Why do I get phished? The role of persuasion, design authenticity and contextualization

Submission Type: Full Paper

Baidyanath Biswas
International Management Institute, Kolkata
b.biswas@imi-k.edu.in

Arunabha Mukhopadhyay
Indian Institute of Management, Lucknow
arunabha@iiml.ac.in

Abstract

Phishing emails employ a multitude of persuasion techniques that may include reward schemes (such as a gift coupon), losses (such as a social urgency), the commonality of email structure and design, or related to a recent topic. These persuasion techniques appeal individual users to respond and share personal information by clicking on the URL shared via the email. In this study, we conducted a detailed investigation through a social experiment and identified those predictors of phishing emails, which makes them trustworthy. We considered the following persuasion techniques: (a) loss-based; (b) reward-based, (c) design authenticity, and (d) reference to a relevant topic. Additionally, we considered whether the cyber-hygiene of the participants could moderate persuasive factors and mislead the user to click on the link. We grounded our findings in behavioral IS theories that explain human susceptibility to phishing. We recommend that loss-based persuasion and design similarity are the two most influential factors that contribute to phishing attacks. Further, presence of prior cyber-hygiene knowledge and contextualized emails can moderate the actual user response towards phishing emails.

Keywords

Phishing, Information Security, Prospect Theory, Protection Motivation, Structural Equation Modelling.

Introduction

Phishing emails have become an emerging threat throughout organizations that comprise of a swift, simple, and inexpensive tactic to attack an enormous target of users with false information. Additionally, attackers are using unique techniques such as nearly authentic company logos, advertisements, email structures, and identical-looking IPs and server domains to send phishing emails. In a series of anti-phishing tests that were conducted internally within organizations, almost ten percent of the total users clicked on unknown URLs and executed potentially insecure software programs (Verizon 2016). Hence, it is gradually becoming a challenging task for the CTO to distinguish fake emails from the genuine ones.

Existing research has confirmed that individuals respond to these influence techniques (such as rewards and losses) in a volatile manner (Butavicius et al. 2015; Goel et al., 2017; Oliveira et al. 2017). For example, if the recipient has recently participated in a customer satisfaction survey, he might be interested in winning an Amazon coupon. On the contrary, another recipient could receive an email with similar action, but with the possibility of a loss, such as monetary penalty, or non-compliance to IT security standards. These instances lead us to endorse that loss appeal has a more detrimental effect on users than a rewarding appeal (Goel et al., 2017; Kahneman and Tversky 1984). Again, as human beings, we use superficial cues that connect with the similar "look and feel" of real websites and products (Sillence et al., 2000). Thus, emails that contain authentic logos, pictorial cues, messages, copyright statements, and other crucial information, are more likely to be trusted by its recipients, who will then be tempted to click on them. In addition to these persuasion and authenticity techniques, recent spear-phishing emails included contextual information that made them more relatable to their recipients, thereby increasing the chance to click on them. Therefore, further research is required in these aspects and explore these potential areas.

In this study, we explore the following research questions. What are the factors that raise the alarm among individuals when they receive an email? Besides, are there any particular environmental features that appeal them to click on the URL? Can the presence of contextual information within the phishing email structure, modify the recipient's perceptions about the email received? Does habitual email behavior affect the way, in which people evaluate email communication?

Literature Review

Phishing is a semantic attack that relies on deceiving people, and therefore it is difficult to detect these attacks with complete accuracy using technology alone (Egelman et al. 2008). Dhamija et al. (2006) found that visual deception attacks could fool even sophisticated users. Their results illustrated that standard security indicators are not effective for a substantial fraction of users and suggested alternative approaches. Schechter et al. (2007) investigated whether participants behaved differently in security usability studies than they would behave in real life. They experimented with online banking tasks and confirmed that the users were ignoring HTTPS indicators, and other alarming clues about an insecure data connection. In a laboratory experiment using simulated spear-phishing attacks, Egelman et al. (2008) examined the effectiveness of passive web-browser based phishing warnings. They found that these indicators needed to be strong enough to provide clear choices to the users and prevent them from being habituated. Vishwanath et al. (2011) demonstrated different predictors of phishing emails that included the following: level of attention to the subject line, urgency cues, grammatical mistakes, and domain-specific knowledge. Through a series of field experiments, Wright et al. (2014) described the relative effectiveness of phishing strategies that compelled users to click on these emails. Drawing from persuasion and motivation theory, they also identified significant security vulnerabilities that could clarify individual behavior to combat phishing through awareness and training efforts in organizations.

Flores and Ekstedt (2016) identified transformational leadership and information security culture as significant predictors of information security awareness and proposed that these factors could shape intention to resist social engineering among the employees in an organization. Arachchilage et al. (2016) designed a mobile game aimed at enhancing the avoidance behavior among online users through protection motivation against phishing threats. They also reported that threat perception, the effectiveness of safeguards, user self-efficacy, perceived severity and susceptibility could positively affect threat-avoidance behavior, whereas the cost of installing safeguards hurt the threat-avoidance behavior. Kearney and Kruger (2016) studied the privacy paradox and found that online users can reveal personal and confidential information regularly, despite administering information security awareness and training programs. They also recommended that a combination of all the three organizational factors namely, management, technology, and human behavior could achieve a state of information security congruence. Wang et al. (2016) examined the overconfidence behavior of online users in misjudging phishing emails and malicious links with the help of cognitive and motivational factors. Goel et al. (2017) studied how contextualization of emails could increase their susceptibility to phishing using fabricated emails. They conducted a social experiment to elicit the fear of losing something valuable or the anticipation of gaining something desirable and recorded the user behavior for each of them. They found that past security training was not effective, and recommended that highly focused and contextualized awareness campaigns could improve the impact of those training programs. In Table 1, we review the extant behavioral literature on phishing attacks.

Study	**Key Findings**	**Theoretical Foundation**		
		PT	**DT**	**PMT**
Dhamija *et al.* (2006)	Malicious strategies	Y	-	Y
Schechter *et al.* (2007)	Usability study of participants	Y	-	-
Egelman *et al.* (2008)	Examination of active and passive warnings	Y	-	Y
Vishwanath *et al.* (2011)	Phishing impacts of individuals	-	Y	Y
Wright *et al.* (2014)	Influencing techniques in phishing	Y	-	-
Flores & Ekstedt (2016)	Resist phishing through culture	-	Y	Y
Arachchilage *et al.* (2016)	Phishing game design framework	Y	-	-
Wang *et al.* (2016)	Over-confidence in judgement	Y	-	Y
Williams and Polage (2018)	News events and design cues	-	Y	Y
Goel *et al.* (2017)	Psychological weakness	Y	-	Y

PT=Prospect Theory; DT=Design Theory; PMT = Protection Motivation Theory

Table 1. Review of extant behavioral literature on phishing

Theoretical Foundation and Hypothesis Development

We model our study based on the different behavioral theories such as (i) Prospect Theory (Kahneman & Tversky, 1979), (ii) Design Theory (Jonassen, 2000) and (iii) Protection Motivation Theory (Rogers, 2003). For every individual, prospect theory supports the idea of differential weighing of a potential loss-

making event in comparison to a potentially profitable event. Design theory provides the evidence for the presence of similarity of design and authenticity cues that attackers can embed within phishing emails for online users. Once an individual receives an email with higher user appeal and trustworthiness, he will click on it and disclose private information. Protection motivation theory states that the presence of good cyber hygiene, and fear appeals towards previous instances of information security attacks can moderate the response of the individual toward the email communication. In the subsequent sub-sections, we discuss these theories in detail, and develop our hypotheses from them.

Prospect Theory: Influence through Persuasion

Individuals are vulnerable to online frauds that are sent via phishing emails, which largely depends on the targeted appeal of the message. Thus, a particular theme of the email can coerce an online user to reveal personal information. Although one might argue that there cannot be significant differences in human response to an email with gain-appeal while compared to that with a loss-appeal, *prospect theory* (Kahneman & Tversky, 1979) advocates the belief that possible damages exercise a stronger impact than associated potential rewards. Further, according to Goel et al. (2017), human beings attribute characteristic values of email communication to those gains and losses, such that the rewards mentally map to positive ranks and the damages map to negative degrees. Thus, messages that threaten the loss of something valuable may be more effective than the ones offering the possibility of gains.

> ***Hypothesis 1****: Emails describing potential loss(es) associated with identity theft and data losses are relatively more appealing to the recipient user.*

> ***Hypothesis 2****: Emails describing potential reward(s) associated with identity theft and data losses are relatively less appealing to the recipient user.*

Design Theory: Similarity and Authenticity

Often the presence of a similar company emblem, copyright symbol, and other authentic cues can increase the perceived acceptability of emails (Sillence et al., 2006). These design elements also improve the 'look and feel' of the entire email structure (Williams and Polage, 2018). Gradually, over the years, such fraudulent email communications have become highly authentic and refined in their design, to impersonate the reputable firms, their brandings, advertisements, keywords, and taglines thereby making them more trustworthy (Hong, 2012). Therefore, we propose that messages with the presence of authentic impersonations will be relatively more appealing to online users than the ones without them.

> ***Hypothesis 3****: Emails with authentic design cues are relatively more appealing to the recipient user as compared to emails that consist of general or no design cues.*

User Appeal and Email Response

For most of the victims of phishing attacks, the challenge lies in deterring the individual from making impulsive and emotional responses (such as clicking on the URL and disclosing sensitive information) instead of rational ones (Biswas and Mukhopadhyay, 2017). In existing studies on information system (IS) use, such as the Technology Acceptance Model (TAM) (Venkatesh and Davis, 2000), behavioral intentions to use an IS may lead to the actual system use. The perceived appeal will influence the actual use of IS (here, the phishing emails) because, other factors held constant, the more appealing and engaging the IS is, the more authentic and useful it can be. Therefore, when the recipient of a phishing email is highly motivated and fascinated by the email, he will click on the URL provided within the email and share critical information.

> ***Hypothesis 4****: High appeal among email users will lead to actual response activity.*

Protection Motivation Theory: Cyber-hygiene and Routine Behavior

The propensity of individuals to fall prey to phishing attacks can widely vary depending on their nature, social mannerisms, and orientation. Previous research on *user susceptibility towards phishing* has demonstrated that individuals with a higher degree of awareness on possible risks of using an online setting may be relatively less susceptible (Vishwanath et al., 2016). Henceforth, online users with occasional interaction with online IT systems and anti-phishing activities such as security training, usage of antivirus and other anti-spyware, will fall victim to these attacks (Vishwanath *et al.*, 2011). On the contrary, previous personal experiences with cyber-attacks, anti-phishing exercises, and related routine behavior will have a differential impact on the appeal of

these emails. Therefore, we propose that routine behavior and apriori cyber-hygiene will moderate the way people evaluate emails and are induced by them.

> ***Hypothesis 5(a)****: High cyber-hygiene and routine behavior among email users will positively moderate the effect of a potential loss on user appeal.*
>
> ***Hypothesis 5(b)****: High cyber-hygiene and routine behavior among email users will positively moderate the effect of a potential reward on user appeal.*
>
> ***Hypothesis 5(c)****: High cyber-hygiene and routine behavior among email users will positively moderate the effect of design similarity on user appeal.*

Role of contextualization

There are additional factors apart from the persuasion methods, design authenticity, and cyber-hygiene that can play a role in phishing. In a spate of recent phishing incidents, the attacks were launched in the aftermath of a data-breach or a cyber-attack, thereby misleading naïve customers to share sensitive and personal information. Further, contextualizing messages to appeal to the psychological weakness of their recipients have increased their susceptibility to phishing (Goel et al., 2017). Similarly, users fell victim to phishing frauds where the emails were linked to recent sporting events, and cultural festivals (BBC News 2017). Therefore, attackers may connect the context of the phishing emails to familiar topics that individuals are more likely to be acquainted with, and this may boost the perceived trustworthiness of the emails. In this manner, the exposure to contextual evidence may make phishing attacks more striking, and throughout the entire event, successfully prepare users for later phishing emails that link to the current information (Meyer and Schvaneveldt 1971).

> ***Hypothesis 6****: Emails with specific concerns and contextualized information will positively moderate the effect of user appeal towards actual response to phishing emails as compared to non-contextualized emails that relate to general or broad concerns.*

Proposed framework

From our proposed framework to examine the role of influence techniques and design authenticity among users as shown in Figure 1, we address the following research questions:

RQ1: What are the significant predictors of user appeal towards phishing emails in organizations?

Mathematically, it can be written as:

$$\text{User Appeal} = f_1(\text{Potential Loss, Potential Rewards, Design Similarity, Routine Behavior}) \quad (1)$$

where f_1 denotes the mathematical relationship among the predictors: *Potential Loss*, *Potential Rewards*, *Design Similarity*, and *Routine Behavior*; and how they constitute the outcome *User Appeal.*

The Partial Least Square based Structural Equation Model (PLS-SEM) for the above mathematical relationship in (1) is given as (2):

$$\begin{aligned}\text{User Appeal} = {} & \beta_1(\text{Potential Loss}) + \beta_2(\text{Potential Rewards}) + \beta_3(\text{Design Similarity}) \\ & + \beta_4(\text{Potential Loss x Routine Behavior}) + \beta_5(\text{Potential Rewards x Routine Behavior}) \\ & + \beta_6(\text{Design Similarity x Routine Behavior}) + \zeta_1 \end{aligned} \quad (2)$$

where β_1, β_2, and β_3 are the path coefficients for the main effects;
β_4, β_5, and β_6 are the path coefficients for the moderation effects;
ζ_1 is the error term.

RQ2: What leads to actual user response towards phishing emails in organizations?

Mathematically, it can be written as:

$$\text{User Response} = f_2(\text{User Appeal, Relevance}) \quad (3)$$

where f_2 denotes the mathematical relationship among the predictors : *User Appeal*, and *Relevance*, and how they constitute the outcome *User Response*.

The Partial Least Square based Structural Equation Model (PLS-SEM) model for the above mathematical relationship in (3) is given as (4):

$$\text{User Response} = \beta_7 (\text{User Appeal}) + \beta_8 (\text{User Appeal x Relevance}) + \zeta_2 \quad (4)$$

where β_7 is the path coefficient for the main effects;
β_8 is the path coefficient for the moderation effect;
ζ_2 is the error term.

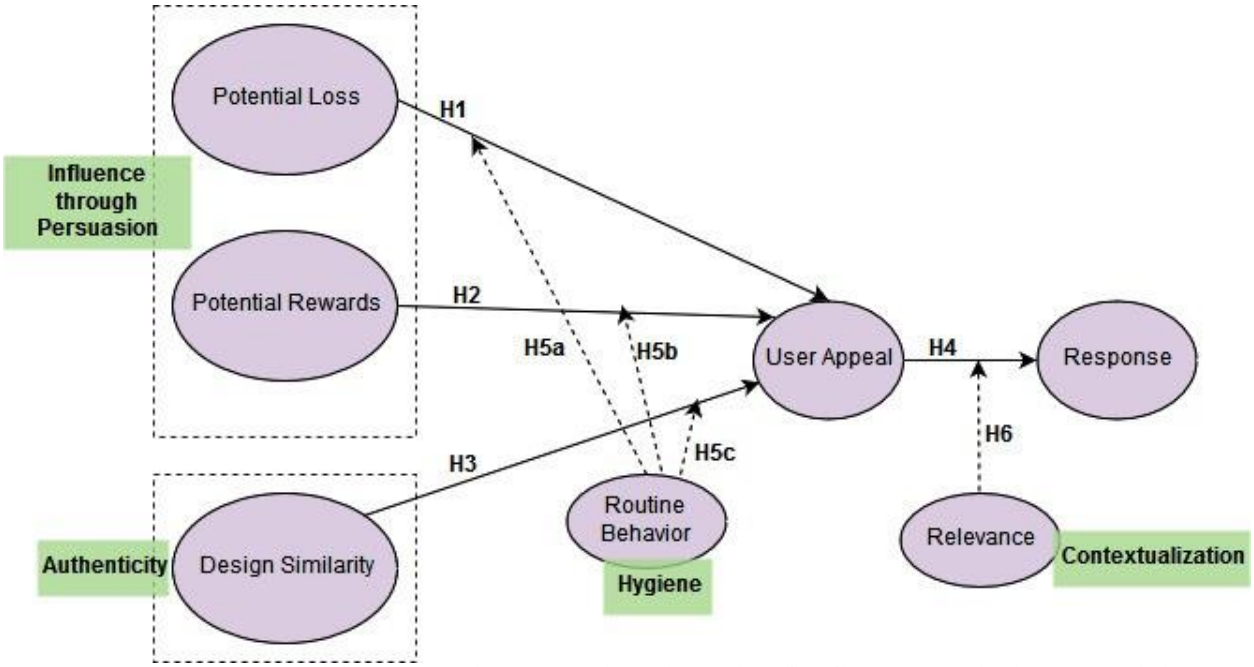


Figure 1. Our proposed framework to examine the role of influence techniques and design authenticity among users receiving phishing emails.

Research Design

To make the analysis as realistic as possible, we applied the imitation strategy in our research design. Extant studies show that such technique is capable of assessing the true responses of the participants who faced a live phishing attack. It consisted of the usage of deception and replicates the environment in a real phishing attack to measure the predictors of phishing success as nearly as possible. Throughout the entire experiment, we intended to identify the answers to the following research questions: (i) what persuasion techniques ensure that the email user is deceived?(ii) what are the most appealing factor(s) that compel an email user to believe in the contents of the email and then click on the phishing URL?

Data

We designed the contents of the tailored emails to test the hypotheses (H1 to H6) in our study. This procedure helped us to study the effects of potential losses (such as monetary penalty, loss of academic credits, missed tutorials, missed academic assistance), potential rewards (such as free e-books, Amazon gift cards, free e-learning tutorials), contextualization (such as news related to the city of Kolkata, recently held cultural festivals, business events, and student competitions). We combined a series of both positive and negative messages to represent rewards and losses, respectively. The participants in our experiments were selected from a business school in Eastern India, where they enrolled as first and second-year postgraduate students.

Our study focussed with an academic setting for the experiments due to the below reasons:

(i) Often students are targets of phishing emails (Johnston & Warkentin, 2010)
(ii) students are an appropriate behavioral research subjects (Gordon et al, 1986)
(iii) students represent the most susceptible group of email users (by age).

Then we grouped the participating students into three sets according to their choice of overall management major(s): marketing, finance, supply-chain and information technology (IT). Overall 75 students participated in our experiments, with a composition of 35 females and 40 males. The decomposition of students baseed on the major subject area is given as: marketing - 22, finance - 13, supply chain - 19, and information technology - 21. Table 2 presents the background information for the users participating in the experiments. We used an electronic survey form, and asked those participants who had clicked the benign (yet artifically crafted phishing link) on the email. The survey questionnaire was meant to assess the (i) potentiallity of loss, (ii) potentiallity of reward, (iii) understanding of the design authenticities, (iv) user appeal, (v) routine hygiene behaviour, and (vi) contextual phishing emails.

	Major	N		Age	N
Male	Marketing	14	Male	21-24	24
	Finance	8			
	Supply Chain	9		25-28	15
	IT	8			
Female	Marketing	8	Female	21-24	19
	Finance	5			
	Supply Chain	10		25-28	17
	IT	13			
Total		75			

Table 2. Description of the participants

Construct	Type	Source	Items
Potential Loss	Reflective	Goel et al. (2017)	2
Potential Rewards	Reflective	Developed for this study	2
Design Similarity	Reflective	Williams and Polage (2018)	3
User Appeal	Reflective	Developed for this study	2
Response	Reflective	Developed for this study	2
Routine Behavior	Reflective	Williams and Polage (2018)	4
Relevance	Reflective	Developed for this study	2

Table 3. Measurement items for our framework and their sources.

Table 3 describes each construct, their type (i.e., reflective or formative), literature sources, and the number of items consisting of them. Table 4 describes each item on a construct level, scale of measurement, mean, standard deviation, and individual loadings for each item. Each item had a significant loading (above the cut-off value of 0.60).

Methodology

To validate our structural model, and the relationships (H1-H6), as proposed earlier in Figure 1, we applied PLS-SEM. PLS based SEM technique offers the following advantages over Ordinary Least Squares (OLS) regression.

(i) There are seven constructs and seventeen measurement items in our proposed framework
(ii) Each of these measures are directed outwards from the constructs
(iii) The inner structure consists of six constructs and is built with theoretical support
(iv) The outer model consists of the measurement items
(v) Our data is relatively smaller in size, with 75 records in the sample dataset
(vi) The data is non-normal in nature and mutually correlated

To examine the PLS-based SEM model, we executed the SmartPLS Version 3.2.3 (Ringle et al. 2015).

Construct	Items	Scale	Mean	Std. Dev.	Loading
Potential Loss (PL)	I will incur a monetary loss if I do not follow the security instructions given in the email.	1-7	6.615	1.615	0.887
	I will face non-monetary penalty If I do not comply with the security instructions given in the email.	1-7	6.178	1.523	0.996
Potential Rewards (PR)	I will gain monetarily or even academic credits if I obey the security instructions given in the email.	1-7	5.751	1.124	0.828
	My compliance performance will improve if I obey the instructions given in the email.	1-7	5.966	1.004	0.869
Design Similarity (DS)	The sender's email address was authentic and never raised any suspicion.	1-7	6.004	1.112	0.845
	The copyright statement at the top of the webpage was convincing to me.	1-7	5.990	1.189	0.894
	The organization logo at the top of the webpage was convincing to me.	1-7	6.304	1.360	0.901
User Appeal (UA)	The email seemed authentic as the institute server sent it.	1-7	5.739	1.178	0.812
	The URL given in the email was authentic as it was similar to previous communication sent by the institute.	1-7	6.573	1.008	0.975
Response (R)	I was excited to click the link in the email after learning about the rewards.	1-7	6.532	1.003	0.868
	I was convinced that the email was not a fake.	1-7	5.739	1.276	0.900
Routine Behavior (RB)	I understand what phishing emails are and how they provoke identity loss.	1-7	6.123	1.313	0.780
	I have experienced phishing attacks or identity thefts before.	1-7	5.769	1.085	0.856
	I have ignored the previous instance(s) of such phishing emails to prevent identity theft.	1-7	5.980	1.100	0.800
	I regularly use anti-virus software or anti-phishing tool with my device(s).	1-7	6.423	0.849	0.932
Relevance (RE)	The phishing email consisted of a recent topic that I have been searching online.	1-7	5.768	1.234	0.889
	I found the content of the phishing email very similar to a recent news event.	1-7	5.410	0.901	0.867

Scale: 1=Not at all ----------> 7=Very much

Table 4. Measurement Items for our framework with descriptive statistics and loadings.

	CA	CR	AVE	PL	PR	DS	UA	R	RB	RE
Potential Loss (PL)	0.801	0.941	0.875	**0.935**						
Potential Rewards (PR)	0.798	0.837	0.694	-0.556	**0.833**					
Design Similarity (DS)	0.885	0.912	0.878	0.591	0.493	**0.937**				
User Appeal (UA)	0.723	0.891	0.789	0.694	0.688	0.567	**0.888**			
Response (R)	0.800	0.877	0.875	0.302	0.455	-0.592	0.432	**0.935**		
Routine Behavior (RB)	0.885	0.908	0.822	0.412	0.396	0.655	0.222	0.188	**0.907**	
Relevance (RE)	0.796	0.871	0.623	-0.118	0.322	-0.321	0.344	0.129	-0.293	**0.789**

CA = Cronbach's Alpha; CR = Composite Reliability; AVE = Average Variance Extracted;
Diagonal cells show the sq. rt. of AVE of each construct in our framework

Table 5. Cronbach Alpha, Composite Reliability, and Correlation coefficients for the variables.

Results and Discussion

Table 5 presents the correlation coefficients, Cronbach Alpha, and composite reliability measures for each construct. As observed from Table 4, each item had a significant loading (above the cut-off value of 0.60). Each construct has a Cronbach's Alpha and Composite Reliability higher than 0.7, and the average variance extracted (AVE) value is higher than 0.5. This result establishes the individual reliability, construct and convergent validity of each item. Next, we observed that the diagonal element (marked in bold) denotes the square root of AVE for each construct. The AVE value is approximately the highest value among all other non-diagonal cell values in each row. This result establishes the discriminant validity of the constructs proposed in our framework. Thus, our chosen items indicate good psychometric properties and are excellent representations of the proposed theoretical framework.

From the PLS-SEM model, we get a coefficient of determination (R^2) of 0.714 for the inner model that explains *user appeal* with *potential loss*, *potential rewards*, and *design authenticity* based on a two-tailed test. This result means that 71 percent of variability in measuring *user appeal* can be explained with the chosen constructs: (i) *potential loss*, (ii) *potential rewards*, and (iii) *design authenticity*. Additionally, we check for the moderator effects of routine cyber-hygiene behavior on each individual relationships. Equation (5) presents the path coefficients for each independent and moderator variable.

User Appeal = 0.678 * (Potential Loss) + 0.432 * (Potential Rewards) + 0.311 * (Design Similarity)
+ 0.278 * (Potential Loss x Routine Behavior) + 0.119 * (Potential Rewards x Routine Behavior)
+0.105 * (Design Similarity x Routine Behavior) (5)

User response is a second order construct and is measured with the help of the first-order construct *user appeal*. We find that the coefficient of determination (R^2) is 0.588 for this model. This means that about 59 percent of variability in measuring *user response* can be explained with the chosen construct: *user appeal*. Equation (6) presents the path coefficients for each independent and moderator variable.

User Response = 0. 298 * (User Appeal) + 0.594 * (User Appeal x Relevance) (6)

H1: Potential Loss affects User Appeal. A path coefficient of 0.678 with moderate statistical significance suggests that potential loss such as monetary penalty and loss of academic credits due to a phishing email affects the appeal of the user towards processing the email communication. This result is in congruence with Goel et al. (2017) and Williams and Polage (2018), who found that emails with potential loss appeals positively to the user.

H2: Potential Rewards affects User Appeal. A path coefficient of 0.432 with moderate statistical significance suggests that potential rewards such as receipt of free e-books and gift coupons due to a phishing email affects the appeal of the user towards processing the email communication. This result is in congruence with Williams and Polage (2018), who also found that emails with potential rewards can appeal to the individual. Additionally, in this study, we considered the effects of rewards and loss simultaneously instead of optional processing as suggested by Goel et al. (2017).

H3: Design Similarity affects User Appeal. A path coefficient of 0.311 with strong statistical significance, suggests that design similarity with copyright sign, company logos and other authentic cues can intensely affect the appeal of the user towards the email communication. Our result concurs with those of Wright *et al.* (2014) and Williams and Polage (2018).

H4: User Appeal affects User Response. A path coefficient of 0.298 with moderate statistical significance suggests that the user appeal built from the email communication can lead to actual activity, such as clicking on the malicious link, sharing critical personal information and much more. Our result is unique to existing studies (Goel et al., 2017; Williams and Polage, 2018), as they ignored this relationship.

H5(a): Routine Behavior moderates User Response towards potential loss appeal. A path coefficient of 0.278 with low statistical significance suggests that routine cyber-hygiene behavior such as previous instances of similar loss-making emails and actual consequences suffered, does little to affect the appeal of the user towards the email communication. Our result is unique than those of existing studies (Flores and Ekstedt, 2016; Williams and Polage, 2018), who considered routine cyber-hygiene behaviour as significant predictors of user appeal and not as a moderator of the original relationship.

H5(b): Routine Behavior moderates User Response towards potential rewarding appeal. A path coefficient of 0.119 with low statistical significance suggests that routine cyber-hygiene behavior such as previous instances of similar reward-gaining emails and actual consequences suffered is not highly effective in building the appeal of the user towards the email communication. Our result is unique than those of existing studies (Flores and Ekstedt, 2016; Williams and Polage, 2018).

H5(c): Routine Behavior moderates User Response. A path coefficient of 0.105 with no statistical significance suggests that routine cyber-hygiene behavior cannot affect the appeal of the user towards the

email communication with authentic design symbols and indicators. Our result is unique than those of existing studies (Flores and Ekstedt, 2016; Williams and Polage, 2018), who considered cyber-hygiene behavior as significant predictors of user appeal and not as a moderator of the original relationship.

H6: Contextualization moderates User Appeal towards actual User Response. A path coefficient of 0.594 with strong statistical significance suggests that contextualization of the phishing email, such as spear-phishing, with instances of recent news items, localized content, and often leads to actual user response activity. Our result is unique than existing studies (Wang *et al.*, 2016; Williams and Polage, 2018), who ignored the moderating effect of contextualization.

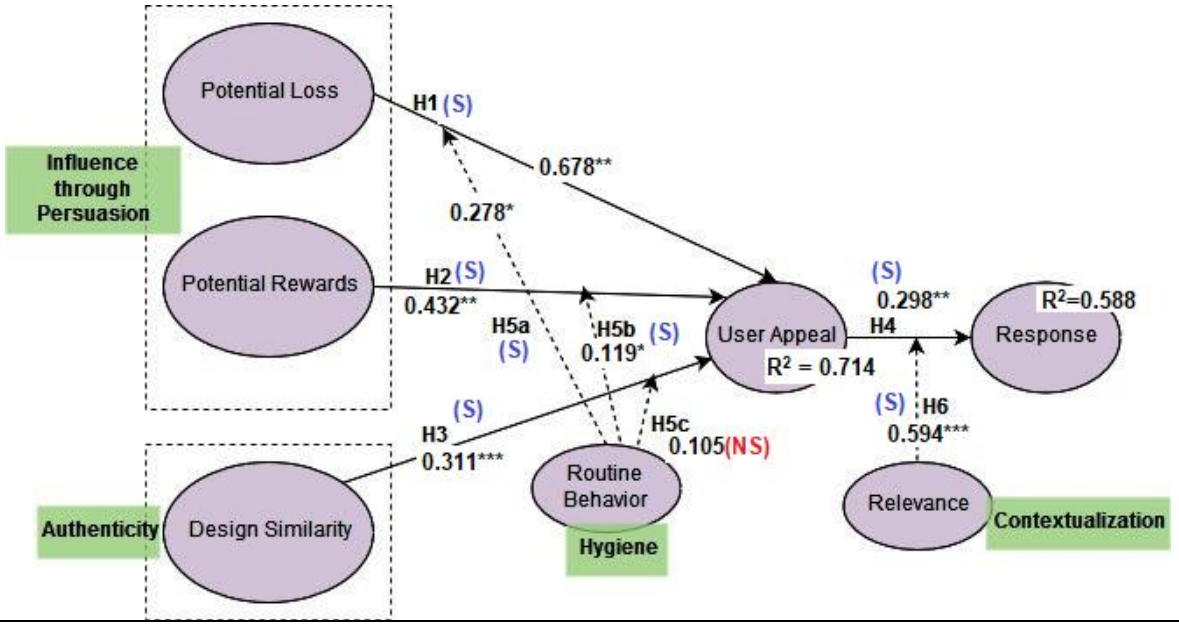
Table 6 presents a summary of the support for hypotheses in our proposed framework.

Figure 2 presents the support for hypotheses and path coefficients for our proposed framework.

Hypothesized Relationship	Path Coeff.	Support
H1: Potential Loss affects User Appeal	0.678**	Moderate
H2: Potential Rewards affects User Appeal	0.432**	Moderate
H3: Design Similarity affects User Appeal	0.311***	Strong
H4: User Appeal affects User Response	0.298**	Moderate
H5(a): Routine Behavior moderates H1	0.278*	Low
H5(b): Routine Behavior moderates H2	0.119*	Low
H5(c): Routine Behavior moderates H3	0.105	No Support
H6: Contextualization moderates H4	0.594***	Strong

*** p < 0.01 , ** p < 0.05 , * p < 0.1

Table 6. – Summary of support for hypotheses in our proposed framework



***Significant at the 0.01 level (2-tailed);
**Significant at the 0.05 level (2-tailed);
*Significant at the 0.10 level (2-tailed);
(S) = Supported
(NS) = Not Supported

Figure 2. Results of the structural model for our proposed framework

Conclusion

Our proposed framework helps to identify the major factor(s) responsible for the judgment of regular email users towards phishing emails. Often email users fall victim to phishing emails with the potential appeal of winning any reward or losing something. Our study identifies that potential loss appeal receives much stronger attention than rewards, and the user response is significantly moderated by the individual's prior cyber-hygiene experience. Further, the replicated design of email content, such as company logo, copyright symbol, secure-sign-on symbols, and digital signatures (in case of e-commerce firms) can often mislead users and fall prey to phishing emails.

References

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. Computers in Human Behavior, 60, pp. 185-197.

Biswas, B., & Mukhopadhyay, A. (2017). Phishing detection and loss computation hybrid model: A machine-learning approach. *ISACA Journal*, *1*, 22-29.

Butavicius, M., K. Parsons, M. Pattinson, and A. McCormac. 2015. "Breaching the Human Firewall: Social Engineering in Phishing and Spear Phishing Emails." In Australasian Conference on Information Systems. arXiv:1606.00887.

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.

Egelman, S., Cranor, L. F., & Hong, J. (2008). You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, pp. 1065-1074.

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, *59*, 26-44.

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability, Journal of the Association for Information Systems, 18(1). pp. 22-44.

Gordon, M. E., Slade, L. A., & Schmitt, N. (1986). The "science of the sophomore" revisited: From conjecture to empiricism. Academy of Management Review, 11(1), pp. 191-207.

Hong, J. (2012). The state of phishing attacks. *Communications of ACM*, *55*(1), pp. 74-81.

Jonassen, D. H. (2000). Toward a design theory of problem solving. *Educational technology research and development*, *48*(4), 63-85.

Kahneman, D., and A. Tversky. 1984. Choices, Values, and Frames, American Psychologist 39 (4): 341–350.

Meyer, D. E., & Schvaneveldt, R. W. (1971). Facilitation in recognizing pairs of words: evidence of a dependence between retrieval operations. *Journal of Experimental Psychology*, *90*(2), 227.

Oliveira, D., H. Rocha, H. Yang, D. Ellis, S. Dommaraju, M. Muradoglu, D. Weir, D. Soliman, T. Lin, and N. Ebner. 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, CHI '17, 6412-6424.

Ringle, C., Da Silva, D., & Bido, D. (2015). Structural equation modeling with the SmartPLS.

Rogers R.W. (1983). Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. In: Cacioppo JT, Petty RE, editors. Social psychophysiology. NewYork: Guilford Press. pp. 153–176.

Schatz, D., & Bashroush, R. (2017). Economic valuation for information security investment: a systematic literature review. Information Systems Frontiers, *19*(5), 1205-1228.

Schechter, S. E., Dhamija, R., Ozment, A., & Fischer, I. (2007, May). The emperor's new security indicators. In *2007 IEEE Symposium on Security and Privacy (SP'07)* (pp. 51-65). IEEE.

Sillence, E., P. Briggs, P. Harris, and L. Fishwick. 2006. "A Framework for Understanding Trust Factors in Web Based Health Advice." International Journal of Human-Computer Studies 64: 697–713.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, *46*(2), pp. 186-204.

Verizon. 2016. "2016 Data Breach Investigations Report." Accessed January 23, 2019.
http://www.verizonenterprise.com/verizon-insights-lab/dbir/

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model, Decision Support Systems, 51(3), pp. 576-586.

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

Williams, E. J. & Polage, D. (2018): How persuasive is phishing email? The role of authentic design, influence and current events in email judgements, *Behaviour & Information Technology*.

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Research note—influence techniques in phishing attacks: an examination of vulnerability and resistance. *Information systems research*, *25*(2), 385-400.