The Role of Human Factors/Ergonomics in the Science of Security: Decision Making and Action Selection in Cyberspace

Robert W. Proctor and **Jing Chen**, Purdue University, West Lafayette, Indiana, USA

Objective: The overarching goal is to convey the concept of science of security and the contributions that a scientifically based, human factors approach can make to this interdisciplinary field.

Background: Rather than a piecemeal approach to solving cybersecurity problems as they arise, the U.S. government is mounting a systematic effort to develop an approach grounded in science. Because humans play a central role in security measures, research on security-related decisions and actions grounded in principles of human information-processing and decision-making is crucial to this interdisciplinary effort.

Method: We describe the science of security and the role that human factors can play in it, and use two examples of research in cybersecurity—detection of phishing attacks and selection of mobile applications—to illustrate the contribution of a scientific, human factors approach.

Results: In these research areas, we show that systematic information-processing analyses of the decisions that users make and the actions they take provide a basis for integrating the human component of security science.

Conclusion: Human factors specialists should utilize their foundation in the science of applied information processing and decision making to contribute to the science of cybersecurity.

Keywords: human information processing, information security, privacy, risk communication, risk perception

Address correspondence to Robert W. Proctor, Department of Psychological Sciences, Purdue University, West Lafayette, IN 47907-2004, USA; proctor@psych.purdue.edu.

HUMAN FACTORS
Vol. XX, No. X, Month XXXX, pp. 1–7
DOI: 10.1177/0018720815585906

> The human factor remains security's weakest link in cyberspace.
>
> B. K. Wiederhold (2014)

The widespread deployment of computers, their rapid miniaturization, and the spread of wired and wireless connectivity over the Internet are changing the ways in which people interact with many human–machine systems as well as with each other. As examples, this extensive connectivity enables a person to monitor her home from afar through security cameras, geographically separated team members to work together, and financial transactions to take place electronically. The downside of the pervasive availability of electronic information and communication is that considerable potential exists for abuse in addition to appropriate use. Hackers with malicious intents ranging from annoyance to criminal activity and terrorism may exploit security vulnerabilities to gain unauthorized access to resources and information, creating havoc for individuals, organizations, and countries.

Cybersecurity has therefore developed as an area of concern in parallel with these developments in computer technology. Beginning with the *National Strategy to Secure Cyberspace* (Executive Office of the President, 2003), the U.S. federal government has devoted much effort to developing a policy that includes support for research and development relating to improved cybersecurity (Harknett & Stever, 2011). Possible roles for human factors in this research have been acknowledged (Boyce et al., 2011), and some research has been conducted (e.g., Dutt, Ahn, & Gonzalez, 2013). However, as Mancuso (2014) noted, "The Human Factors community has begun to address human-centered issues in cyber operations, but in comparison to technological communities, we have yet to scratch the surface" (p. 415).

The calls for greater involvement of human factors specialists in cybersecurity have focused on the "numerous interdependencies, and complexities that arise based on the interaction of humans and technology" (Mancuso, 2014, p. 415). Emphasis on the complexity of human interactions with technology is consistent with HFES's definition of human factors as "the scientific discipline concerned with the understanding of interactions among humans and other elements of a system" (https://www.hfes.org/web/AboutHFES/about.html). Note, though, that this definition also highlights "scientific discipline." We think that human factors and ergonomics (HF/E) specialists can make a contribution of at least equal importance to that of system interaction by applying their scientific perspective to analyses of cybersecurity issues involving humans, in the context of interdisciplinary research teams. After describing the science of security, we illustrate this point using phishing detection and mobile app selection as examples.

SCIENCE OF SECURITY

In 2011, the National Science and Technology Council (NSTC) published a strategic plan for the federal cybersecurity research and development program. One thrust in the plan is *Developing Scientific Foundations*. The plan describes the current state of research as a patchwork of solutions to specific vulnerabilities and states, "A more fruitful way to ground research efforts, and to nurture and sustain progress in the kinds of improved cybersecurity solutions that benefit society, is to develop a science of security" (p. 10). The idea is to develop scientific laws, principles, and models that can be applied to a range of cybersecurity issues as they arise. "Sound methods for integrating humans in the system: usability and security" (p. 11) is among seven areas specified in which research is needed.

As part of the science of security research effort, the National Security Agency (NSA) has fostered development of a research community for which the goal is "to bring scientific rigor to research in the cybersecurity domain" (Science of Security, 2014). Closely following the NSTC strategic plan, one of the "hard problems" targeted by NSA is "understanding and accounting for human behavior." Interest exists in methods to model adversaries and for integrating humans in the system, with an emphasis on usability (Networking and Information Technology Research and Development Program, 2014). More specifically, a central concern is to bring scientific knowledge of human cognition to bear on understanding perceptions of security risks, security-related decisions, and the choices among alternative actions that humans make that may protect or imperil system security.

Scientific principles of risk perception, decision making, action selection, and training have been developed in basic and applied cognitive research conducted from the "cognitive revolution" in the 1950s to the present (Healy, Schneider, & Bourne, 2012; Proctor & Vu, 2010; Wickens, Hollands, Banbury, & Parasuraman, 2012), and these can provide a principled basis for analyzing the factors affecting security-related human decisions and choices. We demonstrate the value of taking an approach to cybersecurity based on scientific principles using two vulnerabilities, phishing attacks and malicious applications (apps), as examples. These vulnerabilities were selected because HF/E scholars should be familiar with them and because they have been identified as the primary cyberthreats to mobile devices (Ruggiero & Foote, 2011), which now exceed PCs in Internet usage.

DETECTION OF PHISHING ATTACKS

Phishing is defined by the *Merriam-Webster Dictionary* (2014) as "a scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly." Phishing attacks, like most violations of information privacy and security, rely on deception. An interchange between a deceiver and a target receiver occurs, but the decisions made by the receiver ultimately determine whether the deception is successful. Phishing is of concern because sophisticated phishing messages arrive regularly in e-mail, and people are not accurate at distinguishing well-designed phishing messages and sites from genuine ones (Dhamija, Tygar, & Hearst, 2006; Downs, Holbrook, & Cranor, 2006).

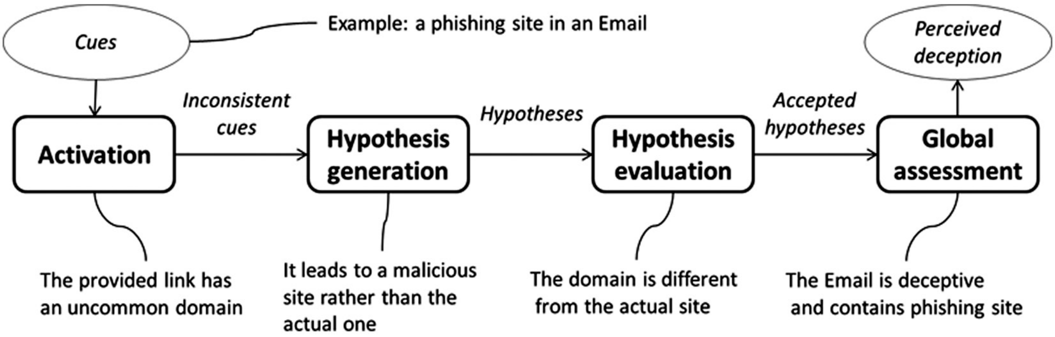
Cues
Example: a phishing site in an Email
Perceived deception
Inconsistent cues
Hypotheses
Accepted hypotheses
Activation
Hypothesis generation
Hypothesis evaluation
Global assessment
The provided link has an uncommon domain
It leads to a malicious site rather than the actual one
The domain is different from the actual site
The Email is deceptive and contains phishing site

Figure 1. Model of deception detection (adapted from Grazioli, 2004) as applied to detecting a phishing email. In the *activation* stage, the user attends to cues that mismatch with expectations, suggesting "something may be wrong." At the stage of *hypothesis generation*, the user generates hypotheses to explain the mismatch with expectations, at least one hypothesis of which must include deception if the deception is to be detected. Hypothesis evaluation, which follows, involves *evaluation* of the generated deception hypotheses, with the user deciding whether to accept the deception hypothesis for each cue. In the fourth, *global assessment* stage, the user assigns different weights to the individual hypotheses, along with information cues relating to trust and assurance, in an overall assessment of deception. The decision that there has been deception can be based on a single, strong deception hypothesis or the sum of several weaker ones.

To reduce susceptibility to phishing, it is essential to understand the processes by which users assess the risks associated with phishing, detect that a message may be a phishing attack, and decide whether to submit the requested information (Downs, Barbagallo, & Acquisti, 2015). A variety of software tools have been developed to display a warning when a possible phishing message or site is detected. However, these have not been very successful, in part because they miss as many as 50% of phishing sites (Cranor, Egelman, Hong, & Zhang, 2006). Because user decisions still must be made even with an automatic phishing detector, how the user decides to trust particular messages and makes decisions whether to act on them must be considered (e.g., Shahriar & Zulkernine, 2011).

A human information-processing theory that has been applied to detection of deception in computer-mediated environments is the theory of deception detection (Grazioli, 2004; Johnson, Grazioli, Jamal, & Berryman, 2001). This theory specifies four processing stages that affect whether a receiver will detect the deception: activation, hypothesis generation, hypothesis evaluation, and global assessment (see Figure 1 for descriptions). The different stages in the model enable detailed examination for the determinants of successfully detecting an Internet deception such as a phishing attack. Specifically, Grazioli (2004) found that the major factor differentiating persons who were able to detect a deceptive Web site was in their ability to evaluate cues (hypothesis evaluation), from which he concluded, "Domain-specific knowledge about how to evaluate individual cues is a strong performance differentiator" (p. 164).

A model by Vishwanath, Herath, Chen, Wang, and Rao (2011) places more emphasis on attention and memory. It includes an initial attention stage that comprises whether the user attends to the cues. Greater perceived relevance of the message to the user's needs is assumed to lead to greater attention to its details. Detection, hypothesis generation, and evaluation are attributed to an elaboration process, which, in agreement with Grazioli (2004), requires comparison of the cues with domain-specific knowledge stored in memory. E-mail load—the number of e-mails that the individual receives daily—is considered to be critical. As with mental workload in general (Wickens, 2008), the increase in e-mail load is presumed to reduce the amount of effort the user can devote to specific messages and their details, increasing the likelihood of being phished.

The models of Grazioli (2004) and Vishwanath et al. (2011) illustrate how the processes in which a user engages when deciding whether to respond to a phishing message can be analyzed and evaluated systematically. However, the models address only explicitly perceived deception and not the implicit processes that many decision-making models consider to also play an important role (Evans & Stanovich, 2013; Hommel, 2013). In Kahneman's (2011) words, whereas explicit processes allocate "attention to the effortful mental activities that demand it," implicit processes operate "automatically and quickly, with little or no effort" (pp. 20–21).

Downs et al. (2015) showed that it is essential to take implicit as well as explicit processes into account by analyzing people's responses to phishing attacks. Participants role-played being an office worker performing an e-mail management task and chose among actions for each message that were not mutually exclusive. Participants whose stated intentions were to use stronger strategies to prevent being phished, and who evidenced explicit knowledge of phishing, showed a more conservative decision criterion of responding less frequently to both phishing and legitimate messages but not greater sensitivity at distinguishing them. But participants who exhibited implicit procedural knowledge (ability to ascertain legitimacy of a URL) yielded a decreased frequency of responding to phishing attacks without an increase in false alarms for legitimate e-mails (i.e., greater sensitivity). These studies demonstrate a need for researchers to measure actual choices among actions in studies of phishing and to ground the research in contemporary knowledge of decision-making processes and information processing, both of which fall within the purview of human factors specialists.

SELECTION OF MOBILE APPS

Another way in which malicious agents collect users' privacy data without users' awareness is through mobile apps. With the advent of mobile devices, online stores have developed that enable users to download apps for various purposes. For example, in the Google Play store for Android apps, an icon for the app is accompanied by an average user rating score (one to five filled stars) and the number of users on which it is based. A user can judge from these values whether an app is perceived by other users as useful and appropriate for carrying out its intended function. However, privacy risks are more difficult to evaluate. The risks associated with a specific app are identified in lengthy verbal permissions that are available to the user only after making the initial decision to download that app.

Because a preliminary decision to download the app has already been made, if the permissions indicate that the risks associated with the app are high, the user must now make a contrary decision that requires returning to the list of relevant apps and beginning the evaluation process anew. Based on the fact that people tend to minimize effort and rely on heuristics to simplify decisions (e.g., Kahneman, 2011; Wickens, 2014), it can be predicted that users will be reluctant to take such action that requires additional effort and movement away from the goal of installing an app. Indeed, Kelley, Cranor, and Sadeh (2013) showed that when permissions were displayed in simplified form on the main app screen prior to the initial decision, users selected apps that requested fewer permissions.

Even when permissions are presented earlier in the decision process, users will likely have difficulty comprehending them and may even ignore them. Felt et al. (2012) conducted an Internet survey of Android users, as well as a laboratory study. Only 17% of participants attended to the permissions when installing an app, and only 3% could correctly answer all of three permission-comprehension questions. Felt et al. concluded, "This indicates that current Android permission warnings do not help most users make correct security decisions" (p. 1).

We have been conducting interdisciplinary research on risk communication in app selection intended to remedy this problem (e.g., Chen, Gates, Li, & Proctor, in press). The human factors component is based on principles of decision making, including that information framing influences decisions (Kahneman & Tversky, 1979) and that people often rely on gist representations rather than on detailed verbatim representations (Brust-Renck, Royer, & Reyna, 2013). Central to our approach is an assumption that most users will prefer less detailed displays of risk information, such as a summary risk score (Chen et al., in press; Gates, Chen, Li, & Proctor, 2014) and indication of risk categories (Jorgensen et al., 2015).

With regard to summary risk scores, progress is being made toward developing techniques that can provide a reliable measure of overall risk for an app (Gates, Li, et al., 2014). Summary risk information has been shown to be effective in online app-selection studies and more tightly controlled laboratory experiments. When verbal risk indexes (low, medium, high) accompany two apps, the risky app is chosen less often and the users indicate that they paid more attention to the apps' permissions and the associated risks (Gates, Chen, et al., 2014). Presentation of the risk information in the form of filled circles (more filled circles indicates greater risk), much like the user ratings, is similarly effective to the verbal indexes at influencing users' app-selection choices.

When the filled circles are framed as amount of safety (more filled circles indicates greater safety) rather than risk, the influence is greater, and the users show less confusion about what the symbols indicate when subsequently asked in a survey question (Chen et al., in press; Gates, Chen, et al., 2014; see also Choe, Jung, Lee, & Fisher, 2013). A similar idea that positive framing of privacy information is beneficial is incorporated into assigning privacy grades (A, B, C, D) to Android apps (http://privacygrade.org/).

In addition to a summary risk (or safety) index, research has also identified the major risk categories (personal information privacy, monetary, and device availability/stability) that can be utilized by users who want more detailed information (Jorgensen et al., 2015). Principles of display design (e.g., Bennett & Flach, 2011) can form the basis for research to determine the most effective way to convey the risks associated with these categories to users when choosing among apps.

CONCLUSION

We have illustrated the applicability of scientifically based analyses of decision making to the domain of cybersecurity in the areas of detection of phishing attacks and mobile app-selection decisions. In each area, understanding the users and how they process information is key to developing tools that are effective in yielding actions that support cybersecurity. Both areas can be characterized as requiring users to make choices under conditions involving risk. In these conditions, (a) users' knowledge of the risks is often limited, (b) the specific risks are difficult to comprehend, (c) attention needs to be directed to appropriate cues, and (d) decisions are likely impacted by both explicit and implicit processes.

Although we focused on only two areas, decision making and choice are also central to other areas in the domain of cybersecurity: Individual users must make decisions about passwords to use (Das, Bonneau, Caesar, Borisov, & Wang, 2014) and the privacy offered by Web sites (Vu, Chambers, Creekmur, Cho, & Proctor, 2010), which involve processes similar to those of phishing detection and app selection. System administrators must configure access control policies, detect intrusions, and take appropriate actions (Corchado & Herrero, 2011), and security analysts need to anticipate adversaries' reactions to particular security actions (Proctor, Vu, & Schultz, 2009; Schultz, 2012). There is a need for research to integrate these areas of cybersecurity using scientifically based principles of perception, decision making, and action. The knowledge of human information processing in applied contexts possessed by human factors specialists and cognitive scientists, particularly when coupled with the knowledge of technology possessed by computer scientists and cybersecurity experts, should facilitate transformative advances in the science of security.

ACKNOWLEDGMENTS

Robert W. Proctor is a fellow, and Jing Chen a student, in the Center for Education and Research in Information Assurance and Security at Purdue University. Funding for this research was provided by the National Security Agency as part of a Science of Security lablet and by the National Science Foundation under Grant 1314688.

KEY POINTS

- Cybersecurity is a national and international priority.
- The science of security takes a scientific approach to security-related issues.

- Human factors considerations are key components of many cybersecurity areas.
- Information-processing analyses have been applied to the areas of detection of phishing attacks and selection of mobile applications.
- Human factors specialists can contribute to the science of security as members of interdisciplinary teams.

REFERENCES

Bennett, K. B., & Flach, J. M. (2011). *Display and interface design: Subtle science, exact art*. Boca Raton, FL: CRC Press.

Boyce, M. W., Duma, K. M., Hettinger, L. J., Malone, T. B., Wilson, D. P., & Lockett-Reynolds, J. (2011). Human performance in cybersecurity: A research agenda. In *Proceedings of the Human Factors and Ergonomics Society annual meeting* (pp. 1115–1119). Santa Monica, CA: HFES.

Brust-Renck, P. G., Royer, C. E., & Reyna, V. F. (2013). Communicating numerical risk: Human factors that aid understanding in health care. In D. G. Morrow (Ed.), *Reviews of human factors and ergonomics: Healthcare human factors/ergonomics* (Vol. 8, pp. 235–276). Santa Monica, CA: HFES.

Chen, J., Gates, C. S., Li, N., & Proctor, R. W. (in press). Influence of risk/safety information framing on Android app-installation decisions. *Journal of Cognitive Engineering and Decision Making*.

Choe, E. K., Jung, J., Lee, B., & Fisher, K. (2013). Nudging people away from privacy-invasive mobile apps through visual framing. In *Human-computer interaction–INTERACT 2013* (pp. 74–91). Berlin, Germany: Springer.

Corchado, E., & Herrero, Á. (2011). Neural visualization of network traffic data for intrusion detection. *Applied Soft Computing*, *11*, 2042–2056.

Cranor, L., Egelman, S., Hong, J., & Zhang, Y. (2006). *Phinding phish: An evaluation of anti-phishing toolbars* (CMU-CyLab-06-018). Pittsburgh, PA: Carnegie Mellon University.

Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014, February). The tangled web of password reuse. In *Symposium on network and distributed system security (NDSS)*. Retrieved from https://www.internetsociety.org/doc/tangled-web-password-reuse

Dhamija, R., Tygar, J. D., & Hearst, M. (2006, April). Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 581–590). New York, NY: ACM.

Downs, J. S., Barbagallo, D., & Acquisti, A. (2015). Predictors of risky decisions: Improving judgment and decision making based on evidence from phishing attacks. In E. A. Wilhelms & V. F. Reyna (Eds.), *Neuroeconomics, judgment, and decision making* (pp. 239–253). New York, NY: Psychology Press.

Downs, J. S., Holbrook, M., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. In *Proceedings of the Second Symposium on Usable Privacy and Security* (pp. 79–70). New York, NY: ACM.

Dutt, V., Ahn, Y.-S., & Gonzalez, C. (2013). Cyber situation awareness: Modeling detection of cyber attacks with instance-based learning theory. *Human Factors*, *55*, 605–618.

Evans, J. S. B., & Stanovich, K. E. (2013). Dual-process theories of higher cognition advancing the debate. *Perspectives on Psychological Science*, *8*, 223–241.

Executive Office of the President. (2003). *The national strategy for securing cyberspace*. Retrieved from http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). Android permissions: User attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (pp. 1–14). New York, NY: ACM.

Gates, C., Chen, J., Li, N., & Proctor, R. W. (2014). Effective risk communication for Android apps. *IEEE Transactions on Dependable and Secure Computing*, *11*, 252–265.

Gates, C., Li, N., Peng, H., Sarma, B., Qi, Y., Potharaju, R., Nita-Rotaru, C., & Mollay, I. (2014). Generating summary risk scores for mobile applications. *IEEE Transactions on Dependable and Secure Computing*, *11*, 238–251.

Grazioli, S. (2004). Where did they go wrong? An analysis of the failure of knowledgeable Internet consumers to detect deception over the Internet. *Group Decision and Negotiation*, *13*, 149–172.

Harknett, R. J., & Stever, J. A. (2011). The new policy world of cybersecurity. *Public Administration Review*, *71*, 455–460.

Healy, A. F., Schneider, V. I., & Bourne, L. E., Jr. (2012). Empirically valid principles of training. In A. F. Healy & L. E. Bourne, (Eds.), *Training cognition: Optimizing efficiency, durability, and generalizability* (pp. 13–39). New York, NY: Psychology Press.

Hommel, B. (2013). Dancing in the dark: No role for consciousness in action control. *Frontiers in Psychology*, *4*, 380.

Johnson, P. E., Grazioli, S., Jamal, K., & Berryman, G. (2001). Detecting deception: Adversarial problem solving in a low base rate world. *Cognitive Science*, *25*, 355–392.

Jorgensen, Z., Chen, J., Gates, C. S., Li, N., Proctor, R. W., & Yu, T. (2015). Dimensions of risk in mobile applications: A user study. In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy* (pp. 49–60). New York, NY: ACM.

Kahneman, D. (2011). *Thinking, fast and slow*. New York, NY: Farrar, Straus and Giroux.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica: Journal of the Econometric Society*, *47*, 263–291.

Kelley, P. G., Cranor, L. F., & Sadeh, N. (2013). Privacy as part of the app decision-making process. In *Proceedings of the 2013 ACM Annual Conference on Human Factors in Computing Systems* (pp. 3393–3402). New York, NY: ACM.

Mancuso, V. F. (2014). Human factors in cyber warfare II: Emerging perspectives. In *Proceedings of the Human Factors and Ergonomics Society 58th Annual Meeting* (pp. 415–418). Santa Monica, CA: HFES.

Merriam-Webster. (2014). *Phishing*. Retrieved from http://www.merriam-webster.com/dictionary/phishing

National Science and Technology Council. (2011). *Trustworthy cyberspace: Strategic plan for the federal cybersecurity research and development program*. Washington, DC: National Coordination Office.

Networking and Information Technology Research and Development Program. (2014). *Federal cybersecurity game—change R&D: Science of security*. http://cybersecurity.nitrd.gov/page/science-of-security

Proctor, R. W., & Vu, K.-P. L. (2010). Cumulative knowledge and progress in human factors. *Annual Review of Psychology*, *61*, 623–651.

Proctor, R. W., Vu, K.-P. L., & Schultz, E. (2009). Human factors in information security and privacy. In J. N. D. Gupta & S. K. Sharma (Eds.), *Handbook of research on information security and assurance* (pp. 402–414). Hershey, PA: Information Science Reference.

Ruggiero, P., & Foote, J. (2011). *Cyber threats to mobile phones*. Washington, DC: U.S. Computer Emergency Readiness Team.

Schultz, E. E. (2012). Human factors and information security. In G. Salvendy (Ed.), *Handbook of human factors and ergonomics* (4th ed., pp. 1250–1266). Hoboken, NJ: John Wiley.

Science of Security. (2014). *NSA announces new "lablets" in support of the science of security*. Retrieved from http://cps-vo.org/node/12317

Shahriar, H., & Zulkernine, M. (2011). Information source-based classification of automatic phishing website detectors. In *2011 IEEE/IPSJ International Symposium on Applications and the Internet* (pp. 190–195). Piscataway, NJ: IEEE.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*, 576–586.

Vu, K. P. L., Chambers, V., Creekmur, B., Cho, D., & Proctor, R. W. (2010). Influence of the Privacy Bird® user agent on user trust of different web sites. *Computers in Industry*, *61*, 311–317.

Wickens, C. D. (2008). Multiple resources and mental workload. *Human Factors*, *50*, 449–455.

Wickens, C. D. (2014). Effort in human factors performance and decision making. *Human Factors*, *56*, 1329–1336.

Wickens, C. D., Hollands, J. G., Banbury, S., & Parasuraman, R. (2012). *Engineering psychology and human performance* (4th ed.). Upper Saddle River, NJ: Pearson.

Wiederhold, B. K. (2014). The role of psychology in enhancing cybersecurity. *Cyberpsychology, Behavior, and Social Networking*, *17*, 131–132.

Robert W. Proctor earned his master's and PhD in experimental psychology from the University of Texas at Arlington. He is a distinguished professor in the Department of Psychological Sciences and a fellow of the Center for Education and Research in Information Assurance and Security at Purdue University. His research interests include basic and applied aspects of human performance in a variety of tasks and settings.

Jing Chen earned her bachelor's and master's degrees in psychology from Zhejiang University in China. She is completing a PhD in cognitive psychology and a master's degree in industrial engineering at Purdue University.

Date received: June 18, 2014
Date accepted: April 16, 2015