Computers & Security 92 (2020) 101731

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Holistic cyber hygiene education: Accounting for the human factors

Alexis R. Neigel[a,*], Victoria L. Claypoole[a], Grace E. Waldfogle[a,#], Subrata Acharya[b,#], Gabriella M. Hancock[c]

[a] University of Central Florida, Department of Psychology, College of Sciences, Orlando, FL, United States
[b] Towson University, Department of Computer and Information Sciences, Towson, MD, United States
[c] California State University – Long Beach, Long Beach, Department of Psychology, CA, United States

ARTICLE INFO

Article history:
Received 18 January 2019
Revised 19 November 2019
Accepted 20 January 2020
Available online 23 January 2020

Keywords:
Computer education
Cyber education
Cyber hygiene
Human factors

ABSTRACT

Cybersecurity is paramount in modern cyberdefense. One important factor linked to reducing human-instigated breaches of cybersecurity includes cyber hygiene. Cyber hygiene is the adaptive knowledge and behavior to mitigate risky online activities that put an individual's social, financial, and personal information at risk – a danger that is significantly compounded when discussing the risk to entire countries as opposed to a single individual. Interestingly, even though the human is the greatest risk to cybersecurity, very little research has examined the latent individual differences associated with developing cyber hygiene-related knowledge, attitudes, and behaviors. Thus, the goal of the present study was to address this gap in cyber hygiene research. The results from 173 university participants demonstrated that several factors, such as information handling, incident reporting, and password management were associated with better cyber hygiene. Individual differences such as trust in technology and intrinsic motivation were predictive of improved cyber hygiene – but were subject to significant sex differences. Differences across academic majors, such as science and technology majors, also emerged. Finally, we discuss the importance of understanding the role of human factors in modern cybersecurity and the potential practical implications associated with refining current course curricula in computer and information sciences.

"Cybersecurity throughout much of the world is in a shameful state of unpreparedness." – John Arquilla, 2016

1. Introduction

Over the past decade, there has been an enormous increase in the spending allocated to cybersecurity on the magnitude of billions of dollars (Arquilla, 2016; Garfinkel, 2012). Meanwhile, large-scale data breaches and data leaks have been increasing (Symantec, 2012). Taken together, the increase in resources allocated to cybersecurity have not definitively overcome or prevented cyberattacks. According to several estimates, this continuance in compromised security is because human error comprises the primary cause for breaches of personal data and secure information (Arquilla, 2016; Butler, 2014; Dupuis, 2017; Garfinkel, 2012; Parsons et al., 2017; Sawyer and Hancock, 2018; Wiederhold, 2014).

Meaning, the fallibility of the human user is the central target for socially engineered cyberattacks, phishing scams, and data leaks. Thus, there are several "human factors" that raise or diminish the likelihood of being the victim of a cyberattack, hack, or data breach – and even being victimized a second or third time (Wiederhold, 2014). Put another way, unfavorable outcomes can be traced back to the fact that some users have better cyber hygiene than others, which in turn is linked to several individual differences.

Cyber hygiene involves establishing and maintaining important cyber health behaviors. Routinely monitoring technology for threats or attempted hacking, changing passwords and avoiding recycled passwords, updating virus protection software, storing online information securely, and running appropriate security scans are but a few examples of such effective, adaptive, and "healthy" behaviors. Cyber hygiene is certainly important in maintaining cybersecurity, but it is not necessarily synonymous with cybersecurity. For example, cybersecurity is the objective measurement of behaviors taken to maintain security and remain defensive toward cyberattacks (Han et al., 2017), whereas cyber hygiene is related to the knowledge about online security *and* the practices associated with increasing cybersecurity (Parsons et al., 2017). Thus, in order to improve cybersecurity, we must improve cyber education. One

* Corresponding author at: Performance Research Laboratory, University of Central Florida, 4000 Central Florida Boulevard, Orlando, FL 32816, United States.
E-mail address: alexis.neigel@gmail.com (A.R. Neigel).
# Both authors contributed equally to this work and both authors shall be regarded as third author.

https://doi.org/10.1016/j.cose.2020.101731
0167-4048/

area in which to improve cyber education is within the classroom, as the number of students enrolling in computer science-based courses has increased, especially for female students (Roberts et al., 2002). Thus, as the demographics and enrollment in these course (and ultimately, careers) change, it would be especially beneficial to include a discussion of cyber hygiene and individual differences in cybersecurity risk factors.

1.1. Human factors and cyber hygiene

1.1.1. Cyber education

One individual difference linked to improving cybersecurity includes knowledge related to cybersecurity, or cyber education. While Internet security guidelines for consumers are freely available, it is questionable how many users read these reports and if these security guidelines are written in a digestible language for both tech savvy consumers and tech laggards (Symantec, 2012). One proposed solution for overcoming the educational gap in cybersecurity advocated for mandatory cyber hygiene education for all individuals, including both cyber and non-cyber professions (Dupuis, 2017; Sobiesk et al., 2015). However, this is not necessarily a feasible solution, and it is unclear how this idea could be enforced en masse.

While mass cyber education may serve to offset poor cybersecurity behaviors, mandatory education becomes a moot point if the curriculum is not focused on user behaviors or human factors, which currently appears to be the case. Many computer science, information system, and cybersecurity courses do not contain content explicitly addressing the weaknesses associated with human users. Moreover, at many institutions, specific coursework related to human cognition and human behavior is not required of computer science or information systems majors, which is problematic given a human user will ultimately be using a computer-based product. Fortunately, many programs of study are shifting to a more multi-disciplinary approach (Dupuis, 2017). Due to this shift in the current cyber educational system, it is an opportune time to investigate specific individual differences that may be associated with better cyber hygiene so as to broaden and strengthen the revised curricula associated with these new multi-disciplinary approaches. Further, such an understanding of individual differences in cybersecurity behaviors provides significant practical implications for areas outside of education, such as the United States Government, where cyber security training is mandatory for all employees (Cone et al., 2007).

1.1.2. Individual differences related to cyber hygiene

In one study, Whitty and colleagues observed that older individuals, and individuals who score high in "self-monitoring," were more likely to share their passwords with another individual (2015). Yet, in a more recent study, age and gender were not related to information security awareness (Parsons et al., 2017). Rather, Parsons et al., (2014, 2017) determined that specific cyber-related knowledge and attitudes shape several cyber hygiene behaviors, including password management, opening unfamiliar links through websites or via email, privacy settings, and cybersecurity when working in public places. Similarly, Butler (2014) demonstrated that knowledge, capability, and motivation were all human factors that influenced poor password practices.

Finally, in a landmark study of human behavior and cybersecurity, Tischer et al. (2016) placed 297 USB flash drives, loaded with malware, throughout a large university campus. Cyberattacks were successful approximately 45 – 98% of the time and malware was connected in less than six minutes. Importantly, the flash drives' appearance did not increase attack success (Tischer et al., 2016). Instead, users reported that they installed the flash drive for altruistic reasons – they intended to find the owner of the missing drive.

1.2. The present study

Consequently, the purpose of the present study is two-fold: 1) understand the unique human factors that may impact cyber hygiene, and 2) use these findings to justify the need to discuss individual differences in cyber hygiene in modern computer and information science course curricula. By understanding the human factors that both pose and offset cybersecurity risks, we provide students with a holistic education. More specifically, we seek to understand the role of cybersecurity knowledge (Parsons et al., 2014, 2017), motivation and self-efficacy (Butler, 2014; Tischer et al., 2016) Whitty et al., 2015), and demographics (Parsons et al., 2017; Whitty et al., 2015), such as age and gender, in predicting cyber hygiene-related knowledge, attitudes, and behaviors.

We also elected to explore the impact of trust on cyber hygiene – given the importance of this topic in the field of human-computer interaction and automation (Balfe et al., 2018; Hancock et al., 2011; Hensel, Cains, Hoffman, and Kelley, 2015; Linkov et al., 2019; Schaefer et al., 2016). While there is a great deal of literature on the role of trust in technology, it remains understudied in the context of cyber hygiene.

The present research is largely exploratory in nature as the individual differences in this study have not been examined collectively or in tandem as predictors of effective cybersecurity behaviors. This begs a broader research question that we attempt to address: what is the relationship between known and unknown human factors that influence greater cyber hygiene?

2. Materials and methods

2.1. Participants

We surveyed one hundred and seventy-three graduate and undergraduate students (7 students from Towson University; 166 students from the University of Central Florida) using validated and reliable measures of trust, motivation, computer self-efficacy, and cyber hygiene. Participants were recruited via the online experiment systems at Towson University and the University of Central Florida. University. Participants completed this experiment for partial course credit.

The age range for participants was 18 to 43 years of age ($M = 21.42$ years, $SD = 4.81$ years, $Median = 20.00$ years). This research complied with the American Psychological Association ethical guidelines and standards for human research (1986) and was approved the U.S. Army Research Laboratory Institutional Review Board (Protocol: ARL 18–010). All participation was voluntary. Demographic information is included in Table 1.

2.2. Procedure

Participants voluntarily registered for the present study through an online survey system at their respective university (data were collected over the course of the month of March in 2018). Next, participants were provided with a link to the surveys which were hosted using Qualtrics survey software. Participants first reviewed an electronic Informed Consent Document, then read a definition of cyber hygiene (see the Appendix). If participants agreed that they understood the definition of cyber hygiene, they were then able to begin the surveys. If they did not understand this definition, they were screened out of the study. Participants then completed four individual difference measures (described in detail below), which were randomized in their administration to control for order effects. Finally, participants completed a demographics form

Table 1
Sample Demographic Information ($N = 173$).

Characteristic	Frequency	Proportion (%)
Sex		
Female	100	57.80%
Male	73	42.20%
Academic Major		
STEM	84	48.80%
Non-STEM	82	47.70%
Class Standing		
Freshman	72	41.90%
Sophomore	30	17.40%
Junior	31	18.00%
Senior	34	19.80%
Graduate Student	4	2.30%
Other	1	.60%

Note. Older participants did not indicate significantly different responses to survey materials compared to younger adults.

and were given more information about the study. Approximately 20–30 min were required to complete the study.

2.3. Measures

2.3.1. Human aspects of information security questionnaire (HAIS-Q)

The HAIS-Q (Parsons et al., 2017) is a measure of information security and awareness that measures an individual's knowledge, attitudes, and behaviors as they relate to cybersecurity practices. There are 63 items on the HAIS-Q and participants respond to the HAIS-Q items on a five-point Likert scale. Negatively worded items are reversed scored to create a composite HAIS-Q score. Scores across seven subcomponents of the HAIS-Q can also be calculated. These include: password management, email use, Internet use, social media use, mobile device use, information handling, and incident reporting.

2.3.2. Computer self-efficacy questionnaire (CSE)

The CSE (Thatcher et al., 2008) measures an individual's ability to use technology independently and successfully. The CSE consists of ten items that participants respond to on a Likert scale. Responses to these items are then summed to create a computer self-efficacy composite score.

2.3.3. Trust in technology scale (TTS)

The TTS (McKnight et al., 2011) measures general attitudes and feelings of trust toward technology (broadly defined). The TTS includes seven items related to trust in technology. Participants respond to these items on a Likert scale. All seven items are then summed to create a composite trust in technology score.

2.3.4. Work preference inventory (WPI)

The WPI (Amabile et al., 1994) is designed to assess individual differences in intrinsic and extrinsic motivation orientations. Conceptually, this does not necessarily measure preference to be more intrinsically or extrinsically motivated at work, rather it relates to the reasons why individuals engage in their work. Participants respond to 30 items on a Likert scale. Responses to these items are then summed to create two scores: an extrinsic motivation score and an intrinsic motivation score.

2.4. Data cleaning and outlier removal

Participants were excluded from the study if they indicated that they did not understand the provided definition of cyber hygiene. This resulted in the removal of 28 participants. Participants were removed from the study for malingering, which included responding to all survey items with the same response (i.e., indicating "Strongly Agree" for all surveys) or responding with consistent patterns (i.e., responding with "1", "2", "3", "4" across all surveys). This resulted in the removal of 56 participants. Using this cleaning criteria, usable data from 173 participants remained.

3. Results

3.1. Measure reliability

On average, participants indicated that they were both highly aware of and actively engaged in several factors related to cyber hygiene, including password management (e.g., using the same password, sharing passwords, using a strong password), email use (e.g., clicking on links in emails from known or unknown senders, opening attachments from known or unknown senders), Internet use (e.g., downloading files, accessing dubious websites, entering information online), social media use (e.g., social media privacy settings, considering the consequences of posting on social media), mobile device use (e.g., physically securing mobile devices, sending sensitive information over Wi-Fi, "shoulder surfing"), information handling (e.g., disposing of sensitive or personal information, inserting removable media devices like USBs, leaving sensitive or personal material unsecured), and incident reporting (e.g., reporting suspicious activities, ignoring poor security measures taken by peers).

Participants indicated moderate extrinsic motivation (motivation toward external motivators such as money or accolades), intrinsic motivation (motivation toward internal motivators such as a sense of enjoyment or accomplishment), and computer self-efficacy, which refers to one's ability to use a computer effectively and efficiently to accomplish a task. Participants indicated lower trust in technology.

All measures indicated high to very high reliability, except for the measure of extrinsic motivation, which was only moderately reliable in its measurement of the construct. Thus, extrinsic motivation was excluded from further multiple regression analyses. Means, standard deviations, and reliability are reported in Table 2.

3.2. Intercorrelations between cyber hygiene measures

Bivariate correlations indicated strong positive relationships between HAIS-Q constructs and its respective subscales. Such affinity is to be expected given that this instrument focuses on information security awareness, and the constituent constructs should be interrelated. The bivariate correlations revealed that computer self-efficacy and intrinsic motivation, more often than trust in technology and extrinsic motivation, were moderately positively correlated with specific hygiene factors, such as attitudes and behaviors (i.e., email use).

Age and sex were moderately correlated with various cyber hygiene behaviors. These bivariate correlations indicated that as age increased, cyber hygiene knowledge increased. Older individuals indicated stronger cyber hygiene attitudes and engaged in more cyber hygiene-related behaviors. The bivariate correlations indicated that women reported more cyber hygiene knowledge than men, stronger cyber hygiene attitudes, and engaged in more cyber hygiene-related behaviors than men. As significant sex differences in cyber behaviors have been studied in the literature (Cain et al., 2018), and we have replicated similar findings here, we performed separate stepwise multiple regression analyses for men and women. These analyses seek to extend the present literature by further examining specific factors that predict cyber hygiene knowledge, attitudes, and behaviors across men and women. Intercorrelations are reported in Table 3 (uploaded as supplementary material based on file size).

Table 2
Means, Standard Deviations, and Reliabilities across all Self-Report Cyber Hygiene Measures ($N = 173$).

Measure	M	SD	Cronbach's α	No. of Items
HAIS-Q Knowledge	80.66**	11.49**	.85	21
HAIS-Q Attitudes	77.93**	10.34**	.89	21
HAIS-Q Behaviors	82.84**	11.75**	.87	21
HAIS-Q Password Management	37.06*	5.66*	.78	9
HAIS-Q Email Use	34.37	5.76	.74	9
HAIS-Q Internet Use	35.84*	5.90*	.83	9
HAIS-Q Social Media Use	34.78**	5.61**	.76	9
HAIS-Q Mobile Device Use	36.66	6.09	.86	9
HAIS-Q Information Handling	36.16**	6.47**	.84	9
HAIS-Q Incident Reporting	35.23**	5.59**	.82	9
Computer Self-efficacy	36.98	7.35	.90	10
Trust in Technology	21.48	3.85	.85	7
Extrinsic Motivation	40.58	5.35	.61	15
Intrinsic Motivation	43.83	6.30	.80	15

Note. HAIS-Q = Human Aspects of Information Security Questionnaire. ** indicates significance at the $p < .01$ level and * indicates significance at the $p < .05$ level between men and women on this measure.

3.3. Multiple regression analyses

Multiple regression analyses were performed to predict overall cyber hygiene knowledge, attitudes, and behaviors, derived from HAIS-Q subscales including, password management, email use, Internet use, social media use, mobile device use, information handling, incident reporting, as well as measures of computer self-efficacy, trust in technology, intrinsic motivation, age, and academic major across men and women. Stepwise regression was selected due to the limited research on individual differences in cyber hygiene and cybersecurity.

From the small body of literature that does exist, we elected to perform separate multiple regressions for female and male participants as sex differences in cyber hygiene behaviors have been noted in the literature (Cain et al., 2018; Parsons et al., 2014; Whitty et al., 2015). We expand upon previous work on individual differences and cybersecurity by investigating the relationships between factors that foster improved cyber hygiene behaviors by accounting for differences in computer self-efficacy, trust in technology, and intrinsic motivation. These are variables that have not been previously examined as a set in the literature.

3.3.1. Predictors of cyber hygiene knowledge, attitudes, and behaviors for women

A stepwise multiple regression indicated that Internet use, mobile device use, email use, social media use, password use, and information handling significantly predicted cyber hygiene-related knowledge for women, $F(6, 93) = 138.64$, $p < .01$, adjusted $R^2 = 0.89$.

A second stepwise multiple regression indicated that information handling, social media use, password management, mobile device use, incident reporting, email use, Internet use, and intrinsic motivation significantly predicted attitudes toward cyber hygiene for women, $F(8, 91) = 125.05$, $p < .01$, adjusted $R^2 = 0.91$.

A third stepwise multiple regression indicated that information handling, incident reporting, password management, email use, social media use, mobile device use, Internet use, and academic major (i.e., STEM or non-STEM) significantly predicted cyber behaviors in women, $F(8, 91) = 100.06$, $p < .01$, adjusted $R^2 = 0.89$.

Thus, across these three models, trust in technology, computer self-efficacy, and age did not significantly account for variance in cyber hygiene knowledge, attitude, or behavior scores in women. These regression models are included in Table 4 (uploaded as supplementary material based on Table size).

3.3.2. Predictors of cyber hygiene knowledge, attitudes, and behaviors for men

A stepwise multiple regression indicated that Internet use, incident reporting, email use, information handling, social media use, and computer self-efficacy significantly predicted cyber hygiene-related knowledge in men, $F(6, 66) = 91.55$, $p < .01$, adjusted $R^2 = 0.88$.

A second stepwise multiple regression indicated that mobile device use, password management, email use, information handling, computer self-efficacy, social media use, and trust in technology significantly predicted attitudes toward cyber hygiene for men, $F(7, 65) = 97.35$, $p < .01$, adjusted $R^2 = 0.90$.

A third stepwise multiple regression indicated that mobile device use, password management, incident reporting, information handling, Internet use, email use, and trust in technology significantly predicted cyber behaviors in men, $F(7, 65) = 97.91$, $p < .01$, adjusted $R^2 = 0.90$.

Thus, across these three models, intrinsic motivation, academic major, and age did not significantly account for the variance in cyber knowledge, attitude, and behavior scores in men. These regression models are included in Table 5 (uploaded as supplementary material based on Table size).

4. Discussion

Human error has been theorized to be the primary cause for underlying breaches in cybersecurity (Wiederhold, 2014). Importantly, maintaining good cyber hygiene has been found to improve cybersecurity at the user level. Unfortunately, relatively little is known about the individual differences that comprise the attitudes and behaviors related to maintaining effective cyber hygiene practices. The primary purpose of the present study was therefore to understand the human factors and individual differences that influence cyber hygiene. The results demonstrated an informative pattern of outcomes.

First, several common factors were predictive of cyber hygiene knowledge, attitudes, and behaviors. Across both men and women, Internet use, information handling, and social media use were predictive of cyber hygiene-related knowledge. Similarly, information handling, social media use, password management, mobile device use, and email use were predictive of attitudes toward cyber hygiene. Information handling, incident reporting, password management, email use, and Internet use were predictive of cyber hygiene behaviors. Given that specific cyber hygiene factors were reported across individuals, it will be important to target and address these factors in cyber education and training. For instance, modern com-

puter and information science course curricula should frame cybersecurity material around the importance of internet use, information handling, and social media use in the behaviors, attitudes, and knowledge of cyber hygiene. Second, unique factors related to human factors and cyber hygiene characteristics emerged between men and women. For example, computer self-efficacy was predictive of men's cyber hygiene knowledge, but not for women. Intrinsic motivation was important in predicting women's attitudes toward cyber hygiene, but trust in technology and computer self-efficacy were important for predicting men's attitudes toward cyber hygiene. Academic major (science, technology, engineering, or mathematics [STEM] versus non-STEM) was predictive of the cyber hygiene behaviors in which women engage. However, trust in technology was predictive of the cyber hygiene behaviors in which men engaged.

Several factors were not predictive of cyber hygiene-related knowledge, attitudes, or behaviors. For example, trust in technology, computer self-efficacy, and age were not predictive human factors for women's cyber knowledge, attitudes, or behaviors. Intrinsic motivation, academic major, and age were not predictive human factors for men's cyber knowledge, attitudes, or behaviors. Interestingly, age was not a predictive factor for knowledge, attitudes, or behaviors for either sex, and such results indicate that cyber hygiene education need not target a particular sex or age group in terms of content or delivery method – which contradicts previous findings (Whitty et al., 2015). Rather, such practical literacy and skills remain important considerations for computer and Internet users of any age (van Duersen and van Dijk, 2009) or gender.

4.1. Limitations

Though the present study provided valuable information regarding the human factors that impact cyber hygiene, there are limitations that must be discussed. First, although the study was sufficiently powered, the sample distribution (i.e., age and sex distributions) is not necessarily reflective of the entire population. Furthermore, the sample was comprised predominately of undergraduate students at a university in the south eastern United States. As we collected data from undergraduate students, it is difficult to generalize and extend these results to other groups.

4.1.1. Theoretical applications

While there is no single theoretical model for cyber hygiene, though the HAIS-Q framework is a start (Parsons et al., 2017), the present findings paired with earlier research performed by Parsons and colleagues should be utilized to develop an empirically supported educational framework. The present research provides the foundation for developing a holistic, articulated model of cyber hygiene education that links knowledge, attitudes, and behaviors to important individual differences. This is an extension of the current literature and can again be utilized to craft and support overarching theories of cyber hygiene.

4.1.2. Practical applications

This research demonstrates how specific individuals are targeted through malicious social engineering attempts. For example, men tend to demonstrate greater trust in technology, and this could bias them as a group in their cyber hygiene behaviors and practices. For reasons such as this, the results of the present study could better inform cybersecurity, computer science, and information technology courses that teach cybersecurity practices. By providing awareness of potential biases, students can have a better understanding of these principles and be better prepared for potential future social engineering attempts in their personal and professional lives.

Individual differences related to cyber hygiene are crucial to disseminate in science, technology, engineering, and mathematics (STEM) classes, and are an important incorporation into a cyber education curriculum given that the human user is the most significant threat to effective cybersecurity. Thus, the practical application of this work is in its application to the classroom. Finally, by tailoring cyber hygiene training to suit the user's needs based on their current knowledge, attitudes, and behaviors (Hancock et al., 2009), one can expect greater efficacy and transfer of such education – particularly when it comes to the protection of personal and confidential information (Bansal et al., 2010).

5. Conclusion

To conclude, cyber education is currently underpreparing graduates in terms of considering the human factors associated with breaches to cybersecurity. The human factor may be the primary cause of such security violations and is the weakest link in terms of cyber resiliency. The present study helps identify *why* humans may be the weakest and *where* they are most vulnerable to cyber-attacks, which has both important practical and theoretical applications within the context of cyber education.

Disclosure statement

This research was sponsored by the United States Army Research Laboratory and was accomplished under Oak Ridge Associated Universities Cooperative Agreement Number W911NF-17–2–0088. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.cose.2020.101731.

Appendix

Definition of cyber hygiene provided to participants

Cyber hygiene involves establishing and maintaining important cyber health behaviors, which includes routinely monitoring technology for threats or attempted hacking, occasionally changing passwords and developing strong passwords, updating virus protection software, back-up information securely, and running appropriate security scans (to name a few). Do you understand the definition of cyber hygiene?

References

Amabile, T.M., Hill, K.G., Hennessey, B.A., Tighe, E.M., 1994. The work preference inventory: assessing intrinsic and extrinsic motivational orientations. J. Pers. Soc. Psychol. 66 (5), 950–967.

Arquilla, J., 2016. Crafting a national cyberdefense, and preparing to support computational literacy. Commun. ACM 60 (4), 10–11.

Balfe, N., Sharples, S., Wilson, J.R., 2018. Understanding is key: an analysis of factors pertaining to trust in a real-world automation system. Hum. Factors 60 (4), 477–495. doi:10.1177/0018720818761256.

Bansal, G., Zahedi, F., Genfen, D., 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decis. Support Syst. 49 (2), 138–150.
Butler, M.J., 2014. Towards online security: key drivers of poor user behaviour and recommendations for appropriate interventions. South African J. Busi. Manage. 45 (4), 21–32.
Cain, A.A., Edwards, M.E., Still, J.D., 2018. An exploratory study of cyber hygiene behaviors and knowledge. J. Inform. Secur. Appl. 42, 36–45.
Cone, B.D., Irvine, C.E., Thompson, M.F., Nguyen, T.D., 2007. A video game for cyber security training and awareness. Comp. Secur. 26 (1), 63–72.
Dupuis, M.J., 2017. Cyber security for everyone: an introductory course for non technical majors. J. Cybersecur. Edu. Res. Practice 2017 (1), 1–17.
Garfinkel, S.L., 2012. Inside risks: the cybersecurity risk. Commun. ACM 55 (6), 29–32.
Han, J., Kim, Y.J., Kim, H., 2017. An integrative model of information security policy compliance with psychological contract: examining a bilateral perspective. Comp. Secur. 66, 52–65.
Hancock, P.A., Billings, D.R., Schaefer, K.E., Chen, J.Y.C., de Visser, E.J., Parasuraman, R., 2011. Hum. Factors 53 (5), 517–527. doi:10.1177/0018720811417254.
Hancock, P.A., Hancock, G.M., Warm, J.S., 2009. Individuation: the N=1 revolution. Theoret. Issues Ergonom. Sci. 10 (5), 481–488.
Henshel, D., Cains, M.G., Hoffman, B., Kelley, T., 2015. Trust as a human factor in holistic cyber security risk assessment. Procedia Manufact. 3, 1117–1124. doi:10.1016/j.promfg.2015.07.186.
McKnight, D.H., Carter, M., Thatcher, J.B., Clay, P.F., 2011. Trust in a specific technology: an investigation of its components and measures. Trans. Manage. Inform. Syst. (TMIS) 2 (2). doi:10.1145/1985347.1985353.
Linkov, V., Zámečník, P., Havlíčková, D., Pai, C.-H., 2019. Human factors in the cybersecurity of autonomous vehicles: trends in current research. Front. Psychol. doi:10.3389/fpsyg.2019.00995.
Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., Zwaans, T., 2017. The human aspects of information security questionnaire (HAIS-Q): two further validation studies. Comp. Secur. 66, 40–51.
Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C., 2014. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Comp. Secur. 42, 165–176.
Roberts, E.S., Kassianidou, M., Irani, L., 2002. Encouraging women in computer science. ACM SIGCSE Bull. 34 (2), 84–88.
Sawyer, B.D., Hancock, P.A., 2018. Hacking the human: the prevalence paradox in cybersecurity. Hum. Factors 60 (5), 597–609.
Schaefer, K.E., Chen, J.Y.C., Szalma, J.L., Hancock, P.A., 2016. A meta-analysis of factors influencing the development of trust in automation: implications for understanding autonomy in future systems. Hum. Factors 58 (3), 377–400. doi:10.1177/0018720816634228.
Sobiesk, E., Blair, J., Conti, G., Lanham, M., Taylor, H., 2015. Cyber education: a multi-level, multi-discipline approach. In: Proceedings of the 16th Annual Conference on Information Technology Education, pp. 43–47.
Symantec. (2012). Internet Security Threat Report: 2011 Trends. Symantec Corporation.
Thatcher, J.B., Zimmer, J.C., Gundlach, M.J., McKnight, D.H., 2008. Internal and external dimensions of computer self-efficacy: an empirical examination. IEEE Trans. Eng. Manage. 55 (4), 628–644.
Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., Bailey, M., 2016. Users Really Do Plug in USB Drives They Find. 2016 IEEE Symp. Secur. Priv. 306–319. doi:10.1109/SP.2016.26.
van Duersen, A.J.A.M., van Dijk, J.A.G.M., 2009. Using the internet: skill related problems in users' online behavior. Interact. Comput. 21 (5–6), 393–402.
Whitty, M., Doodson, J., Creese, S., Hodges, D., 2015. Individual differences in cyber security behaviors: an examination of who is sharing passwords. Cyberpsychol. Behav. Soc. Netw. 18 (1), 3–7.
Wiederhold, B.K., 2014. The role of psychology in enhancing cybersecurity. Cyberpsychol. Behav. Soc. Netw. 17 (2), 1–2. doi:10.1089/cyber.2014.1502.

Alexis R. Neigel is currently a Senior Design Researcher in the Pacific Northwest. She earned her Ph.D. in Applied Experimental and Human Factors Psychology and M.S. in Modeling and Simulation from the University of Central Florida. She earned her B.S. in Psychology from Washington State University. Her research interests include cyber vigilance, attention, and decision making.

Victoria L. Claypoole earned her Ph.D. in Human Factors and Cognitive Psychology and M.S. in Modeling and Simulation from the University of Central Florida. She earned her B.S. in Psychology from the University of Florida. Her research interests include vigilance, decision making, and social facilitation.

Grace E. Waldfogle is currently a graduate student at the University of Central Florida. She earned her B.S. in Psychology, Human Factors, and Design from the Pennsylvania State University – Erie. Her research interests include training for vigilance and individual differences in human performance.

Subrata Acharya is currently an Associate Professor of Computer Science at Towson University in Maryland. She received her Ph.D. in Computer Science from the University of Pittsburgh in 2008 and her M.S. in Computer Engineering from Texas A&M University - College Station in 2004. She has published over 75 peer-reviewed book chapters and journal articles in the area of computer and information security. Of note is Dr. Acharya's US patent 7966655 B2, awarded in 2011 with Drs. Wang, Ge, and Greenberg for firewall optimization. Dr. Acharya has also developed new courses in the area of healthcare informatics and computer security. She has mentored various students who have appeared as co-authors on her papers, and has supervised numerous undergraduate research projects, masters' graduate projects, and doctoral dissertations.

Gabriella M. Hancock is currently an Assistant Professor in the Department of Psychology at California State University – Long Beach and the Director of the Stress & Technology Applied Research (STAR) Laboratory. She earned her Ph.D. in Applied Experimental and Human Factors Psychology, M.S.I.E. in Industrial Engineering, and B.S. in Psychology from the University of Central. She earned her M.S. in Applied Physiology and Kinesiology from the University of Florida. Her research focuses on human performance under stress and workload, psychophysiological assessment of cognitive and affective states, individual differences, and human-technology interaction.