Cognitive Engineering Modeling of Phishing

Tiffani Bragg, Esa M. Rantanen, Justin M. Pelletier, and Ehsan Rashedi
Rochester Institute of Technology, Rochester, NY, USA

Using signal detection theory (SDT) and fuzzy SDT, the influence of familiarity with phishing and having a background in cybersecurity on phishing behavior was examined. The results from SDT analysis indicated that familiarity with phishing only accounted for 11% of the variance in sensitivity and 5% in bias. When examining the same using Fuzzy SDT, familiarity with phishing accounted for 6% of the variance in bias. Background in cybersecurity had a statistically significant effect on sensitivity and bias in classical SDT but only on bias in fuzzy SDT. A confusion matrix revealed that the percentage of successfully transmitted information from the stimuli to the judgements made by participants was only 26%. Participants most frequently identified requests for personal information in stimulus emails as phishing cues. Future research should continue to explore application of the different cognitive engineering models to phishing identification.

INTRODUCTION

Cybersecurity is a growing field that is becoming increasingly important. Cyberattacks have steadily increased on varying platforms including social media, email, and even phone calls. Many information technology or -security departments use encryption technologies, firewalls, and email privacy interventions to aid in minimizing cyberattacks (Prince, 2018). However, the last line of defense in cybersecurity is the human's ability to detect and act on a potential threat.

Relying on humans to make judgments about threats to cybersecurity can be problematic. Previous research suggests that human decision making does not always align with their best interests (Tversky & Kahneman, 1974). In cybersecurity, humans often overlook or misjudge the consequences of their behavior by not having strong passwords, falling for phishing attacks, and ignoring other malicious attempts to access their personal information (Guo, 2013).

Milkovich (2020) reported that approximately every 39 seconds a cyberattack or security breach takes place. A security breach is any incident where information that is confidential or sensitive has been accessed without permission (Sobers, 2020). Individuals who fall victim to security breaches can have their identity stolen or coerced into giving up money, passwords, or account information (Retruster, 2019). Misjudgments from humans accounted for 90% of security breaches in 2019, most related to phishing attacks (Hill, 2019; Spadafora, 2019). The rise in cyberattacks on different companies and individual people has resulted in the investment of billions of dollars in boosting defenses against cyberattacks (Shalal & Selyukh, 2015).

User-Level Threats to Cybersecurity

Cyberattacks that rely on human error include email fraud or phishing, social phishing or phishing using social media, spear phishing, where the messages are personalized for the recipient, and vishing or "voice phishing" (Aldawood & Skinner, 2019; Griffin & Rackley, 2008). One of the best ways to counter these different types of attacks is knowledge. Having knowledge about and understanding of different types of cyberattacks and their indicators has been shown to decrease the likelihood of falling victim to them. Factors that predict knowledge of cyber hygiene behaviors include internet use, information handling, incident reporting, email use, and password management (Neigel, Claypoole, Waldfogle, Acharya, & Hancock, 2020).

Phishing attacks are very common cyberattack vectors that originate as messages that are designed to give the illusion of legitimate communication in an attempt to coerce individuals to reveal private information or inadvertently perform an action that compromises security. Oftentimes, the targets of these attacks are not the individuals themselves, but rather the organizations they are affiliated with (Molinaro & Bolton, 2018).

Health concerns, disposition to trust, risk-taking propensity, and cognitive tendencies have been shown to affect susceptibility to phishing attacks (Abdelhamid, 2020; Molinaro & Bolton, 2019). Attackers make messages appear convincing to the receiver through visual deception, bounded attention, and the impact of the message involvement (Dhamija, Tygar, & Hearst, 2006; Wang, Herath, Chen, Vishwanath, & Rao, 2012). Message involvement is the amount that an individual perceives an email to be related to their goals, needs, or interests (Wang et al., 2012).

Spear phishing is similar to phishing, but rather than a general email message, the message is tailored to the person receiving it (Aldawood & Skinner, 2019). It has been shown that older women are most susceptible to spear phishing attacks, especially if the phishing attacks are related to legal matters (Oliveira et al., 2017) and people who scored higher on a measure of contentiousness are more likely to fall victim to a spear phishing attack (Halevi, Memon, & Nov, 2015).

Purpose of the Research and Hypotheses

The purpose of this research was to investigate the application of different cognitive engineering models to human responses to phishing attempts. We conducted an online survey to collect participant responses to both phishing attempts and legitimate emails, and analyzed these survey responses using SDT, fuzzy SDT and Shannon's information theory. This research was primarily exploratory. We expanded upon previous work to specifically test the following hypotheses:

1. Familiarity with phishing and background in cybersecurity have significant positive impact on d' and β (Neigel et al., 2020);

2. Participants exhibit a liberal bias (cf. Lawson, Pearson,

Crowson, & Mayhorn, 2020); and

3. There is observable information transmittal from stimuli to judgement and that the percentage of information about "phishiness" successfully transmitted will be low, given the prevalence of successful phishing attacks in the wild.

We specifically chose to not examine characteristics such as personality traits, age, gender, or contentiousness, to explore instead the generalized application of these models in a way that allows us to demonstrate whether or not the models apply to phishing identification at all.

METHODS AND MATERIALS

Participants

The sample consisted of 207 students, faculty and staff of a middle-sized private university. Participants had a mean age of 21.86 years (SD = 6.53 years). On average participants rated their familiarity with phishing at a 3.34 (SD = 1.18) on a scale from 1-5, which indicates moderate familiarity. Participants included 91 people who identified as women (44%), 107 people who identified as men (51.7%), and 9 people who identified as non-binary (4.3%). Most participants (60.9%) reported they have completed some college as their highest level of education but also said they did not have a background in cybersecurity; only 38.6% reported studying or working in this field. This demographic information was used to determine the representativeness of the sample but not as factors in data analyses.

Independent Variables

All participants were shown 30 emails, manipulated as an independent variable. Of these, 20 emails contained phishing messages and 10 emails were legitimate. The 20 phishing emails were broken down into two categories: novel phishing emails and phishing emails taken from different Phish Bowls which are updated regularly with newly reported phishing emails. The novel emails were created by the experimenter to give variety to the emails and ensure that the cues were manipulated appropriately. A phishing detection expert explicitly suggested this 2:1 ratio during personal interview during the preparation phase of this study, and we did not find alternative ratios in the available literature.[1] Though participants were unaware of the 2:1 phishing to legitimate email ratio, follow-on research could consider the moderating effect of different presentation ratios.

Of the 30 emails presented, 7 did not have links visible, 10 did not have the sender email visible, and 4 did not have either visible to the participant. If all stimuli had the email addresses and link destination visible the cues would have been too salient. It is also more realistic if this information is not shown to participants because they may not have the ability to further examine the links before clicking (i.e. using a mobile device), or may not care to further examine the links/sender emails that are associated with the email present. If the participants determine the email is legitimate even though they cannot see the link, they would probably not hover over them for further examination.

Other independent (subject) variables included participant degree level, college affiliation, phishing familiarity, and cybersecurity background as indicated by the participants.

Dependent Variables

Following each email stimulus, participants were asked to determine the type of email (phishing or legitimate) and rate their confidence in this response. Following the confidence rating, participants were asked to identify any phishing cues present in the email.

In the SDT and fuzzy SDT analyses, the dependent variables were d' and β (Parasuraman, Masalonis, & Hancock, 2000; Wickens, Hollands, Banbury, & Parasuraman, 2013). These values were computed from the participant responses to the stimuli and the experimenter classification of the stimuli. For the confusion matrix analysis, the output was the channel capacity represented by the ratio of H_T and H_S.

Design

This study used a within-subjects design where all participants were shown all stimuli. To examine the data using SDT and fuzzy SDT, correlation was used to determine the relationship between d'/β and familiarity with phishing. To examine the relationship between d'/β and background in cybersecurity, t-tests were used to compare the mean d' and β values between participants who indicated they did not have a background in cybersecurity and those who did.

The confusion matrix yielded the ratio of information transmitted to the information in the stimuli. This was derived from a series of equations using all participant responses to the categorization of stimuli (legitimate or phishing). Use of a confusion matrix in this research was purely descriptive.

Procedure

The experiment used an online survey platform (Qualtrics). Each participant was shown both phishing and legitimate messages in email form. To begin the survey, participants gave informed consent and were asked for demographic information followed by the various email messages. These messages were shown in a random order to prevent ordering effects. Participants were then asked to rate their confidence in the correctness of their response and identify phishing cues present in the message. We used Martin, Dubé, and Coovert (2018) and Molinaro and Bolton (2018) as a basis for the methodology.

RESULTS

Data Clean-Up and Formatting

The data from Qualtrics, an online survey platform, were exported into Excel for clean-up. All identifying information including IP address, start time, and location was deleted. Each demographic category was coded numerically to allow for analysis in SPSS. For the area of study, the college each participant is affiliated with was coded by hand, as this question was asked with an open-ended response.

[1] The phishing expert is the person primarily responsible for phishing detection and response for a 20,000+ person organization; he has more than 15 years of cybersecurity experience.

Signal Detection Theory

Signal detection theory calculations were completed using Excel. Conditional formatting was used to determine the type of response (hit, miss, correct rejection, false alarm) for each question answered by participants. For each participant, the number of hits, misses, correct rejections, and false alarms were calculated using the COUNTIF function in Excel.

HR values of exactly 1.0 or FAR values of 0.0 result in invalid responses for d' and β calculations. Twenty-two participants had HR of 1.0. In these cases, one hit was subtracted from the total number of hits and one miss was added. Similarly, 22 participants had an FAR of 0.0, and one false alarm was added to and one correct rejection subtracted from their results. We justify these modifications by the purpose of this research, which was not to examine the responses directly but to evaluate various cognitive engineering models applied to phishing.

There was a positive correlation between familiarity with phishing and sensitivity, and a negative correlation between familiarity with phishing and bias. Similarly, those who reported having a background in cybersecurity also had a higher d' and lower β than those without such a background. Overall, the bias was neutral (β values very close to 1). The mean bias was 1.031 ($SD = .529$) which does not support hypothesis 2.

A regression analysis was conducted with d' or sensitivity as the criterion variable and familiarity with phishing as the predictor. Familiarity was a significant predictor of d', $R^2 = .11, F(2, 201) = 12.24, p < .01$. The association between familiarity and sensitivity was positive, the higher the rating of familiarity, the higher d'. These results support hypothesis 1. While the relationship between d' and familiarity with phishing was statistically significant, the R^2 value of only .11 indicates the relationship was small, or familiarity with phishing only accounts for a small portion of the variance in d' values. An independent samples t-test showed a statistically significant positive association between d' and background in cybersecurity, $t(202) = 2.18, p = .03$, supporting hypothesis 1.

The regression analysis conducted with β as the criterion variable and familiarity with phishing as the predictor indicated that familiarity is a significant predictor of β. This did not support hypothesis 1, $(R^2 = .05), F(1, 205) = 9.88, p < .01$. The association between familiarity and bias was negative; the higher the rating of familiarity, the lower β value. While the relationship between β and familiarity with phishing was statistically significant, the R^2 value of only .05 indicates that familiarity with phishing only accounts for a small portion of the variance in β values.

An independent samples t-test was used in determining the relationship between β and background in cybersecurity. Levene's test for homogeneity of variance revealed that equal variances could not be assumed. When correcting for this, the association was significant $t(168.8) = -3.36, p < .01$. This negative association does not support hypothesis 1.

Fuzzy Signal Detection Theory

Fuzzy signal detection theory uses the same base equations as signal detection theory but accounts for different inputs and therefore different interpretations of results. After indicating if an email was phishing or legitimate, participants were asked to rate their confidence in that response. Ratings were on a scale from 1-5, 1 being not at all confident and 5 being extremely confident. To calculate d' and β using fuzzy SDT, the confidence ratings needed to be adapted for a scale from 0-1. Using conditional formatting, this rating was then changed to either 0, .25, .5, .75. or 1 to get a value between 0-1 that would correspond to their confidence ratings accordingly (1 being 0, 2 being .25, etc.). This was done for each participant and each question. Hit, miss, false alarm, and correct rejection values were determined for each question and each participant. To do this, calculations as indicated by Parasuraman et al. (2000) were used.

HR was calculated by adding the hit values of each question and dividing them by the sum of the phishiness ratings. FAR was calculated by adding the false alarm values and dividing them by the sum of 1-phishiness rating. d' and β values were calculated for each participant in Excel using the same base formulas as were used for analysis using SDT.

Similar to SDT, HR values of exactly 1.0 or FAR values of 0.0 result in invalid responses for d' and β calculations. After completing the above calculations, six participants had an HR of exactly 1.0, in these cases, HR was changed to .99. In addition, there was one participant who had an HR of 1.0 and an FAR of 1.0; in this case, HR was changed to .999 and FAR was changed to .99. To run the analysis, HR and FAR cannot be equivalent, explaining why these two values were slightly different.

The d' values calculated were consistent across participant reports of familiarity with phishing, however the β values decreased as the familiarity rating increased. In addition, the d' values were similar for participants who reported having a background in cybersecurity and those who reported having no background in this field. The β values were different between these two groups with the higher β value being associated with those who do not have a background in cybersecurity. The mean reported bias was .416 ($SD = .24$) which would indicate a liberal bias, supporting hypothesis 1.

A regression analysis was conducted with d' as the criterion variable and familiarity with phishing as the predictor. Familiarity was not a significant predictor of $d', R^2 = .002, F(1, 204) = .328, p = .567$, which indicates that hypothesis 1 was not supported. An independent samples t-test showed no significant association between d' and background in cybersecurity, $t(202) = .252, p = .801$. This does not support hypothesis 1.

A regression analysis conducted with β as the criterion variable and familiarity with phishing as the predictor showed familiarity as a significant predictor of $\beta, R^2 = .06), F(1, 202) = 12.35, p < .01$. The association between familiarity with phishing and β was negative, the higher the rating of familiarity, the lower β. These results do not support hypothesis 1, but still indicate that familiarity with phishing accounts for a small portion of the variability in β. While the relationship between β and familiarity with phishing was statistically significant, the R^2 value of only .06 indicating that the relationship was small.

An independent samples t-test showed a significant association between β and background in cybersecurity, $t(202) = -2.259, p = .025$. This negative association does not support hypothesis 1, but does indicate that there is a statistically signif-

icant relationship between β and background in cybersecurity.

Confusion Matrix

Using the response data, exploratory analysis using a 2 × 2 confusion matrix was completed. This was done by plotting the response (phishing or legitimate) against the message type (phishing or legitimate). The number of participant response in each category was calculated for each question. Once this was calculated, all of the responses for the phishing and legitimate stimuli were added together by response type to form one matrix. Once the matrix was formed, H_s, H_r, H_{s+r} and H_t were calculated.

The results showed H_s = .918 bits, H_r = .960 bits, and H_{s+r} = 1.636 bits. These calculations allowed for H_t to be calculated which resulted in a value of .242. H_t/H_s determined percentage of information transmitted through the channel to be 26.39%. These results support hypothesis 3.

Phishing Cues

While each image was displayed, participants were asked to indicate which phishing cues were present in the message. Of the cues presented, participants indicated that the message requests personal information more often than the other cues, whereas text substitution was chosen least often. Most often, participants reported that the message was requesting personal information. This cue was correctly identified 947 times; when compared to text substitution that was correctly identified only 14 times, this is a large difference.

Responses to phishing cues were then separated by background in cybersecurity. There were very minimal differences between the responses from those who did have a background in cybersecurity and those who did not. Of the total responses from individuals who had a background in cybersecurity, 74.83% were correct. Of the total responses from individuals who did not have a background in cybersecurity, 74.29% were correct, further highlighting the similarity of responses from the different groups.

Responses to phishing cues were also separated by familiarity with phishing. Overall, those who indicated a higher level of familiarity had higher percentages of correct responses over those who indicated they were not familiar with phishing, though this difference was only by about 7%.

In addition to the selection of provided phishing cues, participants had the option of writing in phishing cues in addition to the predetermined cues. Of the written in responses, 103 of them were accounted for in the predetermined phishing cues. A large majority (109) of the written responses included phrases such as "I could just tell" or "something seemed off". Responses detailing the message was asking for some sort of payment was another common response (51).

DISCUSSION

The application of SDT to phishing response has also been examined by Lawson et al. (2020) and Martin et al. (2018). Both of these previous studies also determined that SDT is a viable option for analyzing phishing identification. This analysis method works to analyze the abilities of people to detect phishing as a signal. Understanding how people respond in a "lab setting" to phishing and legitimate stimuli can aid in understanding how they may respond in real world applications. Being able to track this difference in response while understanding the bias and sensitivity measures that directly result from SDT analysis can inform better training techniques.

Fuzzy SDT has not yet been applied to phishing responses, but the current study did support the idea that it could be used in the future. This novel application of fuzzy SDT aligns with the basis of the theory that there is a degree of variability that the signal is in fact a signal. Accounting for this variability in phishing messages aids in the understanding of how the phishiness of an email impacts user responses. The method of determining phishiness in the current study was also unprecedented, and allows for further investigation. It is noteworthy that Fuzzy SDT, being more "fine-grained" than classical SDT, yielded very different results from the classical SDT. Different experiments are required to determine which model is most accurate.

The confusion matrix illustrates the information conveyed through a channel to inform a decision. The channel represents the participant shown the stimuli and the selection of the email type is the decision made. This showed how much information was taken in by the user and applied to their decision. In this sample, the percentage of information transmitted was rather low at only 26.39%. This suggests that users do not apply a majority of the information conveyed within the stimuli when determining if a message is phishing or legitimate.

To the best of our knowledge, confusion matrices have not been applied to phishing before this study. The current study demonstrated that the confusion matrix can indeed be applied to phishing, but only in such a way that one option was chosen over the other; in this case, that choice would be phishing versus legitimate. This is useful in understanding how much information is truly transmitted by phishing emails to those receiving the emails, which allows for a better understanding of the context phishing emails are received under.

Understanding what within an email indicates to a user that they should be weary of the email is important. Participants most frequently recognized when an email requested personal information. This could suggest that people are sensitive to sharing their personal information or that they are aware of the risks of sharing their personal information. In contrast, text substitution was the least recognized phishing cue. It is possible that participants are not as familiar with text substitution or they did not notice the minor changes in spelling. When examining responses by background in cybersecurity, no difference was seen. However, familiarity with phishing did seem to have an impact on responses; participants with higher familiarity had higher percentages of correct responses than those with little to no familiarity. This suggests that general cybersecurity training may not be enough to teach individuals what to look for in phishing messages and more specific training may be useful. The other notable responses participants wrote in included cues that were already present in front of them. There are multiple potential reasons for this. Participants might have wanted to reiterate the salience of these cues. Alternatively, participants could have overlooked the cues that were presented to them or might not have known what all of them meant.

Limitations

The cues presented to participants did not have any definitions associated with them. This could have impacted participant responses being that some of the cues could have been interpreted differently than intended. Some of these terms could have been unfamiliar to the participants, leading to written in responses that correspond to the cues presented. Short definitions could have been useful in minimizing any potential confusion regarding the presented phishing cues.

Recommendations

To further examine this line of research, additional application of the cognitive engineering models outlined should be examined. Specifically, the application of fuzzy SDT to phishing identification is recommended. There are multiple ways the fuzzy gradient can be determined. The current study focused on only one determination of the fuzzy gradient; establishing a best practice would be beneficial for future use of this model. Research also suggests that Brunswick's lens model is an appropriate tool to analyze phishing data (Molinaro & Bolton, 2018, 2019). However, data collected directly from participants detailing the cues present has not been analyzed using this method.

The online survey limited the data to be collected. If an in-person study was conducted, situation awareness (SA) could have been evaluated to give more context to what participants gave their attention to during the study. It is also possible that participants were primed to seek out phishing emails. Conducting this type of research in a more natural way would help to determine if these results can be generalized to real life or if these phenomena observed are results of the environment the research is being conducted in. Conducting this research in a more "real life" scenario can also highlight how participants might actually react to these different types of emails in their own inbox.

This information can be further applied to training materials. Our results suggest that a broader understanding in cybersecurity is not necessarily beneficial in identifying cues of phishing emails, but rather a more focused understanding of phishing may be more impactful. This would allow further examination of other factors that have the potential to influence phishing identification. In addition to training, other cybersecurity techniques could be explored including further pop-up messaging in emails and different filtering techniques to flag phishing messages before they arrive to the user.

Finally, given this initial and general success in applying cognitive engineering models in phishing identification future work could consider the specific modifying effects of personality traits, age, gender, contentiousness, and alternative real-to-phishing email presentation rates other than the 2:1 ratio we employed.

REFERENCES

Abdelhamid, M. (2020). The role of health concerns in phishing susceptibility: Survey design study. *J Med Internet Res*, *22*(5), e18394. doi: 10.2196/18394

Aldawood, H., & Skinner, G. (2019). Contemporary cyber security social engineering solutions, measures, policies, tools and applications: A critical appraisal. *International Journal of Security (IJS)*, *10*(1), 1.

Dhamija, R., Tygar, J., & Hearst, M. (2006). Why phishing works. In (p. 581-590). ACM.

Griffin, S. E., & Rackley, C. C. (2008). Vishing. In *Proceedings of the 5th annual conference on information security curriculum development* (pp. 33–35).

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers security*, *32*, 242-251.

Halevi, T., Memon, N., & Nov, O. (2015). Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. *Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks (January 2, 2015)*.

Hill, M. (2019). *90% of uk data breaches due to human error in 2019.* Retrieved from `https://www.infosecurity-magazine.com/news/90-data-breaches-human-error/`

Lawson, P., Pearson, C. J., Crowson, A., & Mayhorn, C. B. (2020). Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy. *Applied Ergonomics*, *86*, 103084.

Martin, J., Dubé, C., & Coovert, M. D. (2018). Signal detection theory (sdt) is effective for modeling user behavior toward phishing and spear-phishing attacks. *Human Factors: The Journal of Human Factors and Ergonomics Society*, *60*(8), 1179-1191.

Milkovich, D. (2020). *15 alarming cyber security facts and stats.* Retrieved from `https://www.cybintsolutions.com/cyber-security-facts-stats/`

Molinaro, K. A., & Bolton, M. L. (2018). Evaluating the applicability of the double system lens model to the analysis of phishing email judgments. *Computers security*, *77*, 128-137.

Molinaro, K. A., & Bolton, M. L. (2019). Using the lens model and cognitive continuum theory to understand the effects of cognition on phishing victimization. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *63*(1), 173-177.

Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S., & Hancock, G. M. (2020). Holistic cyber hygiene education: Accounting for the human factors. *Computers security*, *92*, 101731.

Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., ... Ebner, N. (2017). Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing. In *Proceedings of the 2017 chi conference on human factors in computing systems* (pp. 6412–6424).

Parasuraman, R., Masalonis, A. J., & Hancock, P. A. (2000). Fuzzy signal detection theory: Basic postulates and formulas for analyzing human and machine performance. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *42*(4), 636-659.

Prince, D. (2018). Cybersecurity: The security and protection challenges of our digital world. *Computer*, *51*(4), 16-19. doi: 10.1109/MC.2018.2141025

Retruster. (2019). *2019 phishing statistics and email fraud statistics: All the phishing email stats for 2019.* Retrieved from `https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html`

Shalal, A., & Selyukh, A. (2015). *Obama seeks $ 14 billion to boost u.s. cybersecurity defenses.*

Sobers, R. (2020). *107 must-know data breach statistics for 2020.* Retrieved from `https://www.varonis.com/blog/data-breach-statistics/`

Spadafora, A. (2019, May 8). *90 percent of data breaches are caused by human error.* Retrieved from `https://www.techradar.com/news/90-percent-of-data-breaches-are-caused-by-human-error`

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science (American Association for the Advancement of Science)*, *185*(4157), 1124-1131.

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE transactions on professional communication*, *55*(4), 345-362.

Wickens, C. D., Hollands, J. G., Banbury, S., & Parasuraman, R. (2013). *Engineering psychology and human performance* (4th ed.). Pearson.