analytical problem-solving. People activate skill- or rule-based behaviours in familiar situations, whereas they activate knowledge-based behaviours in uncertain and novel situations (Rasmussen, 1983; Vicente and Rasmussen, 1992). These are not discrete in practice. While these levels are described individually, interaction with a complex environment requires simultaneous activation of all three levels of processing (Rasmussen and Vicente, 1989; Reason, 1990). An operator supported with carefully designed interface will seamlessly activate and transition between all three levels of cognitive processing contingent on the operator's competency with skills, efficacy of applicable heuristics or rules and knowledge pertinent to that context. The degree to which the operator can leverage perceptual processing is also a function of the expertise level (Leplat, 1988; Sanderson and Harwood, 1988; Olsen and Rasmussen, 1989; Rasmussen, 1990). Thus, effective interaction design requires a clear understanding of knowledge, skills and understanding of how individuals apply different heuristics in different situations.

In accordance with the SRK taxonomy, the three broad cognitive components that govern security expert behaviours would be: security-related skills, rules and knowledge (Security SRK). From our results, we identified four "skill-" and "knowledge-" based factors predictive of security expertise in end users. In related work, Egelman *et al.* identified four security factors on rules/heuristics. We posit security expertise instrument for end user should effectively measure these three components: security skills, rules and knowledge.

We argue that these can form a basis for building a framework on the SRK taxonomy – one that is repeatable and can be iterated. Factors for measuring skills could assess perception-based actions end users can take with a wide range of security interfaces and controls. This could include assessment of skills such as interaction with authentication systems, system security configuration, spam filtering, secure Web browsing, to name a few. Factors for measuring rules should enable assessment of rules that end users have for responding to different security contexts and interfaces. There is a large body of work that has identified a plethora of heuristics that people should be using while interacting with security interfaces. Factors for measuring knowledge should assess comprehension on a multitude of security concepts that end users would use while analysing novel and rare security events.

We have offered the first steps on an expertise instrument. A next step is to validate our expertise instrument against security behaviours that span all three levels of cognitive processing. This would require observing users' interactions with different security interfaces, eliciting whether they used automatic processes or rules while taking those actions, and finally assessing how users analyse novel security situations by leveraging their comprehension of relative concepts. We argue that people would be using one or more of these cognitive processes in security interaction. For example, while entering a passcode on a personal mobile device or deleting known spam e-mails, people would be activating skill-based behaviours. In contrast to today's requirement that individuals look for the "green lock icon" before entering personal information, interactions grounded in the appropriate framework could engage people in activating appropriate rule-based behaviours. Similarly, user actions to security updates and alerts would enable knowledge-based behaviours because they are less frequent, relatively un-familiar and would require more cognitive effort.

7. Conclusion

We addressed the lack of standardized instruments for measuring end-user security expertise by designing a questionnaire combining skills- and knowledge-based question. Through qualitative analysis and exploratory factor analysis, we identified four skills and knowledge-based factors of expertise. We validated these factors using logistic regression modelling. We close by proposing a framework called Security SRK to guide further research on end user security expertise. Future work on expertise could leverage the high-level framework by combining contextual rules with skills and knowledge factors identified here. In future work, we will continue to explore relevant computer and security skills, rules and knowledge variables to ensure we have identified consistent and reliable predictors for end-user expertise. Future work includes validation against security skill-, rule- and knowledge-based behaviours as proposed earlier.

References

Albrechtsen, E. (2007), "A qualitative study of users' view on information security", *Computers & security*, Vol. 26 No. 4, pp. 276-289.

Almuhimedi, H., Felt, A.P., Reeder, R.W. and Consolvo, S. (2014), *Your Reputation Precedes You: History, Reputation, and Chrome Malware Warning*, SOUPS, Menlo Park, CA, pp. 113-128.

Arianezhad, M., Camp, L.J., Kelley, T. and Stebila, D. (2013), "Comparative eye tracking of experts and novices in web single sign-on", *Proceedings of the third ACM Conference on Data and Application Security and Privacy*, *New York, NY*, ACM, pp. 105-116.

Asgharpour, F., Liu, D. and Camp, L.J. (2007), "Mental models of security risks", *Financial Cryptography and Data Security*, Springer, Berlin Heidelberg, pp. 367-377.

Barrett, R., Kandogan, E., Maglio, P.P., Haber, E.M., Takayama, L.A. and Prabaker, M. (2004), "Field studies of computer system administrators: analysis of system management tools and practices", *Proceedings of 2004 ACM conference on CSCW*, *New York, NY*, ACM, pp. 388-395.

Ben-Asher, N. and Gonzalez, C. (2015), "Effects of cyber security knowledge on attack detection", *Computers in Human Behavior*, Vol. 48, pp. 51-61.

Bernard, H.R. (2011), *Research Methods in Anthropology: Qualitative and Quantitative Approaches*, Rowman, Altamira.

Bertenthal, B. (2015), "Tracking risky behavior on the web: distinguishing between what users", *2015 AAAS Annual Meeting, 12-16 February 2015*, *San Jose, CA*.

Butler, D.J., Huang, J., Roesner, F. and Cakmak, M. (2015), "The privacy-utility tradeoff for remotely teleoperated robots", *Proceedings of the Tenth Annual ACM/IEEE International Conference on Human-Robot Interaction*, *Portloand, OR*, ACM, pp. 27-34.

Cranor, L.F., Reagle, J. and Ackerman, M.S. (2000), "Beyond concern: understanding net users' attitudes about online privacy", AT&T Labs Technical Report TR 99.4.3.

Egelman, S. (2009), Trust me: design patterns for constructing trustworthy trust indicators (Doctoral dissertation, Carnegie Mellon University).

Egelman, S. and Peer, E. (2015), "Scaling the security wall: developing a Security Behavior Intentions Scale (SeBIS)", *ACM Human Factors in Computing Systems*, *Seoul*, pp. 2873-2882.

Egelman, S., Harbach, M. and 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*, *San Jose, CA*, ACM, pp. 5257-5261.

Fan, J. and Zhang, P. (2011), "Study on e-government information misuse based on General Deterrence Theory", *ICSSSM11*, *Tianjin*, IEEE, pp. 1-6.

Frank, J., Shamir, B. and Briggs, W. (1991), "Security-related behavior of PC users in organizations", *Information & Management*, Vol. 21 No. 3, pp. 127-135.

Furnell, S.M., Jusoh, A. and Katsabas, D. (2006), "The challenges of understanding and using security: a survey of end-users", *Computers & Security*, Vol. 25 No. 1, pp. 27-35.

Garg, V., Huber, L., Camp, L.J. and Connelly, K. (2012), "Risk communication design for older adults", *Gerontechnology*, Vol. 11 No. 2, p. 166.

Garg, V., Camp, L.J., Lorenzen-Huber, L., Shankar, K. and Connelly, K. (2014), "Privacy concerns in assisted living technologies", *Annals of Telecommunications*, Vol. 69 Nos 1/2, pp. 75-88.

Gelman, A. and Loken, E. (2013), "The garden of forking paths: Why multiple comparisons can be a problem, even when there is no 'fishing expedition' or 'p-hacking' and the research hypothesis was posited ahead of time", Department of Statistics, Columbia University, Columbia.

Goodall, J.R., Lutters, W.G. and Komlodi, A. (2004), "I know my network: collaboration and expertise in intrusion detection", *Proceedings of ACM Conference on CSCW*, *Chicago, IL*, pp. 342-345.

Herath, T. and Rao, H.R. (2009), "Encouraging information security behaviors in organizations: role of penalties, pressures & perceived effectiveness", *DSS*, Vol. 47 No. 2, pp. 154-165.

Ion, I., Reeder, R. and Consolvo, S. (2015), "…no one can hack my mind: comparing expert and non-expert security practices", *Eleventh SOUPS 2015*, *Ottawa*, pp. 327-346.

Kleinbaum, D.G. and Klein, M. (2010), "Maximum likelihood techniques: an overview", *Logistic Regression*, Springer, New York, NY, pp. 103-127.

Kline, P. (2014), *An Easy Guide to Factor Analysis*, Routledge, Abingdon.

Kruger, H.A. and Kearney, W.D. (2006), "A prototype for assessing information security awareness", *Computers & Security*, Vol. 25 No. 4, pp. 289-296.

Leplat, J. (1988), "Task complexity in work situations", *Tasks, Errors, and Mental Models*, Taylor & Francis, Abingdon, pp. 105-115.

McCormac, A., Calic, D., Parsons, K., Zwaans, T., Butavicius, M. and Pattinson, M. (2016), "Test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q)", *Australian Conference on Information Systems*, *Wollongong*.

Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004), "Internet users' information privacy concerns (IUIPC)", *Information Systems Research*, Vol. 15 No. 4, pp. 336-355.

Maxion, R.A. and Reeder, R.W. (2005), "Improving user-interface dependability through mitigation of human error", *International Journal of Human-computer Studies*, Vol. 63 No. 1, pp. 25-50.

Netemeyer, R.G., Bearden, W.O. and Sharma, S. (2003), *Scaling Procedures: Issues and Applications*, Sage Publications, Thousand Oaks, CA.

Ng, B.Y., Kankanhalli, A. and Xu, Y.C. (2009), "Studying users' computer security behavior: a health belief perspective", *Decision Support Systems*, Vol. 46 No. 4, pp. 815-825.

Nielsen, J. (2016), *The Distribution of Users' Computer Skills: Worse Than You Think*, available at: www.nngroup.com/articles/computer-skill-levels/

OECD (2016), *Skills Matter: Further Results from the Survey of Adult Skills*, OECD Publishing, Paris.

Olsen, S.E. and Rasmussen, J. (1989), "The reflective expert and the prenovice: notes on skill-, rule-and knowledge-based performance in the setting of instruction and training", *Developing Skills with Information Technology*, Wiley, Hoboken, NJ.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014), "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)", *Computers & Security*, Vol. 42, pp. 165-176.

Rasmussen, J. (1983), "Skills, rules, and knowledge; signals, signs, & symbols, and other distinctions in human perfrm. models", *IEEE Transactions on Systems, Man and Cybernetics*, No. 3, pp. 257-266.

Rasmussen, J. (1990), "Mental models and the control of action in complex environments", *Mental Models and Human-Computer Interaction*, North-Holland Publishing, Amsterdam, Vol. 1, pp. 41-69.

Rasmussen, J. and Vicente, K.J. (1989), "Coping with human errors through system design: implications for ecological interface design", *International Journal of Man-Machine Studies*, Vol. 31 No. 5, pp. 517-534.

Reason, J. (1990), *Human Error*, Cambridge University Press, Cambridge, MA.

Reisberg, D. (1997), *Cognition: Exploring the Science of the Mind*, WW Norton & Co, New York, NY.

Sanderson, P.M. and Harwood, K. (1988), "The skills, rules and knowledge classification: a discussion of its emergence and nature", *Tasks, Errors, and Mental Models*, Taylor & Francis, Abingdon, pp. 21-34.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. and Downs, J. (2010), "Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Atlanta, GA*, ACM, pp. 373-382.

Sotirakopoulos, A., Hawkey, K. and Beznosov, K. (2011), *On the Challenges in Usable Security Lab Studies: Lessons Learned From Replicating A Study on SSL Warnings*, SOUPS, Pittsburgh, PA, p. 3.

Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J. (2005), "Analysis of end user security behaviors", *Computers & Security*, Vol. 24 No. 2, pp. 124-133.

Stephanou, A. (2009), "The impact of information security awareness training on information security behaviour", Doctoral dissertation, University of the Witwatersrand, Johannesburg.

Vicente, K.J. and Rasmussen, J. (1992), "Ecological interface design: theoretical foundations", *IEEE Transactions on Systems, Man, and Cybernetics*, Vol. 22 No. 4, pp. 589-606.

Further reading

Buchanan, T., Paine, C., Joinson, A.N. and Reips, U.D. (2007), "Development of measures of online privacy concern and protection for use on the Internet", *Journal of the American Society for Information Science and Technology*, Vol. 58 No. 2, pp. 157-165.

Corresponding author

Prashanth Rajivan can be contacted at: prajivan@andrew.cmu.edu