

RESEARCH QUESTION

We begin our research question by presenting frequency table that characterizes the properties of phishing emails in our dataset.

RQ1: What are the characteristics of the reported phishing emails?

1. What are the most targeted sectors?
2. What are the reasons frequently used?
3. What are the methods used?
 - a) How many emails that contain and do not contain hyperlink?
 - b) How many emails that contain hyperlink AND/OR obfuscated link?
 - c) How many emails that contain and do not contain attachment (PDF attachment OR ZIP attachment OR HTML attachment OR Unknown attachment)?
 - d) How many emails that contain hyperlink AND/OR attachment?
 - e) How many emails that contain hyperlink AND NOT request to click link?
 - f) How many emails that contain attachment AND NOT request to open attachment?
 - g) How many emails that request to click link OR request to open attachment OR request email reply OR request to call by phone?
 - h) How many emails that request to click link also request to open attachment?
 - i) How many emails that request to click link AND request to open attachment AND request to email reply AND request to call by phone?

In our coding cialdini's principles, we identified phishing emails with fake logos and signatures that may mistakenly regard them as legitimate by average internet users. For example in the context of phishing email, signature such as "Copyright 2013 PayPal, Inc. All rights reserved" or "Administrator Team" and Amazon logo were used to show the "aura of legitimacy". In the real world society, telemarketers

and seller has been using authoritative element to increase the chance of potential consumer's compliance [?]. It means that they have to provide information in a confident way. Consumers will have their doubt if sellers unsure and nervous when they offer their product and services to consumers. This principle has been one of the strategies in a social engineering attack to acquire action and response from a target [?]. Based on this conception, phishers may also have applied the same principle and as a dominance principle of all other principles. Therefore, we hypothesize that

H1: Authoritative principle is dominating than other principles

It makes sense if government has the authority to compose laws and regulations and to control its citizens. Government sector includes court and police department also authorize to execute penalties if any wrongdoing happens within their jurisdiction. However, government may not have to be likeable to enforce their rules and regulation. Similarly, an administrator who control his network environment may behave in a similar fashion as government. Hence, in our dataset we hypothesize that

H2: There is a significant association between Government sector and authority principle

H3: There is a significant association between Administrator and authority principle

Similar to authority principle that may trigger reactance, scarce items and shortage may produce immediate compliance from people. In essence, people will react when their freedom is restricted about valuable matter when they think they are capable to make a choice among different options [?]. In the phishing email context, an email from Royal Bank inform us that we have not been logged into our online banking account for a quite some time, as a security measure, they must suspend our online account and if we would like to continue to use the online banking facility, we have been asked to click the link provided. Potential victim may perceives their online banking account as their valuable matter to access facility and information about their savings. Consequently, potential victim may react to the request because of their account could be scarce and restricted. In the real world example, a hard worker bank customer who perceives money is a scarce item may immediately react when his bank inform him that he is in danger of losing his savings due to "security breach". We therefore hypothesize that

H4: There is a significant association between Financial sector and scarcity principle

As we describe in our decision making consideration section, people tend to trust those they like. In a context of persuasion, perpetrators may find it more difficult to portray physical attractiveness, instead they are relying on emails, websites and phone calling [?]. To exhibit charm or charisma to the potential victims, perpetrators may gain their trust by establishing friendly emails, affectionate websites and soothing voice over the phone. In the phishing email context, Amazon praises our existence in an appealing fashion and extremely values our account security so that no one can break it. Based on that scenario, E-commerce/Retails sector may applied likeability principles to gain potential customers. We therefore hypothesize that

H5: There is a significant association between E-Commerce/Retails sector and likeability principle

Tajfel, et al. argued that people often form their own perception based on their relationship with others in a certain social circles [?]. This lead to affection of something when significant others have something to do with it. Social proof is one of the social engineering attacks based on the behavioral modeling and conformance [?]For example, we tend to comply to a request when a social networking site asks us to visit a website or recommends something and mention that others have been visiting the website as well. Thus, we hypothesize that

H6: There is a significant association between Social networks sector and social proof principle

As we describe in our decision making consideration section, authority has something to do with “aura of legitimacy”. This principle may lead to suggest the limitation on something that we deemed valuable. For example, a perpetrator masquerades as an authority and dressed as police officer halted us on the road, the perpetrator may tell us that we did something wrong and he will held our driving license if we do not pay him the fine. In the phishing email context, an email masquerades as “System Administrator” may tell us that we exceeded our mailbox quota, so the administrator must freeze our email account and we could re-activate it by clicking the link provided in the email. Based on that scenario, we know that it has authority principle and also has scarcity principle. Therefore, we hypothesize that

H7: There is a significant association between authority principle and scarcity principle

We often stumbled a group of people requesting to donate some of our money to the unfortunate people. Evidently, they would use physical attractiveness and kind words to get our commitment to support those people. Once they have got our commitment, they start asking for donation and we tend to grant their request and give some of our money to show that we are committed. Phishing email could be similar, for example, Paypal appreciates our membership on their system and PayPal kindly notifies us that in the membership term of agreement, they would performing annual membership confirmation from its customers. Based on that scenario, we know that the email has likeability principle and also has consistency principle. We would like to know if it is the case with phishing email in our dataset. Therefore, we hypothesize that

H8: There is a significant association between likeability principle and consistency principle

In contrast, physical attractiveness and kind words will not work if there is an element of fear or authoritative instructions. Based on this, we hypothesize that

H9: There is no significant association between authority principle and likeability principle

We think it make sense if a fraudster tries to make his fake product as genuine as possible and hide the fabricated element of his product. There are also fraudster that did not make his product as identical as the legitimate product. In the phishing email context, we perceives fake product as hyperlink in the email, phishers do not necessarily obfuscates the real URL with something else. Logically, such phishers do not aim to make a high quality of bogus email, rather they aim to take chances in getting potential victims that are very careless. This leads to our hypothesis that say

H10: There is a significant association between phishing email that contain hyperlinks and obfuscated link variable

It is conspicuous from our knowledge if a sales agent tries to sell us a product, it would be followed by the request element to buy the product as well. However, it will not make sense if he tries to sell his product but he requests to buy another company's product. In the phishing context, phishers do not put hyperlink or attachment if they do not request an action to somehow tell potential victim to open the link or attachment. This leads us to two hypotheses which state

H11: There is a significant association between phishing email that contain hyperlink and request to click a link

H12: There is a significant association between phishing email that contain attachment and request to open attachment

We sometimes find it suspicious if a person dressed as police officer that does not have a badge carried with him, unless he is a fake police officer. Consequently, to build up even more “aura of legitimacy”, a fake police officer may carry a fake badge with him. In phishing email scenario, he dressed as police officer as authority principle and a fake badge as the presence of fake logo or fake image in the content of the email. In the phishing email context, an email that says from Apple, would not be believable if the logo from Apple is not included. Thus, we hypothesize that

H13: There is a significant association between authority principle and the presence of image variable

Apart from the target analysis, we also investigate the reason why potential victim responds to phisher’s request. Phishing email that implies our account expiration would have scarcity principle because the account itself may very valuable for us and is in danger to be expired or terminated. Therefore, we hypothesize that

H14: There is a significant association between account related reason and scarcity principle

Similar from the hypothesis H14, it is sensible if a phishing email which contains account related reason such as reset password or security update, would tend to have a hyperlink for the potential victim to redirected towards phisher’s fake website or malware. This leads to our hypothesis that say

H15: There is a significant association between account related variable and hyperlink variable

When an email is requesting to review some reports or reviewing the attached ticket, potential victim may turn his attention to the aura of legitimacy of the email design. Whether potential victim may look for logo/image/signature or sender’s email address to justify the perception of authentic email. Based on this scenario, we know that the email has document related variable and authority principle. Thus, we hypothesize that

H16: There is a significant association between document related reason and authority principle

Analogous with the hypothesis **H15**, it is make sense if a phishing email which has document related reason such as reviewing contract agreement or reviewing resolution case, would tend to have a file to be attached. We therefore hypothesize that

H17: There is a significant association between document related reason and attachment variable

We think it is make sense if a phishing email which use HTML to present their email design may tend to increase the attractiveness to the potential victim. Consequently, unsuspected victim may respond to the request just because of the email design is attractive. Therefore, we hypothesize that

H18: There is a significant association between UseHTML variable and likeability principle
