What Can Johnny Do?–Factors in an End-User Expertise Instrument

Prashanth Rajivan, Pablo Moriano, Timothy Kelley and Jean Camp
School of Informatics and Computing, Indiana University, Bloomington, USA
e-mail: {prajivan; pmoriano; kelleyt; ljcamp}@indiana.edu

Abstract

Security and computer expertise of end users can be significant predictors of user behaviour and interactions in the security and privacy context. Standardized, externally valid instruments for measuring end-user security expertise are non-existent. To address this need, we developed a questionnaire to identify critical factors that constitute expertise in end-users. It combines skills and knowledge based questions. Using exploratory factor analysis on the results from 898 participants from a range of populations, we identified 12 questions within 4 factors that correspond to computing and security expertise. Ordered logistic regression models were applied to measure efficacy of proposed security and computing factors in predicting user comprehension of security concepts (phishing and certificates). We conclude with a framework for informing future user-centered security expertise research.

Keywords Expertise, Security, Privacy, Psychometrics, Security Comprehension

1. Introduction

Security technologies are increasingly being developed with a user-centric approach. However, people interacting with security systems possess tremendously different levels of computer and security knowledge and even different levels of basic literacy. Developing appropriate security systems requires taking security expertise as well as computer expertise into consideration. The need to identify and operationalize valid factors that constitute security expertise in end-users motivates this work. Validated instruments for measuring the security (and computer) expertise of end users along the lines of instruments developed for evaluating user privacy concerns on Internet (IUIPC) (Malhotra et al., 2004) are needed. It is widely recognized that security and computing expertise affect security attitudes and behaviours. There are three common practices in behavioural and usable security research today. One way security expertise is addressed is by participant selection; for example, choosing computer science students at CMU (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.

Please reference as *International Symposium on Human Aspects of Information Security & Assurance*, Frankfurt, Germany, (HAISA 2016) 19-21 July 2016. This replaces a previous version of "Measuring Computing and Security Expertise"

Expertise is granular (Reisberg, 1997) even in 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), security awareness (Stephanou, 2009), and also in terms of interactions with security interfaces (Bertenthal, 2015). Expert users can leverage their extensive security background 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 don't know.

To address the need for standardized and valid measures of security expertise in end-users', 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 (e.g., "I backup my computer″) for a comprehensive expertise instrument.

2. Related Work

Previous research in the usable security and privacy domain, online risk communication, and some work in behavioural economics has informed our instrument design. We provide examples of such research acknowledging that this is not a comprehensive survey. Specifically, we have drawn on work by Egelman and Sotirakopoulos, Hawkey, and Beznosov to develop questions dealing with technical expertise (Egelman, 2009; Sotirakopoulos et al., 2011).

Other 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 attack detection, detection of vulnerabilities, contextual awareness, and assessments of risk and attack response.

With respect to end-users, past security research has placed significant emphasis on identifying security attitudes and practices of end-users. There has been research done to understand novice users' views about security practices and awareness (Albrechtsen, 2007; Ion et al., 2015; Herath et al., 2009). These 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. Past research has also focused on exploring end user behaviours that affect the security posture of an organization (Stanton et al., 2005). Such research has focussed on novice users but does not include measures of security and computer expertise.

Measures of privacy perceptions inspired much of this work. The standard we hope to meet is that set for measuring privacy through Internet users' information privacy concerns (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. Another rigorous option for measurement of online privacy is (Buchanan et al., 2007). Yet the most widely used 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. Table 1 presents the expertise questions in our instrument.

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 your ever installed a computer program?
	Have your ever written a computer program?
	Have your ever designed a website?
	Have your ever registered a domain name?
	Have your 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 1: Questions in the instrument

3. Instrument Design

Our goal was to design an instrument that could be used to measure and differentiate end-users' computer and security expertise. Towards this, we first generated a list of common yet essential computer security skills and knowledge an end-user would need to make risk aware choices online. Relevant computer security skills and knowledge was operationalized through a questionnaire composed of open-response questions, Boolean-type questions, and multiple choice queries. In the following, we describe the questions used in the instrument for measuring computer and security expertise. For the open response questions, we describe the qualitative analysis performed along with the coding scheme used for analysis.

Academic and professional background in security can be strong predictors of security expertise. Hence, questions that queried end-users' security-related academic and professional experience were asked. Hands-on computer and security experience can play a vital role in shaping one's expertise and knowledge as it would involve active learning through trial and

error and reading online manuals. Furthermore, we identified questions that queried the participants' interactions and behaviour with computing devices in their everyday lives. More interactions could be causal for improved computer and security 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 on a daily basis.

4. Experiment Methods

We recruited 898 participants for this study from five different populations which includes participants from MTurk (696 participants), 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 includes responses from people visiting their local farmers' market. The Dashcon population includes responses from enthusiasts attending the blogging (Tumblr) conference. This population is young and spends many hours on the Internet. Mini University includes retired University alumni attending a week-long adult learning experience. Finally, the Grace Hopper population includes responses largely from woman technologists attending the annual Grace Hopper conference.

4.1. Demographics

The median age of survey participants was 34 (median age of US population is 36.8). The minimum age of participants was 18 and the maximum age was 68. The average age of participants is slightly skewed (younger) than the US population as a whole despite the inclusion of the Mini University population. In terms of gender makeup, 47 percent of survey participants were male whereas 53 percent were female. (Higher number of female participants could be due to Grace Hopper participants.) Fewer than 11 percent of the survey participants were students whereas 78 percent of them were employed. In terms of income, the median income level of the US population as a whole shows a peak at the $25,000-$30,000 level, with a median income of $51,000 per year. However, that is skewed by the 4 percent of households making more than $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 $20,000 to less than $30,000, close to the distribution of overall US population.

4.2. Qualitative Analysis

Notable components of the instrument are the 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 came together to develop the final order of classification based on consensus as shown in Table 2 and Table 3.

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 info (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	Don't Know

Table 2: Qualitative codes for phishing ordered by level

Table 2 presents the list of codes used to bin the responses to the question about phishing. Phishing is something we expected to be far more common and well-known than certificates. However, 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. Table 3 presents the list of codes that was used to bin 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. The second surprising result was the optimism with respect to the scope and the function of a security certificate. These two open-ended questions were used as dependent variables in the regression models.

5. Exploratory factor analysis

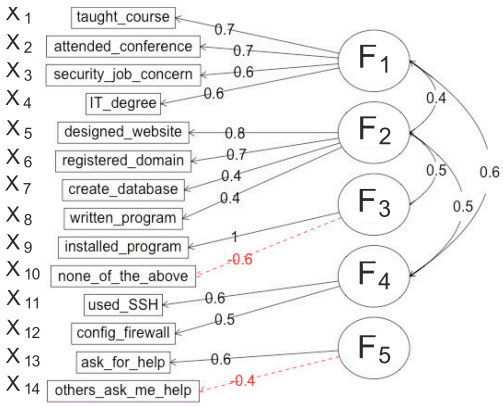
Exploratory factor analysis using PCA (principal component analysis) was used for factor extraction. PCA was used to summarize the relationships among the original variables in terms of a smaller set of dimensions. The responses of 898 participants were used to calculate the factor loadings of 15 variables 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. A Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy revealed that the use of factor analysis was adequate, given the data (KMO = 0.83). A Bartlett's test of Sphericity revealed that the correlation matrix came from a population of independent samples (χ^2=4087.4, df =105, $p<0.001$) further indicating that the factor analysis is justified by the properties of the correlation matrix. We identified and extracted five factors based on the Kaiser's criterion for Eigenvalues.

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	Don't know

Table 3: Qualitative codes for certificates ordered by level of accuracy

In order 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, variables within factors and their respective loadings are shown in the diagram in Figure 1. The five factors are arranged in a decreasing order of variance, such that $\text{Var}(F_1) \geq \text{Var}(F_2) \geq \ldots \geq \text{Var}(F_5)$. Similarly, the variables (i.e., $X_1, X_2, \ldots, X_{14}$) 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% of the total variance within the data.

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 1, it can be seen that 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 1, 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.



Factor	Eigenvalue	Accounted Variance
F1	4.574	32%
F2	2.004	27%
F3	1.191	19%
F4	1.099	13%
F5	0.9	9%

Figure 1: (Left) Factor Analysis Diagram. (Right) Eigenvalue & variance per factor

Based on final factor analysis configuration, we defined two scores: computer and security scores. Specifically, let $\Omega=\{X_5, X_6, X_7, X_8\} \cup \{X_9, X_{10}\}$ 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 1. Similarly, let $\Phi=\{X_1, X_2, X_3, X_4\} \cup \{X_{11}, X_{12}\}$ 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 1. The Computer Score (CS) of a participant is defined as $\Sigma_{X\epsilon\Omega}\{X^*\Lambda_X\}$ 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. Similarly, 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 and found a positive association between them which implies that security expertise is predicated on computer expertise. This result provides some validation for the instrument and also validates the merging of factors to create computer and security scores.

5.1. Regression Analysis

Based on the qualitative analysis (described earlier), a set of codes (shown in Table 2 and Table 3) were derived to substitute the participants' answers to the two open-ended questions on security concepts 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 security score (SS_i) and computer scores (CS_i) serving as non-parametric independent variables. In this analysis, we considered only participants who responded to both the questions resulting in 781 participants. The results of logistic regression analysis on phishing responses are shown in Figure 2A. To check the proportional odds assumption (i.e., an ordinal model), 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 (χ^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 2A, 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. Similarly, we ran an ordered logistic regression to predict the X.509 certificate responses using computer and security score. The results of the regression analysis are shown in Figure 2B. The proportional model odds assumption was checked and was found

to be satisfied (χ^2=155.746, df = 2, p<0.01). In addition, estimates of the intercepts and coefficients were found to be statistical significant. In the case of certificates as well as for phishing, both predictors (CS and SS) were statistically significant.

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

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 2: Ordered Logistic Regression for Phishing (A) and Certificates (B)

6. Discussion

Qualitative analysis reveals a tremendous variability in terms of end-user comprehension of security terminologies: certificates and phishing. Even though end-users are broadly classified as security novices, there are levels to their computer and security expertise that could be reasonably measured and operationalized. The four factors identified in our analyses were operationalized as predictors (computer and security scores) in a logistic regression model. Identified computer and security expertise factors were found to be predictive of user comprehension on certificates and phishing. Future work includes validation against observed security behaviours such as attention to browser security cues, password behaviour, and mobile apps.

On further inspection, we found that the four factors clearly classify 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 four skill and knowledge based factors are crucial predictors of computer security expertise in end users. The cluster analyses show 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 real world. The regression analysis also reveals 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 on security concepts.

The four categories identified through this work have encouraged us to propose a high-level theoretical framework for measuring end-user security expertise. Such a framework could guide future research which impinges security expertise. Depending on context, familiarity, and expertise levels people employ three main types of cognitive processes (Skills, Rules, Knowledge or SRK (Rasmussen, 1983)). Therefore, it is critical to identify computer and security related *Skills*, *Rules/heuristics*, and *Knowledge* factors that reflect end-user expertise. From our results, we found four "Skill" and "Knowledge" based factors predictive of security expertise in end-users. In a related but independent work, researchers have developed a 16

item, scale-based instrument to measure the security rules end-users employ (Egelman et al., 2015). The categories of rules covered multiple usable security domains, e.g., password creation, device locking, and software updates. Future work could leverage the high-level framework enabled 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.

7. References

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

Albrechtsen, E. (2007). A qualitative study of users' view on information security. Computers & security, 26(4), 276-289.

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

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

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

Bertenthal, B. (2015, February). Tracking Risky Behavior on the Web: Distinguishing Between What Users\. In 2015 AAAS Annual Meeting (12-16 February 2015). aaas.

Buchanan, T., Paine, C., Joinson, A. N., & 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, 58(2), 157-165.

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

Cranor, L. F., Reagle, J., & 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.

Egelman, S., & Peer, E. (2015). Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). ACM Human Factors in Computing Systems (pp. 2873-2882).

Garg, V., Huber, L., Camp, L. J., & Connelly, K. (2012). Risk communication design for older adults. Gerontechnology, 11(2), 166.

Garg, V., Camp, L. J., Lorenzen-Huber, L., Shankar, K., & Connelly, K. (2014). Privacy concerns in assisted living technologies. Annals of Telecommunications, 69(1-2), 75-88.

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

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures & perceived effectiveness. DSS, 47(2), 154-165.

Ion, I., Reeder, R., & Consolvo, S. (2015). "... no one can hack my mind": Comparing Expert and Non-Expert Security Practices. In Eleventh SOUPS 2015. (pp. 327-346).

Kline, P. (2014). An easy guide to factor analysis. Routledge.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC). Information Systems Research, 15(4), 336-355.

Maxion, R. A., & Reeder, R. W. (2005). Improving user-interface dependability through mitigation of human error. International Journal of human-computer studies, 63(1), 25-50.

Rasmussen, J. (1983). Skills, rules, and knowledge; signals, signs, & symbols, and other distinctions in human perfrm. models. IEEE Trans. Sys., Man & Cybernetics, (3), 257-266.

Reisberg, D. (1997). Cognition: Exploring the science of the mind. WW Norton & Co.

Sotirakopoulos, A., Hawkey, K., & Beznosov, K. (2011, July). On the challenges in usable security lab studies: lessons learned from replicating a study on SSL warnings. SOUPS (p. 3).

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. Computers & Security, 24(2), 124-133.

Stephanou, A. (2009). The impact of information security awareness training on information security behaviour (Doctoral dissertation).