Acknowledgement. We acknowledge National Science Foundation (NSF) to partially sponsor the work under grants #1620868, #1620871, #1620862, and #1651280. We also thank the Florida Center for Cybersecurity for a seed grant. Moreover, we thank the JHU team that provided their study design document with some data used in this research. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied of NSF.

References

[1] Li, Y., Xiong, K. and Li, X. (2019) An analysis of user behaviors in phishing email using machine learning techniques. In *Proceedings of The 16th International Conference on Security and Cryptography (SECRYPT) and the 16th International Joint Conference on e-Business and Telecommunications* (ICETE).

[2] (Accessed May 13, 2018) *Gartner survey shows phishing attacks escalated in 2007; More Than 3 Billion Lost to These Attacks*. https://www.gartner.com/newsroom/id/565125.

[3] Almomani, A., Gupta, B., Atawneh, S., Meulenberg, A. and Almomani, E. (2013) A survey of phishing email filtering techniques. *IEEE communications surveys & tutorials* **15**(4): 2070–2090.

[4] Chin, T.J., Xiong, K. and Hu, C. (2018) Phishlimiter: A phishing detection and mitigation approach using software-defined networking. In *IEEE Access*.

[5] Puthal, D., Nepal, S., Ranjan, R. and Chen, J. (2017) A dynamic prime number based efficient security mechanism for big sensing data streams. *Journal of Computer and System Sciences* **83**(1): 22–42.

[6] Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L.F., Hong, J. and Nunge, E. (2007) Protecting people from phishing: the design and evaluation of an embedded training email system. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (ACM): 905–914.

[7] Downs, J.S., Holbrook, M. and Cranor, L.F. (2007) Behavioral response to phishing risk. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (ACM).

[8] Arachchilage, N.A. and Cole, M. (2011) Design a mobile game for home computer users to prevent from "phishing attacks". In *International Conference on Information Society (i-Society)* (IEEE): 485–489.

[9] Kirlappos, I. and Sasse, M.A. (2012) Security education against phishing: A modest proposal for a major rethink. *IEEE Security & Privacy, 2012* **10**(2).

[10] Yang, W., Chen, J., Xiong, A., Proctor, R.W. and Li, N. (2015) Effectiveness of a phishing warning in field settings. In *Proceedings of the Symposium and Bootcamp on the Science of Security* (ACM): 14.

[11] Brase, G.L. (2009) How different types of participant payments alter task performance. *Judgment and Decision Making* **4**(5): 419.

[12] Drake, C.E., Oliver, J.J. and Koontz, E.J. (Accessed Jan 20, 2020) *Anatomy of a Phishing Email*. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.59.9431&rep=rep1&type=pdf.

[13] Hong, J. (2012) The state of phishing attacks. *Communications of the ACM* **55**(1): 74–81.

[14] Wang, J., Herath, T., Chen, R., Vishwanath, A. and 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.

[15] Jang-Jaccard, J. and Nepal, S. (2014) A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences* **80**(5): 973–993.

[16] Vishwanath, A., Herath, T., Chen, R., Wang, J. and Rao, H.R. (2011) Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, Elsevier, 2011*, **51**(3).

[17] Dhamija, R., Tygar, J.D. and Hearst, M. (2006) Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (ACM).

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

[19] Alnajim, A. and Munro, M. (2009) An anti-phishing approach that uses training intervention for phishing websites detection. In *Sixth International Conference on Information Technology: New Generations* (IEEE): 405–410.

[20] Burns, M.B., Durcikova, A. and Jenkins, J.L. (2013) What kind of interventions can help users from falling for phishing attempts: a research proposal for examining stage-appropriate interventions. In *46th Hawaii International Conference on System Sciences (HICSS)* (IEEE): 4023–4032.

[21] Liang, H. and Xue, Y. (2010) Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 2010*, **11**(7).

[22] Wu, M., Miller, R.C. and Garfinkel, S.L. (2006) Do security toolbars actually prevent phishing attacks? In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (ACM).

[23] Downs, J.S., Holbrook, M.B. and Cranor, L.F. (2006) Decision strategies and susceptibility to phishing. In *Proceedings of the second symposium on Usable privacy and security* (ACM).

[24] Stuart, L.M., Park, G., Talor, J.M. and Raskin, V. (2014) On identifying phishing emails: Uncertainty in machine and human judgment. In *IEEE Conference on Norbert Wiener in the 21st Century (21CW)* (IEEE): 1–8.

[25] Ma, L., Torney, R., Watters, P. and Brown, S. (2009) Automatically generating classifier for phishing email prediction. In *10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN)* (IEEE): 779–783.

[26] Smadi, S., Aslam, N., Zhang, L., Alasem, R. and Hossain, M. (2015) Detection of phishing emails using data mining algorithms. In *9th International Conference on Software, Knowledge, Information Management and Applications (SKIMA)* (IEEE): 1–8.

[27] Shirazi, H., Haefner, K. and Ray, I. (2017) Fresh-phish: A framework for auto-detection of phishing websites. In *IEEE International Conference on Information Reuse and Integration (IRI)* (IEEE): 137–143.

[28] Zeng, Y.G. (2017) Identifying email threats using predictive analysis. In *International Conference on Cyber Security And Protection Of Digital Services (Cyber Security)* (IEEE): 1–2.

[29] Şentürk, Ş., Yerli, E. and Soğukpinar, İ. (2017) Email phishing detection and prevention by using data mining techniques. In *International Conference on Computer Science and Engineering (UBMK)* (IEEE): 707–712.

[30] Park, G., Stuart, L.M., Taylor, J.M. and Raskin, V. (2014) Comparing machine and human ability to detect phishing emails. In *IEEE International Conference on Systems, Man and Cybernetics (SMC)* (IEEE): 2322–2327.

[31] Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M.A. and Pham, T. (2009) School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of Symposium On Usable Privacy and Security (SOUP)* (ACM).

[32] Kawakami, M., Yasuda, H. and Sasaki, R. (2010) Development of an E-learning content-making system for information security (ELSEC) and its application to anti-phishing education. In *International Conference on E-Education, E-Business, E-Management, and E-Learning* (IEEE): 7–11.

[33] Tseng, S.S., Chen, K.Y., Lee, T.J. and Weng, J.F. (2011) Automatic content generation for anti-phishing education game. In *Proceedings of International Conference on Electrical and Computer Engineering (ICECE)* (IEEE).

[34] Stembert, N., Padmos, A., Bargh, M.S., Choenni, S. and Jansen, F. (2015) A study of preventing email (spear) phishing by enabling human intelligence. In *Intelligence and Security Informatics Conference* (IEEE).

[35] Underhay, L., Pretorius, A. and Ojo, S. (2016) Game-based enabled E-learning model for E-Safety education. In *IST-Africa Week Conference* (IEEE).

[36] Muthal, S., Li, S., Huang, Y., Li, X., Dahbura, A., Bos, N. and Molinaro, K. (2017) A phishing study of user behavior with incentive and informed intervention. In *Proceedings of the National Cyber Summit*.

[37] (Accessed February 10, 2018) *Phish Bowl Database*. https://it.cornell.edu/phish-bowl.

[38] (Accessed February 5, 2018) *Amazon Mechanical Turk - Welcome - MTurk*. https://www.mturk.com/mturk/welcome.

[39] Ping Liang and Kaiqi Xiong (1999) On the analysis of neural networks with asymmetric connection weights or noninvertible transfer functions. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)* **29**(5): 632–636.

[40] Sontag, E.D. (1998) VC dimension of neural networks. In *NATO ASI Series F Computer and Systems Sciences*.

[41] Chin, T., Xiong, K., Hu, C. and Li, Y. (2018) A machine learning framework for studying domain generation algorithm (DGA)-based malware. In *International Conference on Security and Privacy in Communication Systems* (Springer): 433–448.

[42] Li, Y., Xiong, K., Chin, T. and Hu, C. (2019) A machine learning framework for domain generation algorithm-based malware detection. *IEEE Access* **7**: 32765–32782.

APPENDICES

A. ON-SITE STUDY SURVEY QUESTIONS:

Age	Age
Gender	Gender
Native_Spk	Are you a native English speaker?
Edu1	Are you currently, or have you previously been enrolled in a computer science/engineering or cybersecurity related degree program?
Edu2	Have you taken any cybersecurity courses?
Habit1	How often do you check your social media accounts?
Habit2	How often do you check your emails?
SelfEff1	Please rate your agreement with the following: I am very confident with my computer skills.
SelfEff2	Please rate your agreement with the following: I consider myself to be a cybersecurity expert.
SelfEff3	I feel confident in my ability to determine which emails are legitimate.
SelfEff4	I believe I was successful in the email sorting task.
Susp1	I was not generally suspicious of the emails.
Susp2	I generally noticed nothing unfamiliar about the emails.
Susp3	Overall, I thought that clicking on links/attachments would not make me vulnerable.
HP1	I skimmed through the emails.
HP2	I briefly looked at the sender/source of the emails.
HP3	I ignored the message content of the emails.
SP1	I thought about the action I took based on what I saw in the email.
SP2	I found myself making connections between the emails' requests and what I have heard about emails requesting such information.
SP3	I spent some time thinking about the request before I made my decision.
RB1	The risk of a security compromise is a lot less on a public computer than your personal computer.
RB2	The risk of a security compromise is a lot more when you click on a link in an email than when you respond to it.
HabStgth1	Checking messages and social media are something I start doing before I realize I'm doing it.

HabStgth2	Checking messages and social media are something I have been doing for a long time.
HabStgth3	Checking messages and social media are something I do automatically.
HabStgth4	Checking messages and social media belong in my daily routine.
HabStgth5	I feel my social media use and the amount of time spent checking messages has gotten out of control.
HabStgth6	I have tried unsuccessfully to cut down the amount of time I spend checking my messages and social media.
HabStgth7	I feel anxious when I am offline without access to messages and social media for an extended period of time.
Study_Know	How did you come to know about our study?

B. ONLINE STUDY SURVEY QUESTIONS:

Pre-Survey Questions:

Age	Age
Gender	Gender
Native_Spk	Are you a native English speaker?
Student	Are you currently a student?
Degree_program	What degree program are you currently enrolled in?
Highest_education	What is your highest level of completed education?
Completed_degrees	What is(are) your completed degree(s) in?
Cyber_experience	Have you completed any network engineering and/or cybersecurity courses or certifications?
Cyber_courses	Please list the cybersecurity courses/certifications you have taken.
Comp_type	What type of computer are you using to complete this experiment?
Input_type	Are you controlling the cursor with an external mouse or a trackpad?
Computer_agreement_1	I am very confident with my computer skills.
Computer_agreement_2	I consider myself to be a cybersecurity expert.
Beliefs_agreement_1	The risk of getting a computer virus is a lot less on a public computer than your personal computer.

Beliefs_agreement_2	The risk of getting a computer virus is a lot less on a mobile device than on a computer.
Beliefs_agreement_3	The risk of getting a computer virus is a lot more when you click on a link in an email than when you open an attachment.
Beliefs_agreement_4	Only Windows machines can get a computer virus.
Beliefs_agreement_5	If you have antivirus or anti-malware software, your computer is completely safe.
Email_habits_agreeme_1	Checking email is something I do frequently.
Email_habits_agreeme_2	Checking email is something I do without having to consciously remember.
Email_habits_agreeme_3	Checking email is something I have no need to think about doing.
Email_habits_agreeme_4	Checking email is something I start doing before I realize I'm doing it.
Email_habits_agreeme_5	Checking email is something I would find hard not to do.
Email_habits_agreeme_6	Checking email is something I have been doing for a long time.
Email_habits_agreeme_7	Checking email is something I do automatically.
Email_habits_agreeme_8	Checking email belongs in my daily routine.
SM_habits_agreement_1	Checking social media is something I do frequently.
SM_habits_agreement_2	Checking social media is something I do without having to consciously remember.
SM_habits_agreement_3	Checking social media is something I have no need to think about doing.
SM_habits_agreement_4	Checking social media is something I start doing before I realize I'm doing it.
SM_habits_agreement_5	Checking social media is something I would find hard not to do.
SM_habits_agreement_6	Checking social media is something I have been doing for a long time.
SM_habits_agreement_7	Checking social media is something I do automatically.
SM_habits_agreement_8	Checking social media belongs in my daily routine.
email_reg_agreement_1	I feel my email use has gotten out of control.
email_reg_agreement_2	I have tried unsuccessfully to cut down the amount of time I spend checking my email.
email_reg_agreement_3	I feel anxious when I am offline without access to email for an extended period of time.

SM_reg_agreement_1	I feel my social media use has gotten out of control.
SM_reg_agreement_2	I have tried unsuccessfully to cut down the amount of time I spend checking my social media.
SM_reg_agreement_3	I feel anxious when I am offline without access to social media for an extended period of time.

Post-Survey Questions:

Sort_correct_1	How many emails do you think you sorted correctly?
Sort_confident_1	How confident are you in your assessment of the number of correctly sorted emails?
Sort_agreement_1	I felt hurried and rushed when sorting emails.
Sort_agreement_2	Completing the email sorting task was mentally demanding.
Sort_agreement_3	It took a lot of effort to sort emails.
Sort_agreement_4	I felt irritated and stressed while sorting emails.
Sort_agreement_5	I spent more time thinking about each email while doing this task than I usually would.
Strat_gen	What is your general strategy for determining if an email was legitimate?
Strat_cues1_1	Importance of Sender Display Name
Strat_cues1_2	Importance of Sender Email Address
Strat_cues1_4	Importance of Hyperlinked URL
Strat_cues1_5	Importance of HTTPS in URL
Strat_cues2_1	Importance of Amount of Logos/Branding
Strat_cues2_2	Importance of Overall Design/Formatting
Strat_cues2_5	Importance of In-email Security Scanning Notices/Indicators
Strat_cues3_1	Importance of Spelling and Grammar Errors
Strat_cues3_2	Importance of Lack of Personalization
Strat_cues3_3	Importance of Type of Information Requested
Strat_cues3_5	Importance of Use of Time Pressure (ex. "you have 24hrs to respond")
Strat_cues3_6	Importance of Use of Threats (ex. threatening legal action)
Strat_cues3_7	Importance of Too Good to be True Offers (ex. you won $4,000,000)

Incent_strat	Did the possibility for a financial incentive change your strategy for identifying suspicious emails?
Incent_strat_change	How did your strategy change?
Incent_agreement_1	I spent more time thinking about each email while doing this task than I usually would.
BFI_BFI_1	I am someone who: Is talkative
BFI_BFI_2	I am someone who: Tends to find fault with others
BFI_BFI_3	I am someone who: Does a thorough job
BFI_BFI_4	I am someone who: Is depressed, blue
BFI_BFI_5	I am someone who: Is original, comes up with new ideas
BFI_BFI_6	I am someone who: Is reserved
BFI_BFI_7	I am someone who: Is helpful and unselfish with others
BFI_BFI_8	I am someone who: Can be somewhat careless
BFI_BFI_9	I am someone who: Is relaxed, handles stress well
BFI_BFI_10	I am someone who: Is curious about many different things
BFI_BFI_11	I am someone who: Is full of energy
BFI_BFI_12	I am someone who: Starts quarrels with others
BFI_BFI_13	I am someone who: Is a reliable worker
BFI_BFI_14	I am someone who: Can be tense
BFI_BFI_15	I am someone who: Is ingenious, a deep thinker
BFI_BFI_16	I am someone who: Generates a lot of enthusiasm
BFI_BFI_17	I am someone who: Has a forgiving nature
BFI_BFI_18	I am someone who: Tends to be disorganized
BFI_BFI_19	I am someone who: Worries a lot
BFI_BFI_20	I am someone who: Has an active imagination
BFI_BFI_21	I am someone who: Tends to be quiet
BFI_BFI_22	I am someone who: Is generally trusting
BFI_BFI_23	I am someone who: Tends to be lazy
BFI_BFI_24	I am someone who: Is emotionally stable, not easily upset

BFI_BFI_25	I am someone who: Is inventive
BFI_BFI_26	I am someone who: Has an assertive personality
BFI_BFI_27	I am someone who: Can be cold and aloof
BFI_BFI_28	I am someone who: Perseveres until the task is finished
BFI_BFI_29	I am someone who: Can be moody
BFI_BFI_30	I am someone who: Values artistic, aesthetic experiences
BFI_BFI_31	I am someone who: Is sometimes shy, inhibited
BFI_BFI_32	I am someone who: Is considerate and kind to almost everyone
BFI_BFI_33	I am someone who: Does things efficiently
BFI_BFI_34	I am someone who: Remains calm in tense situations
BFI_BFI_35	I am someone who: Prefers work that is routine
BFI_BFI_36	I am someone who: Is outgoing, sociable
BFI_BFI_37	I am someone who: Is sometimes rude to others
BFI_BFI_38	I am someone who: Makes plans and follows through with them
BFI_BFI_39	I am someone who: Gets nervous easily
BFI_BFI_40	I am someone who: Likes to reflect, play with ideas
BFI_BFI_41	I am someone who: Has few artistic interests
BFI_BFI_42	I am someone who: Likes to cooperate with others
BFI_BFI_43	I am someone who: Is easily distracted
BFI_BFI_44	I am someone who: Is sophisticated in art, music, or literature

C. Attributes in All Experiments:

Attributes Name:	**Description**	**Study**
Performance Score	Overall performances for the participants	Both
Condition	Condition 0 means this participant did not have monetary incentive, and condition 1 means the participant had monetary incentive	Both
Intervention	In round two, which type of phishing email we gave as an intervention based on the participants' performance of the first round	On-site
R1_P1_Time	Time used for sorting the phishing type 1 emails in round 1	On-site

R1_P1_Score	Score got for sorting the phishing type 1 emails in round 1	On-site
R1_P2_Time	Time used for sorting the phishing type 2 emails in round 1	On-site
R1_P2_Score	Score got for sorting the phishing type 2 emails in round 1	On-site
R1_P3_Time	Time used for sorting the phishing type 3 emails in round 1	On-site
R1_P3_Score	Score got for sorting the phishing type 3 emails in round 1	On-site
R1_Nr_Time	Time used for sorting the normal emails in round 1	On-site
R1_Nr_Score	Score got for sorting the normal emails in round 1	On-site
R1_Time	Time used for sorting all the emails in round 1	On-site
R1_Score	Score got for sorting all the emails in round 1	On-site
R2_P1_Time	Time used for sorting the phishing type 1 emails in round 2	On-site
R2_P1_Score	Score got for sorting the phishing type 1 emails in round 2	On-site
R2_P2_Time	Time used for sorting the phishing type 2 emails in round 2	On-site
R2_P2_Score	Score got for sorting the phishing type 2 emails in round 2	On-site
R2_P3_Time	Time used for sorting the phishing type 3 emails in round 2	On-site
R2_P3_Score	Score got for sorting the phishing type 3 emails in round 2	On-site
R2_Nr_Time	Time used for sorting the normal emails in round 2	On-site
R2_Nr_Score	Score got for sorting the normal emails in round 2	On-site
R2_Time	Time used for sorting all the emails in round 2	On-site
R2_Score	Score got for sorting all the emails in round 2	On-site
R3_P1_Time	Time used for sorting the phishing type 1 emails in round 3	On-site
R3_P1_Score	Score got for sorting the phishing type 1 emails in round 3	On-site
R3_P2_Time	Time used for sorting the phishing type 2 emails in round 3	On-site
R3_P2_Score	Score got for sorting the phishing type 2 emails in round 3	On-site
R3_P3_Time	Time used for sorting the phishing type 3 emails in round 3	On-site
R3_P3_Score	Score got for sorting the phishing type 3 emails in round 3	On-site
R3_Nr_Time	Time used for sorting the normal emails in round 3	On-site
R3_Nr_Score	Score got for sorting the normal emails in round 3	On-site
R3_Time	Time used for sorting all the emails in round 3	On-site
R3_Score	Score got for sorting all the emails in round 3	On-site

R1_Phis_Time	Time used for sorting all phishing emails in round 1	On-site
R1_Phis_Score	Score got for sorting all phishing emails in round 1	On-site
R2_Phis_Time	Time used for sorting all phishing emails in round 2	On-site
R2_Phis_Score	Score got for sorting all phishing emails in round 2	On-site
R3_Phis_Time	Time used for sorting all phishing emails in round 3	On-site
R3_Phis_Score	Score got for sorting all phishing emails in round 3	On-site
Num_sorted	The number of all emails that have been sorted in the task	Online
Phis_sorted	The number of phishing emails that have been sorted	Online
Phis_accuracy	The accuracy of phishing emails that have been sorted	Online
Nr_sorted	The number of normal emails that have been sorted	Online
Nr_accuracy	The accuracy of normal emails that have been sorted	Online
Pay	The amount money paid to participants	Online
Avg_rating	The average rating of confidence level	Online
Median_rating	The median rating of confidence level	Online
All_percent	The ratio of correctly sorted emails to all emails	Online
Phis_percent	The ratio of correctly sorted phishing emails to all emails	Online
Nr_percent	The ratio of correctly sorted normal emails to all emails	Online

Note: The attributes of survey questions can be found in Appendices A and B.