2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)
Banff Center, Banff, Canada, October 5-8, 2017

"To Click or Not to Click is the Question": Fraudulent URL Identification Accuracy in a Community Sample

Ed Pearson III, Cindy L. Bethel
Department of Computer Science and Engineering
Mississippi State University
Mississippi State, Mississippi 39762
Email: ep602@msstate.edu, cbethel@cse.msstate.edu

Andrew F. Jarosz, Mitchell E. Berman
Department of Psychology
Mississippi State University
Mississippi State, Mississippi 39762
Email: afj62@msstate.edu, mberman@pschology.msstate.edu

***Abstract*—Technology is in a constant state of evolution, which allows for new and cunning cyber-attacks and tactics. Out of all these tactics, the exploitation of human cognitive biases in response to phishing attacks is challenging to defend against. The purpose of this study was to determine if humans could discriminate fraudulent Uniform Resource Locators (URLs) or links from legitimate URLs without the aid of specific hardware or software. We also explored whether simple textual manipulations were easier to detect compared to complex manipulations. Participants (N = 1044) completed the following: (1) A demographic questionnaire including their internet and email usage, (2) a role-playing exercise where participants were shown a series of emails from an inbox and had to select the action(s) that they would take, and (3) a series of questions related to technology and security to assess their prior knowledge and awareness of phishing. Results indicated that it was difficult for participants to correctly identify URLs when checking email. Results also revealed that difficulty in detecting simple textual manipulations versus complex manipulations was category dependent.**

***Index Terms*—phishing, social engineering, human-computer interaction and security (HCI-Sec/HCI-S), information security.**

I. Introduction

We live in an era where social networking is perfectly acceptable if not the preferred form of communication. Even in those rare cases that a person does not belong to a social network, he or she will likely have an email account. In essence, most humans exist in cyberspace. Because of this fact, technology has made tremendous advancements with software and hardware defenses against malicious attacks. However, malicious attackers have made advancements of their own, which exploit a vulnerability that has not been accounted for in existing cyber-security systems. Attackers are now capitalizing on social engineering, which is the process of persuading an individual to commit some action or divulge some information [1]. The most common form of social engineering is a phishing attack. The severity of phishing has become a hot topic of discussion in cyber-security. The realm of cognitive science offers some explanations as to why so many of the common methods of deception used in phishing are so successful. The results from this study can contribute to the design and development of human defense mechanisms against phishing. These results can be used to improve *Standard Operating Procedures (SOPs)* related to internet and network use.

A. Social Engineering

Jared Kee [1] proposed six vectors to successfully conduct social engineering: (1) telephone, (2) online, (3) dumpster diving, (4) shoulder surfing, (5) reverse social engineering, and (6) persuasion; which are used as mechanisms to accomplish social engineering. The telephone (both mobile and land lines) can be used to obtain confidential information or convince a person to perform some action. Online consists of compiling or coaxing information from users via internet chat sessions, emails, or any means of communication that requires the internet or a network. Dumpster diving implies searching for or obtaining information from rejected materials, literally rummaging through a person's trash. Shoulder surfing refers to gathering information by silently peering over an individual's shoulder; this strategy may be used from both close and long-range distances. Reverse social engineering is achieved when the attacker succeeds in getting the victim to make the initial contact with the attacking entity. This in turn increases the degree of difficulty for the victim to establish the legitimacy of the interaction. Persuasion results from gathering information from a person through deception or just plain asking for it [1].

B. Phishing

Phishing is a semantic attack where victims are deceived by fabricated emails, fraudulent websites, spoofed phone calls, and so on. Though phishing can be achieved through multiple vectors; forged emails and counterfeit websites seem to be the most popular approaches [2][3][4][5][6]. Based on a report released in 2014 by the Federal Bureau of Investigation Internet Crime Complaint Center [7], the total number of internet crime-related complaints reported was 269,422, with 123,684 of those cases reported losses of $800,492,073 [7].

Proofpoint [8] reported that 76% of Information Technology (IT) security personnel and operations staff have been victims of malware, with 95% of those threats derived from phishing

emails. A key result from this report was that even IT professionals were vulnerable, whether by accident or intent, to clicking on malicious links. In addition, about ten percent of users accounted for all fatal clicks within an organization. The report highlighted that the majority of these fatal clicks were made by repeat-clickers. The article identified a key factor that plays a role in how often or when a person clicks: *the quantity of malicious emails received*. Ironically, receiving either a small number or a large number of malicious emails resulted in higher clicking rates. From a percentage perspective, once a person has received 100 malicious emails, their click rate is estimated to be about 60%.

The remainder of the paper is structured with Related Work in Section II and Methods discussed in Section V. Results and Discussion are presented in Sections VI and VII respectively. Finally, in Section VIII, our Conclusions and Future Work are presented.

II. Related Work

Dhamija, Tygar, and Hearst [2] identified three cognitive dimensions utilized as successful tactics in phishing attacks: *insufficient knowledge*, *visual tricks*, and *inadequate attention*. *Insufficient knowledge* was described as lacking knowledge of computer systems and/or lacking knowledge of security indicators. *Visual tricks* fall into four groups: (1) visually distorted text, (2) images used to hide the actual text, (3) distorted use of browser windows, and (4) deceitfully crafted websites. The last dimension, *inadequate attention*, includes the absence of attention to security indicators and the lack of attention to missing security indicators.

To further explore these three cognitive dimensions, Dhamija; Tygar; and Hearst [2] conducted a study where participants received an email message asking them to click a link within an email. The objective was to click the links from the list and interact with the website and make a judgment on its authenticity. Participants were warned that some links were authentic and others were not. They were also asked to talk aloud during their decision-making process and to state the following: if the website was legitimate, give their confidence level, and their reasoning for their decision/rating.

Dhamija, Tygar, and Hearst [2] established support for two of their predictions related to the three cognitive dimensions. First, it confirmed that participants made inaccurate judgments because of insufficient knowledge of computer system functions. A lack of knowledge or the misunderstanding of security systems were also indicators that contributed to incorrect judgments. Second, the prediction associated with visual deception was confirmed; the more skilled or expert participants were also deceived by visual tricks. The third prediction pertaining to the lack of attention was not supported because their study design prohibited this evaluation. Some interesting aspects revealed from the study were that participants did not know that fabricating a website was possible, and consequently did not question a website's authenticity. Also, some participants misunderstood what website/browser features indicated that security measures were in place. The approach from Dhamija et al. [2] shaped the research direction presented in this paper.

III. Explanations from Cognitive Science

Theories from cognitive science are relevant toward understanding why and how these types of security concerns may occur. Treisman and Gelade's feature-integration theory of attention research [9] is the first study from the cognitive science literature that shaped the research direction for our study. Five primary components were examined from the *feature-integration theory* that directly relate to our current study. Those five components are as follows:

1) *Visual Search* - a perceptual task that demands attention, commonly requires active scanning for a feature or target surrounded by other features known as distractors.
2) *Texture Segregation* - To divide visual stimuli by distinguishing between spatial discontinuities among groups.
3) *Illusory Conjunctions* - the impact of incorrectly combining features when multiple unattended objects are presented.
4) *Identity and Location* - the understanding that identifying an object and knowing its position are two different operations, and that location must precede identification.
5) *Interference from Unattended Stimuli* - stimuli that is not being attended to only registers at the feature level. The degree of distraction it has on attended tasks depends on the features it is composed of and should not be affected by any conjunctions from where the features occurred.

These five components suggest that some textual manipulations and complex visual tricks are harder to identify than others. Through experiments conducted by Treisman and Gelades [9], it was established that separable features were detected and identified via parallel search, and conjunctive features were identified via serial search. This knowledge serves as the foundation for our hypotheses:

- *Hypothesis 1 (H1)*: The detection of *additional text* will be the easiest discrepancy to identify because it can be done via a parallel search process.
- *Hypothesis 2 (H2)*: The detection of *crafted text*, *manipulation combinations*, and *obfuscated manipulations* will be more challenging to identify because these require serial search.

Further support for these predictions is derived from Treisman and Gelade's [9] findings that parallel searches expose texture segregation and figure-ground groupings. However, to reveal individual features requires extra operations, but if attention is averted or exhausted, then illusory conjunction may surface. Serial searches require central attention to be guided consecutively and exclusively to significant locations, but serial searches cannot expose texture segregation. Texture segregation is not uncovered until extra spatial localization has occurred.

A second influential study from cognitive science is based on research from Simons and Chabris [10] associated with sustained *inattentional blindness* for dynamic events. Inattentional blindness is when individuals fail to pay attention

to unexpected stimuli that is viewable and in plain sight. The results from their study established that when engaged in a primary task of monitoring, individuals can fail to acknowledge continuing and highly conspicuous but unexpected events. Their study confirmed that the degree of *inattentional blindness* is prone to the detection of unexpected events if the events are similar in visual aspects to the events currently being attended. The last important factor established by the Simons and Chabris' study was that objects may pass through the area of attentional focus and still may not be detected if a person is not exclusively attending for that specific object.

The results from the Simons and Chabris study [10] supports our hypotheses because it offers a possible explanation as to why the discrepancies in the URLs may go unnoticed. The theory of inattentional blindness for dynamic events [10] explains that discrepancies go unnoticed simply because the focus of attention is on something else. The actual URL is not being attended to, but more specifically the user is not focused on determining if the URL is legitimate and instead is focused on other aspects within the email, text message, instant message, tweet, etc. If the users do not suspect the email, text message, tweet, etc. is malicious then they will not analyze its content for possible malicious material.

IV. Common Methods of Deception

For the purposes of the research in this paper, the following terms are used to describe four different types of discrepancies that are often found in URLs:

- *Additional Text* can be described as a URL with too many or extra characters, for example wwww.google.com.
- *Crafted Text* URLs include numbers, texts, or special characters to deceive the user, for example, www.goog1e.com, in which the number one is used to replace the lowercase 'L' in google.
- *Manipulation Combinations* make use of multiple tactics to deceive the user for instance, www.google.corn. In this example 'r' and 'n' are used to form the m in .com. Also, the font size of the 'r' and 'n' have been changed.
- *Obfuscation* describes the process of hiding a malicious URL behind a legitimate URL, for example www.google.com (there is a malicious URL hidden behind this hyperlink that can viewed if the link is hovered over before clicking on it).

When discussing the different categories used to deceive users one must keep in mind, that font style may have a significant role. The use of serif and sans serif fonts can cause the detection process to switch from a parallel search to a serial search, this is due to the structure and form of the characters generated. When serif font styles (Times New Roman) are used certain characters are displayed identically (the number one and lower case 'L'), in which case spacing among characters must be accounted for to differentiate between them.

Additional text is expected to be more noticeable because it is detected through a parallel search and there is only a single degree of change in this type of manipulation, while the other three manipulations contain more than one degree of change within the URL. For example, this manipulation wwww.google.com (disjunctive, only one degree of discrepancy to check for) is easy to spot as opposed to www.goog1e.com (conjunctive, more than one degree of manipulation to check for - the lower case 'L' replaced with the number '1', which is two degrees of manipulation because the substitution of an alphabetic character is one manipulation and the use of a numeric character alters the spacing between characters, which is the second manipulation).

V. Method

This sections presents an overview of the methodological approach for this research. It provides information related to the characteristics of the participants, equipment used, materials generated, examples of the stimuli presented, and the procedures for this study. The role playing tactic was used to minimize participants' risks. The emails were designed to resemble real-life situations. Participants were not informed about the emails' legitimacy because this study was disguised as a usability study to validate if participants used or attended to the security cues.

A. Participants

There were a total of 1044 participants (N=1044), ranging in ages from 18 to 60 and older. The motivation for selecting this age range is attributed to [7], which exposed the fact that people under the age of 20 accounted for about 3.51% of complaints, while people ranging from ages 20-39 accounted for 38.97% of complaints. Baby boomers reported the most complaints, with people between the ages of 40-59 reporting 40.95% and those 60 and over accounted for 16.57% of complaints.

A total of 580 males, 460 females, two participants who selected no response, and two participants who skipped this question in our study. This population allowed for the investigation of whether one gender was more prone to clicking over the other. In [7], the results illustrated that 52.05% of males and 47.95% of females accounted for the total complaints [7]. These results indicated that both genders were similarly responsible for complaints; however, in the same report, the breakdown of monetary losses showed that in some cases men accounted for most of the reports and vice-versa in other cases. One thousand of the participants for our study came from Amazon Mechanical Turk and were paid $0.40 for their participation; while 44 participants were unpaid student volunteers from Alabama A & M University.

B. Equipment

The sample email messages and URLs were created using a MacBook Pro with a retina display. The email messages were composed using a fictitious gmail account and the URLs were composed in Microsoft Word from the Microsoft Office 360 Suite for Mac. The survey was composed and hosted by SurveyGizmo. Participants could use their own devices to complete the survey. Participants accessed the survey one of two ways, by going to Amazon Mechanical Turk or by

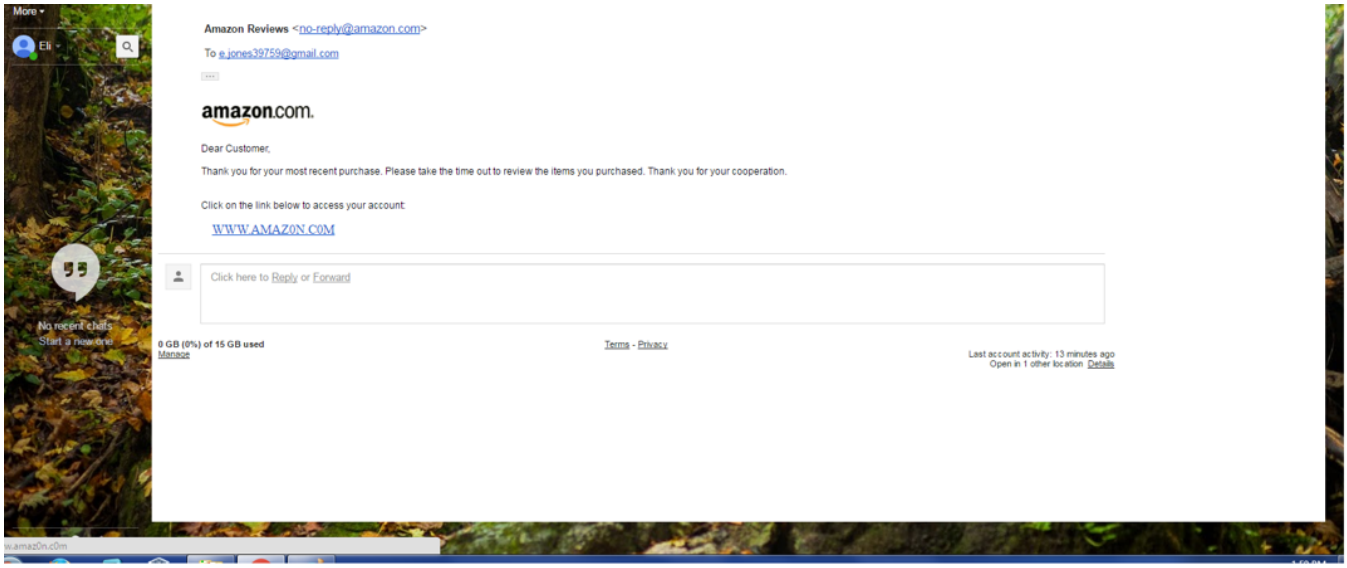

Fig. 1. This is a sample email from a fictitious email account as part of the role-playing exercise in the study.

TABLE I
THE DIFFERENT CATEGORIES OF URL DISCREPANCIES AND THE LINKS WITHIN EACH CATEGORY THAT WERE USED IN THE EMAILS IN THE STUDY.

Legitimate	Additional Text	Crafted Text	Manipulation Combination	Obfuscated Text
https://www.yahoo.com/	http://www.amazonn.com/	http://wvvw.wellsfargo.com/	http://www.grnail.com/	https://www.google.com/
https://www.facebook.com/	http://www.bankoffamerica.com/	http://www.tvvitter.com/	http://www.yah00.com/	https://www.facebook.com/

direct access via SurveyGimzo through a web link that was provided. Reaction times were logged using SurveyGizmo, but the results of this part of the study are beyond the scope of this paper.

C. Stimuli

The URLs used in this study were composed using both serif and sans serif fonts, which were used in isolation or in combination to create a single URL. The font size used in Microsoft Word was 12; however, when the URLs were uploaded to SurveyGizmo the font size was set to medium. For some of the URLs the size of the characters varied in MS Word before going into SurveyGizmo as a part of their manipulation. There were ten emails used in this study, containing two links from each category (*additional text*, *crafted text*, *manipulation combinations*, *obfuscation*, and *legitimate*). Table I depicts examples of the links contained within the emails. The emails themselves were screenshot images from a fictitious email account. Figure 1 shows an example of the screenshot images used in this study.

D. Procedure

The primary task for this study was a role-playing exercise, where participants were given the following scenario: *As a participant in this phase of the experiment, you will play the role of "Eli Jones." You will be shown a series of images from Eli's inbox along with a series of responses. The task here is to evaluate the email as if it was your own, and select the response or responses that best describe the action(s) you would take. When selecting your actions, base your decision on if you feel safe to click on the link within the email. To advance to the next page click the next button below the question. You may also click the back button, below the question, to access the previous page.*

After reading the scenario statement, participants were shown ten emails in a random order along with a series of responses to choose from. The choices were as follows: *click Reply to reply by email, click the link, copy and paste the link, communicate with the sender in person, delete the email or other (which allowed participants to write-in their response)*. This entire study was designed to resemble an email usability study, but it was actually a security study to test if lay users were able to determine legitimate and illegitimate URLs.

VI. RESULTS

The first step in the analysis process was to evaluate the manipulation check, which was to determine if the participants were able to correctly identify the legitimate emails. Participants in this study were able to correctly identify the legitimate emails, which indicated that participants attended to each individual email and passed the manipulation check for this phase of the study. The manipulation check was done by rating participants' responses as secure (coded as 1) or unsecure (coded as 0) in the role-playing phase of this study.

Because we used a repeated-measures within subjects design with dichotomous variables a Cochran's Q was performed on the role-playing phase, which indicated a statistically significant difference in the proportion of participants who were able to accurately differentiate legitimate URLs from fraudulent URLs, $\chi^2(9, N=961) = 1808.80$, $p<.001$, $\phi = .49$ (medium-large effect size). This led to a pairwise comparison using a continuity-corrected McNemar Test with Bonferroni correction, which revealed a statistically significant difference between the secure emails and all four discrepancy categories (*additional text* emails, *crafted text* emails, *manipulation combination* emails, and *obfuscation* emails). The results from these tests are shown in Table II.

TABLE II
THE TEST STATISTICS FROM THE MCNEMAR TEST (PAIRWISE COMPARISON) - S. INDICATES *Secure* OR LEGITIMATE LINKS, C. INDICATES *Crafted Text*, M.C. INDICATES *Manipulation Combinations*, O. INDICATES *Obfuscation*, AND A. INDICATES *Additional Text*.

Test Statistics

	N	Chi-Square	Asymp. Sig.
S. Email1 & C. Email1	1018	345.003	p <.001
S. Email1 & M.C. Email1	1018	175.006	p <.001
S. Email1 & O. Email1	1010	510.002	p <.001
S. Email1 & A. Email1	1016	486.002	p <.001
S. Email1 & C. Email2	1020	261.004	p <.001
S. Email1 & M.C. Email2	1024	250.004	p <.001
S. Email1 & A. Email2	1019	531.002	p <.001
S. Email1 & O. Email2	1018	417.002	p <.001
S. Email2 & C. Email1	1029	350.003	p <.001
S. Email2 & M.C. Email1	1027	176.006	p <.001
S. Email2 & O. Email1	1018	511.002	p <.001
S. Email2 & A. Email1	1027	492.002	p <.001
S. Email2 & C. Email2	1029	267.004	p <.001
S. Email2 & M.C. Email2	1033	255.004	p <.001
S. Email2 & A. Email2	1028	534.002	p <.001
S. Email2 & O. Email2	1029	421.002	p <.001

Table III displays the results from the pairwise comparison of the two *crafted text* emails, which was statistically significant, and shows the proportion of participants who could correctly identify the links as not being legitimate, $\chi^2(2, N=1016) = 16.76$, $p<.001$, $\phi = .19$ (small-medium effect size). Table IV shows the results from the pairwise comparison of the two *manipulation combinations* emails, here there was also a statically significant difference for the number of participants who correctly identified the URLs as not genuine, $\chi^2(2, N=1020) = 26.45$, $p<.001$, $\phi = .16$ (small-medium effect size). The pairwise comparison of the two emails in the *obfuscation* category also had a statistically significant difference for the participants who correctly identified the URLs as not being authentic, $\chi^2(2, N=1007) = 23.13$, $p<.001$, $\phi = .15$ (small-medium effect size) as shown in Table V. The last pairwise comparison was performed between the two *additional text* emails and the results are shown in Table VI and just as the others there was a statically significant difference in the number of participants who correctly identified the links as not authentic, $\chi^2(2, N=1015) = 6.069$, $p<.05$, $\phi = .08$ (small effect size).*[Note: The difference between email1 and email2 in each category are (a) the type of email used (i.e. solicitation or account related) and (b) the links used within each email (see Table I for examples.)]*

TABLE III
PAIRWISE COMPARISON OF *Crafted Text* EMAILS

Crafted_email_1 & Crafted_email_2

Crafted_email_1	Crafted_email_2	
	Unsecure_Action	Secure_Action
Unsecure_Action	95	253
Secure_Action	168	500

TABLE IV
PAIRWISE COMPARISON OF *Manipulation Combinations* EMAILS

Manip_Combine_1 & Manip_Combine_2

Manip_Combine_1	Manip_Combine_2	
	Unsecure_Action	Secure_Action
Unsecure_Action	96	78
Secure_Action	158	688

TABLE V
PAIRWISE COMPARISON OF *Obfuscated* EMAILS

Obfuscated_email_1 & Obfuscated_email_2

Obfuscated_email_1	Obfuscated_email_2	
	Unsecure_Action	Secure_Action
Unsecure_Action	281	225
Secure_Action	133	368

TABLE VI
PAIRWISE COMPARISON OF *Additional Text* EMAILS

Additionalt_email_1 & Additionalt_email_2

Additionalt_email_1	Additionalt_email_2	
	Unsecure_Action	Secure_Action
Unsecure_Action	349	137
Secure_Action	182	347

VII. DISCUSSION

From the results of the pairwise comparisons in Tables III-VI and the frequency data in Table VII, *H1* was not supported as it turned out that the simple visual tricks associated with *additional text* were the most difficult to detect and not the easiest as predicted. The results show that when given the second email from that category the count for the *additional text* emails (A. Email1 and A. Email2) increased from 494 (48.1%) unsecure to 536 (51.3%) unsecure.

TABLE VII
FREQUENCY TABLE FOR THE ROLE-PLAYING PHASE OF THE STUDY. C. INDICATES *Crafted Text*, M.C. INDICATES *Manipulation Combinations*, O. INDICATES *Obfuscated Text*, AND A. INDICATES *Additional Text*.

Frequency Table

URL Types:	N	Unsecure	Secure
C. Email1	1029	352 (34.2%)	677 (65.8%)
M.C. Email1	1027	178 (17.3%)	849 (82.7%)
O. Email1	1018	513 (50.4%)	505 (49.6%)
C. Email2	1029	269 (26.1%)	760 (73.9%)
A. Email1	1027	494 (48.1%)	533 (51.9%)
M.C. Email2	1033	257 (24.9%)	776 (75.1%)
A. Email2	1028	536 (51.3%)	492 (47.9%)
O. Email2	1029	423 (41.1%)	606 (58.9%)

In H2, we predicted that more complex visual tricks (i.e., crafted text, manipulation combinations, and obfuscated text) would be the most difficult to detect. The category of obfuscation (hidden links) was the second most difficult to detect with the counts (O. Email1 and O. Email2) showing only a slight decrease from 513 (50.4%) unsecure to 423 (41.1%) unsecure. Conversely the two easiest cases to detect were *crafted text* and *manipulation combinations*, with the latter being the easiest. From Table VII it can be observed that the unsecure responses decreased in the case of *crafted text* emails (C. Email1 and C. Email2) from 352 (34.2%) to 269 (26.1%), but a small increase occurred in the *manipulation combinations* emails (M.C. Email1 and M.C. Email2) from 178 (17.3%) to 257 (24.9%), which was the lowest of all categories. In addition, looking at all of the categories together it was interesting to notice that the two most difficult cases, *additional text* and *obfuscation*, the overall performance had a 50/50 split of secure versus unsecure responses. The only justification for the results we could derive was based on the write-in responses where participants indicated that the extra characters and other manipulations were spelling errors, or the participants did not attend to the security cues. Another explanation, purely speculation, for the results from our study was that some participants had more prior knowledge and awareness related to phishing, which they used when selecting their responses.

VIII. CONCLUSIONS AND FUTURE WORK

Similar to previous studies in this area, our results revealed that users have difficulty detecting legitimate URLs from illegitimate URLs. Specifically, our study illustrated that when a user's primary task is "checking email" he/she has a hard time deciphering fraudulent emails from genuine emails. This study did not fully support our hypotheses that complex visual tricks such as crafted text, obfuscation, and manipulation combinations would be the most difficult to detect as opposed to simple textual manipulations, such as additional text. Nevertheless, the results from the role playing phase of this study indicated that participants had the most difficulty with *additional text* URLs. The next category participants had the most trouble with was *obfuscation*. The third category, was *crafted text*, which was the second easiest to detect. Last, was *manipulation combinations*, which was the easiest of them all to detect. Some of the results are not intuitive and further investigation needs to be performed.

After reviewing the results, our next phase of this research will be to analyze the data from the post survey administered at the end of this study to determine the affects of prior knowledge of phishing and computer/information security. We plan to conduct an analysis of the response times recorded from our study to identify any effects. We also plan to analyze the results for how users handle a single URL in isolation (not included in an email). Finally, we plan to evaluate if there is a correlation between the participants' demographic information; internet and email habits; educational background or occupation and their ability to correctly identify legitimate URLs. All of these results should appear in forthcoming publications.

ACKNOWLEDGMENTS

The authors would like to thank and recognize Dr. Dave Dampier, the Director of the Distributed Analytics and Security Institute (DASI) at Mississippi State University for funding this research and those individuals who volunteered to participate in this study from Alabama A & M University.

REFERENCES

[1] J. Kee, "Social engineering: Manipulating the source," *GCIA Gold Certification*, 2008.

[2] R. Dhamija, J. D. Tygar, and M. Hearst, "Why Phishing Works," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '06. New York, NY, USA: ACM, 2006, pp. 581–590. [Online]. Available: http://doi.acm.org/10.1145/1124772.1124861

[3] P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "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*, ser. CHI '07. New York, NY, USA: ACM, 2007, pp. 905–914. [Online]. Available: http://doi.acm.org/10.1145/1240624.1240760

[4] B. M. Bowen, R. Devarajan, and S. Stolfo, "Measuring the human factor of cyber security," in *2011 IEEE International Conference on Technologies for Homeland Security (HST)*, Nov. 2011, pp. 230–235.

[5] M. Khonji, Y. Iraqi, and A. Jones, "Phishing Detection: A Literature Survey," *IEEE Communications Surveys Tutorials*, vol. 15, no. 4, pp. 2091–2121, 2013.

[6] S. Gupta, A. Singhal, and A. Kapoor, "A literature survey on social engineering attacks: Phishing attack," in *2016 International Conference on Computing, Communication and Automation (ICCCA)*, Apr. 2016, pp. 537–540.

[7] F. B. o. I. Internet Crime Complaint Center(IC3), "Internet Crime Complaint Center (IC3) | Annual Reports." [Online]. Available: https://www.ic3.gov/media/annualreports.aspx

[8] Proofpoint, "The Human Factor: How attacks exploit people as the weakest link in security." [Online]. Available: https://whitepapers.theregister.co.uk/paper/view/3768/how-attacks-exploit-people-as-the-weakest-link-in-security

[9] A. M. Treisman and G. Gelade, "A feature-integration theory of attention," *Cognitive Psychology*, vol. 12, no. 1, pp. 97–136, Jan. 1980. [Online]. Available: http://www.sciencedirect.com/science/article/pii/0010028580900055

[10] D. J. Simons and C. F. Chabris, "Gorillas in our midst: sustained inattentional blindness for dynamic events," *Perception*, vol. 28, no. 9, pp. 1059–1074, 1999.