1

DISCUSSION & CONCLUSION

In the previous chapter , we have addressed the results of our study in considerable detail. Now in this chapter, we look at how our findings answer our research questions and whether the findings are consistent with the hypotheses we described in **??**.

Before we conclude our main analysis, we would like to conclude of our experimental exploration on phishing bad neighborhood and the differences between phishing vs original. Our data suggests that there are some possibilities of phishing bad neighborhood (10% hacked, 35% higher possibilities, 55% less possibilities), there are much more legitimate domains that are exist. When we look at phishing vs original analysis, it suggests 87% of the total HTML codes are maintaining the appearance closer as the target while 12.5% are completely different with its target. Based on this, we can conclude while there are small possibilities of "bad neighborhood" in term of phishing, phishers generally do not host their phish in one certain networks of internet infrastructure. The consequence is that it hinders the effort of security expert to detect phishing in a certain networks of internet infrastructures. We can also conclude that most of the phishes appear the same as its target considering to replicate a web page can be done with a little effort. However, fragments of suspicious codes can be spotted when the HTML source is closely examined. This can help an automated phishing detection in HTML source level.

Our research was mainly aimed to to characterize phishing email properties considering persuasive principles by finding the association within generic properties as well as the relationship between persuasive principles and these generic properties. We looked at what are the generic properties of phishing email and how relevant are the persuasive principles to its generic properties. The data was obtained from national security organization based in Netherlands that handles reports on fraud including phishing.

An important aspect of our research was that persuasive principle has variety of strengths in respect of influence depending on the individual person. Thus we have addressed our rationale in synthesizing persuasive principles on phishing emails. In addition, persuasion technique as a social engineering has been and remains successful in exploiting human factor vulnerability in order to influence people to have a positive response in favor of the person who requested it. Yet, it is almost absent from the computing literature perspective[**?**].

To answer the first research question *RQ1*, based on our findings, we can conclude in respect to the characteristics of reported phishing emails in the following points:

- When an attachment(s) is included in a phishing email, it will likely to attach ZIP or HTML file.
- Requesting to click URL is the most prevalent method
- Most of the phishes are using HTML code with the presence of URL(s)
- Financial sector is the most common target
- Most of the phishing emails use account related as a pretext to manipulate intended victims
- Authority principle distributed throughout the sample
- Phishing email which has account related reason as a pretext, will likely to include URL(s)
- Clear instructions to request an action from recipients
- URL most likely to be obfuscated
- A government targeted phish will likely to have a document related reason
- Phishing email which has document related reason as a pretext, will likely to include an attachment(s)

To answer the second research question *RQ2*, we look at how relevant are the persuasive principles to phishing email properties, we find that 100% government targeted emails are having authority principle and 95.9% of non government targeted email are also having authority principle. Our data suggests that there is no significant association between government targeted email and authority principle. Similarly, administrator and non administrator targeted emails are both high in respect to authority principle. Moreover, our result on authority principle and image(s) presence in a phishing email suggests that there is no association between these two variables. This indicates that authority is indeed a dominating principle and have higher chance to be the main technique of a phishing email. When we look at financial targeted sector and scarcity principle, we find that both financial and non financial targeted emails are less chance to have scarcity principle. Apart from our hypothesis related to financial sector and scarcity principle, if we look deeper, administrator targeted emails are likely to have scarcity principle. In contrary, non administrator targeted emails are less likely to have scarcity principle. When we look at account related phishing and scarcity, we find that

there is a highly significant relationship between them. This means that if a phishing email involve in account related reason, the higher chance of scarcity principle as a persuasion technique. Our next finding for relationship between e-commerce/retails targeted emails indicates that this sector contributes less number of likeability principle as both e-commerce/retails and non-ecommerce/retails targeted emails have high number of non-likeability principle. Similarly, our data suggests that there are no significant association between social media targeted emails and social proof principle. However, we find that there is a significant relationship between the use of HTML and likeability principle, this suggests that likeability phishing email tend to use HTML code to persuade unsuspecting victim.

Another observation on authority and scarcity principle suggests that there is no significant association between them, as both authoritative and non-authoritative emails contribute less percentage on scarcity principle. We have also observed whether likeability and consistency have a relationship, our data suggests that there is a significant association between them. Our result signifies that the higher likeability, the lower chance to have consistency principle.

Table 1: Overview of verified hypotheses

Hypotheses	Category	Accept	Reject
H1	A[a]		X
H2	A		X
H3	A		X
H4	A		X
H5	A		X
H6	A		X
H7	A		X
H8	B[b]	X	
H9	B	X	
H10	B	X	
H11	A		X
H12	A	X	
H13	B	X	
H14	B	X	
H15	B	X	
H16	A	X	

a Related to persuasion principles
b Related to generic structural properties

Overall, although there are many hypotheses in respect of persuasion principles are rejected, some of them are accepted. This conclude the extent of involvement is low between persuasion principles and generic structural properties of a phishing email. Our research sheds light on the characteristics of phishing email considering persuasive principle as human factor in the real world analysis which has not been done yet. Table 1 summarizes the overview of verified hypotheses.