Using the Lens Model and Cognitive Continuum Theory to Understand the Effects of Cognition on Phishing Victimization

Kylie A. Molinaro
University at Buffalo
Johns Hopkins University Applied Physics Laboratory

Matthew L. Bolton
University at Buffalo

With the growing threat of phishing emails and the limited effectiveness of current mitigation approaches, there is an urgent need to better understand what leads to phishing victimization. There is a limited body of phishing research that identified cognitive automaticity as a potential factor, but more research on the relationship between user cognition and victimization is needed. Additionally, the current phishing research has not considered the characteristics of the environment in which phishing judgments are made. To fill these gaps, this work used the analysis capabilities afforded by the double system lens model (a judgment analysis technique) and the cognitive continuum theory, specifically the task continuum index and the cognitive continuum index. By calculating a task continuum index score, the cognition best suited for the email sorting task was identified. This calculation resulted in a value which indicated that more analytical cognition was most effective. The cognitive continuum index score evaluated the participants's cognition level while making judgments. The relationships between these measures and achievement were evaluated. Results indicated that more analytical cognition was associated with lower rates of phishing victimization. This work provides a deeper insight into the phishing problem and has implications for combating phishing.

INTRODUCTION

The threat phishing emails (messages designed to appear legitimate in an attempt to get individuals to reveal personal information download malicious files, or perform other compromising actions) pose to cybersecurity is a continually growing problem (Molinaro, 2019). Some of the most damaging data breaches and wire transfer frauds in recent years, like those against Ubiquiti Networks Inc. and the Scoular Co., began with a phishing attack (Krebs, 2016). The phishing problem continues to grow, with the Anti-Phishing Working Group identifying over 1.2 million separate phishing attacks in 2016, a 65% increase from 2015 (Anti-Phishing Working Group, 2017). Further, phishing attacks are the most used delivery mechanism for malware with 95% of the phishing attacks that led to a breach in 2017 being followed by software installation (Verizon, 2017).

While there are automatic detection and filtering technologies to stop phishing emails from reaching a user's inbox, these are not completely effective and cannot be relied on as the sole solution to the phishing problem (Furnell, 2009;Gupta, Tewari, Jain, & Agrawal, 2017;Sumathi & Damodaram, 2018). The human user will always be the last line of defense against phishing attacks. While there is an urgent need to understand how users are assessing the veracity of an email, little work has focused on modeling these human judgments (Pfleeger & Caputo, 2012). The work that has been done on this subject was focused on assessing susceptibility based on general individual differences (Canfield, Fischhoff, & Davis, 2016;Vishwanath, Harrison, & Ng, 2016;Wang, Herath, Chen, Vishwanath, & Rao, 2012;Williams, Beardmore, & Joinson, 2017) and detection strategies (Downs, Holbrook, & Cranor, 2006;Zielinska, Welk, Mayhorn, & Murphy-Hill, 2015).

Additionally, we (Molinaro and Bolton (2018)) assessed the effectiveness of using the lens model to understand user judgments about phishing emails. The lens model is a statistical modeling judgment analysis technique that allows analysts to understand and predict how people synthesize information sources (cues) into judgments (Brunswik, 1955;Cooksey, 1996). The lens model uses symmetric statistical models of the environment and the judgment values made by the human to evaluate judgment performance. Although our preliminary work Molinaro and Bolton (2018) provided meaningful insights, there were many analysis capabilities that we did not explore. The presented work aims to build upon the previous research by capitalizing on the additional lens model afforded analysis capabilities.

Previous research identified cognitive automaticity as a potential reason behind victimization (Vishwanath et al., 2016). However, this research has not fully considered the characteristics of the environment in which judgments are made. This includes accounting for the interaction between user cognition and task characteristics and their effects on victimization. The overlap between the lens model and the cognitive continuum theory (CCT; a human judgment theory that places cognitive modes along a continuum from intuitive to analytical cognition) suggests that the effect of automaticity (intuitive cognition in CCT terms) on phishing detection could be studied at a higher fidelity than was previously possible (Hammond, Hamm, Grassia, & Pearson, 1987). While the CCT and lens model are known for these analysis capabilities, they have not previously been used to understand the cognitive aspects of phishing judgments. The specific details of these topics are presented next.

BACKGROUND

Below, the necessary lens model and cognitive continuum theory information relevant to this research is presented.

Judgment Analysis

Judgment analysis, which is based on Egon Brunswik's probabilistic functionalism (Brunswik, 1952, 1955), is a technique for analyzing how people make judgments of distal criteria (the environment) using proximal cues (information in the environment) (Cooksey, 1996). It is based on a systems approach where the organism (people), the environment, and their relationships to environmental cues in an integrated manner (Brunswik, 1955).

Although there are multiple types of judgment analysis, this work focuses on the double system lens model (Cooksey, 1996). The double system lens model (Figure 1) uses symmetric statistical models of the environment (also called the criterion) and the judgment values made by the human to evaluate judgment performance (Hammond et al., 1987). Specifically, the same measurable environmental cues are used as predictors (independent variables) in two fitted regression models: one to the criterion (the actual value of the environmental quality that is being judged, Y_e) and one to judgment values (Y_s). The cue weights from the regression models allow analysts to compare how differently the cues factor into the prediction of the criterion (ecological validities) and the judgment (cue utilizations).

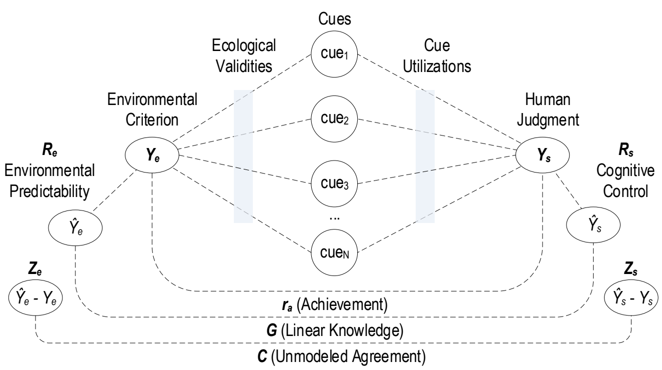

Figure 1. Graphical representation of the double system lens model.

Further, the lens model equation, originally proposed by Hursch, Hammond, and Hursch (1964) and later modified by Tucker (1964),

$$r_a = GR_eR_s + C\sqrt{1-R_e^2}\sqrt{1-R_s^2} \quad (1)$$

gives analysts a means of evaluating the achievement of the judge (how well the judge performed on the judgment task) while accounting for the different factors that affect it. r_a is the achievement of the judge represented as the correlation between the criterion (Y_e) and judgment (Y_s). Thus, achievement is measured from low to high by a value between 0 and 1. G represents linear knowledge: a measure of the correspondence between the environment and human judgment model predictions. This is measured as the correlation between $\hat{Y}_e$ and $\hat{Y}_s$. R_e is a measure of the environmental predictability, how well the model of the environment corresponds to the environmental criterion, measured as a correlation between Y_e and $\hat{Y}_e$. Similarly, R_s represents cognitive control in that it is a measure of how well the human judgment model matches the actual human judgment (the correlation between Y_s and $\hat{Y}_s$). Finally, C represents unmodeled agreement: the correspondence between the information not captured between the two models. This is measured as the correlation between the residuals of the environment model ($\hat{Y}_e - Y_e$) and the judgment model ($\hat{Y}_s - Y_s$).

The traditional lens model equation uses linear regression to create both models. For situations where the human judgment and criterion are dichotomous variables, logistic regression can be used (Hamm & Yang, 2017;Molinaro, 2019). Logistic regression requires the use of a modified lens model equation. As presented by Cooksey (1996), the modified lens model equation,

$$r_a = r_{\hat{Y}_e\hat{Y}_s}R_eR_s + C\sqrt{1-R_e^2}\sqrt{1-R_s^2} + r_{\hat{Y}_eZ_s}R_e\sqrt{1-R_s^2} + r_{Z_e\hat{Y}_s}R_s\sqrt{1-R_e^2} \quad (2)$$

defines $r_{\hat{Y}_e\hat{Y}_s}$, which represents G as the correlation between the predicted values of the criterion and judgment models, $r_{\hat{Y}_eZ_s}$ as the correlation between the criterion model's predicted values and the residuals of the judge's model, and $r_{Z_e\hat{Y}_s}$ as the correlation between the residuals of the criterion model and the predicted values of the judgment model. This gives analysts a means of using logistic regression to evaluate achievement.

Cognitive Continuum Theory

The CCT is a human judgment theory that places cognitive modes along a continuum from intuitive to analytical cognition (Hammond et al., 1987). Properties of intuitive cognition include low conscious awareness, fast data processing, low cognitive control, and high confidence in the answer, but low confidence in the method. The opposite are true for analytical cognition (Hammond et al., 1987). A fundamental aspect of the CCT is the importance of an integrated evaluation of the human making judgments and the environmental context in which the judgments are made. The environment, or task, also has properties that can be placed along the cognitive continuum. Because the basis of this theory is a continuum, the human and the task may exhibit properties of each cognition type.

Hammond et al. (1987) outlined how information provided by a lens model analysis and other measures can be combined to understand both human cognition and the cognitive implications of the task. The task continuum index (TCI) allows for the task properties to be evaluated and combined to place the task along the continuum. The task's location on the continuum provides an indication of the cognitive mode most effective for that task (Hammond et al., 1987). The cognitive continuum index (CCI) provides a means of understanding human cognition during a judgment task by placing it along the continuum from intuitive to analytical. The specifics of calculating TCI and CCI scores are discussed below in the data analysis methodology. Creating both the TCI and CCI allows for the analysis of the congruence between task and cognitive properties, and how the correspondence between TCI and CCI affects judgment accuracy. The literature has shown judgment accuracy is higher when there is a higher degree of correspondence between the judge's cognitive activity on the cognitive continuum and the task's location on the TCI (Friedman, Howell, & Jensen, 1985;Hammond et al., 1987). In other words, performance is better when the cognitive mode used by the human matches the cognitive mode most appropriate for the properties of the task.

OBJECTIVES

This work had two objectives: 1) understand and characterize the analytical and intuitive implications of a realistic email judgment task where people classified emails, and 2) characterize judge cognition and evaluate its effects with the cognitive implications of the task on achievement.

To achieve these objectives, the relevant CCT literature were used to create metrics for understanding the cognitive implications of both the task in general and for each of the participants. First, a TCI score was calculated using task characteristics, which included lens model statistics and other measures, to understand how the task influenced cognition.

> Hypothesis 1: The task will have a TCI score oriented towards the analytical side of the continuum.

Hammond et al. (1987) noted that erroneous judgments can occur when there is a large difference between the type of cognition most appropriate for the task characteristics and the type of user cognition. Because of the previous phishing literature on automaticity and victimization, it was a reasonable hypothesis that more analytical cognition was more effective for the task, resulting in a mismatch between cognition types.

For the second objective, a CCI score was calculated for each participant based on lens model statistics and other collected measures. This gave insight into each participant's cognitive mode while making judgments.

> Hypothesis 2: Achievement will be positively correlated with CCI score.

Vishwanath et al. (2016) reported higher rates of phishing victimization for participants exhibiting more automatic, or intuitive cognition. Furthermore, Hammond et al. (1987) noted that a higher CCI score corresponds to more analytical cognition. Because achievement is representative of task performance, it was hypothesized that these measures would have a significant positive correlation.

Then, the relationship between TCI score, CCI scores, and achievement were investigated.

> Hypothesis 3: Achievement will be negatively correlated with the absolute value of the difference between CCI and TCI scores.

Because the task was hypothesized to be best suited for analytical cognition and achievement was hypothesized to be positively correlated with CCI score, it was then hypothesized that there would be a negative correlation between achievement and the difference between CCI and TCI scores. Additionally, this was expected because, as previously described, mismatches between the cognition most appropriate for the task and actual human cognition can result in judgment error.

Next, the data collection and analysis methods to achieve these objectives are described.

METHODS

The data analyzed in this work were part of an existing larger dataset collected for another effort. For clarity, the following sections outline the methodology only relevant to the subset of data used for the presented research. Other analyses on these data can be found in Shonman, Li, Zhang, and Dahbura (2018); Zhang, Singh, Li, Dahbura, and Xie (2018).

Experimental Task

For the experimental task, participants were instructed that they were an administrative assistant and that the department chair, Dr. Jane Smith, asked them to sort through her emails while she was on vacation. Participants were told that the chair uses her email for many different accounts, both work and personal. Participants did not need to respond to any of the emails, only sort them into either a "keep" or "suspicious" folder. Participants also rated their confidence for each email judgment. Participants were asked to only base their judgment of the email on the information within the email and email client. Participants had 30 minutes to sort the 40 emails. Twenty emails were legitimate and 20 were phishing; participants were not aware of this distribution. All phishing emails were link-based attacks.

The experiment was conducted through Amazon Mechanical Turk. Participants interacted with Roundcube (web-based email client) to sort the emails. This allowed for realistic email interactions (e.g., hovering over links or the sender's display name and moving emails into different folders). Qualtrics was used to present task instructions and the demographics and post task questionnaires.

Participants

To keep the environmental model consistent, only participants who sorted all 40 emails were included, resulting in 74 participants. Participants averaged around 34 years of age, with a median of 31.5 years, a maximum of 61 years, and a minimum of 20 years. Fifty-five participants identified as male and 19 identified as female. All but one participant reported English as their native language. Seventy participants reported not currently being a student. Seven participants reported having previously completed network engineering and/or cybersecurity courses or certifications.

Independent Variables

The criterion for each email was coded as a dichotomous variable, where an email was either a phishing email (coded as 1) or not (coded as 0). Phishing cues were also coded as dichotomous variables for each email, where a 1 meant the cue was present and 0 meant it was not (see Molinaro (2019) for detailed cue descriptions).

The emails were presented in a random order for each participant. All emails were created from real emails with only personally identifiable information modified to prevent the distribution of any personal data. Legitimate emails were derived from actual emails received by the research team. Phishing emails were derived from a semi-random sample of emails in Cornell University's "Phish Bowl" database[1].

Dependent Measures

Dependent measures included the judgment the participants made about an email: 1 if the participant moved the email to the suspicious folder and 0 if the email was moved to the keep folder. Participants also reported a judgment confidence rating for each email judgment on a scale from not at all confident (1) to extremely confident (10) with increments of one. The time to complete the email sorting task was also collected.

Data Analysis

Nine cues were included in the lens model analyses: spelling and grammar errors, generic greeting, URL hyperlinking, lack of signer details, requests for personal information, suspicious sender, poor overall design, suspicious link, and use of time pressure/threatening language. It should be noted that URL hyperlinking represented whether or not the

[1]https://it.cornell.edu/phish-bowl

URL in the email was hyperlinked, while suspicious link represented whether or not the actual link URL was suspicious. On average, there were more cues present in the phishing emails ($M = 5.350$, $SD = 1.089$) compared to the legitimate emails ($M = 2.500$, $SD = 0.889$). Because both the criterion and human judgment were dichotomous variables, logistic regression, with the modified lens model equation (Equation 2), was used.

Cognitive Continuum Theory Analyses. The TCI score was calculated using measures standard in the literature and that were available in the existing dataset (Dunwoody, Haarbauer, Mahan, Marino, & Chu-Chun, 2000;Hammond et al., 1987). These measures were the number of cues, the redundancy among cues (average inter-cue correlation), the standard deviation of cue weights, the degree of nonlinearity in the organizing principle, and the degree of certainty in the task system (R_e^2). The degree of nonlinearity in the organizing principle was measured by taking the difference in R^2 values of a linear and nonlinear model of the environment. TCI score calculation used a modified version of the equation presented by Dunwoody et al. (2000), which standardized and averaged the measures:

$$TCI = \frac{(10-n) + 10\cdot(1-r) + 10\cdot SD + 10\cdot L + 10\cdot R^2}{5} \quad (3)$$

This combined the measures listed above, where n was the number of cues, r was cue redundancy, SD was the standard deviation of cue weights in the criterion model, L was the degree of nonlinearity in the organizing principle, and R^2 was the degree of certainty in the task system. This work used a modified version of the Dunwoody et al. (2000) TCI equation, because the original equation did not include the degree of nonlinearity in the organizing principle. It was important to include this measure to ensure all applicable task characteristics were included in the TCI score calculation. Because the number of cues varies by email, the TCI score calculation used the average number of cues across the 40 emails.

It was hypothesized that the TCI score would be oriented towards the analytical side of the index. The TCI is scaled from 1-10 meaning a score greater than five would indicate more analytical cognition as most effective for the task.

A CCI score was calculated for each participant using standardized measures that were available in the existing dataset. These measures included cognitive control (R_s), the degree of nonlinearity in the judge's organizing principle, response rate, overestimation, and overprecision. The degree of nonlinearity in the judge's organizing principle was calculated by taking the difference in R^2 values of a linear and nonlinear model of the judge. Overestimation is the difference between perceived accuracy and actual accuracy. Overprecision is the difference between average judgment confidence and judgment accuracy. These measures were deemed appropriate based on the CCT literature and the availability of data. Cognitive control, the degree of nonlinearity in the judge's organizing principle, and response rate are standard measures used in the CCI score calculation (Dunwoody et al., 2000;Hammond et al., 1987). The error distribution is also a common measure in the CCI score calculation, but was not appropriate for this work because both the criterion and judgment were dichotomous. Additionally, the existing dataset did not include necessary data to include self-insight into policy or differential confidence (Dunwoody et al., 2000;Hammond et al., 1987). Because the dataset included each judge's perceived overall accuracy and a judgment confidence rating for each judgment, this work included measures identified in the phishing literature (overestimation and overprecision) shown to affect cognition in the CCI score calculations (Wang, Li, & Rao, 2016). Wang et al. (2016) reported that, as overestimation and overprecision increased, cognitive effort decreased. As is standard for a CCI score calculation, each measure was linearly transformed into a 1-10 scale and then averaged together (Dunwoody et al., 2000;Hammond et al., 1987). Because of their inverse relationship with cognition as compared to the other measures, overestimation and overprecision were reversed before transformation (Wang et al., 2016).

It was hypothesized that there would be a significant, positive relationship between achievement and CCI score. To test this, a Pearson correlation coefficient was computed between achievement and CCI score.

Because large differences between CCI and TCI scores may lead to incorrect judgments (Hammond et al., 1987), the absolute value of the difference between CCI and TCI scores was calculated with,

$$Dif_i = |CCI_i - TCI| \quad (4)$$

where i represented the participant.

It was hypothesized that there would be a significant, negative relationship between achievement and the value of Dif_i. To test this, a Pearson correlation coefficient was computed between achievement and Dif_i values.

RESULTS

Using Equation 3, where $n = 3.925$, $r = 0.066$, $SD = 1.233$, $L = 0.124$, and $R^2 = 0.889$, the overall TCI score was 7.574. This result supports hypothesis 1 which stated that the email sorting task would have a TCI score oriented towards the analytical side of the continuum.

A CCI score was calculated for each participant ($M = 5.505$, $SD = 1.248$, $Med = 5.542$, $Min = 3.113$, and $Max = 8.267$). To understand the relationship between achievement and CCI score, a Pearson correlation was conducted. Results of the Pearson correlation indicated that there was a strong significant positive association between achievement and CCI score, ($r(72) = 0.744$, $p < 0.001$). This result supports hypothesis 2: that achievement would be positively correlated with CCI score.

The absolute value of the difference between CCI and TCI scores (Dif_i) was calculated for each participant ($M = 2.100$, $SD = 1.194$, $Med = 2.032$, $Min = 0.013$, and $Max = 4.461$). To understand the relationship between achievement and Dif_i, a Pearson correlation was conducted. Results of the Pearson correlation indicated that there was a strong significant negative association between achievement and Dif_i, ($r(72) = -0.741$, $p < 0.001$). This result supports hypothesis 3: that achievement would be negatively correlated with Dif_i.

DISCUSSION AND CONCLUSION

These results provide insight into numerous aspects of the phishing problem. The cognition of participants, the cognitive implications of the task, and their effects on achievement are better understood. Because the CCI score was positively correlated with achievement, the relationship between automaticity and phishing victimization posited in Vishwanath et al. (2016) was supported. This means that participants with higher CCI scores, or those who exhibited more analytical cognition, performed significantly better than participants with lower, or more intuitive, CCI scores. This is a significant finding because of the limited research on the topic and the novel data analysis approach used in this work. Evaluating both the task characteristics and judges provided a more comprehensive understanding of the problem. TCI score calculations resulted in a value that indicated that more analytical cognition was most effective for the task. This is important when considering that CCT literature indicates that achievement is higher when judge cognition is similar to the cognitive mode most appropriate for the task (Friedman et al., 1985;Hammond et al., 1987). Because achievement was negatively correlated with Dif_i, this conclusion also holds true. These results provide valuable insight into how phishing victimization can result from the interaction between task characteristics and user cognition.

Although this work presents only a portion of the capabilities afforded by the CCT and the lens model (see Molinaro (2019) for additional analyses), the results have implications for combating phishing. Manipulations to the user interface can be used to move users' cognition towards the cognition most effective for the task. This is important considering that the results indicated that the task was best suited for more analytical cognition and that achievement was positively correlated with CCI scores. Thus, it would be expected that interface changes which promote more analytical cognition would result in better task performance. Additionally, a similar email sorting task could be used as a screening protocol by an organization. This would identify the users who exhibit more intuitive cognition and thus, are more likely to be victimized. This, along with a detailed evaluation of the specific ecological validity and utilization of each phishing cue, would allow for customized and directed training.

While the distribution of emails in the experiment was consistent with previous phishing research, future work should should investigate more realistic distributions (Canfield et al., 2016;Dhamija, Tygar, & Hearst, 2006).

Overall, this work builds upon the previous phishing literature by evaluating the posited relationship between automaticity and victimization using a novel approach. Applying the CCT and the lens model to the phishing domain provides a deeper and more comprehensive understanding of the problem. Future work should continue to capitalize on the analysis capabilities afforded by these techniques to inform the design of more effective phishing mitigation approaches.

ACKNOWLEDGMENTS

The authors would like to thank Dr. Anton Dahbura and Dr. Xiangyang Li from the Johns Hopkins University Information Security Institute and Dr. Nathan Bos from the Johns Hopkins University Applied Physics Laboratory for allowing them to use the data collected under the National Science Foundation Award 1544493 for the work presented here.

REFERENCES

Anti-Phishing Working Group. (2017, feb). *Phishing activity trends report 4th quarter 2016.* http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf.

Brunswik, E. (1952). The conceptual framework of psychology. *Psychological Bulletin*, *49*(6), 654–656.

Brunswik, E. (1955). Representative design and probabilistic theory in a functional psychology. *Psychological Review*, *62*(3), 193–217.

Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying phishing susceptibility for detection and behavior decisions. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *58*(8), 1158–1172.

Cooksey, R. W. (1996). *Judgment analysis: Theory, methods, and applications*. Academic Press.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In *Proceedings of the sigchi conference on human factors in computing systems* (pp. 581–590).

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. In *Proceedings of the second symposium on usable privacy and security* (pp. 79–90).

Dunwoody, P. T., Haarbauer, E., Mahan, R. P., Marino, C., & Chu-Chun, T. (2000). Cognitive adaptation and its consequences: A test of cognitive continuum theory. *Journal of Behavioral Decision Making*, *13*(1), 35–54.

Friedman, L., Howell, W. C., & Jensen, C. R. (1985). Diagnostic judgment as a function of the preprocessing of evidence. *Human Factors*, *27*(6), 665–673.

Furnell, S. M. (2009). The irreversible march of technology. *Information Security Technical Report*, *14*(4), 176–180.

Gupta, B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, *28*(12), 3629–3654.

Hamm, R. M., & Yang, H. (2017). Alternative lens model equations for dichotomous judgments about dichotomous criteria. *Journal of Behavioral Decision Making*, *30*(2), 527–532.

Hammond, K. R., Hamm, R. M., Grassia, J., & Pearson, T. (1987). Direct comparison of the efficacy of intuitive and analytical cognition in expert judgment. *IEEE Transactions on Systems, Man, and Cybernetics*, *17*(5), 753–770.

Hursch, C. J., Hammond, K. R., & Hursch, J. L. (1964). Some methodological considerations in multiple-cue probability studies. *Psychological Review*, *71*(1), 42–60.

Krebs, B. (2016, Apr). *FBI: 2.3 billion lost to ceo email scams.* https://krebsonsecurity.com/2016/04/fbi-2-3-billion-lost-to-ceo-email-scams/.

Molinaro, K. A. (2019). *Understanding the phish: Using judgment analysis to evaluate the human judgment of phishing emails* (Unpublished doctoral dissertation). State University of New York at Buffalo.

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. (10.1016/j.cose.2018.03.012)

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, *31*(4), 597–611.

Shonman, M., Li, X., Zhang, H., & Dahbura, A. (2018). Simulating phishing email processing with instance-based learning and cognitive chunk activation. In *International conference on brain informatics* (pp. 468–478).

Sumathi, K., & Damodaram, R. (2018). Survey and analysis on phishing detection techniques. *International Journal of Advanced Research in Computer Science*, *9*(1), 270–275.

Tucker, L. R. (1964). A suggested alternative formulation in the developments by Hursch, Hammond, and Hursch, and by Hammond, Hursch, and Todd. *Psychological Review*, *71*(6), 528–530.

Verizon. (2017). *2017 data breach investigations report 10th edition.* http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.

Vishwanath, A., Harrison, B., & Ng, Y. J. (2016). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*.

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication*, *55*(4), 345–362.

Wang, J., Li, Y., & Rao, H. R. (2016). Overconfidence in phishing email detection. *Journal of the Association for Information Systems*, *17*(11), 759–783.

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, *72*, 412–421.

Zhang, H., Singh, S., Li, X., Dahbura, A., & Xie, M. (2018). Multitasking and monetary incentive in a realistic phishing study. In *British human computer interaction conference.*

Zielinska, O. A., Welk, A. K., Mayhorn, C. B., & Murphy-Hill, E. (2015). Exploring expert and novice mental models of phishing. In *Proceedings of the human factors and ergonomics society annual meeting* (Vol. 59, pp. 1132–1136).