2016 49th Hawaii International Conference on System Sciences

Measuring the Human Factor in Information Security and Privacy

Marc J. Dupuis
University of Washington
marcjd@uw.edu

Robert E. Crossler
Mississippi State University
rob.crossler@msstate.edu

Barbara Endicott-Popovsky
University of Washington
endicott@uw.edu

Abstract

In this paper, we describe the development and validation of three survey instruments designed to measure the human factor in information security and privacy. These instruments are intended to measure the extent to which people engage in the responses necessary to mitigate three different information security and privacy threats: computer performance compromise, personal information compromise, and loss of data and files. This paper makes a significant contribution by providing validated survey instruments that can be used by other researchers in the future. The instruments may be used in combination with various theoretical approaches, such as Protection Motivation Theory. Likewise, researchers may opt to use one, two, or all three survey instruments, depending on the particular needs of the research question(s) being addressed. Response pattern statistics are also provided along with suggestions for how the instruments may be used.

1. Introduction

Understanding the information security and privacy behavior of home users is a complex task that requires careful planning and a thoughtful approach. One could simply develop a list of best practices related to information security and privacy behaviors and assume that those who engage in more of these practices have superior information security and privacy behavior compared to those who do not. However, this approach ultimately does not take into account the context of the behavior. This may not be critical in all research that examines the information security and privacy behaviors of home users [1], but in the current research it is considered important given the different motivations that may come into play in response to varying threats. Therefore, the approach employed here examines three significant information security and privacy threats to home users and the responses necessary to mitigate these threats.

The use of threat response pairs is an effective way to account for varying contexts and the approach employed here is similar to the one used by Crossler and Bélanger [2] in their examination of the responses necessary to protect one from the threat of losing data and files. This involves first identifying a threat and then determining the response(s) necessary to mitigate the threat. For example, one of the responses necessary to mitigate the threat of losing one's data and files may be keeping current backups of data.

Following the general guidelines from Churchill [3] and Straub [4], three new survey instruments were developed to assess the responses necessary to protect individuals from three different information security and privacy threats: loss of data and files, personal information compromise, and computer performance compromise. These three threats were chosen based on their potential to negatively impact the three primary areas of concern for information security and privacy: confidentiality, integrity, and availability [5]–[9].

The development of these three new survey instruments included an extensive literature review, convening an expert panel review, pre-testing the resulting instruments, pilot testing the revised instruments, and finally administration of the main study with slight revisions made from the pilot study.

The remainder of this article discusses an important distinction between behavioral intention and self-reported behavior, describes the process employed, outcomes, and associated statistical analyses, followed by some recommended uses of these new instruments. We start with a discussion on using self-reported behavior rather than behavioral intentions.

2. Behavioral Intention vs. Self-Reports of Behavior

This study used information on an individual's reported behavior rather than behavioral intentions. Although most of the theories that have been used to understand behavior within the information systems domain include a behavioral intention construct that acts as the main determinant of behavior (Ajzen, 1985; Fishbein & Ajzen, 1975; Rogers, 1975; Triandis, 1977), it may not be the most appropriate way to

1530-1605/16 $31.00 © 2016 IEEE
DOI 10.1109/HICSS.2016.459

measure the information security behavior of home users [14]. According to Crossler and Bélanger [14], "intentions to protect one's computer may not be enough, particularly with the rapid spread of computer threats" [14, p. 85].

Additionally, most of the research that has reviewed the literature on the intention-behavior relationship has examined primarily correlational studies, which make inferences regarding causation problematic [15]. In a meta-analysis of research that employed experimental manipulations, Webb and Sheeran [15] found the strength of the hypothesized relationship to be much lower. In fact, a medium-to-large change in intention only led to a small-to-medium change in behavior [15, p. 260].

Finally, there are two others factors that weaken the argument for measuring behavioral intention in the current research. First, the information security behaviors of interest in the current research designed to mitigate the three threats (i.e., computer performance compromise, personal information compromise, and loss of data and files) may have become largely habitual for a great number of users. There is a weaker relationship between intention and behavior for behaviors that are more routine and stable over time (i.e., habits) [16], [17]. Second, the current research does not include an experimental manipulation. While it is possible that the survey instrument itself may increase a participant's intention of performing a certain information security behavior, that is not the purpose of the survey instrument. Instead, the focus is on understanding the relationship between certain constructs and an individual's current behavior. Therefore, self-reports of behavior were measured in the current study, which is considered an important step towards measuring actual behavior.

Next, we begin our discussion on the process employed in developing the survey instruments.

3. Construct Domain

The first step in survey instrument development is specifying the domain of the construct. For purposes of this research, an examination of the information security and privacy behavior of home users, we begin by delineating the scope of the home user and their behavior. In particular, the home user domain in this research is limited to an examination of the user behavior that occurs outside of the traditional work environment [18].

Additionally, we are only concerned with home users' behavior on their primary computer, which can be defined as the computing device they use a majority of the time and that is not owned or issued by their employer. It was important to specify a primary computer given the number of individuals today who have more than one computing device they use on a regular basis [19]. Admittedly, their use of secondary and tertiary computing devices could make them vulnerable to certain threats; however, the significant variability in the number and types of devices individuals own make it impractical to examine this other behavior through the same survey instrument.

From a conceptual standpoint the instruments developed herein are concerned with the responses necessary for a home user to effectively mitigate three different information security and privacy threats: loss of data and files, personal information compromise, and computer performance compromise. In other words, the three instruments are concerned with specifying the types of information security and privacy responses that are required to ensure that these threats are minimized. Thus, each of the instruments includes different dimensions of information security and privacy behavior with each dimension representing a specific type of response (e.g., updating software) and with each response consisting of one or more specific tasks (e.g., updating the OS, updating other software). For example, one response that may be necessary to mitigate the threat of one's personal information from being compromised may be to use antimalware software. However, this response may include several different tasks, such as keeping virus definitions current and having scans performed automatically.

The more tasks and thus responses performed by the individual then the lower the associated risk from a given threat. While some of the tasks are related to one another, as are the responses, they are all considered necessary in order to effectively mitigate a specific threat. Therefore, the model employed here is considered formative first-order, formative second-order [20]–[24].

Finally, some responses to information security and privacy threats are dichotomous—users either perform the response or they do not. Other responses may be more convoluted than this, such as password usage. For example, in one sense a password is either used or not; however, in many instances this may not be an option. What may be more important is how a password is used: changed frequently, complex, difficult to guess, etc. Regardless of whether the potential responses are simple or perhaps more intricate, home users often do not know what information security and privacy tasks they perform versus those they do not [25]–[31]. For example, a firewall is an incredibly important tool that can help mitigate many different types of threats. However, many of these types of tools are too complex for the

average user to understand, let alone know whether or not they are using it. In some instances, a firewall may be included as part of the operating system, while in other instances this may not be true. Users may not know for sure, but may have an idea that can be expressed as a certain level of confidence.

Therefore, the current study examines the degree they believe they perform certain tasks by using a 5-point Likert scale. This allows for participants to indicate a certain level of certainty and uncertainty in their responses in accordance with their actual knowledge of their behavior. Research that has used Likert scales to represent an individual's uncertainty have largely involved general information security and privacy questions [1] or had only a narrow focus (e.g., [29], [32]), while those that have developed comprehensive survey instruments with greater granularity have employed questions that did not provide as much opportunity for this lack of certainty (e.g., [2]). Therefore, the goal of these instruments is to capture both the uncertainty and granularity related to the information security and privacy behavior of home users. Next, we discuss the generation of items for the survey.

4. Samples of Item Generation

4.1. Literature Search

The next step in developing a survey instrument is the generation of items to be measured. This involved two distinct components: literature search and the convening of a subject matter expert panel. The goal of the literature search was to identify existing instruments and measures specific to home users and related to information security and privacy responses necessary to mitigate the three threats previously identified. Fourteen information security and privacy responses were identified through this search with one of them being removed (i.e., use of pop-up blocking software) after the expert panel review.

The information security and privacy responses each consisted of one or more indicators that are measured on a 5-point Likert agreement scale (e.g., "I am confident that I have a firewall enabled for my primary computer."). After an exhaustive search on the various information security and privacy responses necessary to mitigate the numerous threats, a subject matter expert panel was convened.

4.2. Subject Matter Expert Panel Review via the Delphi Technique

Individuals were considered subject matter experts if they engaged in information security and privacy work more than 50% of their day, whether it was work in industry, government, military, teaching, private consulting, or research. Participants were recruited from the Anti-Phishing Working Group (APWG) listserv (N=10) and through qualifying questions using Amazon's Mechanical Turk (N=9); they had an average of 15.1 and 7.6 years of experience within information security and privacy, respectively. A majority of the respondents were from the United States with each major geographic region represented. Other respondents were from Asia, South America, and Europe. Approximately two-thirds of the respondents were male. Several different sectors were represented, including the military, academia, private industry, and public industry.

The Delphi technique was used for the subject matter expert portion of survey development [43]–[47], which has been used in the past for expert panel review in instrument development within information systems research [48]. This included a slight modification in that participants were not provided with individualized surveys that contained their prior responses during the second and third rounds of review. Due to both privacy concerns and practical considerations, this modification was considered necessary. Nonetheless, participants were encouraged to print out their responses after each round in order to mitigate this modification.

The goal of the Delphi technique is consensus; however, what is meant by consensus varies significantly from one study to the next [47]. Therefore, it is important for researchers to specify what is meant by consensus in each study that employs the technique. In the current study, consensus was considered met if 75% or more of the participants were in agreement. This level of agreement was chosen based on the desire to balance other consensus thresholds, such as 51% and 100%. Additionally, the 75% level is of historical significance in consensus decision making by the Iroquois Confederacy Grand Council and may date back to possibly the 12th century AD [49].

While consensus is the goal, it does not happen immediately. Several rounds are employed in which the survey instrument is transformed from one with very open-ended questions to a final instrument [46]. The number of rounds necessary for this to take place may vary significantly, but generally speaking three rounds is considered a good balance between participant fatigue and additional movement toward consensus. In the current study, three rounds were utilized.

The first round consisted of a survey instrument that had open-ended questions for each response and threat-response pairing. Initial measurement items (i.e., indicators) for each of the responses were provided based on the literature search, but participants were asked to validate the adequacy of indicators for each response and suggest new and/or modified ones, if necessary. Additionally, participants were asked to determine which responses were necessary for each of the three threats. Since this was the first round, they were given three options: necessary responses, not sure if these responses are necessary, and unnecessary responses. Using the Qualtrics survey platform, participants moved each of the responses into one of those three categories for each of the three threats.

Several changes were made based on the results from the first round. This included wording changes to make the items clearer, modifications to some of the items, and additional measurement items added. One such change involved rewording an item designed to gauge the level of caution in providing credit card information online to one that measured personal financial information more broadly. No items were deleted after this round as it is generally considered important to limit the removal of items when it is still early in the process [45]–[47].

Additional refinements were made after the second round, including consolidation of some items and the separating of others that were considered confusing. The third and final round was concerned primarily with quantitative ratings of the items, although there was still some room for comments at the end of each of the two major sections (i.e., responses and their indicators, threat-response pairs) of the instrument. Also, participants were limited to choosing either necessary responses or unnecessary responses for the section that contained the threat-response pairs. Only those items that met the 75% consensus threshold were included in the survey instrument. While the response related to home users employing pop-up blocking software on their computers was considered a good response, it did not meet the 75% threshold for any of the threats.

5. Pretesting

5.1. Pretest, Part 1: Initial Technical Review

The first part of pretesting involved a review by 10 academics that engage in survey research, including both PhD students and faculty at various professorial ranks. The primary concern during this step of pretesting was survey item construction. In other words, were the items written in a clear and unambiguous manner, while adhering to general principles related to the structure of survey question items [50]?

Several changes were made, including limiting the length and complexity of some of the items. A few of the items were made more general, while a few others were broken into two or three separate questions. Finally, it was pointed out that a few of the responses appeared more Windows operating system specific and thus did not make sense for Mac owners or those that ran Linux-based operating systems (e.g., Ubuntu). These responses were modified such that they would only be included if the participant indicated in a filter question that her primary computer used the Windows operating system.

Changes were made to several questions, but these changes involved structure rather than substance. Thus, the results of the subject matter expert panel review were not altered in any meaningful way.

5.2. Pretest, Part 2: Potential Participant Review via Cognitive Interviews

Next, we interviewed several individuals who were representative of potential participants. Although it is important for the items to be worded in a clear manner, the previous review was limited to structure and syntax. In order to assess the viability and clarity of the questions to potential participants, cognitive interviews were conducted with 15 individuals. These individuals were not graduate students, did not have advanced degrees, and did not work in or have more than average knowledge of information security and privacy matters. In other words, they represented the average survey participant.

The general process employed for this part of pretesting was based on the cognitive interviewing process commonly used in research [51], [52]. The participants were provided with a copy of the survey instrument and asked to describe their interpretation of each of the questions. When it became apparent a question was unclear or confusing to a participant, notes were taken so that they could be compared with the other cognitive interviews. Ultimately, some minor changes were made to a few of the items. Additionally, one of the participants mentioned that she was unsure what was meant by encryption. In the next iteration of the survey instruments a simple definition of encryption was included.

5.3. Pretest, Part 3: Final Technical Review

The final part of pretesting involved another technical review. The composition of the participants for this review consisted of a similar number of academics as the first part of pretesting, including an

equal split between PhD students and faculty members in the professorial ranks. This was an opportunity for other academics to identify issues that perhaps were not noticed previously. Likewise, since some minor changes were made during the second part of pretesting, this final technical validation provided a review of the items that might have been reworded slightly. As would be expected in a third round of pretesting, only a couple of very minor changes were made.

6. Data Collection

6.1. Part 1: Pilot Study

After the extensive development and review stages outlined above, we conducted a pilot study to ascertain the viability of the measurement items. Participants were recruited from Amazon's Mechanical Turk and provided with 50 cents compensation. They clicked on a URL that took them to the survey. Within the survey instrument itself, they were randomly assigned to complete one of the three survey instruments developed herein. Included in each of the three surveys was a quality control question: "I am able to fly a car to the moon right now if I wanted to." Only those that passed the quality control question by indicating "strongly disagree" were included in the data analysis portion.

The main issue that surfaced during the pilot study outside of the items themselves was that the compensation rate may have been too low based on the amount of time that was required to obtain the responses in comparison to prior studies [53], [54]. Possibly as a result, participants failed to submit responses to the longer survey at a disproportionate rate compared to the other two shorter surveys. Thus, the final number for the *Personal Information Compromise* survey is lower than that of the others. Therefore, we decided to increase the compensation level for the main study to mitigate these two issues.

6.2. Measure Purification

In addition to the compensation issue discovered in the pilot study, there were a few adjustments made to the measurement items themselves. This included an examination of items that contained excessive verbiage, distinguished between manually performing a task and the task configured to be performed automatically, and slight rewording of other reflective indicators that showed a lower reliability than what would be expected. The number of indicators was reduced as a result for both the *Computer Performance Compromise* and *Loss of Data and Files* surveys; the number of indicators did not change for the *Personal Information Compromise* survey.

Based on the results from the pilot study, discussions with content experts, and a reexamination of the data collected during the pretests and subject matter expert review stages, a few indicators were removed. This was done in order to more accurately and efficiently capture the degree to which a task is performed. The number of indicators for the response *Computer Maintenance* went from two to one. Likewise, the number of indicators for *Software Updates* was reduced from four to two. Finally, the number of indicators for the response *Backup Data* decreased from four to two. The purified measurement items were used in the main study, as was a greater compensation rate for participants.

6.3. Part 2: Main Study

The main study was conducted in a similar manner to the pilot study, but participants from Amazon's Mechanical Turk were compensated $1.15 rather than 50 cents. This was determined based on the amount of time it took to complete the survey and ensure that respondents were paid at least $6.00 per hour for participating, which is considered an acceptable wage for completing surveys on Amazon's Mechanical Turk. It is difficult to directly compare the rejection rate between the studies since the quality control questions were slightly different; the pilot study had a single quality control question, while the main study had two quality control questions that specifically told them how to answer (e.g., "for this question, please select agree."). However, the increased compensation did appear to have a significant effect on how quickly responses were received. In the main study, all of the responses were received within a day when it took over a week for the pilot study, which had only one third of the total number of participants. Additionally, there did not appear to be a significant number of survey non-completions due to the length of the instruments. Thus, anecdotally the increased compensation helped in a meaningful way with respect to both data collection time and participant dropout rates.

7. Statistical Assessment and Analysis of Instruments

The measurement model used to test these instruments is considered first-order formative, second-order formative; therefore, the statistical assessment contained herein does not include traditional reliability assessment techniques used for reflective items. The

validity assessment of the instruments consisted of several steps.

First, the measurement models of the instruments were assessed. This began with the assessment of construct validity using principal component analysis in SPSS, version 19. The number of components was determined *a priori* to represent the number of dimensions for each of the three instruments. While traditionally components with Eigen values below 1.0 or that do not meet the Scree plot criterion are not retained [55], this criterion did not adequately apply to the current instrument given that some of the dimensions consisted of single indicators. Varimax rotation was employed since high multicollinearity among the indicators is not presumed. During this step all items were retained to preserve content validity, which is considered especially important for formative models [23], [56].

Second, we tested for multicollinearity. High multicollinearity may suggest that some indicators are reflective rather than formative or consideration should be given to removing one or more indicators. This was tested by calculating the VIF using SPSS, version 19. The general rule of thumb for formative indicators is to have VIFs below 3.3 [23], [57].

The instruments developed and validated in this paper demonstrated good validity and reliability. Complete statistical analysis results may be found on the first author's webpage: http://faculty.washington.edu/marcjd/data

8. Recommended Uses of the Instruments

The three survey instruments developed and validated in this article may be used in a variety of ways. A researcher may employ one, two, or all three of them in research examining how people respond to different information security and privacy threats. The simplest way to use these instruments may be through treating them as summated rating scales [59]. This would be done by calculating the mean for each of the responses that has two or more indicators and adding these values with the responses that are determined by a single indicator. Thus, a threat that requires three responses will have a minimum value of three and a maximum value of 15 (5-point Likert scale used). These scales can then be used in a combination of ways, such as regression and determinations involving correlations.

In addition to using a summated rating scale as noted above, researchers may choose to incorporate the instruments into a statistical model using tools analytical approaches such as partial least squares structural equation modeling. If this approach is chosen, then it must be determined how to most appropriately represent the indicators in the measurement model. Since each of the indicators is considered an integral part of the required responses and removing any single one of them would present problems with respect to content validity, they are considered formative indicators. Likewise, since each of the responses is required to mitigate its associated threat(s), the responses themselves are considered formative.

Therefore, the most appropriate way to model the indicators in a partial least squares structural equation model will be to treat the dependent variable as a multi-dimensional first-order formative, second-order formative construct.

9. Conclusion

In this article, we explained the techniques employed to develop, test, and validate three separate instruments designed to measure the information security and privacy responses necessary to mitigate three threats: computer performance compromise, personal information compromise, and the loss of data and files. Overall, the instruments demonstrate good reliability and validity. The hope is that these instruments will be used in future research so that adequate comparisons can be made between different research models and approaches. In the past, the continual use of different instruments (often improperly developed ones) makes it difficult to confidently compare the other contributions the research may be making to the field of information security and privacy.

10. References

[1] C. L. Anderson and R. Agarwal, "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Q.*, vol. 34, no. 3, pp. 613–643, 2010.

[2] R. Crossler and F. Bélanger, "The Quest for Complete Security Protection: An Empirical Analysis of an Individual's 360 Degree Protection from File and Data Loss," 2012.

[3] G. A. Churchill, "A paradigm for developing better measures of marketing constructs.," *J. Mark. Res.*, vol. 16, no. 1, pp. 64–73, 1979.

[4] D. W. Straub, "Validating Instruments in MIS Research.," *MIS Q.*, vol. 13, no. 2, 1989.

[5] M. Bishop, *Computer Security: Art and Science*. Boston: Addison-Wesley, 2003.

[6] M. Bishop, *Introduction to Computer Security*. Boston: Addison-Wesley, 2005.

[7] D. Gibson, *Managing Risk in Information Systems*. Sudbury, MA: Jones & Bartlett Learning, 2011.

[8] S. Harris, *CISSP exam guide*, Sixth edition. New York: McGraw-Hill, 2013.

[9] R. Johnson, *Security Policies and Implementation Issues*. Sudbury, Mass: Jones & Bartlett Learning, 2011.

[10] I. Ajzen, "From intentions to actions: A theory of planned behavior," in *Action-control: From cognition to behavior*, J. Kuhl and J. Beckman, Eds. Heidelberg, Germany: Springer, 1985, pp. 11–39.

[11] M. Fishbein and I. Ajzen, *Belief, attitude, intention, and behavior : an introduction to theory and research*. Reading, Mass.: Addison-Wesley Pub. Co., 1975.

[12] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change," *J. Psychol.*, vol. 91, no. 1, p. 93, 1975.

[13] H. C. Triandis, *Interpersonal behavior*. Monterey, Calif, 1977.

[14] R. Crossler and F. Bélanger, "Determinants of Individual Security Behahaviors," presented at the The Dewald Roode Information Security Workshop, Waltham, Massachusetts, 2010, pp. 78–127.

[15] T. L. Webb and P. Sheeran, "Does changing behavioral intentions engender behavior change? A meta-analysis of the experimental evidence," *Psychol. Bull.*, vol. 132, no. 2, pp. 249–268, 2006.

[16] J. A. Ouellette and W. Wood, "Habit and intention in everyday life: the multiple processes by which past behavior predicts future behavior.," *Psychol. Bull.*, vol. 124, no. 1, p. 54, 1998.

[17] W. Wood, J. M. Quinn, and D. A. Kashy, "Habits in everyday life: Thought, emotion, and action," *J. Pers. Soc. Psychol.*, vol. 83, no. 6, pp. 1281–1297, 2002.

[18] A. E. Howe, I. Ray, M. Roberts, M. Urbanska, and Z. Byrne, "The psychology of security for the home computer user," in *Security and Privacy (SP), 2012 IEEE Symposium on*, 2012, pp. 209–223.

[19] M. B. W. Kobus, P. Rietveld, and J. N. van Ommeren, "Ownership versus on-campus use of mobile IT devices by university students," *Comput. Educ.*, vol. 68, no. 0, pp. 29–41, Oct. 2013.

[20] J.-M. Becker, K. Klein, and M. Wetzels, "Hierarchical latent variable models in PLS-SEM: guidelines for using reflective-formative type models," *Long Range Plann.*, vol. 45, no. 5, pp. 359–394, 2012.

[21] A. Diamantopoulos, P. Riefler, and K. P. Roth, "Advancing formative measurement models," *J. Bus. Res.*, vol. 61, no. 12, pp. 1203–1218, 2008.

[22] C. B. Jarvis, S. B. Mackenzie, P. M. Podsakoff, D. G. Mick, and W. O. Bearden, "A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research.," *J. Consum. Res.*, vol. 30, no. 2, 2003.

[23] S. Petter, D. Straub, and A. Rai, "Specifying formative constructs in information systems research," *MIS Q*, vol. 31, no. 4, pp. 623–656, 2007.

[24] M. Wetzels, G. Odekerken-Schröder, and C. Van Oppen, "Using PLS Path Modeling for Assessing Hierarchical Construct Models: Guidelines and Empirical Illustration," *Mis Q.*, vol. 33, no. 1, 2009.

[25] A. Adams and M. A. Sasse, "Users are not the Enemy," *Commun. ACM*, vol. 42, no. 12, pp. 41–46, 1999.

[26] R. Dhamija, J. D. Tygar, and M. Hearst, "Why Phishing Works," in *CHI 2006 Proceedings, Security*, Montréal, Québec, Canada, 2006.

[27] S. Furnell, P. Bryant, and A. D. Phippen, "Assessing the security perceptions of personal Internet users," *Comput. Secur.*, vol. 26, pp. 410–417, 2007.

[28] S. Furnell, A. Jusoh, and D. Katsabas, "The challenges of understanding and using security: A survey of end-users," *Comput. Secur.*, vol. 25, no. 1, pp. 27–35, 2006.

[29] H. Liang and Y. Xue, "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *J. Assoc. Inf. Syst.*, vol. 11, no. 7, pp. 394–413, 2010.

[30] I. Woon, G.-W. Tan, and R. Low, "A Protection Motivation Theory Approach to Home Wireless Security," 2005.

[31] S. Youn, "Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk-Benefit Appraisal Approach," *J. Broadcast. Electron. Media*, vol. 49, no. 1, pp. 86–110, 2005.

[32] D.-H. Shin, "The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption," *Model. User Exp. - Agenda Res. Pract.*, vol. 22, no. 5, pp. 428–438, Sep. 2010.

[33] K. Aytes and T. Connolly, "Computer Security and Risky Computing Practices: A Rational Choice Perspective.," *J. Organ. End User Comput.*, vol. 16, no. 3, 2004.

[34] B.-Y. Ng and M. A. Rahim, "A socio-behavioral study of home computer users' intention to practice security," in *Proceedings of the Ninth Pacific Asia Conference on Information Systems*, 2005, pp. 7–10.

[35] J. Fogel and E. Nehmad, "Internet social network communities: Risk taking, trust, and privacy concerns," *Comput. Hum. Behav.*, vol. 25, no. 1, pp. 153–160, Jan. 2009.

[36] D. Shin, "The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption," *Model. User Exp. - Agenda Res. Pract.*, vol. 22, no. 5, pp. 428–438, Sep. 2010.

[37] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The Memorability and Security of Passwords," in *Security and usability : designing secure systems that people can use*, L. F. Cranor and S. Garfinkel, Eds. Beijing; Farnham; Sebastopol, CA: O'Reilly, 2005, pp. 129–142.

[38] A. C. Johnston and M. Warkentin, "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Q.*, vol. 34, no. 3, pp. 548–566, 2010.

[39] P. Klasnja, S. Consolvo, J. Jung, B. M. Greenstein, L. LeGrand, P. Powledge, and D. Wetherall, "'When I am on Wi-Fi, I am fearless': privacy concerns & practices in everyday Wi-Fi use," 2009.

[40] J. S. Downs, M. Holbrook, and L. F. Cranor, "Behavioral Response to Phishing Risk," in *Proceedings of the Anti-Phishing Working Groups 2nd Annual Ecrime Researchers Summit*, Pittsburgh, PA, 2007, pp. 37–44.

[41] J. A. Cazier and B. D. Medlin, "Password Security: An Empirical Investigation into E-Commerce Passwords and Their Crack Times," *Inf. Syst. Secur.*, vol. 15, no. 6, pp. 45–55, 2006.
[42] M. Mannan and P. C. van Oorschot, "Security and usability: the gap in real-world online banking," 2008.
[43] R. Boulkedid, H. Abdoul, M. Loustau, O. Sibony, and C. Alberti, "Using and Reporting the Delphi Method for Selecting Healthcare Quality Indicators: A Systematic Review.," *PLoS ONE*, vol. 6, no. 6, pp. 1–9, Jun. 2011.
[44] N. Dalkey and O. Helmer, "An Experimental Application of the DELPHI Method to the Use of Experts," *Manag. Sci.*, vol. 9, no. 3, pp. 458–467, Apr. 1963.
[45] C. Duffield, "The Delphi Technique," *Aust. J. Adv. Nurs. Q. Publ. R. Aust. Nurs. Fed.*, vol. 6, no. 2, 1988.
[46] F. Hasson, S. Keeney, and H. McKenna, "Research Guidelines for the Delphi Survey Technique," *J. Adv. Nurs.*, vol. 32, no. 4, pp. 1008–1015, 2000.
[47] C. Powell, "The Delphi Technique: Myths and Realities," *J. Adv. Nurs.*, vol. 41, no. 4, pp. 376–382, 2003.
[48] A. M. Aladwani and P. C. Palvia, "Developing and validating an instrument for measuring user-perceived web quality," *Inf. Manage.*, vol. 39, no. 6, pp. 467–476, May 2002.
[49] M. P. Keesler and B. Keesler, *Mohawk: Discovering the Valley of the Crystals*. [New York]; Utica, N.Y.: The Keesler Family ; Distributed by North Country Books, 2008.
[50] D. Krathwohl, *Methods of educational and social science research : an integrated approach*, 2nd ed. Long Grove Ill.: Waveland Press, 2004.
[51] P. Housen, "What the Resident Meant to Say: Use of Cognitive Interviewing Techniques to Develop Questionnaires for Nursing Home Residents," *Gerontologist*, vol. 48, no. 2, pp. 158–169, 2008.
[52] M. Rosal, E. Carbone, and K. V. Goins, "Use of cognitive interviewing to adapt measurement instruments for low-literate Hispanics.," *Diabetes Educ.*, vol. 29, no. 6, 2003.
[53] M. Dupuis, R. Crossler, and B. Endicott-Popovsky, "The Information Security Behavior of Home Users: Exploring a User's Risk Tolerance and Past Experiences in the Context of Backing Up Information," presented at the The Dewald Roode Information Security Workshop, Provo, Utah, 2012.
[54] M. Dupuis, B. Endicott-Popovsky, and R. Crossler, "An Analysis of the Use of Amazon's Mechanical Turk for Survey Research in the Cloud," presented at the International Conference on Cloud Security Management, Seattle, Washington, 2013.
[55] J. Hair, W. Black, B. Babin, and R. Anderson, *Multivariate data analysis*, 7th ed. Upper Saddle River, NJ: Prentice Hall, 2010.
[56] K. Bollen and R. Lennox, "Conventional wisdom on measurement: A structural equation perspective.," *Psychol. Bull.*, vol. 110, no. 2, p. 305, 1991.
[57] A. Diamantopoulos, "Formative Versus Reflective Indicators in Organizational Measure Development: A Comparison and Empirical Illustration," *Br. J. Manag.*, vol. 17, no. 4, pp. 263–282, 2006.
[58] P. E. Spector, *Summated rating scale construction: an introduction*. Newbury Park, Calif: Sage Publications, 1992.

Appendix

The survey instruments below were broken up into sections based on the response being measured. The definitions were above the questions for each response grouping. This was designed to make it easier for participants to find the definitions for questions they were currently answering. Additionally, for sections with more than one question (e.g., malware) the text "I am confident that…" was immediately above the set of questions with each question beginning with "…". This was done to reduce redundancy and improve overall flow.

Computer Performance Compromise Survey Instrument

Definition Primary Computer: Your primary computer is the computing device you use a majority of the time that is NOT owned or issued by your employer. The Operating System (OS) of my primary computer is... ○ Windows ○ OS X (Macintosh) ○ Unix/Linux ○ Other		
Please indicate the amount you agree or disagree with each statement using the following scale: Strongly Disagree, Disagree, Not Sure, Agree, Strongly Agree		
Definitions Anti-malware Software: Software that protects a computer from spyware, viruses, Trojan horses, worms, etc. Computer Maintenance Tasks: Defragmenting the hard drive, emptying the trash, removing cached files, etc. Firewall: A piece of hardware or software that restricts incoming and outgoing Internet traffic to help protect a computer from malicious activity. Malware: Spyware, viruses, Trojan horses, worms, etc. Primary Computer: Your primary computer is the computing device you use a majority of the time that is NOT owned or issued by your employer.		
Indicator	Conditional	Question Text

Updates 1	OS is Windows	I am confident that important updates to the OPERATING SYSTEM are installed on my primary computer on a monthly or more frequent basis.
Updates 2	OS is Windows	I am confident that important updates to SOFTWARE (e.g., Word, Skype) are installed on my primary computer on a monthly or more frequent basis.
Malware 1	OS is Windows	I am confident that my primary computer has anti-malware software that is updated automatically on a weekly or more frequent basis.
Malware 2	OS is Windows	I am confident that my primary computer is automatically scanned for malware in real-time (e.g., during downloads, when I visit websites, etc.).
Malware 3	OS is Windows	I am confident that a full system scan for malware is performed on my primary computer on a weekly or more frequent basis.
Firewall 1	None	I am confident that I have a firewall enabled for my primary computer.
Maintenance 1	None	I am confident that computer maintenance tasks are performed on my primary computer on a monthly or more frequent basis.

Personal Information Compromise Survey Instrument

Definition
Primary Computer: Your primary computer is the computing device you use a majority of the time that is NOT owned or issued by your employer.
The Operating System (OS) of my primary computer is...
○ Windows ○ OS X (Macintosh) ○ Unix/Linux ○ Other

Please indicate the amount you agree or disagree with each statement using the following scale: Strongly Disagree, Disagree, Not Sure, Agree, Strongly Agree

Definitions
Anti-malware Software: Software that protects a computer from spyware, viruses, Trojan horses, worms, etc.
Encryption: Encryption is the conversion of plain text data into a format that cannot be easily understood by unauthorized people. For example, a simple word that in plain text is "cat", instead appears as something that makes no sense (e.g., H)&*HGHas87a1) to unauthorized individuals.
Firewall: A piece of hardware or software that restricts incoming and outgoing Internet traffic to help protect a computer from malicious activity.
Important Logins: Computer login, banking, financial, and e-commerce websites, etc.
Less Important Logins: Discussion forums, blogs, social networking sites (e.g., Facebook), etc.
Long and Complex Passwords: 8 or more characters in length with special characters, numbers, and a combination of upper and lower casing
Malware: Spyware, viruses, Trojan horses, worms, etc.
Personal Financial Information: Credit card numbers, bank routing information, etc.
Primary Computer: Your primary computer is the computing device you use a majority of the time that is NOT owned or issued by your employer.

Indicator	Conditional	Question Text
Educate 1	Additional option provided: N/A – I live alone.	I am confident that someone in my home (i.e., you, someone else) regularly educates others in the home about proper information security behaviors.
Malware 1	OS is Windows	I am confident that my primary computer has anti-malware software that is updated automatically on a weekly or more frequent basis.
Malware 2	OS is Windows	I am confident that my primary computer is automatically scanned for malware in real-time (e.g., during downloads, when I visit websites, etc.).
Malware 3	OS is Windows	I am confident that a full system scan for malware is performed on my primary computer on a weekly or more frequent basis.
Firewall 1	None	I am confident that I have a firewall enabled for my primary computer.
Wireless 1	None	I am confident that my wireless network is using some type of encryption.
Wireless 2	None	I am confident that the default password on the device (e.g., router) I use for wireless access to the Internet has been changed.
Passwords 1	None	I am confident that I use long and complex passwords for important logins.
Passwords 2	None	I am confident that my passwords for less important logins are NOT the same as those for important logins.
Passwords 3	None	I am confident that I use a unique password for each important login.
Passwords 4	None	I am confident that my usernames for less important logins are NOT the same as those for important logins.
Passwords 5	None	I am confident that I change the passwords for important logins at least once every 12 months.
Email 1	None	I very rarely, if ever, click on the links in emails I receive.
Email 2	None	If I were to click on a link in an email I received, I would check to make sure

		that the link goes to a site that appears legitimate.
Email 3	None	I do not click on links in emails I receive that are reportedly from a bank or other financial institution.
Financial 1	Additional option provided: N/A – I do not store my personal financial information online.	I only store my personal financial information on websites that I do regular business with.
Financial 2	Additional option provided: N/A – I do not store my personal financial information online.	I only store my personal financial information on websites that I trust.
Financial 3	Additional option provided: N/A – I do not store my personal financial information online.	I check to make sure the website is using encryption (e.g., verifying the URL starts with https://, not just http://) prior to entering personal financial information online.
InfoShar 1	None	I am careful about the information I make public on the Internet.
InfoShar 2	None	I am selective with whom I share my private information with on the Internet.
InfoShar 3	None	I only put information on social networking sites that can be viewed by friends/connections that I trust with that information.
InfoShar 4	None	I understand that once I put something on the Internet, it is basically available forever, even if I delete it.
Connections 1	None	I am selective in who I choose to be a friend/connection with on social networking sites.
Connections 2	None	I trust those that I choose to be a friend/connection with on social networking sites.

Computer Performance Compromise Survey Instrument

Definition Primary Computer: Your primary computer is the computing device you use a majority of the time that is NOT owned or issued by your employer. The Operating System (OS) of my primary computer is... ○ Windows ○ OS X (Macintosh) ○ Unix/Linux ○ Other		
Please indicate the amount you agree or disagree with each statement using the following scale: Strongly Disagree, Disagree, Not Sure, Agree, Strongly Agree		
Definitions Anti-malware Software: Software that protects a computer from spyware, viruses, Trojan horses, worms, etc. Firewall: A piece of hardware or software that restricts incoming and outgoing Internet traffic to help protect a computer from malicious activity. Malware: Spyware, viruses, Trojan horses, worms, etc. Primary Computer: Your primary computer is the computing device you use a majority of the time that is NOT owned or issued by your employer.		
Indicator	Conditional	Question Text
Educate 1	Additional option provided: N/A – I live alone.	I am confident that someone in my home (i.e., you, someone else) regularly educates others in the home about proper information security behaviors.
Malware 1	OS is Windows	I am confident that my primary computer has anti-malware software that is updated automatically on a weekly or more frequent basis.
Malware 2	OS is Windows	I am confident that my primary computer is automatically scanned for malware in real-time (e.g., during downloads, when I visit websites, etc.).
Malware 3	OS is Windows	I am confident that a full system scan for malware is performed on my primary computer on a weekly or more frequent basis.
Firewall 1	None	I am confident that I have a firewall enabled for my primary computer.
Permissions 1	None	I am confident that I have created (or modified) the default administrator password on my primary computer.
Permissions 2	None	I am confident that the main account I use on my primary computer has restricted permissions (i.e., unable to perform some tasks, such as installing new programs).
Backup 1	None	I am confident that all of the important information and files on my primary computer are backed up to an external source (e.g., external hard drive, cloud storage, USB flash drive, etc.).