NURUL AKBAR

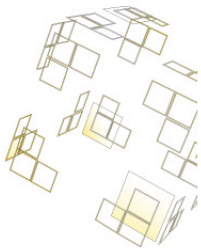
TITLE WILL GO HERE

Put something HERE

HERE

HERE & HERE

(refer to **??** for more information)



UNIVERSITEIT TWENTE.

TITLE WILL GO HERE

NURUL AKBAR

UNIVERSITY OF TWENTE.

Supervisors:
Prof.Dr.P.H. Hartel
E.E.H. Lastdrager MSc.

SERVICES, CYBERSECURITY AND SAFETY RESEARCHGROUP
Faculty of Electrical Engineering, Mathematics and Computer Science
University of Twente
August 2014 – version 1

The life of this world is only the enjoyment of deception.

— Quran 3:185

ABSTRACT

Short summary of the contents in English...

ZUSAMMENFASSUNG

Kurze Zusammenfassung des Inhaltes in deutscher Sprache...

We have seen that computer programming is an art,
because it applies accumulated knowledge to the world,
because it requires skill and ingenuity, and especially
because it produces objects of beauty.

— **?** [**?**]

ACKNOWLEDGMENTS

acknowledgments here

The LyX port was initially done by Nicholas Mariette in March 2009 and continued by Ivo Pletikosić in 2011. Thank you very much for your work and the contributions to the original style.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LISTINGS

ACRONYMS

AOL American Online

URL Uniform Resource Locator

IP Internet Protocol

TLD Top Level Domain

1 INTRODUCTION

1.1 PROBLEM STATEMENT

With the enormous growing trends of information technology in modern generation, the evolution of digital era has become more mature in the sense of effectiveness and easiness for societies. Trusted entities such as financial institutions may offer their products and services to the public through the Internet. Consequently, societies are hoping to utilize technology advancement such as emails, websites, online payment system, social networks to achieve their tasks efficiently, affordable and more relevant. However, the advancement in information and communication technology has been a double-edged sword. It becomes easier to get personal information about someone in the cyber world. Cyber criminals see this opportunity as a way to manipulate consumers and exploit their confidential information such as usernames, passwords, bank account information, credit card or social security numbers.

One of the well known cyber crimes is called phishing. Phishing attacks aim to gain a financial benefit by masquerading legitimate institutions [31]. Moreover, phishing techniques may associated with fake emails and fake websites, however, the essence of this malicious behavior is the art of social engineering and deception [31][2][14][32][29] i.e. how to trick the potential victims into disclosing their sensitive information. To illustrate one specific example; a phisher impersonates a well-known bank institutions and sends fake email announcing there is system upgrade to its customers, so the phisher would ask the customers to verify their usernames, passwords and credit card numbers in order to complete the system upgrade. In worst case, a clueless bank customer would have no idea and fail to ascertain that legitimate bank institutions would never ask for such things. Consequently, an unsuspecting victim might took the bait into divulging their sensitive information to the perpetrators. More concrete mechanism to carry out phishing attacks is that when the phishers send a large number of phishing emails which include malicious link or URL which redirect recepient to a fake website. A phishing email might be resembling a legitimate email so that unsuspecting victim might think that it is a genuine. By looking like a genuine email, it would help to circumvent the filtering system [47]. One of phishing email methods is providing a malicious URL within its content, however, filtering systems of phishing email may have access to blacklist database of URLs that are currently being pushed, such as crowd

sourced Phishtank. So the phishers might diverge the URL to bypass the matches.

To make phishing email efficient, its context might require potential victim to urgently act upon it, for example an email informs about suspended account in a banking website. Phishing attacks are carried out using fake emails, fake websites and often phishers may exploit the end user's web browser to bypass warnings and URL information. Several countermeasures have been studied to detect phishing emails, such as the technique of looking for bit string that are previously determined as spams and phishing emails [74]. The common characteristics of fake email sent by the phishers would be misleading hyperlinks and misleading header information [82, 83]. Furthermore, one of the non technical approach to defense against cyber fraud such as security awareness education to the public to ignore links within an email, even though the source of the email appear to be legitimate [68].

1.2 RESEARCH GOAL

The main goal of this research is to synthesize persuasive principle and characterize phishing email properties. These properties can be divided into several parts. Each of these parts and persuasive principle will be introduced as a variable in our main analysis. We will look for relationship and correlation between these variables. The integration of persuasive principles can be used to generate a new method of detecting phishing email as one of the primary delivery techniques of phishing attacks.

1.3 RESEARCH QUESTIONS

To be able to meet the goal, we formulated two main research questions as follows:

- RQ1: What are the characteristics of reported phishing emails?
- RQ2: How relevant are the persuasive principles to the generic phishing email properties?

To answer our research questions, several aspects of phishing email characteristics and hypotheses will be established in Chapter 4.

1.4 STRUCTURES

This research project is structured as follows. Problem statement and research goal has been explained in chapter 1. Background and literature reviews will be discussed in chapter 2. Preliminary analyses will be conducted in chapter 3 along with preliminary methods and

results. In chapter 4, we will explain more about our main research questions and hypotheses. In chapter 5, we will discuss our main data analysis and results. Lastly, in chapter 6 we will present our discussion and conclusion of the research project.

2

BACKGROUND & LITERATURE REVIEW

While the Internet has brought convenience to many people for exchanging information, it also provides opportunities to carry malicious behavior such as online fraud on massive scale with a little cost to the attackers. The attackers can manipulate the Internet users instead of computer system (hardware or software) that significantly increase the barriers of technological crime impact. Such human centered attacks could be done by social engineering. Phishing is a form of social engineering that aims to retrieve credential from online users by mimicking trustworthy and legitimate institutions [31]. These fraudulent attacks are most frequently done by electronic communication such as emails to direct users to fake websites and prompt for sensitive information.

This chapter provides an overview to phishing modus operandi and its current countermeasures such as detection and prevention techniques along with a brief exploration of direct and indirect cost of phishing attacks.

2.1 WHAT IS PHISHING?

Phishing has a similar basic principle as 'fishing' in the physical world. Instead of fish, online users are lured by authentic looking communication and hooked by authentic looking websites. Not only that, online users also may be lured by respond to a phishing email, either replying or clicking an obfuscated link within its content. There are diverse definitions of phishing in our literature reviews, therefore, we would like to discuss about its universal definition in later section. However, one of phishing definitions accoding to Oxford dictionary:

> "A fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online" [15].

Several studies suggest that phishing is form of online criminal activity by using social engineering techniques [31][79][29][4]. An individual or a group who uses this technique is called *Phisher(s)*. After successfully gaining a sensitive information from the victim, phishers use this information to access victim's financial accounts or committing credit card frauds. The technique of phishing may vary, but the most common technique of phishing attacks done by using fraudulent emails and websites [32]. A fraudulent website is designed in

such a way that it may be identical to its legitimate target. While it may be true, phishing website also could be completely different with its target as there is no level of identicalness. However, Preliminary analysis on what changed or added in phishing website would be conducted in the later section.

2.1.1 *The History*

The first time the term "phishing" was published by the American Online (AOL) UseNet Newsgroup on January 2, 1996 and was started to expand in 2004 [62]. Since then, we considered phishing development in cyberspace has been flourishing by phishers to make profit. Total losses due to phishing in 2004 reached more than U.S. $ 2 billion, it was involving more than 15,000 sites that become victims [21]. We will try to discuss about direct and indirect cost at present days in the later section. Evidently, Jakobsson, et al. [31] mentioned that in the early years of 90's (according to [62] it was around 1995) many hackers would create bogus AOL user accounts with automatically generated fraudulent credit card information. Their intention to give this fake credit card information was to simply pass the validity tests performed by AOL. By the time the tests were passed, AOL was thinking that these accounts were legitimate and resulted to activate them. Consequently, these hackers could freely access AOL resources until AOL tried to actually bill the credit card. AOL realized that these accounts were using invalid billing information, thus deactivated the account.

While creating false AOL user accounts with fake credit card information was not exactly phishing attacks, but AOL's effort to counter against the attacks was leading to development of phishing. This countermeasure includes directly verifying the legitimacy of credit card information and the associated billing identity, forced hackers to pursue alternative way [31]. Hackers were masquerading as AOL's employees asking to other users for credit card information through AOL instant messenger and email system [62]. Jakobsson et al. suggest that phishing attacks were originating from this incident [31]. Since such attack has not been done before, many of users have been victimized by then. Eventually, AOL enforced warning system to the most of its customers to be vigilant when it comes to sensitive information [62]. At the present day, phishing attacks might not only being motivated by financial gain but also political reason, and they have been emerging not only aim to AOL users, but also any online users. Consequently, large number of legitimate institutions such as PayPal and eBay are being spoofed.

2.1.2 *The universal definition*

Before we begin to understand deeper about how and why phishing attack works, we will briefly explore common phishing definition. Currently, there is no consensus definition, since almost in every research papers, academic textbook or journals has its own definition of phishing [31, 32, 71, 9, 60, 30, 14]. Phishing is also constantly evolving, so it might be very challenging to define its universal terminology. There is not so much study that specifically addresses the standard of phishing definition. However, one research conducted by Lastdrager [39] addressed to achieve consensual definition of phishing. Before we comply with one consensual phishing terminology, we will take a look at various phishing definitions from other sources:

> *"Phishing is the act of sending a forged e-mail (using a bulk mailer) to a recipient, falsely mimicking a legitimate establishment in an attempt to scam the recipient into divulging private information such as credit card numbers or bank account passwords"* [32]

> *"Phishing is a form of Internet scam in which the attackers try to trick consumers into divulging sensitive personal information. The techniques usually involve fraudulent E-mail and web sites that impersonate both legitimate E-mail and web sites"* [71]

> *"Phishing is an attack in which victims are lured by official looking email to a fraudulent website that appears to be that of a legitimate service provider"* [9]

> *"In phishing, an automated form of social engineering, criminals use the internet to fraudulently extract sensitive information from businesses and individuals, often by impersonating legitimate web sites"* [60]

It is noteworthy that the definition described by James, et al, Tally, et al, and Clayton, et al. [32, 71, 9] specifies that the phishers only use email as a communication channel to trick potential victims. While it might be true because using email would greatly cost effective, but we believe that phishing is not only characterized by one particular technological mean, as phishers can also use any other electronic communication to trick potential victims (i.e private message on online social network). This definition is also similar to dictionary libraries [15, 16, 75] that mention email as a medium communication between phishers and users.

We believe that standard definition of phishing should be applicable in most of phishing concept that are presently defined. Consequently, the high level of abstraction and is required to build common definition on phishing. We also argued that the definition of phishing should not focus on the technology being used but rather on the methodology how the deception being conducted, an "act" if you

will. Therefore, We follow the definition of phishing by Lastdrager [39] which stated:

> *"Phishing is a scalable act of deception whereby impersonation is used to obtain information from a target"*

According to Lastdrager [39], to achieve this universal definition, a systematic review of literature up to August 2013 was conducted along with manual peer review, which resulted in 113 distinct definitions to be analyzed. We thereby agree with Lastdrager [39] that this definition addresses all the essential elements of phishing and we will adopt it as universally accepted terminology throughout our research.

2.2 THE COSTS OF PHISHING ATTACKS

It is a challenging task to find a real cost from phishing attacks in term of money or direct cost. This due to financial damage for bank is only known by banks and most institutions do not share this information with the public. Evidently, Jakobsson et al. argue that phishing economy is consistent with black market economy and does not advertise its successes [31]. On this section, a brief explanation of direct and indirect cost on phishing attack will be illustrated based on literature reviews.

According to Jakobsson et al., direct cost is depicted by the value of money or goods that are directly stolen through phishing attack [31]. While indirect cost is the costs that do not represent the money nor goods that are actually stolen, but it is the costs has to be paid by the people who handle these attacks [31] (i.e. time, money and resources spent to reset people password).

As we mentioned earlier, the difficulty of assessing the damage on phishing attacks is caused by banks and institutions that keep this information themselves and the unwillingness of many users to share to acknowledge that they have been victimized by phishing attacks. This happens because of fear of humiliation, financial loses, or legal liability [31]. Evidently, studies estimate the damage ranging from $61 million [26] to $3 billion per year [50] of direct losses to victims in the US only [27][55]. In addition, the Gartner Group claimed to estimate of $1.2 billion direct losses of phishing attack to US banks and credit card companies for the year 2004 [41]. By the 2007, it escalated to more than $3 billion loss [51]. The estimation also performed by TRUSTe and Ponemon Institute that stated the cost of phishing attack was up to $500 millions losses in the US for the same year [1]. Recently, RSA FraudAction gives monthly reports of how much the global phishing cost and we compiled them together to make a line graph in Figure 1 [22]. However, they do not specify whether this

1 http://www.theregister.co.uk/2004/09/29/phishing_survey/

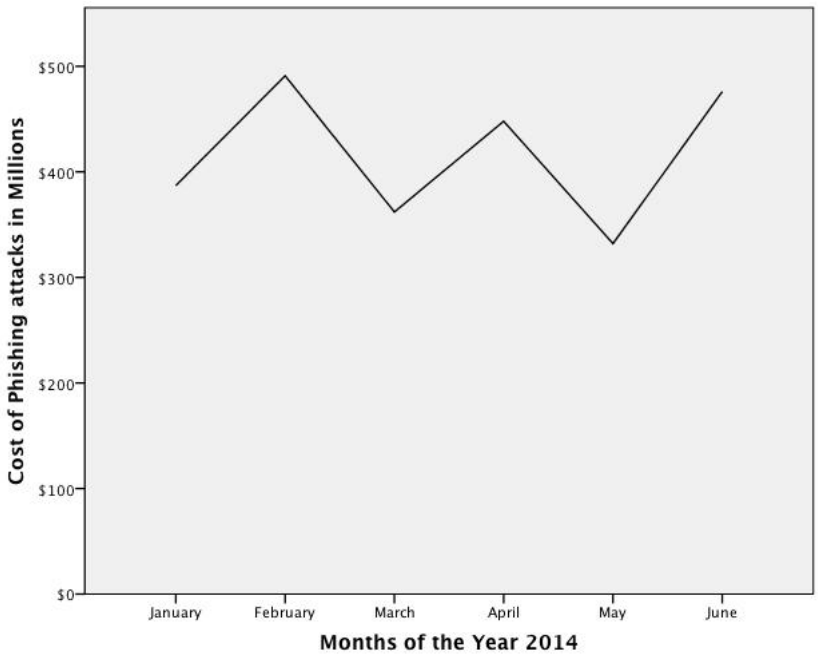


Figure 1: Global phishing cost from January 2014 until June 2014 [22]

damage is direct cost or indirect cost. In their study, we can see that there are fluctuation of losses in term of money. Furthermore, this total cost is indeed in accordance with the total cost ranging from $61 million to $3billion per year [26, 50, 27, 55].

2.3 HUMAN FACTOR

Phishing attacks generally aim to manipulate end users to comply phisher's request. Such manipulation in phishing attacks is achieved by social engineering. It means that human element is tightly associated with phishing. But how do phishers compose such deception? How come online users are gullible to these attacks?

Cialdini suggests that there are six basic principles of persuasion [8], that is, the technique of making people grant to one's request. These principles include; *reciprocation, consistency, social proof, likeability, authority and scarcity*. Reciprocation is the norm that obligates individuals to repay in kind what they have received, return the favor or adjustment to smaller request [8]. Consistency is a public commitment where people become psychologically become vested in a decision they have made [79][8]. Social proof is when people model the behavior of their peer group, role models, important others or because it is generally "fashionable" [79]. Stajano, et al. suggest people will let their guard down when everybody around them appears to share the same risk [69]. Likeability is when people trust and comply with requests from others who they find attractive or having credibility [79, 8]. While it is our human nature not to question authority,

it can be used to engender fear, where people obey commands to avoid negative consequences such as losing a privilege or something of value, punishment, humiliation or condemnation [8, 79]. Stajano, et al suggest that scarcity is related to time principle, that is, when we are under time pressure to make important choice, we tend to have less reasoning to make decision [69]. We will use these principles as our foundation in synthesizing phishing email corpus with human factor.

Human as the "weakest link" in computer security has been exists and exploited for ages. And yet, security designers blame on users and whine "the system I designed would be secure, if only users were less gullible" [69]. Stajano, et al. stated that "a wise security designer would seek a robust solution which acknowledge the existence of these vulnerabilities as unavoidable consequence of human nature and actively build countermeasures that prevent this exploitation" [69].

2.4 MODUS OPERANDI

As we mentioned earlier, Phishing attack is a form of cybercrime. The modus operandi usually carried out firstly by creating a fake website that spoofs legitimate website such as financial website, either identical or not identical as long as the phishers get responds from unsuspected victims. After that, the phishers will try to trick the potential victim to submit important information such as usernames, passwords, PINs, etc. through a fake website that they have created or through email reply from victims. With the information obtained, they will try to steal money from their victims if target institution is a bank. Phishers employ variety of techniques to trick potential victims to access their fraudulent website. One of the typical ways is by sending illicit email in a large scale claiming to be from legitimate institution. In the email content, they usually imitate an official-looking logo, using good business language style and often also forge the email headers to make it look like originating from legitimate institution. For example, the content of the email is to inform the user that the bank is changing its IT infrastructure, and request urgently that the customer should update their data with the consequence of loosing their money if the action does not take place. When the user click the link that was on the email message, they will be redirected to a fraudulent website, which will prompt the victim to fill in the details of their information. While there are various techniques of phishing attack, we will address the common phases of phishing that we analyzed by literature survey by several studies and also we will address our own phishing phases. These phases are compiled in Table 1.

Table 1: Compilation of phishing phases

J. Hong [27]
1. Potential victims receive a phish 2. The victim may take a suggested action in the message 3. The phisher monetizes the stolen information
Frauenstein, et al. [23]
1. Planning 2. Email Design 3. Fabricated story 4. Threatening tone/Consequences 5. Spoofed website
Wetzel [77]
1. Planning 2. Setup 3. Attack 4. Collection 5. Fraud 6. Post-attack
Tally, et al. [71]
1. The attacker obtains E-mail addresses for the intended victims 2. The attacker generates an E-mail that appears legitimate 3. The attacker sends the E-mail to the intended victims in a way that appears legitimate and obscures the true source 4. The recipient opens a malicious attachment, completes a form, or visits a web site 5. Harvest and exploitation
Emigh [20]
1. A malicious payload arrives through some propagation vector 2. The user takes an action that makes him or her vulnerable to an information compromise 3. The user is prompted for confidential information, either by a remote web site or locally by a Web Trojan 4. The user compromises confidential information 5. The confidential information is transmitted from a phishing server to the phisher 6. The confidential information is used to impersonate the user 7. The phisher engages in fraud using the compromised information
Nero et al. [56]
1. Preparation 2. Delivery of the Lure 3. Taking the Bait 4. Request for Confidential Information 5. Submission of Information 6. Collection of Data 7. Impersonation 8. Financial Gain

Based on the example scenario explained earlier, phishing attacks may consist of several phases. J. Hong [27] argued that there are three major phases. while Frauenstein, et al. [23] suggested that there are five main processes are used to perform phishing attacks based on the perpective of the attacker.

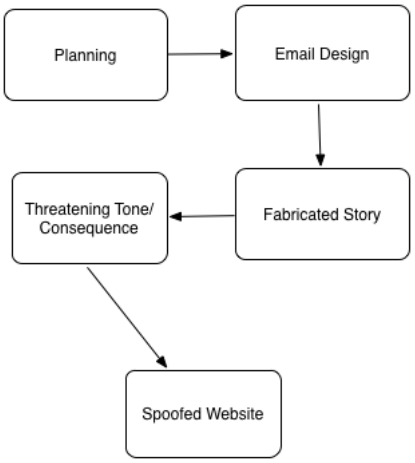


Figure 2: Phishing processes based on Frauenstein[23]

As we illustrated in Figure 2, on the first process is called *Planning*, a phisher usually would do some reconnaissance on how would the attack is executed and what information would be obtained from the victim. On the second process, the phisher would think about the design of the email. This email is desired by the phisher to look as legit as possible to potential victim. For this purpose, target institutions logo, trademark, symbol, etc. are used to make the content look official to the victim. The author called this process as *Email Design*. Figure 3 illustrates the example of fake ING bank logo in a phishing email to create "legitimate" feel[2]. On the third process, the phisher *fabricates* a story to make potential victim think that email is important. To achieve users attention, phisher might build up a story about system upgrade, account hijacked or security enhancement so that the victim would feel obliged to be informed. Evidently, this technique corresponds with Cialdini [8] that suggests there are six principles to persuade people to comply with a request. On the fourth process, a phisher usually include *threatening tone* or explain the urgency and consequences if the potential victim chooses not to take action desired by the phisher (for example; account removal, account blocked, etc.). Consequently, users may fear of their account being deleted. The last process involved with fraudulent website that has been created by the phisher. Users may falsely believe to the message given in the email and may click a Uniform Resource Locator (URL) that is embedded in the email. Subsequently, the URL would redirect users to a *spoofed website* which may prompt users' sensitive information. Furthermore, the website might be created to be as similar as possible to the target institution's website, so that potential victim may still believe that it is authentic. We will explain more on Cial-

2 http://www.martijn-onderwater.nl/wp-content/uploads/2010/03/ing-phishing.jpg

Figure 3: Example of fake ING logo in phishing email

dini's six basic tendencies of human behavior in generating positive response to persuasion [8] in a later section.

Considering that phishing attack is a process, Wetzel [77] suggested a taxonomy to make sense of the complex nature of the problem by mapping out a common attacks lifecycle, and a possible set of activities attackers engage in within each phase. The taxonomy is illustrated in Figure 4. We speculated that Wetzel's taxonomy is not analogous with Frauenstein's main phishing processes [23]. The difference is that Frauenstein et al. only focus in the design of the attack while Wetzel has added several phases like *Collection*, *Fraud* and *Post-attack*, therefore, Wetzel taxonomy is more holistic in term of phishing.

As we listed Wetzel's taxonomy in Table 1, we explain more of the taxonomy as follows:

1. *Planning*: Preparation carried out by the phisher before continue to the next phase. Example activities include identifying targets and victims, determine the method of the attack, etc.

2. *Setup*: After the target, victim and the method are known, the phisher would craft a platform where the victim's information could be transmitted and stored, for example: fraudulent website/email.

3. *Attack*: Phisher distributes their fraudulent platform so that it can be delivered to the potential victims with fabricated stories.

4. *Collection*: Phisher collects valuable information via response from the victims

5. *Fraud*: Phiser abuses victim's information by impersonates the identity of the victim to the target. For example, A has gained B's personal information to access C so that A can pose as B to access C.

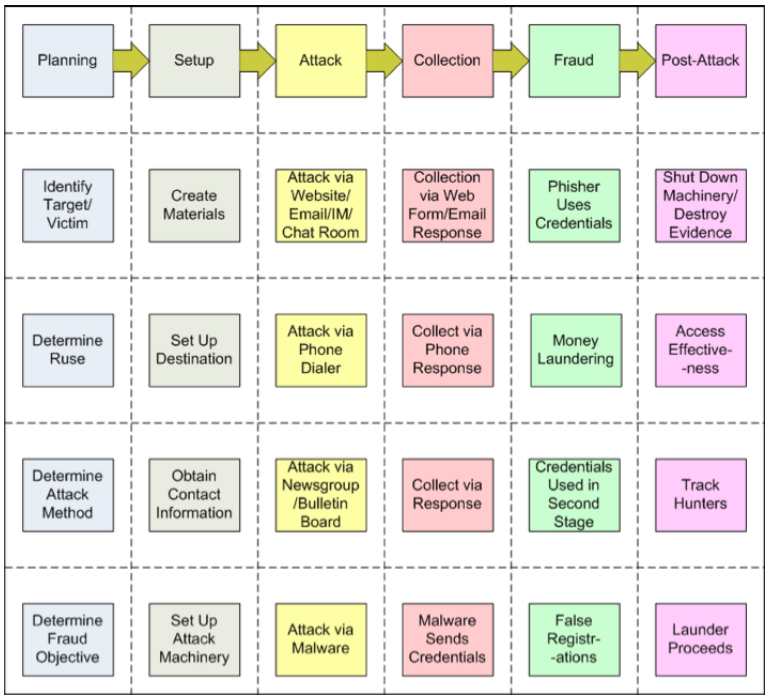


Figure 4: Phishing attack taxonomy and lifecycle[77]

6. *Post-attack*: After the phisher gained profit from the attack and abuse phases, a phisher would not want to be noticed or detected by authority. Thus, phisher might need to destroy evidence of the activities that he/she previously were executed.

Tally, et al. suggest that there are several phases involved in phishing attack based on the attacker's point of view [71]:

> "*1. The attacker obtains E-mail addresses for the intended victims. These could be guessed or obtained from a variety of sources*" this fits with planning phase.
>
> "*2. The attacker generates an E-mail that appears legitimate and requests the recipient to perform some action*" - fits with design phase.
>
> "*3. The attacker sends the E-mail to the intended victims in a way that appears legitimate and obscures the true source*" - fits with delivery and attack phase.
>
> "*4. Depending on the content of the E-mail, the recipient opens a malicious attachment, completes a form, or visits a web site*" - fits with attack phase.
>
> "*5. The attacker harvests the victim's sensitive information and may exploit it in the future*" - fits with fraud phase.

Aditionally, the phases described by Tally, et al. [71] are comparable with the information flow explained by Emigh[20] represented in Figure 5.

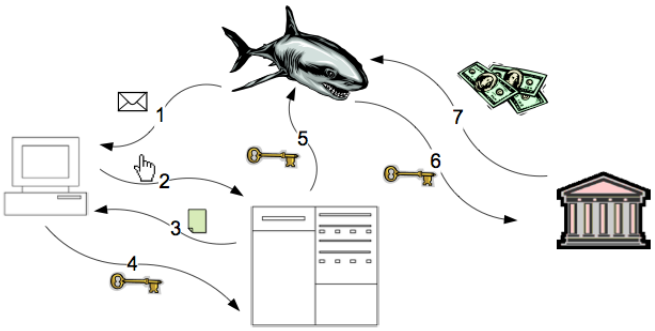


Figure 5: Flow of information in phishing attack [20]

Emigh [20] suggests the information flow of phishing attacks has seven phases. These phases is explained as follow:

> "1. A malicious payload arrives through some propagation vector.
>
> 2. The user takes an action that makes him or her vulnerable to an information compromise.
>
> 3. The user is prompted for confidential information, either by a remote web site or locally by a Web Trojan.
>
> 4. The user compromises confidential information.
>
> 5. The confidential information is transmitted from a phishing server to the phisher.
>
> 6. The confidential information is used to impersonate the user.
>
> 7. The phisher engages in fraud using the compromised information." [20]

Phishing attack steps performed by the phisher are also addressed by Nero, et al [56]. In their study, a successful phishing attack involves several phases:

> "1. Preparation
>
> 2. Delivery of the Lure
>
> 3. Taking the Bait
>
> 4. Request for Confidential Information
>
> 5. Submission of Information
>
> 6. Collection of Data
>
> 7. Impersonation
>
> 8. Financial Gain" [56]

Based on our analysis by looking at other phases from various sources, there is a major similarity between them. Therefore, we would like

to define and design our own phase that are integrated with three key components suggested by Jakobsson, et al. [31]. These key components are include *the lure*, *the hook* and *the catch*. As we designed in Figure 6, we synthesized these three components with our phases based on the attacked point of view as follows:

- The lure

1. Phishers prepare the attack
2. Deliver initial payload to potential victim
3. Victim taking the bait

- The hook

4. Prompt for confidential information
5. Disclosed confidential information
6. Collect stolen information

- The catch

7. Impersonates victim
8. Received pay out from the bank

It is important to know that in the phase 3, there are different scenarios such as; victim might be redirected to a spoofed website, victim may comply to reply the email, victim may comply to open an attachment(s) or victim may comply to call by phone. However, in Figure 6, we have only illustrated the phases if the bait was using spoofed website.

2.5 TYPES OF PHISHING

In January 2014, 8300 patients data are being compromised in medical company in the US [24]. The data includes names, addresses, date of birth and phone numbers were being stolen. Other than demographic information, clinical information associated with this data was also stolen, including social security numbers. In the April 2014, phishers have successfully stolen US$163,000 from US public school based on Michigan [3]. It has been said that the email prompted to transfer money is coming from the finance director of the school. In March 2014, Symantec has discovered phishing attack aimed at Google drive users [65]. The attack was carried firstly with incoming email asking for opening document hosted at Google docs. Users that have clicked on the link are taken to fraudulent Google login page prompted Google users credentials. Interestingly, the URL seems

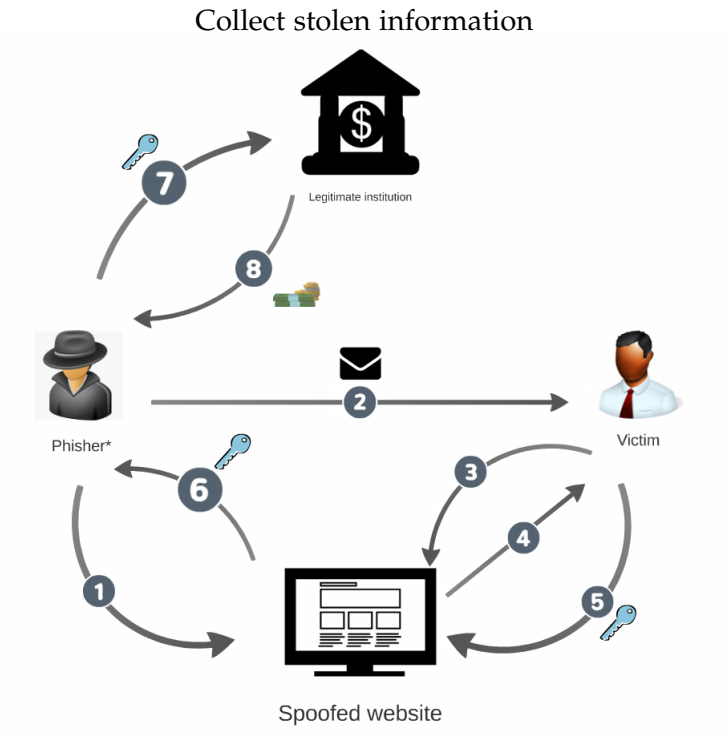


Figure 6: Information flow phishing attack

very convincing because it hosted on Google secure servers. We hypothesized that even more phishing incidents on financial area as well, but sometimes the news is kept hidden due to creditability reason.

One may ask, what type of phishing are these? What type of phishing commonly used nowadays? Evidently, based on the cost of phishing attacks in Section 2.2, the threat of phishing attacks is still alarming and might be evolving in the future with more sophisticated technique of attacks. For this reason, it might be useful to provide a brief insight on popular variants of phishing that currently exist. We will briefly explain the types of phishing which are the most relevant to our research based on Jakobsson, et al. [31]. These types of phishing is strongly related to the phishing defintion that we used, because all phishing based act of deception by the phishers.

2.5.1 *Deceptive phishing*

There are many variations based on deceptive phishing schemes. Typical scenario of deceptive phishing schemes is to send a large amount of illicit emails containing call to action asking recipients to click embedded links [31]. These variations include cousin domain attack. For example, legitimate PayPal website addressed as www.paypal.com, this cousin domain attacks confuse potential victims to believe that www.paypal-security.com is a subdivision of the legitimate website

due to identical looking addresses. Similarly, homograph attacks create a confusion using similar characters to its addresses. For example, www.paypal.com and www.paypa1.com, both addresses look the same but on the second link, it uses "1" instead of "l".

Moreover, phishers may embed a login page directly to the email content. This suggests the elimination of the need of end-users to click on a link and phishers do not have to manage an active fraudulent website. IP addresses are often used instead of human readable hostname to redirect potential victim to phishing website and JavaScript is used to take over address bar of a browser to make potential victims believe that they are communicating with the legitimate institution. We will also see few examples of malicious JavaScript on our preliminary analysis section.

Another type of deceptive phishing scheme is rock-phish attacks. They held responsible for half a number of reported incidents worldwide in 2005 [52]. These attacks evade email filters by utilizes random text and GIF images which contain the actual message. Rock phish attacks also utilize a toolkit that capable to manage several fraudulent websites in a single domain. Sometimes, deceptive phishing schemes lead to installation of malware when users visit fraudulent website and we will describe malware based phishing scheme in the next section.

2.5.2 *Malware-based phishing*

Generally, malware based phishing refers to any type of phishing which involves installing malicious piece of software onto users' personal computer [31]. Subsequently, this malware is used to gather confidential information from victims instead of spoofing legitimate websites. This type of phishing incorporates malwares such as keyloggers/screenloggers, web Trojans and hosts file poisoning.

2.6 BAD NEIGHBORHOODS ON PHISHING

In the physical world, there are parts of certain area that have higher crime rates than others (eg. Bronx in the US) which called hotspots. Evidently, it is statistically more likely that a crime will occur compared to other locations [54]. To better illustrate this analogy, the police department in Belgium [13] has put up statistical information regarding crime rates in the country. Figure 7 shows an example in 2013; there were up to 5525 car theft incidents recorded and we can see there are certain areas that have higher probability that a car got stolen. For example, Antwerp had 415 incidents whereas Berlare had only 1 car theft incident [12]. The data is not necessarily based on cities, it can be based on the residential area within a city. This

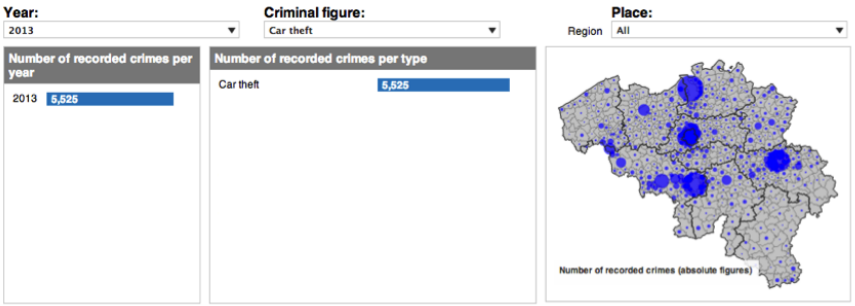


Figure 7: Belgium police record on car theft incidents in 2013

holds true that much higher crime rates in a concentrated location compared to any other locations. It is called bad neighborhood.

To reduce the crime rates in a bad neighborhood, it makes sense that the authority should put more enforcement in this location. Moreover, the citizen should avoid this location as much as they can if they want to feel much safer. Evidently, Moura, et al. suggest that the existence of bad neighborhood phenomenon also occurs in the Internet world called "Internet bad neighborhoods" [54]. There are certain networks of Internet infrastructure that contain more malicious activities that other networks. For our preliminary analysis, we will adopt formal definition of Internet bad neighborhoods or Internet Badhoods by [54] which states:

> *"Internet bad neighborhood is a set of IP addresses clustered according to an aggregation criterion in which a number of IP addresses perform a certain malicious activity over a specified period of time"*

Several studies have suggested that the source of the Internet Badhoods tend to be concentrated in certain portions of Internet Protocol (IP) address space [64, 10, 5]. Moura, et al. suggest that Internet Badhoods do not always only based on network prefixes level (e.g. /24, /32, etc..) but it can be aggregated into several levels (ISPs, Countries) [54]. Moreover, Internet Badhoods may vary depending on which application exploited. While spam is most likely distributed all around the world, however, phishing Badhoods are most likely concentrated in developed countries (e.g. US) [54]. This suggests that phishing sites are required to have more reliable hosts in term of availability, while spams are not. We will see on Chapter 3 that consists of our preliminary analysis on phishing Badhoods.

2.7 CURRENT COUNTERMEASURES OF PHISHING ATTACKS

There are various types of phishing countermeasures that implemented in different levels. Purkait has conducted an extensive research in reviewing these countermeasures which are available up until 2012

and their effectiveness [63]. He suggests that there is a classification of phishing countermeasures in separate groups and according to Purkait [63], these groups are listed as follow:

- Stop phishing at the email level
- Security and password management toolbars
- Restriction list
- Visually differentiate the phishing site
- Two facto and multi channel authentication
- Takedown, transaction anomaly detection, log files
- Anti phishing training
- Legal solution

In addition, Parmar, et al. suggests that phishing detection can be classified into two types; user training approach and software classification approach [59]. He illustrated a diagram and a table that summarizes phishing detection as countermeasures in a broad view [59]. They also argued the advantages and disadavantages of each category [59]. However, as our research mainly focuses in synthesizing phishing email with cialdini's six principles of persuasion [8], we will only briefly discuss phishing countermeasures at *restriction list* group (i.e. Phishtank), *email level* (i.e. machine learning) and *anti phishing training* group (i.e PhishGuru).

2.7.1 *Phishing detection*

2.7.1.1 *Phishtank*

One of the common approaches to detect phishing attacks is the implementation of restriction list. As the name suggest, it prevents users to visit fraudulent websites. One of the efforts to achieve restriction list, is to derive phishing URLs from Phishtank. Phishtank is a blacklisting company specifically for phishing URLs and it is a free community web based where users can report, verify and track phishing URLs [58]. Phishtank stores phishing URLs in its database and is widely available for use by other companies for creating resriction list. Some of the big companies that are using Phishtank's data includes; Yahoo Mail, McAfee, APWG, Web Of Trust, Kaspersky, Opera and Avira. In this section, we will discuss how the current literatures have to do with phish data provided by Phishtank. The first step to achieve the list of relevant literatures regarding phishtank is by keyword search in Scopus online library. By putting "Phishtank" as a keyword search, it results in 12 literatures. The next step, we read

the all the abstracts and conclusions of the resulting keyword search and we decided 11 literatures that are relevant to our research. Lastly, Table 2 summarizes the papers selected and its relevancy with Phishtank

Table 2: Summary phishtank studies

Paper title	**First author**	**Country**	**Relevancy with phishtank**
Evaluating the wisdom of crowds in assessing phishing website [53]	Tyler Moore	United Kingdom	Examine the structure and outcomes of user participation in Phishtank. The authors find that Phishtank is dominated by the most active users, and that participation follows a power law distribution and this makes it particularly susceptible to manipulation.
Re-evaluating the wisdom of crowds in assessing web Security [7]	Pern Hui Chia	Norway	Examine the wisdom of crowds on web of trust that has similarity with Phishtank as a user based system.
Automatic detection of phishing target from phishing webpage [42]	Gang Liu	China	Phishtank database is used to test the phishing target identification accuracy of their method.
A method for the automated detection of phishing websites through both site characteristics and image analysis [78]	Joshua S. White	New york, US.	Phishtank database is used to perform additional validation of their method. They also collect data from twitter using twitter's API to find malicious tweets containing phishing URLs
Intelligent phishing detection and protection scheme for online transaction [1]	P.A. Barraclough	Newcastle, United Kingdom	Phishtank features is used as one of the input of neuro fuzzy technique to detect phishing website. The study suggested 72 features from Phishtank by exploring journal papers and 200 phishing website.
Towards preventing QR code based attacks on android phone using security warning [81]	Huiping Yao	New Mexico, US.	Phishtank API is used for lookup whether the given QR containing phishing URL in the Phishtank database.

A SVM based technique to detect phishing URLs [28]	Huajun Huang	China	Phishtank database is used as validation resulting 99% accuracy by SVM method, plus the top ten brand names in Phishtank archive is used as features in SVM method.
Socio technological phishing prevention [25]	Gaurav Gupta	Australia	Analyze the Phishtank verifiers (individual/organization) to be used as anti phishing model.
An evaluation of lightweight classification methods for identifying malicious URLs [19]	Shaun Egan	Grahamstown, South Africa	Indicating that lightweight classification methods achieves an accuracy of 93% to 96% when trained data from Phishtank.
Phi.sh/$oCiaL: The phishing landscape through short URLs [6]	Sidharth Chhabra	Delhi, India	Phishtank database is used to analyze suspected phish that is done through short URLs.
Discovering phishing target based on semantic link network [76]	Liu Wenyin	Hong Kong	Phishtank database is used as test dataset to verify their proposed method (Semantic Link Network)

From our literature survey, we know that Phishtank is crowd-sourced platform to manage phishing URLs. For that reason Moore, et al. aims to evaluate the wisdom of crowds platform accomodated by Phishtank [53]. Moore, et al. suggest that the user participation is distributed according to power law. It uses to model data which frequency of an event varies as a power of some attribute of that event [38]. Power law also applies to a system when large is rare and small is common [3]. For example, in the case of individual weatlh in a country, 80% of the all wealth is controlled by 20% of population in a country. It makes sense that in Phishtank's verification system, a single highly active user's action can greatly impact the system's overall accuracy. Table 3 summarizes the comparison performed by [53] between Phishtank and closed proprietary anti-phishing feeds[4]. Moreover, there are some ways to disrupt Phishtank verification system; submitting invalid reports accusing legitimate website, voting legitimate website as phish, and voting illegitimate website as not phish. While all the scenarios described are for the phishers' benefit, the last scenario is more direct and the first two actions rather subtle intention to undermine Phishtank credibility.

To put it briefly, the lesson of crowd sourced anti-phishing technology such as Phishtank is that the distribution of user participation

3 http://kottke.org/03/02/weblogs-and-power-laws

4 The author conceals the identity of the closed proprietary company

Phishtank	Proprietary
10924 URLs	13318 URLs
8296 URLs after removing duplication	8730 URLs after removing duplication
Shares 5711 URLs in common 3019 Unique to the company feeds while 2585 only appeared in Phishtank	
586 rock-phish domains	1003 rock phish domains
459 rock phish domains found in Phishtank	544 rock phish domains not found in Phishtank
Saw the submission first	11 minutes later appear on the feed
16 hours later after its submission for verification (voting based)	8 second to verified after it appears
Rock phish appear after 12 hours appeared in the proprietary feed and were not verified for another 12 hours	

Table 3: Comparison summary [53]

matters. It means that if a few high value participants do something wrong, it can greatly impact overall system [53]. Also, there is a high probability that bad users could also extensively participate in submitting or verifying URLs in Phishtank.

2.7.1.2 *Machine learning approach*

The fundamental of phishing detection system would be to distinguish between phishing websites and the legitimate ones. As we previously discussed, the aim of phishing attack is to gather confidential information from potential victims. To do this, phishers often prompt for this information through fraudulent websites and masquerade as legitimate institutions. It does not make sense if phishers created them in a way very distinctive with its target. It may raise suspicions with result of unsuccessful attack. To put it another way, while it might be true, we speculated that most of the phishing websites are mostly identical with its legitimate websites as target to reduce suspiciousness from potential victim.

In contrast of one of blacklisting technique we saw in Phishtank that heavily depend on human verification, researchers make use of machine learning based technique to automatically distinguish between phishing and legitimate either websites or email. Basically, machine-learning system is a platform that can learn from previous data and predict future data with its classification, in this case, phish-

URL	www.naturenilai.com/form2/paypal/webscr.php?cmd=_login	
Auto-Selected	name=www, name=naturenilai, tld=com, dir=form2, dir=paypal file=webscr, ext=php, arg=cmd, arg=login	
Obfuscation-Resistant	URL	len=54, n_dot=3, blacklist=1
	Domain Name	len=19, IP=0, port=0, n_token=3, n_hyphen=0, max_len=11
	Directory	len=14, n_subdir=2, max_len=6, max_dot=0, max_delim=0
	File Name	len=10, n_dot=1, n_delim=0
	Argument	len=11, n_var=1, max_len=6, max_delim=1

Figure 8: Example lexical features [40]

ing and legitimate. In order for this machine to learn from data, there should be some kind of inputs to classify the data, it is called features or characteristics.

Furthermore, there are also several learning algorithms to classify the data, such as, logistic regression, random forest, neural networks and support vector machine. However, for the sake of simplicit of our research, we will not discuss about the learning algorithm that is currently implemented. We will only introduce three features that are used in machine learning based detection.

There are vast amount of features to utilize machine learning to detect phishing attack. Literatures are selected by keyword search such as "phishing + detection + machine learning". We analyze three features: lexical feature, host-based feature and site popularity feature. Each of these features will be introduced briefly as follows.

- Lexical features

Lexical features (URL based features) are based on the analysis of URL structure without any external information. Ma, et al. suggest that the structure URL of phishing may "look" different to experts [46]. These features include how many dots exist, the length, how deep the path traversal do the URL has or if there any sensitive words present in a URL. For example the URLs https://www.paypal.com and http://www.paypal.com.example.com/ or http://login.example.com/www.paypal.com/, we can see that the domain paypal.com positioned differently, with the first one being the benign URL. Figure 8 shows an example analysis of lexical features in a phishing URL [40].

Lexical features analysis may have performance advantage and reduces overhead in term of processing and latency, since it only tells the machine to learn URL structure. 90% accuracy is achieved when utilizing lexical features combined with external features such as WHOIS data [40]. Egan, et al. conducted an evaluation of lightweight classification that includes lexical features and host based features in its model [19]. The study found that the classification based on these features resulted in extremely high accuracy and low overhead. Table 4 lists the existing lexical features that are currently implemented

Haotian Liu, et al. [43]	**Guang Xiang, et al. [80]**
- Length of hostname Length of entire URL - Number of dots - Top-level domain - Domain token count - Path token count - Average domain token length of all dataset - Average path token length of dataset - Longest domain token length of dataset - Longest path token length of dataset - Brand name presence - IP address presence - Security sensitive word presence	- Embedded domain - IP address presence - Number of dots - Suspicious URL - Number of sensitive words - Out of position top level domain (TLD)

Table 4: Existing lexical features [43, 80]

by two different studies [80, 43]. However, Xiang, et al.[80] pointed out that URLs structure could be manipulated with little cost, causing the features to fail. For example, attackers could simply remove embedded domain and sensitive words to make their phishing URLs look legitimate. Embedded domain feature examines whether a domain or a hostname is present in the path segment [80], for example, http://www.example.net/pathto/www.paypal.com. Suspicious URL feature examine whether the URL has "@" or "-", the present of "@" is examined in a URL because when the symbol "@" is used, the string to the left will be discarded. Furthermore, according to [80], not many legitimate websites use "-" in their URLs. There are also plenty of legitimate domains presented only with IP address and contains more dots. Nevertheless, lexical analysis would be suitable features to use for first phase analysis in a large data [19].

- Host based features

Since phishers often hosted phishing websites in less reputable hosting services and registrars, host-based features are needed to observe on the external sources (WHOIS information, domain information, etc.). A study suggests host-based features have the ability to describe where phishing websites are hosted, who owns them and how they are managed [46]. Table 5 shows the host-based features from three studies that are currently used in machine learning phishing detection. These studies are selected only for example comparison.

Each of these features does matter for phishing detection. However, as our main objective is synthesizing cialdini's principle with phishing emails, we will not describe each of these features in de-

Justin Ma, et al.[46, 45]	Haotian Liu, et al. [46][43]	Guang Xiang, et al. [80]
- WHOIS data - IP address information - Connection speed - Domain name properties	- Autonomous system number - IP country - Number of registration information - Number of resolved IPs - Domain contains valid PTR record - Redirect to new site - All IPs are consistent	- Age of Domain

Table 5: Host-based features [46, 45, 43, 80]

tail. It is noteworthy that some of the features are subset of another feature, for instance, autonomous system number (ASN), IP country and number of registration information are derived from WHOIS information. Nevertheless, we will only explain few of them that we assume the most crucial.

1. WHOIS information: Since phishing websites and hacked domains are often created at relatively young age, this information could provide the registration date, update date and expiration date. Domain ownership would also be included; therefore, a set of malicious websites with the same individual could be identified.

2. IP address information: Justin Ma, et al. used this information for identify whether or not an IP address is in blacklist [45, 46]. Besides the corresponding IP address, it provides records like nameservers and mail exchange servers. This allows the classifier to be able to flag other IP addresses within the same IP prefix and ASN.

3. Domain name properties: these include time to live (TTL) of DNS associated with a hostname. PTR record (reverse DNS lookup) of a domain could also be derived whether it is valid or not.

- Site popularity features

Site popularity could be an indicator whether a website is phishy or not. It makes sense if a phishing website has much less traffic or popularity than a legitimate website. According to [80], some of the features indicated in Table 6 are well performed when incorporated with machine learning system.

Guang Xiang, et al. [80]	Haotian Liu, et al. [43]
- Page in top search results - PageRank - Page in top results when searching copyright company name and domain - Page in top results when searching copyright company name and hostname	- Number of external links - Real traffic rank - Domain in reputable sites list

Table 6: Site popularity features [80, 43]

1. Page in top search results: this feature originally used by [83] to find whether or not a website shows up on the top N search result. If it is not the case, the website could be flagged as phishy since phishing websites have less chance of being crawled [80]. We believe this feature is similar to Number of external links feature since both of them are implying the same technique.

2. PageRank: this technique is originally introduced by Google to map which websites are popular and which are not, based on the value from 0 to 10. According to [80], the intuitive rationale of this feature is that phishing websites are often have very low PageRank due to their ephemeral nature and very low incoming links that are redirected to them. This feature similar to Real traffic rank feature employed by [43] where such feature can be acquired from alexa.com.

3. Page in top results when searching copyright company name and domain/hostname features are complement features of Page in top search results feature with just different queries. Moreover, we believe they are also similar to Domain in reputable sites list feature since they are determining the reputation of a website. The first two features can be identified by querying google.com [80] and the latter feature can be obtained from amazon.com [43].

2.7.2 *Phishing prevention*

Phishing attacks aim to by-pass technological countermeasures by manipulating users' trust and can lead to monetary losses. Therefore, human factors take a big part on the phishing taxonomy, especially in the organizational environment. Human factor in phishing taxonomy comprised of education, training and awareness [23]. Figure 9 illustrates where human factor takes part on phishing threats [23]. User's awareness of phishing has been explored by several studies [32, 23, 20, 36, 33, 17] as preventive measure against phishing at-

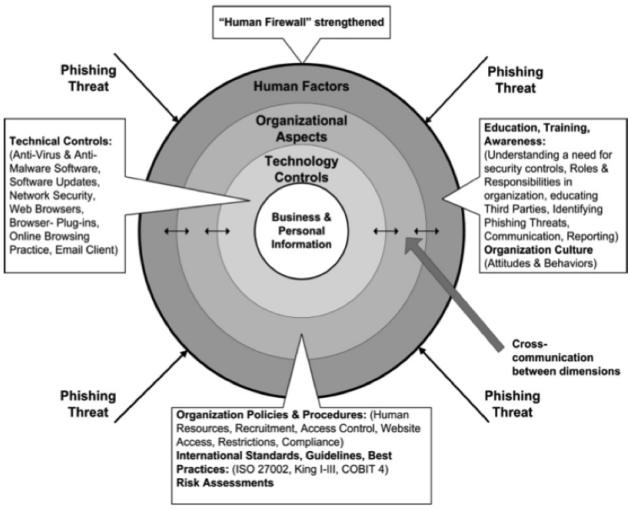
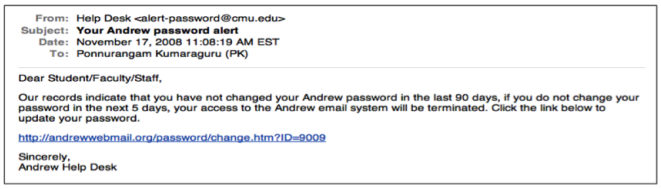


Figure 9: Holistic anti-phishing framework [23]

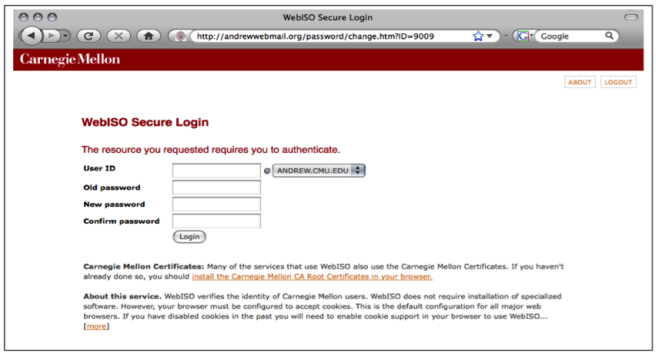
tack. According to ISO/IEC 27002 [23][11], it has been shown that information security awareness is important and it has been critical success factors to mitigate security vulnerabilities that attack user's trust. One approach to hopefully prevent phishing attack was by implementing anti phishing warning/indicator. Dhamija, et al suggest that users often ignore security indicators thus makes them ineffective [14]. Even if users notice the security indicators, they often do not understand what they represent.

Moreover, the inconsistency of positioning on different browsers makes them much difficult to identify phishing [35]. Evidently, Schechter, et al. pointed out that 53% of their study participants were still attempting to provide their confidential information, even after their task was interrupted by strong security warning [66]. Therefore, these suggest that an effective phishing education must be added as a complementary strategy to complete technical anti-phishing measure as a strong remedy to detect phishing websites or emails.

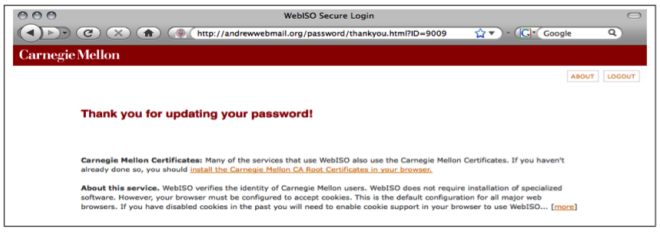
Phishing education for online users often by instructing not to click links in an email, ensure that SSL is present and to verify that the domain name is correct before giving information, and other similar education. This traditional practice evidently has not always effective [20]. One may ask what makes phishing education effective? A study suggests that in order online users to be aware of phishing threats, is to really engage them to so that they understand how vulnerable they are [48]. To do this, simulated phishing attacks often performed internally in an organization. Figure 10 shows a simulated phishing email and website carried out by Kumaraguru, et al. from PhishGuru [37]. As a result, this scenario puts them in the ultimate teachable moment if they fall for these attacks.



(a) simulated phishing email [37]



(b) simulated phishing website [37]



(c) simulated phishing message [37]

Figure 10: Simulated phishing attack [37]

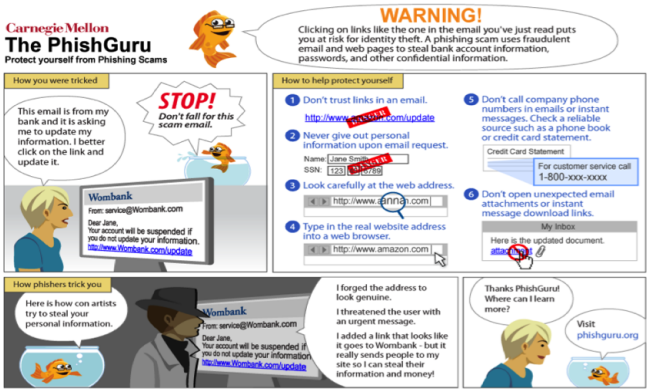


Figure 11: Embedded phishing training [37]

Phishguru is a security training system operated by Wombat security technology that teaches users not to be decieved by phishing attempts by simulation of phishing attacks[67]. They claimed Phishguru provides more effective training than traditional training as it is designed to be more engaging. Figure 11 illustrates how embedded phishing training was presented by PhishGuru.

Kumaraguru, et al. investigates the effectiveness of embedded training methodology in a real world situation [37]. Evidently, they indicated that even after 28 days after training, users trained by PhishGuru were less likely to click the link presented in the simulated phishing email than those who were not trained. They also find that users who trained twice were less likely to give information to simulated fraudulent website than users who were trained once. Moreover, they argue that the training does not decrease the users' willingness to click on the links from legitimate emails; it means that less likely a trained user did a false positive when he or she requested to give information from true legitimate emails [37]. This suggests that user training strategy as an effective phishing education in order to improve phishing awareness especially in organizational environment.

3

PRELIMINARY ANALYSIS

Before we go into our main analysis on phishing email dataset, we would like to conduct preliminary analyses on phishtank and phishload datasets to know more about phishing bad neighborhood and phishing vs original websites. Basic investigation on both datasets will be conducted as initial experiments prior our main analysis to address the existence of phishing bad neighbourhood and finding how many phishing webpages that maintains the "look" of legitimacy on their target.

3.1 PHISHING BAD NEIGHBORHOOD IN PHISHTANK

3.1.1 *Preliminary methods*

To examine whether phishing bad neighbors exist in phishing context, we established what tools we could use for our analysis. These tools include:

- www.yougetsignal.com
- www.majesticseo.com/research/neighbourhood-checker.php
- http://www.ip-address.org/reverse-lookup/reverse-ip.php
- http://www.my-ip-neighbors.com/
- ip-lookup.net
- Mac OS X network utility

We used these tools because they are freely available and capable of doing reverse IP lookup to find bad neighborhood in a particular IP address. We determined that the results given by these tools were sufficient for our basic analysis. We selected 10 valid and online phish URLs from phishtank in sequence on the date of 17 March 2014 and add 21 URLs more in seqence which were valid and online on the date of 24 March 2014.

After preparing 10 valid phishing URL we identified its Top Level Domain (TLD) and Top level IP address. The next step, we evaluated from which country are they from and counted how many characters it has. Next, we identified how many domains are hosted within a neighbors using reverse IP lookup. Lastly, we selected 10 random domains within its domain to be examined whether they are harmful or legitimate.

3.1.2 *Preliminay results*

To fit the table onto the page and avoid a very huge and long table, we put phishing URLs separately in Table 31 of the appendix section.

Table 7: Phishtank URL analysis

URL ID	**TLD**[1]	**TL-IP**[2]	**N**[3]	**Random 10 neighbors**	**Country**	**URL Length**
1	munduslc.com	184.154.233.9	384	3 could not be resolved, 7 legitimate	Chicago, US	163
2	daff-inc.com	203.190.54.3	196	2 could not resolve, 8 legitimate	Jakarta, Indonesia	162
3	cntsiam.com	27.254.67.185	25	1 malware warning, 9 legitimate websites	Bangkok, Thailand	17
4	hockeyfollonica.com	194.184.71.7	297	9 404 error, 1 could not be resolved	Italy	165
5	douban.co.uk	193.61.190.231	18	4 legitimate, 1 phishing warning (douban.co.uk itself), 5 errors	UK	123
6	appsgeo.org	195.154.168.222	52	2 reported as phishing (including appsgeo.org), 1 reported untrustworthy (from WOT plugin), 6 legitimate, 1 error	France	164
7	fatihdabak.com	31.169.91.37	97	7 legitimate, 1 hacked, 1 phishing (WOT), 1 error	Turkey	176
8	edirnewebtasarimi.com	95.173.184.22	95	2 hacked, 2 error, 6 legitimate	Turkey	89
9	clientel-pl.com	209.17.116.6	362	10 legitimate	US	115
10	totalwhiteboard.com.au	203.84.238.17	224	10 legitimate	Australia	161
11	altervista.org	216.127.94.127	222	2 redirect to en.altervista.org (free host provider), 6 legitimate, 2 could not be resolved	US	66

1 Top Level Domain

2 Top Level IP address

3 No. of domain found

12	mytrickworld.com	192.254.71.149	102	1 could not be resolved, 2 empty pages, 7 legitimate	US	244
13	toughbook.cl	190.153.181.184	14	7 legitimate, 1 error, 2 request time out	Chile	162
14	doctorsantis.cl	200.63.97.50	426	2 could not be resolved, 2 404 error, 1 hacked, 5 legitimate	Chile	154
15	ankarabayanmodel.com	37.247.101.252	19	1 could not be resolved, 1 Suspended account, 1 expired domain, 6 legitimate, 1 poor reputation (WOT)	Turkey	105
16	theripe.tv	108.162.199.188	378	1 could not be resolved, 1 Under maintenance (warez), 8 Legitimate	US	185
17	yoursyours.com	204.77.0.196	18	1 warning (yoursyours.com, 1 could not be resolved, 8 legitimate	US	127
18	vidavallarta.com.mx	69.162.95.178	137	7 legitimate, 1 error (bandwidth limit exceeded), 2 could not be resolved	US	207
19	alvaroestrella.com	67.222.145.50	422	3 could not be resolved, 7 legitimate	US	117
20	no domain name	178.210.162.252	25	10 legitimate	Turkey	67
21	310bxgg.com	103.27.127.142	X[4]	hacked domain http://310bxgg.com/	Hong Kong	108
22	affordablebestwebsitehosting.com	173.214.178.24	25	4 suspected phishing (WOT warning), 1 suspended account, 1 could not be resolved, 4 legitimate	US	150
23	alwaysplotting.com	208.97.149.71	25	9 legitimate, 1 error (403 forbidden)	US	138
24	kcn.ru	193.232.252.56	X	X	Russia	124

4 X= No known domains hosted on this IP

25	cleanwheel.net	173.243.123.58	9	3 could not be resolved, 2 domain expired, 1 timeout, 1 error establishing a database connection, 2 legitimate	US	58
26	avatur.net	62.99.79.26	25	1 legitimate, 2 phishing warning, 6 access denied, 1 could not be resolved	Spain	146
27	vicfer.mx	198.27.68.106	X[5]. However, noticed that the last 5 URLs are from the same IP (198.27.68.106) So that it makes them neighbours		Canada	80
28	latitud-x.com.mx	198.27.68.106			Canada	104
29	carycar.com.mx	198.27.68.106			Canada	85
30	gentilee.com.ar	198.27.68.106			Canada	82
31	uniredmx.com	198.27.68.106			Canada	83

Based on our analysis we know that we have 31 phish URLs. We specify two categories that indicate less and higher possibilites in having bad neighbourhood. If one domain has 50% or more suspicious domains, it characterized to have higher possiblities of bad neighbourhood. In countrary, if one domain has less than 50% suspicious domains, it characterized to have less possibilities. The data suggests that 3 of them are hacked domains (10%) while 11 domains (35%) have the possibilities of harmful instances. It makes 17 domains (55%) have less possibilties of bad neighborhoods. In conclusion, while there are some possibilities of bad neighborhood, there are much more of legitimate domains attributed from a phishing domain as well.

5 X = No known domains hosted on this IP

3.2 FINDING DIFFERENCES OF PHISHING VS ORIGINAL IN PHISHLOAD DATABASE

3.2.1 *Preliminary methods*

To find differences between phishing webpage and its legitimate one, we utilized the differences of their HTML source codes. However, Phishtank does not have HTML source code of their phishing webpage, therefore, we decided to shift our analysis to Phishload database [49] which is collected from Phishtank as well. The phishload test database is a set of visited phishing websites and original websites that have been visited and scanned for testing purposes. Over a period of several weeks current phishing links from Phishtank have been collected and then been visited by a controlled instance of Firefox browsers. Derived from readme.txt files of phishload database, it has been created on 22 March 2013. It has 11215 URLs with 1185 non phishing URLs and 3718 assigned phishing pages [49]. Moreover, the tables of the database is already explained by Maurer on his website [49].

The methods to carry out this preliminary analysis are as follows:

1. Select all parent = NULL and site = paypal
    - SQL command: SELECT * FROM ‘websites‘ WHERE ‘name‘ = ’paypal’; does not result in anything/resulting in zero rows
    - SELECT * FROM ‘websites‘ WHERE ‘parent‘ IS NULL AND ‘urlBasedomain‘ = ’paypal.com’; result = 1 row
2. Save the ID and the field of HTML content
    - ID = 34 and HTML content are saved => paypal original.html
3. Find 20 phish websites where parent = ID
    - SELECT * FROM ‘websites‘ WHERE ‘parent‘= 34; Resulting in 1315 rows
    - SELECT * FROM ‘websites‘ WHERE ‘parent‘= 34 LIMIT 20; Resulting in 20 rows Export to SQL file => 20 phish paypal.sql
4. Compare legitimate paypal and the 20 fake paypal websites

All of the 20 examinations were done manually by finding the differences between the original web page against individual phishing web page stored in Phishload database.

3.2.2 *Preliminary results*

Through the HTML source code analysis, we may find malicious irregularities that ask victims to input their financial information or login credentials. Ludl et al. have defined page properties to characterize a web page before it can be analyzed for indication that might reveal it as a phishing site [44], of course in this experiment, all of the web pages are indicated as phishes according to Phishload. These properties are described as follows:

- Forms: Phishing website aims to trick users to input their sensitive information. Consequently, fake website needs some kind of forms as interface to contain those information. Web Forms may provide a good indicator to distinguish phishing and original.
- Input fields: Original web pages may have web forms with its input fields for users to input necessary information. Similarly, phishing web pages may have the same input fields as the original web page. However, the difference lies in where these information go to.
- Links: General properties of a web page is in its link structure. link(s) structure portrayed by not only links to other webpages, but also the link(s) which embedded in an image within a page. Ludl et al. argued that many phishing web pages contain links to the site they spoof, and evidently, often contain original elements from the web page they targeted [44].
- Script tags: Another good indicator to distinguish a phishing web page is to find out whether it has rouge JavaScript or not. There is a possibility that JavaScript may be used to by-passing Anti-phish so that it will not be detected as a phish [34, 44].

To illustrate, HTML source of the phish website row 1 was gathered and evaluated. It is clear that it is a phish website because inside the HTML source it has function called zzzz() that contains variables that manage the input of victim personal information.

```
function zzzz() {
var tes=true;
var first=document.fox.first_name.value;
var lasto=document.fox.last_name.value;
var doxa=document.fox.dob_a.value;
var doxb=document.fox.dob_b.value;
var doxc=document.fox.dob_c.value;
var numbex=document.fox.cc_number.value;
var email=document.fox.email.value;
var address=document.fox.address1.value;
var zipos=document.fox.zip.value;
var villss=document.fox.city.value;
var phonos=document.fox.phone.value;
var fvv=document.fox.cvv2_number.value;
}
```

We also found an explicit hack comment on the phish row 2:

```
<script type="text/javascript"> // This is an ugly hack until there is a reliable ondomready function if(typeof PAYPAL != 'undefined'){PAYPAL.core.Navigation.init(); }</script>
```

Based on our manual analysis, we found out that most of the HTML sources are tampered while maintaining the looks of legitimacy. The alterations consist of irregular scripts, irregular links, suspicious forms and inputs. Only two HTML sources that are completely different from the original source. 4 HTML sources are NULL so overall analysis will be N = 16. In conclusion, 87.5% of HTML sources are tampered while maintaining the appearance of original target and 12.5% are completely different from the original. A detailed of differences table of 20 phishing webpages vs original webpage will be shown in Table 32.

4

RESEARCH QUESTIONS AND HYPOTHESES

This chapter addresses the explanation of our main research questions and hypotheses to meet our goal. We aim answer these research questions by the data collected from fraudehelpdesk.nl. First off, we wanted to know the characteristics of phishing email based on structural properties in our corpus.

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

The characteristics of the reported phishing emails includes:

- How often phishing email include an attachment(s) and what specific attachment is the most frequent.
- Prevalent methods
- Content characteristics
- The most targeted institutions
- The reasons that are frequently being used
- Persuasion principles characteristics
- Relationship between generic properties

To find out these characteristics, variable establishment of structural properties will be addressed in subsection 5.1.3.

Secondy, we wanted to know how relevant are the persuasive principles to the associated phishing eamil properties.

RQ2: How relevant are the persuasive principles to the generic phishing email properties?

We established 16 hypotheses to indicate the relationship between generic properties and relevancy of persuasive principle to these properties. H8, H9, H10, H13, H14, H15 will partly answer RQ1 in respect to the relationship between generic properties and the rest will answer RQ2. We synthesize cialdini's principles with our dataset. In order to conduct synthesization, we established our decision making to classify which persuasive elements that are exist in a phishing email. This process will be explained in subsection 5.1.5.

In our coding of cialdini's principles and phishing email dataset, 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 [72]. 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 [57].

It is 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

---

H1: There will be a significant association between Government sector and authority principle

H2: Phishing emails which targeting Administrator will likely to have 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 [61]. For example in 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 URL provided. Potential victim may perceives their online banking account as their valuable matter to access facility and information about their savings. Consequently, potential vicim 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

---

H3: There will be a significant correlation 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 [18]. 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 this scenario, E-commerce/Retails sector may applied likeability principles to gain potential customers. We therefore hypothesize that

---

H4: Phishing emails which targeting E-Commerce/Retails will likely to have a significant relationship with likeability principle

---

Tajfel, et al. argued that people often form their own perception based on their relationship with others in a certain social circles [70]. 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 [79]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

---

H5: Phishing emails which targeting Social networks will likely to have signification association with 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 URL provided in the email. Based on this scenario, we know that it has authority principle and also has scarcity principle. Therefore, we hypothesize that

---

H6: There will be a significant relationship 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 this 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

---

H7: Phishing emails which have likeability principle will likely to have consistency 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 URL 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

---

H8: Phishing emails that include URL will likely to be obfuscated

---

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 other words, if we have something to sell, we do not just display our product without asking people's attention to look at our product. For example in phishing email context, phishers may include URL or attachment in the body of the email and also they may request unsuspecting victim to click the URL or to open the attachment. This leads us to two hypotheses which state

---

H9: Phishing emails that include URL will likely to request to click the URL

H10: Phishing emails that include attachment will likely to request to open the 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, a fake police officer may use a fake badge to build up even more "aura of legitimacy". Evidently, Cialdini suggests the increment of passerby who have stop and stare at the sky by 350 percent with suit and tie instead of casual dress [8]. Hence, we correlate that a person who wears police uniform and a fake badge in the real world context as authority principle and the precence of image in the phishing mail context. Another example, an email that masquerades Apple company, may clone Apple company logo or trademark to its content to increase the chance of potential victim's response or increase the "believability" if you will. Thus, we hypothesize that

---

H11: Phishing emails that have authority principle will likely to include an image to its content

---

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

---

H12: There will be a significant association between account related reason and scarcity principle

---

Similar from the hypothesis H12, it is sensible if a phishing email which contains account related reason such as reset password or security update, may tend to have a URL for the potential victim to be redirected towards phisher's bogus website or malware. Regardless of the target, based on our initial coding of the dataset we found that account related reason in a phishing email needs an immediate action greater than other reasons. Therefore, phishers may likely to include a URL to have immediate response from the potential victim. This leads to our hypothesis that say

---

H13: Phishing emails which have account related reason will likely to have URL

When a phishing email has document related reason such as review some document reports or court notice, it may tend to impersonate government to make the email sensible enough to persuade potential victim more than other targets. We therefore hypothesize that

---

H14: Phishing emails which targeting government sector will likely to have document related reason

---

Analogous with the hypothesis *H14*, 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

---

H15: Phishing emails which have document related reason will likely to include attachment

---

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

---

H16: Phishing emails which use HTML will have a significant association with likeability principle

---

5 DATA AND ANALYSIS

This chapter explain our research methodology and results in detail. We begin by explain the framework of our method, that consists of steps taken in order to get our results. By the end of this chapter, we present the results of our analyses to answer the research questions that we explained in chapter 4.

5.1 RESEARCH METHODOLOGY

As we illustrate in Figure 12, we processed our data into several steps. Firstly, we collect our raw data from fraudehelpdesk in the form of suspected phishing email reports. Next, we performed our data categorization and we divided it into three categorization tasks. The next step, we determined what variables are needed for our analysis. Next step, we excecuted our data classification into these variables, so that we could reconstruct into SPSS readable dataset. Lastly, we conducted our SPSS analysis to answer our hypotheses.

5.1.1 *Raw data collection*

The data is obtained from *fraudehelpdesk.nl* in the form of phishing emails which were reported between august 2013 and december 2013. Fraudehelpdesk is a national institution based in Netherlands that handles reports on online crime and fraud including phishing [73]. The data consists of 8444 suspected phishing emails in total that we categorized based on the language, whether the reported phishing email is in Dutch or English language. The data was categorized in the confidential environment, which mean we only analyzed the data in Zilverling building of University of Twente.

5.1.2 *Data categorization*

We manually categorized 8444 suspected phishing emails by sorting all the emails by the subject so that we could tell which emails were being distributed with the exact same content. We then examined individual email which has no or empty subject and determined in which language it was delivered. Initial categorization resulted as follows:

- 7756 suspected phishing emails in Dutch language
- 688 suspected phishing emails in English language

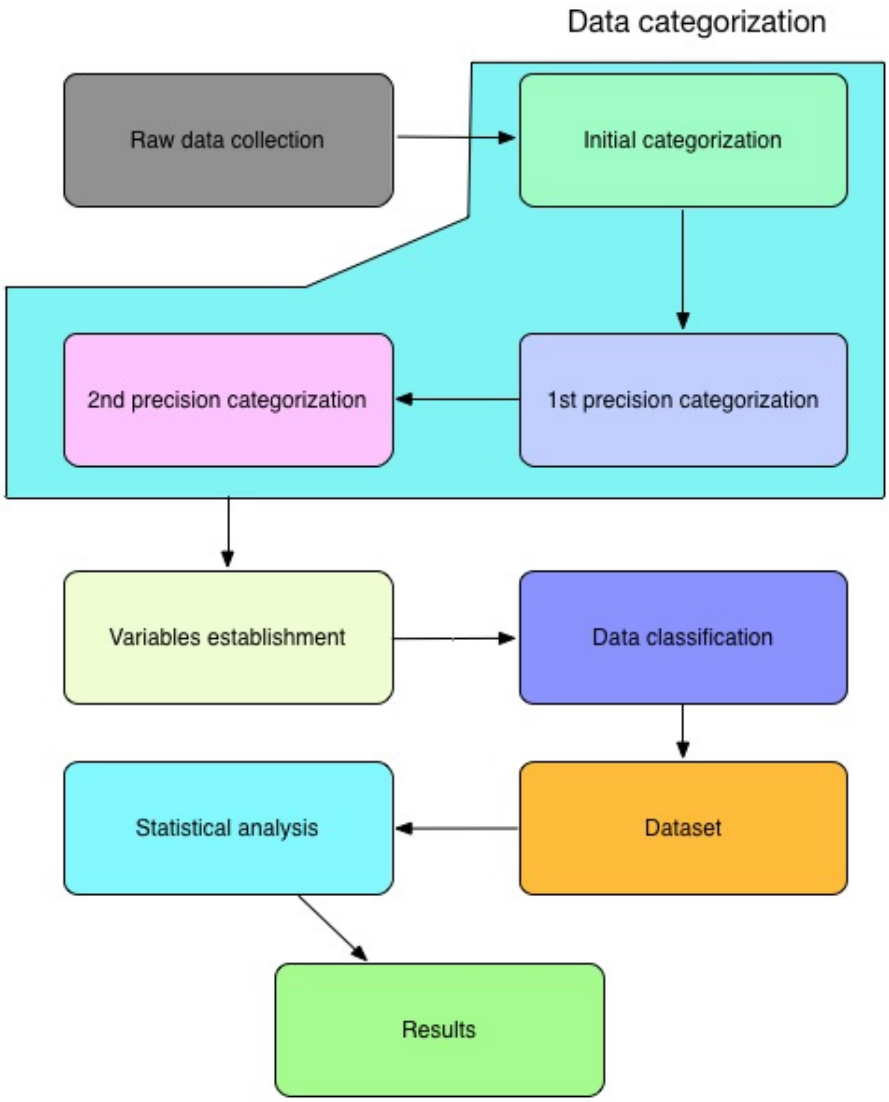


Figure 12: Research methodology diagram

Within 688 suspected phishing emails in English language we further categorized based on phishing, spam and unknown emails. We label this process as 1st precision categorization. Phishing category is determined which email were indeed phishing, spam category is specified which email were spam and unknown category is established by the following guidelines:

- The email which has no content, whether it was removed automatically by antivirus program.
- The email which is presented in the language other than Dutch or English.

The process is resulted as follows:

- 486 phishing emails

- 150 spam emails
- 52 unknown emails

To get a further precision from the 1st precision categorization, we executed 2nd precision categorization within 688 suspected phishing emails in English language. This process is resulted as follows:

- 440 phishing emails
- 180 spam emails
- 50 unknown emails
- 18 legitimate emails

Interestingly, we have 18 legitimate emails that were mistakenly reported as phishes or false positive. Although they are only 18 false positive, this suggest there are still misinterpretation of fraudulent email in our society. From this point we would only code 440 phishing emails to an excel sheet with necessary variables so that we could convert it into SPSS readable file. From 440 phishing emails, we performed query search which email that has a duplicated content. Query search were resulted in 207 unique phishing emails. At the end, in total we will only analyze 207 unique phishing emails in our corpus.

5.1.3 *Variables establishment*

12 Variables were created as part of the methodology processes prior data classification. These variables are explained as follows:

1. *Mail ID* : Unique ID [Scale measurement]
2. *Timestamps*: Implies the date and time when the email is being reported [Scale measurement]
3. *Direct/Indirect*: Whether the phishing email is directly from internal fraudehelpdesk system or from external [0 = Direct, 1= Indirect]
4. *Attachments:* Indicates whether the phishing email has an attachment(s), if so, what kind of attachment
    a) PDFattachment [0 = No, 1 = Yes]
    b) ZIPattachment [0 = No, 1 = Yes]
    c) HTMLattachment [0 = No, 1 = Yes]
5. *Methods*: Implies the inquiry by the phishers in the contents
    a) ReqOpenAttachment [0 = No, 1 = Yes]

   b) ReqClickLink [0 = No, 1 = Yes]
   c) ReqEmailReply [0 = No, 1 = Yes]
   d) ReqCallingByPhone [0 = No, 1 = Yes]

6. *Contents*: Indicates what elements are included in the body
   a) ContainHyperlink [0 = No, 1 = Yes]
   b) UseHTML [0 = No, 1 = Yes]
   c) IncludeImage [0 = No, 1 = Yes]
7. *ObfuscatedURL*: Specifies whether a phishing email has obfuscatedURL [0 = No, 1 = Yes]
8. *CountMessageReporter*: A counter where the reporter includes extra information [Nominal measurement]
9. *Target*: Determined the target institutions
   a) TargetType [Values can be seen in the appendix]
10. *Reason*: Implies he reason why unsuspected victim must grant the phisher's request
    a) ReasonType [Values can be seen in the appendix]
11. *Cialdini's Principles*: Specifies what principle(s) the phishing email signifies. Coding consideration will be explained on subsection 5.1.5
    a) Reciprocation [0 = No, 1 = Yes]
    b) Consistency [0 = No, 1 = Yes]
    c) SocialProof [0 = No, 1 = Yes]
    d) Likeability [0 = No, 1 = Yes]
    e) Authority [0 = No, 1 = Yes]
    f) Scarcity [0 = No, 1 = Yes]
12. *CounterSameContents*: A counter that indicates how many phishing emails have exactly the same contents

It is noteworthy that apart from cialdini's principles, they are generic properties or features of a phishing email.

5.1.4 *Data Classification*

We classified our data accordingly into our variables. As a result, usable dataset has been made to be statistically analysed. Data classification is conducted in a straightforward way. For example if phishing email has a PDF attachment, we put "1" in our "PDFattachment" variable. Similarly, if phishing email has a hyperlink in the content,

we put "1" in our "ContainHyperlink" variable. Lastly, we conducted synthesization on our data with Cialdini's six principles of persuasion will be discussed in subsection 5.1.5.

5.1.5 *Synthesizing Cialdini's principles*

Part of our analysis, we tried to synthesize phishing emails dataset with Cialdini's principles titled "The science of persuasion". The decision making and the rationale in this process are achieved based our perspective of Cialdini's principles as follows:

1. Reciprocation: The norm that obligates individuals to repay in kind what they have received. Return the favor. Adjustment to smaller request [8].

2. Consistency: Public commitment. When people become psychologically become vested in a decision they have made [79].

3. Social proof: When people model the behavior of their peer group, role models, important others or because it is generally "fashionable" [79].

4. Likeability: When people trust and comply with requests from others who they find attractive or are perceived as credible and having special expertise or abilities such as sports figures or actors they like [79].

5. Authority: It can be used to engender fear, where people obey commands to avoid negative consequences such as losing a privilege or something of value, punishment, humiliation or condemnation [79].

6. Scarcity: based on the principle of reactance, where people respond to perceived shortages by placing greater psychological value on perceived scarce items [79].

Reciprocation: When a phisher sends an email containing a message that perceived as a request or obligation towards the recipient to "return the favor". It might be normal for an individual to feel "obligated" to return the favor for things or information that he/she deemed to be valuable. For example in the phishing email context, when PayPal has detected there are suspicious activities on our account, we sometimes believe that PayPal has done a good job in detecting security risk on their system and we feel "obligated" to return the favor of that valuable information. Another example, if the sender gave the information that they have added "extra security" on their system so that we also feel obligated to grant their request.

Consistency: When a phishing email contains a message that perceived to request recipient's "consistency" on a decision they have

made. For example in the phishing email context, when a hotel agent asks us to review the payment details of our reservation that we have previously made, we might feel committed or agreed to review the payment details that has been given. Another example, if Facebook gave a link to change your password that you requested previously to change it. It might be not applicable to those who are not requesting password previously, but we believe it will impact to those who are committed to change the password previously.

Social proof: When a phishing email contains an affiliation of other people that they deemed to be "fashionable". For example, when someone tells us that there are a hundreds of other people who use particular system, so we might want to agree to use it as well just because a lot of other people use it as well. Another example, when Facebook give information that someone wants to be our friend, and we knew who that someone is. We might tend to follow that request and click the link to accept the request.

Likeability: When a phishing email contains a message that attracts recipient to comply the sender's request based the reference on something or someone that likeable for the recipient. Cialdini [1] identified that people usually "trust those they like". For example, if someone is asking us to download and listen to a music that Michael Jackson made, we might be attracted to download and listen to it just because we happen to love Michael Jackson music. It is like someone is asking us to watch a concert and he/she said, "Coldplay will be there", if we are devoted fan of Coldplay, we might find it very interesting. Another example, when a sender gives compliments to us or committed to help us to safeguard our account from the hackers, we tend to think that the sender cares about our safety, which is good for us, and consequently it might attract us to comply with the sender's request.

Authority: When a phishing email contains logo or image or signature or anything that looks like legitimate institutions. It can be used to makes it look trustworthy so that the recipient might accept and obey the sender's request. For example, when an email is presenting somehow authentic looking signature like "Copyright 2013 PayPal, Inc. All rights reserved" or PayPal logo. Cialdini [1] stated authoritative persuasion could be achieved by only presenting "aura of legitimacy". Another example, when the content of the email stated that it is from "System Administrator" asking for password update. It would be not authoritative if only random people asking us to change our password.

Scarcity: When a phishing email contains a message that tells a recipient to react or respond to scarce/turns-into scarce items or things or privileges. For example in the phishing email context, if a sender tells us that he/she will suspend/deactivate/limit our account if not respond to his/her request, we might want to respond to their re-

quest because we are worried we will not able to access our account again or in other words our account become scarce or limited.

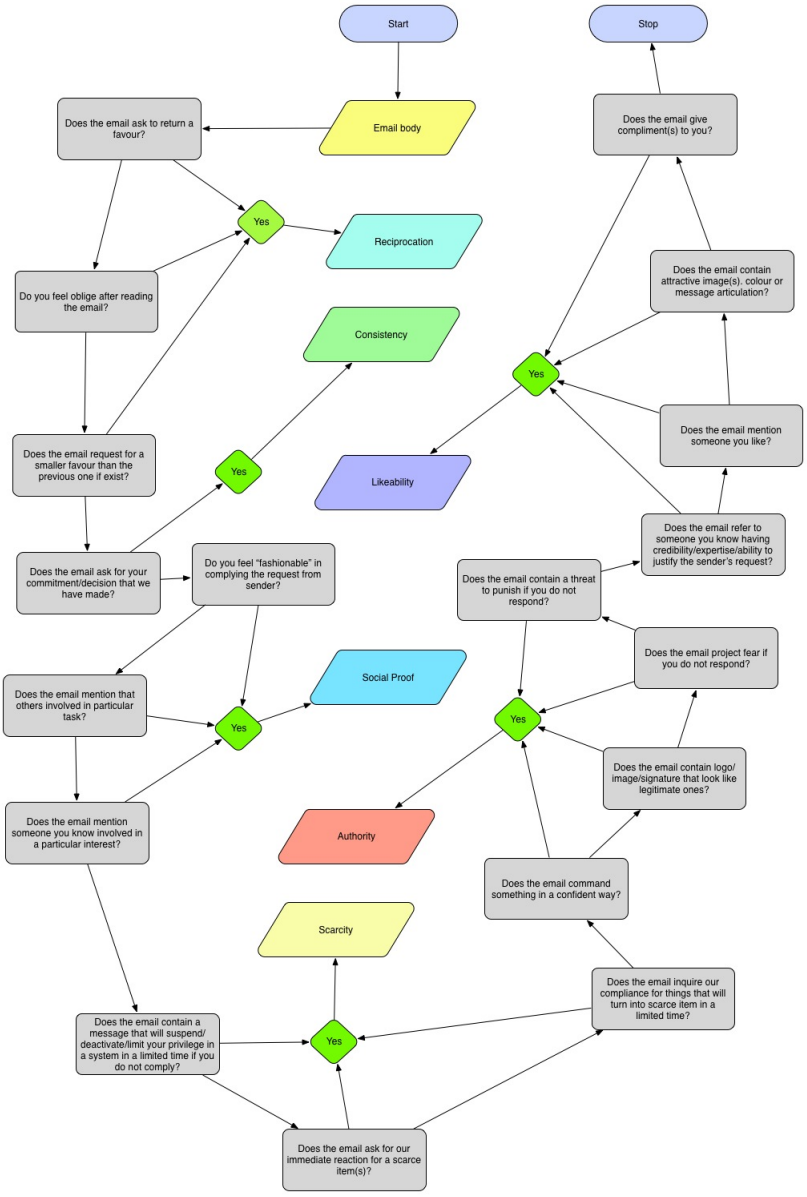


Figure 13: Integration pseudo-code of cialdini's principles

High level pseudo-code in Figure 13 is made to illustrate our integration of cialdini's principles with the dataset.

5.1.6 *Data entry and analyses*

In the previous section, we described the framework of our methodology in some detail. Until data classification, we have used Microsoft Excel to code our data. To perform the analyses, we transform the

data into SPSS readable file. We record our data in 27 variables which could be expanded depending on our analyses.

The data has been analyzed from mainly three different viewpoints; properties characteristics, persuasion principles characteristics and their relationship. We have used cross-tabulations for our analysis and our findings are presented in the next section in detail. As we mentioned in the previous section, our data classification resulted in 207 unique phishing emails.

5.2 RESULTS

To answer the first research question, frequency analyses were conducted and will be explained in this section. When we look at the statistics, we find that 36.2% of the total phishing emails have an attachment(s) included within its content, while 63.8% of them do not have attachment. In addition, we also look at what types of attachment does one has. Of the total emails having attachment, we find that 4% are having PDF attachment, 78.7% are having ZIP attachment, 12% are having HTML attachment and 5.3% of them are having unknown attachment. We are not sure what type of attachments they have, but we determined that the attachment element is still there if the request to open attachment within its content is presence. Table 8 illustrates our finding on attachments variable. It is noteworthy that one email can have more than one attachment with different types.

	Frequency	Percent
PDF Attachment	3	4
Zip attachment	59	78.7
HTML attachment	9	12
Unknown attachment	4	5.3
Total	75	100

Table 8: Attachment analysis

When we look at the methods used in the statistics, we find that 37.2% of the reported phishing emails were requesting to open attachment, 52.7% requesting to click URL(s), 16.9% were requesting for email reply and 4.3% were requesting to call by phone. Moreover. One single email can request multiple methods. Table 9 illustrates our findings in respect of methods are used.

Request	Frequency	Percent
click URL	109	52.7
open Attachment(s)	77	37.2
Email Reply	35	16.9
call by phone	9	4.3

Table 9: Method analysis

As we discussed before, we have also analyzed the content of phishing emails in our corpus. We look at whether it has URL(s), using HTML code or include image within its content. We find that 60.4% have URL(s) while 39.6% do not have URL. 66.2% of the emails used HTML code while 33.8% do not use HTML code within its content. We find 35.3% of them includes image(s) while 64.7% do not include image. Table 10 highlights our findings in respect of content analysis.

Content	Frequency	Percent
URL presence	125	60.4
utilizing HTML	137	66.2
include Image	73	35.3

Table 10: Content analysis

When we look at target classification table in Table 11, we find that 37.7% were targeting financial institutions, 19.3% were targetting e-commerce or retails, 14.5% were impersonating administrator while 28.5% of them consist of social media, postal services, government, travel agencies, ISP, industrials and non-existence/individuals impersonation. Figure 14 illustrates the pie chart of target analysis.

Target	Frequency	Percent
Financial	78	37.7
E-commerce/retails	40	19.3
Administrator	30	14.5
Government	14	6.8
Non-existence/individuals	13	6.3
Social media	11	5.3
Postal service	9	4.3
Travel agency	5	2.4
Industrial	5	2.4
ISP	2	1
Total	207	100

Table 11: Target analysis

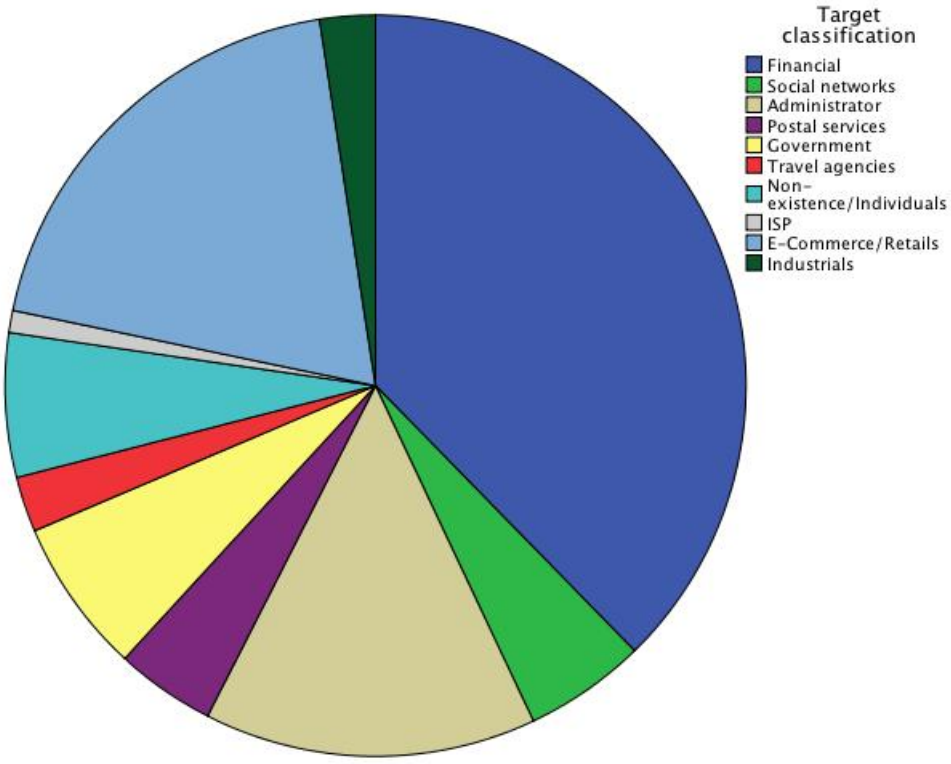


Figure 14: Target classification pie chart

When we look at what reasons are used in Table 12, we find that 48.8% of the total emails are account related, 25% are financial reason and 11.1% are document related reason. In addition, only 9.7% are product and services reason and only 4.8% are social reason. Figure 15 illustrates the bar chart of the reason classification.

Reason	Frequency	Percent
Account related	101	48.8
Financial	53	25.6
Document related	23	11.1
Product and services	20	9.7
Social	10	4.8
Total	207	100

Table 12: Reason classification

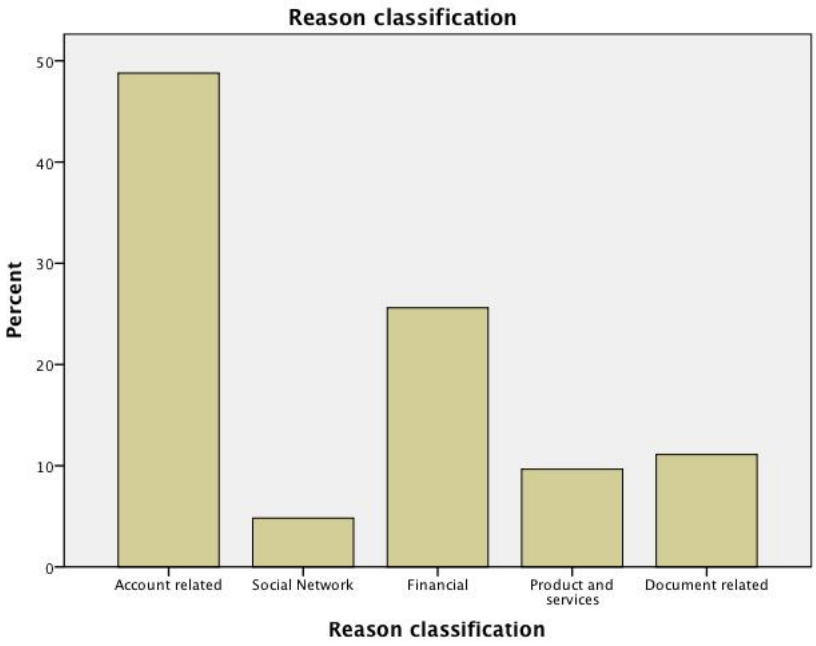


Figure 15: Reason classification bar chart

We look at the result of persuasion theory synthesis based on Cialdini's principles with our corpus. As we can see from Table 13, we find that 96.1% of the total phishing emails are having authority principle, which holds the most prevalent principle. Followed by scarcity principle at 41.1%. While 21.7% of the total are having likeability principle, only 17.4% of them are having consistency principle. We find 9.7% are having reciprocation principle and 5.3% of them are having social proof principle. It is important to know that one email can have multiple principles.

Now we know that authority principle is the dominant principle in our corpus. As we discussed in chapter 4, we have presented the rationale behind our hypotheses and we would test . When we look at

Cialdini's principles	Frequency	Percent
Reciprocation	20	9.7
Consistency	36	17.4
Social proof	11	5.3
Likeability	45	21.7
Authority	199	96.1
Scarcity	85	41.1

Table 13: Persuasion principle analysis

the association between government and authority principle, we find that 95.9% of non-government targeted emails have authority principle and 4.1% of them do not impersonate government nor having authority principle. We find 100% of government targeted emails are having authority principle. A chi-square test was performed and we find that there is no significant association between government sector and authority principle, $X^2(1) = 0.604, p = 0.473$. since p is not less than 0.05, thus we reject hypothesis 1.

Table 14: Government and authority in %

Type of Target		Non-authority	Authority	N
Non-government	A[a]	4.1	95.9	193
	B[b]	100	93	
Government	A	0	100	14
	B	0	7	
N		8	199	207
Pearson chi-square		0.604		

a within government
b within authority

When we look at the relationship between phishing emails which were impersonating administrator and authority principle, we find that 96.7% of adminstrator targeted emails are having authority principle and only 3.3% of them do not have authority principle. A chi-square test was performed and we find that there is no significant relationship between adminstrator target and authority princi-

ple, $X^2(1) = 0.027, p = 0.870$. Since p is not less than 0.05, therefore we reject hypothesis 2.

Table 15: Administrator and authority in %

Type of Target		Non-authority	Authority	N
Non-administrator	A[a]	4	96	177
	B[b]	87	85.4	
Aministrator	A	3.3	96.7	30
	B	12.5	14.6	
N		8	199	207
Pearson chi-square		0.027		

a Within administrator
b Within authority

Now we look at the association between financial sector and scarcity principle. We find that 39.7% of all phishing emails which target financial sector have scarcity principle while 60.3% do not have scarcity principle. We perfomed chi-square test and we find that there is no significant correlation between financial sector and scarcity principle, $X^2(1) = 0.090, p = 0.764$. Since p is not less than 0.05, thus, we reject hypothesis 3.

Table 16: Financial and scarcity in %

Type of Target		Non-scarcity	Scarcity	N
Non-financial	A[a]	58.1	41.9	129
	B[b]	61.5	63.5	
Financial	A	60.3	39.7	78
	B	38.5	36.5	
N		122	85	207
Pearson chi-square		0.090		

a Within financial
b Within scarcity

We look at association between phishing emails which targeting e-commerce/retails and likeability principle, we find that 20% of them have likeability principle while 80% of them do not have likeability principle. A chi-square test was performed and we find that

there is no significant association between phishing emails targeting e-commerce/retails and likeability principle, $X^2(1) = 0.088, p = 0.767$. Since p is not less than 0.05, therefore we reject hypothesis 4.

Table 17: E-commerce/retails and likeability in %

Type of Target		Non-likeability	Likeabillity	N
Non-ecomm/retails	A[a]	77.8	22.2	167
	B[b]	80.2	82.2	
Ecomm/retails	A	80	20	40
	B	19.8	17.8	
N		162	45	207
Pearson chi-square		0.088		

a Within ecomm/retails
b Within likeability

Now we look at the association between phishing emails targeting social networks and social proof principle. We find that only 18.2% of them have social proof principle while 81.8% of them do not have social proof principle. A chi-square test was performed and we find that there is no significant association between phishing emails targeting social networks and social proof principle, $X^2(1) = 3.823, p = 0.051$. Therefore since p is not less than 0.05, we reject hypothesis 5.

Table 18: Social media and social proof in %

Type of Target		Non-social proof	social proof	N
Non-social media	A[a]	95.4	4.6	196
	B[b]	95.4	81.8	
Social media	A	81.8	18.2	11
	B	4.6	18.2	
N		196	11	207
Pearson chi-square		3.823		

a Within social media
b Within social proof

Furthermore, we look at the relationship between authority principle and scarcity principle. Based on the descriptive analysis, we find that 41.7% of authoritative emails have scarcity principle while

58.3% do not have scarcity principle. However, we find that 97.6% of all scarcity emails have authority principle and only 2.4% of them do not have authority principle. A chi-square test suggests that there is no significant relationship between authority principle and scarcity principle, $X^2(1) = 0.887, p = 0.346$. Thus, we reject hypothesis 6.

Table 19: Authority and scarcity in %

		Non-scarcity	Scarcity	N
Non-authority	A[a]	75	25	8
	B[b]	4.9	2.4	
Authority	A	58.3	41.7	199
	B	95.1	97.6	
N		122	85	207
Pearson chi-square		0.887		

a Within authority
b Within scarcity

We look at the relationship beween likeability principle and consistency principle. Based on our result, we find that only 6.7% of likeability emails have consistency principle while 93.3% of them do not have consistency principle. In addition, we find that 20.4% of non likeability emails have consistency principle while 79.6% of them do not have likeability principle. A chi-square test suggests that there is a significant relationship between likeability principle and consistency principle $X^2(1) = 4.603, p = 0.032$. Pearson correlation suggests a negative correlation at -0.149 that indicate as one variable increases, the other variable decrease. This suggests, that higher likeability principle, the less chance of consistency principle in a phishing email. Although there is an association between these principle, however, it does not support hypothesis 7.

Table 20: Likeability and consistency in %

		Non-consistency	Consistency	N
Non-likeability	A[a]	79.6	20.4	162
	B[b]	75.4	91.7	
Likeability	A	93.3	6.7	45
	B	24.6	8.3	
N		171	36	207
Pearson chi-square		4.603*		

a Within likeability
b Within consistency
*p < 0.05 (significant).

Now we move on to find out the correlation between URL presence and obfuscated URL in our corpus. Based on our result, 76% of URL(s) were obfuscated while 24% were not. A chi-square test suggest that there is a highly significant association between URL presence and obfuscated URL, $X^2(1) = 115.191, p = 0.000$. Moreover, pearson correlation suggests a positive correlation at 0.756. This indicates a strong correlation between them. Therefore, we accept hypothesis 8.

Table 21: URL presence and obfuscated URL in %

URL		Not obfuscated	Obfuscated	N
Not exist	A[a]	100	0	82
	B[b]	73.2	0	
Exist	A	24	76	125
	B	26.8	100	
N		112	95	207
Pearson chi-square		115.191***		

a within the URL presence variable
b Within the obfuscated URL variable
*** p < 0.001 (significant).

We look at the relationship between URL presence and the emails which were requesting to click URL. We find 87.2% of phishing emails which have URL also requested to click it, while only 12.8% do not request to click. A chi-square test were performed and suggests that there is a highly significant relationship between URL presence and request to click URL, $X^2(1) = 151.034, p = 0.000$. A pearson correlation suggests that they have strong positive correlation at 0.854. Thus, this data support hypothesis 9.

Table 22: URL presence and Request to click URL in %

URL		does not request to click URL	requests to click URL	N
Not exist	A[a]	100	0	82
	B[b]	83.7	0	
Exist	A	12.8	87.2	125
	B	16.3	100	
N		98	109	207
Pearson chi-square		151.034***		

a within the URL presence variable
b within the request to click URL variable
*** p < 0.001 (significant).

Similarly, We look at the association between the email that includes attachment and the emails which were requesting to open attachment. We find 96% of phishing emails which include attachment also requested to open it, while only 4% do not request to open the attachment. A chi-square test were performed and suggests that there is a significant relationship between URL presence and request to click URL, $X^2(1) = 174.079, p = 0.000$. A pearson correlation suggests that they have strong positive correlation at 0.917. Therefore, we accept hypothesis 10.

Table 23: Include attachment and request to open attachment in %

Attachment		does not request	requests	N
Not exist	A[a]	96.2	3.8	132
	B[b]	97.7	6.5	
Exist	A	4	96	75
	B	2.3	93.5	
N		130	77	207
Pearson chi-square		174.079***		

a within attachment included variable
b within the request to open attachment variable
*** p < 0.001 (significant).

We look at the relationship between authority principle and the emails which include an image(s). We find 35.7% of authoritative emails have image, while 64.3% of them do not include an image. A chi-square test were performed and suggests that there is no significant relationship between authority principle and image presence, $X^2(1) = 0.384, p = 0.535$. A pearson correlation also suggests that they were not strongly correlated at 0.043. Thus, this data rejects hypothesis 11.

Table 24: Authority and image presence in %

Cialdini's principle		does not include image	Includes image	N
Non-authority	A[a]	75	25	8
	B[b]	4.5	2.7	
Authority	A	64.3	35.7	199
	B	95.5	97.3	
N		134	73	207
Pearson chi-square		0.384		

a within authority
b within InlcudeImage variable

Now we look at the association between account related reason and scarcity principle. We find 68.3% of account related phishing emails were having scarcity principle, while 31.7% of them were not. In ad-

dition, we find 81.2% of scarcity emails were having account related reason while 18.8% of them were not. A chi-square test were performed and suggests that there is a significant association between account related reason and scarcity principle, $X^2(1) = 60.535, p = 0.000$. A pearson correlation suggests that they are positively correlated at 0.541. Therefore, we accept hypothesis 12.

Table 25: Accont related reason and scarcity in %

ReasonType		Non-scarcity	Scarcity	N
Not account related	A[a]	84.9	15.1	106
	B[b]	73.8	18.8	
Account related	A	31.7	68.3	101
	B	26.2	81.2	
N		122	85	207
Pearson chi-square		60.535***		

a within Account related reason
b within scarcity
*** p < 0.001 (significant).

Furthermore, we look at the relationship between account related reason and URL presence. We find 78.2% of account related phishing emails which have URL(s), while 21.8% of them do not include URL. A chi-square test were performed and suggests that there is a significant relationship between these two variables, $X^2(1) = 26.216, p = 0.000$. A pearson correlation suggests that they have a positive correlation at 0.356. Therefore, we accept hypothesis 13.

Table 26: Accont related reason and URL presence in %

ReasonType		URL does not exist	URL exists	N
Not account related	A[a]	56.6	43.4	106
	B[b]	73.2	36.8	
Account related	A	21.8	78.2	101
	B	26.8	63.2	
N		82	125	207
Pearson chi-square		26.216***		

a within Account related reason
b within URL presence variable
*** p < 0.001 (significant).

Now we look at the relationship between document related reason and government sector. We find only 21.7% of document related reason phish emails were targeting government, while 78.3% of them were not targeting government.However, A chi-square test suggests that there is a highly significant relationship between these variables, $X^2(1) = 9.203, p = 0.002$. A pearson correlation indicates that they were not strongly correlated at 0.211. Therefore, we accept hypothesis 14.

Table 27: Document related reason and government sector in %

ReasonType		Non-government	Government	N
Not document related	A[a]	95.1	4.9	184
	B[b]	90.7	64.3	
Document related	A	78.3	21.7	23
	B	9.3	35.7	
N		193	14	207
Pearson chi-square		9.203**		

a within document related reason
b within government
** p < 0.01 (significant).

Now we look at the relationship between document related reason and attachment variables. We find 78.3% of document related reason phish emails have attachment included, while 21.7% of them do not. A chi-square test suggests that there is a significant relationship between these variables, $X^2(1) = 19.783, p = 0.000$. a pearson correlation indicates that they were not strongly correlated at 0.309. Thus, this data support hypothesis 15.

Table 28: Document related reason and includes attachment in %

ReasonType		Does not include attachment	includes attachment	N
Not document related	A[a]	69	31	184
	B[b]	96.2	76	
Document related	A	21.7	78.3	23
	B	3.8	24	
N		132	75	207
Pearson chi-square		19.783***		

a within document related reason
b within attachment variable
*** p < 0.001 (significant).

Lastly, we look at the association between HTML usage variable and likeability principle. Based on our statistics, we find 80% of likeability phish emails were using HTML, while 20% of them were not including HTML code within its content. A chi-square test suggests that there is a significant relationship between these variables, $X^2(1) = 4.904, p = 0.027$. A pearson correlation suggests that they are not strongly correlated at 0.154. Therefore, we accept hypothesis 16.

Table 29: use HTML and likeability in %

Content		non-likeability	likeability	N
Not use HTML	A[a]	87.1	12.9	70
	B[b]	37.7	20	
use HTML	A	73.7	26.3	137
	B	62.3	80	
N		162	45	207
Pearson chi-square		4.904*		

a within use HTML
b within likeability
* $p < 0.05$ (significant).

6

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 chapter 4.

Before we conclude our main analyses, we would like to mention the bottom line of our preliminary investigation 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 possibilies), 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.

Our research was aimed to synthesize persuasive principles and characterize phishing email properties. We looked at what are the properties of phishing email and how relevant are the persuasive principles to its associated properties. The data was obtained from fraudehelpdesk as national institution based in Netherlands that handles reports on fraud including phishing.

It was a challenging task to manually code individual phishing email to fit onto our dataset. Our experience tells us that any researcher who wishes to work related with phishing email and persuasion principles as related to human psychology, should devote a lot of time in preparing adequately for the project.

Another aspect of our research was that persuasive principle has variety of strength 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[2].

Looking at our results on the characteristics of reported phishing emails, we found that 36.2% of total phish include attachment while 63.8% of them do not include attachment(s). From chi-square tests result, we conclude that both ZIP attachment and HTML attachment have a highly significant association when a phish email includes attachment(s). From the total amount of 207 unique phishing emails, we found that requesting to click URL is the most prevalent method at more than half of the total phish as oppose to request to call by

phone at less than 5% of the total. When we look at the content characteristics of the phish, most of it utilizes HTML code as modern email clients are able to read HTML based content email. Similarly, URL presence in our analysis also significantly higher at more than half of the total phish. It is notable that content variables may overlap with each other.

When we look at the target sector statistics of phishing mails, we find that financial as the most targeted sector to be impersonated by phishers at 37.7% of the total phish. In addition, E-commerce/retails took the second place of the most targeted sector at 19.3% of the total phish. This finding congruent with our expectation that phishers tend to impersonate financial institutions. Furthermore, when we look at the characteristic of the reasons being used in phishing emails, account related contributes the most frequent reason than others at 48.8% of the total phish. When we look at the persuasion principles, the analysis suggests that authority principle contributes the most prevalent principle at 96.1% followed by scarcity principle at 41% of the total phish. On the other hand, social proof and reciprocation contributes less prevalent principles.

Looking at our results, we conclude that when URL(s) is present in a phishing email, it will likely to be obfuscated and requested by the phisher. Similarly, when an attachment(s) is included, it will likely to be requested by the phisher. Although it seems negligible, it is interesting to know that there are several cases when phisher only include an attachment(s) without requesting to open it. Our investigation on account related reason and URL presence resulted in highly significant relationship between these two properties. It means that when a phishing email is about account related reason, there is a higher chance that it includes URL(s). In addition of the relationship between generic properties, our analsys suggests that when a phishing mail which targeting government, will likely to have document related reason. Similarly, when a phishing email has document related reason, it will likely to include an attachment(s).

When 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 likebility, the lower chance to have consistency principle.

Table 30: Overview of verified hypotheses

Hypotheses	Relevancy	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 Persuasion principles
b Generic properties

Overall, although there are many hypotheses in respect of persuasion principles are rejected, some of them are accepted. This conclude low relevancy in respect between persuasion principles and generic properties of a phishing email. Our research sheds light on the involvement of persuasion principles as human factor and phishing email which has not been extensively studied. Table 30 summarizes the overview of verified hypotheses.

A

PRELIMINARY ANALYSES APPENDIX

A.1 PHISHING URLS FROM PHISHTANK

Table 31: Phistank URL list

URL ID	Phishing URL
1	http://update-mypaypal.woa.wa.directtosignin-cgi-sys-defaultwebpage.cgi.defaultwebpage.cgi.munduslc.com/7d119be5b314a9a159244f884bc87ad0/36fd4df0d83094c6d466fdfdc5ad4aec/
2	http://daff-inc.com/PayPal/cgi-bin/webscr%3fcmd=_login-submit&dispatch=5885d80a13c0db1f8e263663d3faee8d8cdcf517b037b45005cf5d4eda3b985b/f4c476e425cd92c31d6d6452b0ac80b3/
3	http://cntsiam.com/logs/
4	http://www.hockeyfollonica.com/app2/media/bearleague/events/windhoek_tours/7b4b770d7284f852d17dbd7fe3b3154f/validate.php?cmd=53026&dispatch=68c92e699bc27f49aef2aaa5f3293d38
5	http://douban.co.uk/ss/e9023fd16f4f0d79785e91f4b06f6c46/?cmd=_home&dispatch=5885d80a13c0db1f8e&ee=9220c39c535c3317b3743e915aef3adc
6	http://appsgeo.org/paypal/mmp/web.php?#/_flow&SESSION=54cc48e97ad73aaa2519dbb379719301FpG7mo2DssMkja2121545487KJJ9ecd33e80218623592ca5d52281eb16eHHG5548782121548LLOp
7	http://paypal.com.cgi.bin.webscr.cmd.login.submit.15.cgi.bin.webscr.cmd.login.submit.15.cgi.bin.webscr.cmd.login.submit.15154.fatihdabak.com/sc/y/rev/488d0f6f819beb02b29791e111576dec/
8	http://edirnewebtasarimi.com/help/support/help/PP-1124-075-998/00b056620c4cc49fd79b6cb5aa773b0b/
9	http://www.clientel-pl.com/pl/b1999504af89588d08f4679d126f7720/scr.php?cmd=53026&dispatch=61ea2516a84f51c22d86a8fb0151b008
10	http://totalwhiteboard.com.au/.pp/0053d4ae3e2c78154d29d413c1236341/webscr.php?cmd=_login-run&dispatch=5885d80a13c0db1f998ca054efbdf2c29878a435fe324eec2511727fbf3e9efcd8
11	http://classiclogin.altervista.org/-/dados/time/AtualizandoDiaenoite2014/

12	http://ssl.paypal.secure.your.billing.information.mytrickworld.com/update-your-billing-information/8db3caa65cd255d3ae984b35c683952d/Security/Update/Account/Login/?cmd=_login-run&dispatch=e04a132adbe8a628371887da515b33e9e04a132adbe8a628371887da515b33e9
13	http://paypal.com.update.account.toughbook.cl/8a30e847925afc5975161aeabe8930f1/?cmd=_login-run&dispatch=70d1e179bda95563c92cdbb41bd380f670d1e179bda95563c92cdbb41bd380f6
14	http://paypal.com-cgi-bin.webscr.cmd.flowsession.home.locale.en-update.doctorsantis.cl/?cmd=_home&dispatch=5885d80a13c0db1f8e&ee=c2fdde4e9dbbb604104ee20987ae47db
15	http://paypal.ankarabayanmodel.com/PP/?cmd=_home&dispatch=5885d80a13c0db1f8e&ee=37c89453f89e8330ec833a3eb8ca0a77
16	http://www.theripe.tv/wp-content/plugins/justified-image-grid/languages/EN/c40ab55b0b2d4614ef0980c72fbe6007/?cmd=_home&dispatch=b47f8b3f68e40295c379148eb5c7a257b47f8b3f68e40295c379148eb5c7a257
17	http://www.yoursyours.com/templates/ilu/a/e5ad280236ce655dc34f3dedab589e97/scr.php?cmd=53026&dispatch=5b9bcc80064eac725312483dad5f6d46
18	http://www.re-update-your-information-1qs5dc1qs5941q5sf1sqf1qs5.vidavallarta.com.mx/reactivation/e66aea1c3732c4e6f5528af492d34ca0/?cmd=_home&dispatch=adcc48290abfe8c419eebf1df1ac7373adcc48290abfe8c419eebf1df1ac7373
19	http://alvaroestrella.com/secure/webapps/mpp/home/?cmd=_home&dispatch=5885d80a13c0db1f8e&ee=805eb67f9400bc03e8daa639613a16f7
20	http://178.210.162.252/~zeedee/9a70c0acdb2584924f5d0/web.php?#/confirm.php
21	http://310bxgg.com/aa/index.php?cmd=_home&dispatch=6e2b830562361bda74cc627c58f7e9306e2b830562361bda74cc627c58f7e930
22	http://smak.affordablebestwebsitehosting.com/~wxacad99/modules/fr/PayPal.fr/c.html?webscr?cmd=_login-done&login_access=2265929062
23	http://alwaysplotting.com/mokhtarhome/989e5e37528c1cbab8a0e6410ea45ee8/?cmd=_home&dispatch=5885d80a13c0db1f8e&ee=016b39232ee2655d5281db69fdf27aca
24	http://kgmu.kcn.ru/gigitru/images/banners/pp/webapps/mpp/?cmd=_home&dispatch=5885d80a13c0db1f8e&ee=eb70143576d5f26d479f02e2637fe227
25	http://www.cleanwheel.net/images/pics/informationen3/initsec.html
26	http://www.avatur.net/admin/cx/9772515528495d59759dc10765940daa/?cmd=_login-run&dispatch=f9ec5d6a8a348bce8818eb32e1b1d3eff9ec5d6a8a348bce8818eb32e1b1d3ef
27	http://www.vicfer.mx/~screamvi/PayPal/1bfc5540549a80993495b28f7a7b4d07/AccountLogin.php

28	http://www.latitud-x.com.mx/~screamvi/PayPal/1bfc5540549a80993495b28f7a7b4d07/AccountLogin.php?Userid=fxwspckm5
29	http://www.carycar.com.mx/~screamvi/PayPal/1bfc5540549a80993495b28f7a7b4d07/AccountLogin.php
30	http://gentilee.com.ar/~screamvi/PayPal/1bfc5540549a80993495b28f7a7b4d07/AccountLogin.php
31	http://www.uniredmx.com/~screamvi/PayPal/1bfc5540549a80993495b28f7a7b4d07/AccountLogin.php

A.2 HTML CODE ANALYSIS OF PHISHING VS ORIGINAL IN PHISHLOAD

Table 32: Differences phishing webpage vs legitimate website; target: PayPal

No.	What's changed/added?	Details
1	Irregular scripts	- Creation of function zzz() contains variables that holds input value from a form <form onsubmit="return zzzz()" class=" edit" action="getinfo.php" method="post" name="fox">. - There are 17 script tag in the original paypal, whereas there are only 5 script tags - If... else.. logic is added to manage how a user inputs his information
	Irregular link tag	- We are not sure whether the link tag is added by the phisher or it refers to the original paypal with the different source (PayPal has changed its web page from time to time, it means that the source also change periodically) - Most of the links are redirected to pass.php
	Suspicious form	A form used to ask user to submit his creditcard information, upon clicking, it will parse the information to variables hold by zzz() function
2	Html language	Lang=en whereas the original has lang=de
	Country difference	It based on Algeria PayPal country code DZ whereas the original has DE country code

	Irregular scripts	- Script to measure anticlickjack is not present. - Script addition clearly stating that it is a hack script at line 91 - s.prop1="p/gen/login-processing"; s.pageName="p/gen/login-processing::_login-processing"; whereas the original has s.prop1="xpt/Marketing_CommandDriven/homepage/MainHome"; and no s.pageName variable - Function scOnload() is present in the original whereas it is not present
3	Title differences	It has different title than the original
		Paypal object redirected based on 20101108 whereas in the original phishload database is based on 20120210
	Irregular scripts	- Anticlickjack script is not present - New script addition is present which hide from JavaScript-challenged browsers. - More new script addition is present to manage PayPal login flow <script type="text/javascript">PAYPAL.common.loginflow = 'p/gen/login';.... - s.prop1="p/gen/login";
	Css object difference	Paypal object redirected based on 20101108
	Suspicious form	It has <form action="websrc.php" name="login_form" method="post"> as user input for PayPal username and password
6	Different title	Italian vs German language
	Suspicious Form	It has <form action="error_login.php" name="login_form" method="post"> which ask for paypal credentials and redirect them to the wrong action
	Irregular scripts	- It has script to hide from javascript challenge browser. - It has script <script type="text/javascript">PAYPAL.common.loginflow = 'p/gen/login'; contains malicious operation - s.prop1="p/gen/login"; - It does not have the function scOnload()
	Flash object	It seems that there is an additional div tag at the bottom and I think it contains flash object.

7	URL encoding	It has weird URL encoding inside script tag document.write(unescape(. . . . I think the URLencoding inside the document.write is similar with the non URLencoding. So the rest of the result referred to the URLencoding will be similar as well.
	Suspicious form	If I decode the URL encoding, this form is present <form method="post" name="login_form" action="error_logins.php"> The form above exists again in the non encoding html
	Irregular scripts	- Script to hide from javascript challenged browser - The script that contains YAHOO.util.Event.addListener also quite different from the original, yet it exists again at the end - The tag <noscript></noscript> is removed - There is no function scOnload()
8	Different language	Lang=de vs. lang=en
	Suspicious Form	<form action="processing.php" name="login_form" method="post"> which ask for login email and password
	Irregular scripts	- Script to hide from javascript challenged browser - Suspicious script YAHOO.util.Event.addListener
	Flash object	flash object is added at the bottom
9	Title difference	“Log in” title page
	Irregular scripts	Function validateFormOnSubmit(theForm)
	Suspicious Form	form onsubmit="return validateFormOnSubmit(this)" method="post" action="cnd_pay.php">
	Suspicious link tag	All the links are redirect to itself / no absolute URL path
	Based on individual examination I would say that the web page is completely different than the original	

10	Suspicious Form	<form action="error_login.php?cmd=_login-run&dispatch=5885d80a13codb1f998ca054efbdf2c29878a435fe324eec2511727fbf3e9efcd8" name="login_form" method="post"> asking for login email and login password
	Irregular input tag	- <input type="submit" class="button primary" value="Log In" name="submit.x" /> - <input type="hidden" name="operating_system" value="Windows" /><input type="hidden" id="flow_name" name="flow_name" value="p/gen/login" /> - <input type="hidden" id="bp_ks2" name="bp_ks2" /><input type="hidden" id="bp_ks3" name="bp_ks3" /><input type="hidden" name="flow_name" value="p/gen/login" />
	Irregular scripts	- Script to hide from javascript challenged browser - s.prop1="p/gen/login"; - no function scOnload()
	Flash object	flash object is added at the bottom
11	Irregular scripts	- src="/js/lib/yui/animation.js - Script anticlickjack removed - Script PAYPAL.util.lazyLoadRoot removed - Great amount of scripts are removed - Suspicious script <script type="text/javascript">if(typeof PAYPAL != 'undefined'){ PAYPAL.core.Navigation.init(); }</script> - Suspicious script s.prop1="p/gen/login-processing"; - Function scOnload removed - Suspicious script setTimeout("location.href =... at the bottom
12	Irregular input	- <input type="hidden" name="flow_name" value="p/gen/login" /> - <input type="hidden" value="ok" name="login_cmd" /> - <input type="hidden" value="" name="login_params" />

	Irregular scripts	- <script src="files/globaloo.js" type="text/javascript"> - script that hides from javacscript challenged browser - anticlickjack script is removed - <script src="files/pp_jscod.js" type="text/javascript"></script> - s.prop1="p/gen/login"; • function scOnload removed
	Suspicious Form	<form action="" name="login_form" method="post"> which ask user input for login credential
	Suspicious link	some of the links are redirected to itself / not absolute URL path
	Flash object	flash object is added at the bottom
15	Irregular input	<input type="hidden" name="flow_name" value="p/gen/login" /> • <input type="hidden" value="" name="login_cmd" /><input type="hidden" value="" name="login_params" /><fieldset>
	Suspicious form	<form action="error_login.php?cmd=_login-run&dispatch=5885d80a13codb1f998ca054efbdf2c29878a435fe324eec2511727fbf3e9efcd8" name="login_form" method="post"> that asks login credential
	Irregular scripts	- script that hides from javascript challenged browser - anticlickjack script is removed - suspicious script <script type="text/javascript">if(typeof PAYPAL != 'undefined'){ PAYPAL.core.Navigation.init(); }</script> - suspicious script <script type="text/javascript">PAYPAL.common.loginflow = 'p/gen/login'; - s.prop1="p/gen/login"; - function scOnload is removed
	Flash object	flash added at the bottom (perhaps it is from the latest legitimate paypal website)
16	Suspicious form	<form action="Submit.php" name="login_form" method="post">

	Irregular scripts	- script that hides from javascript challenge browser - YAHOO.util.Event.addListener script - s.prop1="xpt/Marketing_CommandDriven/ homepage/IndividualsHome"; - function scOnload() is removed - YUE.addListener script at the bottom
	Irregular links	href="#content
17	Suspicious Form	<form action="processing.php" name="login_form" method="post">
	Irregular scripts	script that hides from javascript challenge browsers function scOnload is removed
	Irregular links	href="#"
18	Irregular input	- <input type="hidden" name="flow_name" value="p/gen/login" /> - <input type="hidden" value="" name="login_cmd" /> - <input type="hidden" value="" name="login_params" />
	Irregular from	<form action="error_login.php" name="login_form" method="post">
	Irregular script	- script that hides from javascript challenge browsers - anticlickjack script removed - PAYPAL.tns.loginflow script - PAYPAL.common.loginflow = 'p/gen/login' added - s.prop1="p/gen/login"; - function scOnload is removed
	Flash object	Flash added at the bottom
19	Irregular script	- <script type="text/javascript"> if (parent.frames.length > 0) {top.location.replace(document.location); }</script> - Script that hides from javascript challenge browsers - <script type="text/javascript">PAYPAL.common.loginflow = 'p/gen/login'; - s.prop1="p/gen/login"; - function scOnload is removed
	Irregular links	<li class="login">Einloggen
	Suspicious form	<form action="websrc.php" name="login_form" method="post">

	Irregular input	<input type="hidden" name="flow_name" value="p/gen/login" />
	Flash object	flash added at the bottom
20	Suspicious form	<form action="asu.php" name="login" method="POST">
	Irregular link	all the links are redirected to itself
	Irregular script	<script type="text/javascript" language="JavaScript">
	Based on individual examination I would say that the web page is completely different than the original	

BIBLIOGRAPHY

[1] PA Barraclough, MA Hossain, MA Tahir, Graham Sexton, and Nauman Aslam. Intelligent phishing detection and protection scheme for online transactions. *Expert Systems with Applications*, 40(11):4697–4706, 2013. (Cited on page 21.)

[2] Mark Blythe, Helen Petrie, and John A Clark. F for fake: four studies on how we fall for phish. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 3469–3478. ACM, 2011. (Cited on pages 1 and 67.)

[3] Ashley Carman. Phishing scam targets michigan public schools. URL http://www.scmagazine.com/phishing-scam-targets-michigan-public-schools/article/343177/. [Online; accessed 13-May-2014]. (Cited on page 16.)

[4] Madhusudhanan Chandrasekaran, Krishnan Narayanan, and Shambhu Upadhyaya. Phishing email detection based on structural properties. In *NYS Cyber Security Conference*, pages 1–7, 2006. (Cited on page 5.)

[5] Zesheng Chen and Chuanyi Ji. Optimal worm-scanning method using vulnerable-host distributions. *International Journal of Security and Networks*, 2(1):71–80, 2007. (Cited on page 19.)

[6] Sidharth Chhabra, Anupama Aggarwal, Fabricio Benevenuto, and Ponnurangam Kumaraguru. Phi. sh/$ ocial: the phishing landscape through short urls. In *Proceedings of the 8th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference*, pages 92–101. ACM, 2011. (Cited on page 22.)

[7] Pern Hui Chia and Svein Johan Knapskog. *Re-evaluating the wisdom of crowds in assessing web security*, pages 299–314. Springer, 2012. (Cited on page 21.)

[8] Robert Cialdini. The science of persuasion. *Scientific American Mind*, 2001. ISSN 1555-2284. (Cited on pages 9, 10, 12, 13, 20, 43, and 49.)

[9] Richard Clayton, Drew Dean, Markus Jakobsson, Steven Myers, Stuart Stubblebine, and Michael Szydlo. A chat at the old phishin'hole. *Lecture Notes in Computer Science*, 3570:88, 2005. (Cited on page 7.)

[10] M Patrick Collins, Timothy J Shimeall, Sidney Faber, Jeff Janies, Rhiannon Weaver, Markus De Shon, and Joseph Kadane. Using

uncleanliness to predict future botnet addresses. In *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, pages 93–104. ACM, 2007. (Cited on page 19.)

[11] Organización Internacional de Normalización. *ISO/IEC 27002: Information Technology, Security Techniques, Code of Practice for Information Security Management*. ISO/IEC, 2005. (Cited on page 28.)

[12] Belgium Police Department. Overzicht per criminele figuur, . URL http://www.polfed-fedpol.be/crim/crim_statistieken/app_crimestat/app_crimestat_dashboard_crimfig_misdrijven_nl.php. [Online; accessed 13-May-2014]. (Cited on page 18.)

[13] Belgium Police Department. Portaal van de belgische politie, . URL http://www.polfed-fedpol.be/. [Online; accessed 13-May-2014]. (Cited on page 18.)

[14] Rachna Dhamija, J Doug Tygar, and Marti Hearst. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pages 581–590. ACM, 2006. (Cited on pages 1, 7, and 28.)

[15] Oxford Dictionaries. Phishing. URL http://www.oxforddictionaries.com/definition/english/phishing. (Cited on pages 5 and 7.)

[16] Collins English Dictionary. Phishing. URL http://www.collinsdictionary.com/dictionary/american/phishing. (Cited on page 7.)

[17] Ronald C Dodge Jr, Curtis Carver, and Aaron J Ferguson. Phishing for user security awareness. *Computers & Security*, 26(1):73–80, 2007. ISSN 0167-4048. (Cited on page 27.)

[18] Douglas P Dotterweich and Kimberly S Collins. The practicality of super bowl advertising for new products and companies. *Journal of Promotion Management*, 11(4):19–31, 2006. (Cited on page 41.)

[19] Shaun Egan and Barry Irwin. An evaluation of lightweight classification methods for identifying malicious urls. In *Information Security South Africa (ISSA), 2011*, pages 1–6. IEEE. ISBN 1457714817. (Cited on pages 22, 24, and 25.)

[20] Aaron Emigh. Online identity theft: Phishing technology, chokepoints and countermeasures. *ITTC Report on Online Identity Theft Technology and Countermeasures*, 3, 2005. (Cited on pages xiii, 11, 14, 15, 27, and 28.)

[21] Philip V Fellman and Robert Rodriguez. The dark side of the internet. In *International Federation for Information Processing, International Meeting, "IT Innovation for Adaptability and Competitiveness"*. (Cited on page 6.)

[22] RSA FraudAction. Rsa monthly fraud report. URL http://www.emc.com/security/rsa-identity-protection-and-verification/rsa-fraudaction/rsa-fraudaction-antiphishing-service.htm. [Online; accessed 6-August-2014]. (Cited on pages xiii, 8, and 9.)

[23] Edwin Donald Frauenstein and Rossouw von Solms. *An Enterprise Anti-phishing Framework*, pages 196–203. Springer, 2013. (Cited on pages xiii, 11, 12, 13, 27, and 28.)

[24] Adam Greenberg. Medical staffers fall for phishing emails, data on 8,300 compromised. URL http://www.scmagazine.com/medical-staffers-fall-for-phishing-emails-data-on-8300-compromised/article/340590/. [Online; accessed 13-May-2014]. (Cited on page 16.)

[25] Gaurav Gupta and Josef Pieprzyk. Socio-technological phishing prevention. *Information Security Technical Report*, 16(2):67–73, 2011. ISSN 1363-4127. (Cited on page 22.)

[26] Cormac Herley and Dinei Florêncio. A profitless endeavor: phishing as tragedy of the commons. In *Proceedings of the 2008 workshop on New security paradigms*, pages 59–70. ACM, 2009. (Cited on pages 8 and 9.)

[27] Jason Hong. The state of phishing attacks. *Communications of the ACM*, 55(1):74–81, 2012. ISSN 0001-0782. (Cited on pages 8, 9, and 11.)

[28] Huajun Huang, Liang Qian, and Yaojun Wang. A svm-based technique to detect phishing urls. *Information Technology Journal*, 11(7), 2012. ISSN 1812-5638. (Cited on page 22.)

[29] Tom N Jagatic, Nathaniel A Johnson, Markus Jakobsson, and Filippo Menczer. Social phishing. *Communications of the ACM*, 50(10):94–100, 2007. (Cited on pages 1 and 5.)

[30] Markus Jakobsson. Modeling and preventing phishing attacks. In *Financial Cryptography*, volume 5. Citeseer. (Cited on page 7.)

[31] Markus Jakobsson and Steven Myers. *Phishing and countermeasures: understanding the increasing problem of electronic identity theft*. John Wiley & Sons, 2006. ISBN 0470086092. (Cited on pages 1, 5, 6, 7, 8, 16, 17, and 18.)

[32] Lance James. *Phishing exposed*. Syngress, 2005. ISBN 0080489532. (Cited on pages 1, 5, 7, and 27.)

[33] K Jansson and R Von Solms. Phishing for phishing awareness. *Behaviour & Information Technology*, 32(6):584–593, 2013. ISSN 0144-929X. (Cited on page 27.)

[34] Engin Kirda and Christopher Kruegel. Protecting users against phishing attacks with antiphish. In *Computer Software and Applications Conference, 2005. COMPSAC 2005. 29th Annual International*, volume 1, pages 517–524. IEEE, 2005. (Cited on page 36.)

[35] Iacovos Kirlappos and Martina Angela Sasse. Security education against phishing: A modest proposal for a major rethink. *IEEE Security and Privacy Magazine*, 10(2):24–32, 2012. (Cited on page 28.)

[36] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. Lessons from a real world evaluation of anti-phishing training. In *eCrime Researchers Summit, 2008*, pages 1–12. IEEE. ISBN 1424429692. (Cited on page 27.)

[37] Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, page 3. ACM, 2009. (Cited on pages xiii, 28, 29, and 30.)

[38] Willy Lai. Fitting power law distributions to data. (Cited on page 22.)

[39] Elmer Lastdrager. Achieving a consensual definition of phishing based on a systematic review of the literature. 2014. (Cited on pages 7 and 8.)

[40] Anh Le, Athina Markopoulou, and Michalis Faloutsos. Phishdef: Url names say it all. In *INFOCOM, 2011 Proceedings IEEE*, pages 191–195. IEEE. ISBN 1424499194. (Cited on pages xiii and 24.)

[41] Avivah Litan. Phishing victims likely will suffer identity theft fraud. *Gartner Research Note (May 14, 2004)*, 2004. (Cited on page 8.)

[42] Gang Liu, Bite Qiu, and Liu Wenyin. Automatic detection of phishing target from phishing webpage. In *Pattern Recognition (ICPR), 2010 20th International Conference on*, pages 4153–4156. IEEE, . ISBN 1424475422. (Cited on page 21.)

[43] Haotian Liu, Xiang Pan, and Zhengyang Qu. Learning based malicious web sites detection using suspicious urls. . (Cited on pages xiii, 25, 26, and 27.)

[44] Christian Ludl, Sean McAllister, Engin Kirda, and Christopher Kruegel. On the effectiveness of techniques to detect phishing sites. In *Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 20–39. Springer, 2007. (Cited on page 36.)

[45] Justin Ma, Lawrence K Saul, Stefan Savage, and Geoffrey M Voelker. Identifying suspicious urls: an application of large-scale online learning. In *Proceedings of the 26th Annual International Conference on Machine Learning*, pages 681–688. ACM, . ISBN 1605585165. (Cited on pages xiii and 26.)

[46] Justin Ma, Lawrence K Saul, Stefan Savage, and Geoffrey M Voelker. Beyond blacklists: learning to detect malicious web sites from suspicious urls. In *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 1245–1254. ACM, . ISBN 1605584959. (Cited on pages xiii, 24, 25, and 26.)

[47] Liping Ma, Bahadorrezda Ofoghi, Paul Watters, and Simon Brown. Detecting phishing emails using hybrid features. In *Ubiquitous, Autonomic and Trusted Computing, 2009. UIC-ATC'09. Symposia and Workshops on*, pages 493–497. IEEE, 2009. (Cited on page 1.)

[48] Steve Mansfield-Devine. Interview: Joe ferrara–fighting phishing. *Computer Fraud & Security*, 2013(7):17–20, 2013. (Cited on page 28.)

[49] Max Emanuel Maurer. Phishload. URL `http://www.medien.ifi.lmu.de/team/max.maurer/files/phishload/index.html`. [Online; accessed 3-April-2014]. (Cited on page 35.)

[50] Tom McCall. Gartner survey shows phishing attacks escalated in 2007; more than $3 billion lost to these attacks. *Stephane GALLAND*, 2007. (Cited on pages 8 and 9.)

[51] Tom McCall. Gartner survey shows phishing attacks escalated in 2007; more than $3 billion lost to these attacks. *Stephane GALLAND*, 2007. (Cited on page 8.)

[52] Tyler Moore and Richard Clayton. An empirical analysis of the current state of phishing attack and defence. In *WEIS*. Citeseer. (Cited on page 18.)

[53] Tyler Moore and Richard Clayton. *Evaluating the wisdom of crowds in assessing phishing websites*, pages 16–30. Springer, 2008. ISBN 3540852298. (Cited on pages xiii, 21, 22, and 23.)

[54] Giovane César Moura. *Internet bad neighborhoods*. Giovane Cesar Moreira Moura, 2013. ISBN 9036534607. (Cited on pages 18 and 19.)

[55] Giovane CM Moura and Aiko Pras. Scalable detection and isolation of phishing. In *Scalability of Networks and Services*, pages 195–198. Springer, 2009. (Cited on pages 8 and 9.)

[56] Philip J Nero, Brad Wardman, Heith Copes, and Gary Warner. Phishing: Crime that pays. In *eCrime Researchers Summit (eCrime), 2011*, pages 1–10. IEEE. ISBN 1457713403. (Cited on pages 11 and 15.)

[57] National Plant Diagnostic Network. Types of social engineering. URL http://www.npdn.org/social_engineering_types. [Online; accessed 16-July-2014]. (Cited on page 40.)

[58] OpenDNS. Phishtank: Out of the net, into the tank. URL http://www.phishtank.com/faq.phpk. [Online; accessed 13-May-2014]. (Cited on page 20.)

[59] Parth Parmar and Kalpesh Patel. Comparison of phishing detection techniques. In *International Journal of Engineering Research and Technology*, volume 3. ESRSA Publications. ISBN 2278-0181. (Cited on page 20.)

[60] Bryan Parno, Cynthia Kuo, and Adrian Perrig. *Phoolproof phishing prevention*. Springer, 2006. ISBN 3540462554. (Cited on page 7.)

[61] James W Pennebaker and Deborah Yates Sanders. American graffiti: Effects of authority and reactance arousal. *Personality and Social Psychology Bulletin*, 2(3):264–267, 1976. (Cited on page 40.)

[62] Phishing.org. History of phishing. URL http://www.phishing.org/history-of-phishing/. (Cited on page 6.)

[63] Swapan Purkait. Phishing counter measures and their effectiveness - literature review. *Information Management & Computer Security*, 20(5):382–420, 2012. ISSN 0968-5227. (Cited on page 20.)

[64] Anirudh Ramachandran and Nick Feamster. Understanding the network-level behavior of spammers. In *ACM SIGCOMM Computer Communication Review*, volume 36, pages 291–302. ACM. ISBN 1595933085. (Cited on page 19.)

[65] Teri Robinson. Phishing scam aimed at google docs, drive users. URL http://www.scmagazine.com/phishing-scam-aimed-at-google-docs-drive-users/article/338369/. [Online; accessed 13-May-2014]. (Cited on page 16.)

[66] Stuart E Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. The emperor's new security indicators. In *Security and Privacy, 2007. SP'07. IEEE Symposium on*, pages 51–65. IEEE. ISBN 0769528481. (Cited on page 28.)

[67] Wombat security technology. Phishguru: Assess and motivate your employees using simulated phishing attacks. URL http://www.wombatsecurity.com/phishguru. [Online; accessed 23-May-2014]. (Cited on page 30.)

[68] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the 28th international conference on Human factors in computing systems*, pages 373–382. ACM. ISBN 1605589292. (Cited on page 2.)

[69] Frank Stajano and Paul Wilson. Understanding scam victims: seven principles for systems security. *Communications of the ACM*, 54(3):70–75, 2011. (Cited on pages 9 and 10.)

[70] Henri Tajfel and John C Turner. The social identity theory of intergroup behavior. 2004. (Cited on page 41.)

[71] Gregg Tally, Roshan Thomas, and Tom Van Vleck. Anti-phishing: Best practices for institutions and consumers. *McAfee Research, Mar*, 2004. (Cited on pages 7, 11, and 14.)

[72] Inspired Telemarketing. 5 tips for getting past receptionists!, 2013. URL http://inspiredtelemarketing.wordpress.com/2013/09/13/5-tips-for-getting-past-receptionists/. [Online; accessed 16-July-2014]. (Cited on page 40.)

[73] Ministerie van Veiligheid en Justitie. Nationale helpdesk voor vragen en meldingen over fraude. URL http://www.fraudehelpdesk.nl/over-ons. [Online; accessed 13-July-2014]. (Cited on page 45.)

[74] Brad Wardman, Gaurang Shukla, and Gary Warner. Identifying vulnerable websites by analysis of common strings in phishing urls. In *eCrime Researchers Summit, 2009. eCRIME'09.*, pages 1–13. IEEE. ISBN 1424446252. (Cited on page 2.)

[75] Merriam Webster. Phishing. URL http://www.merriam-webster.com/dictionary/phishing. (Cited on page 7.)

[76] Liu Wenyin, Ning Fang, Xiaojun Quan, Bite Qiu, and Gang Liu. Discovering phishing target based on semantic link network. *Future Generation Computer Systems*, 26(3):381–388, 2010. ISSN 0167-739X. (Cited on page 22.)

[77] Rebecca Wetzel. Tackling phishing. *Business Communications Review*, 35(2):46–49, 2005. (Cited on pages xiii, 11, 13, and 14.)

[78] Joshua S White, Jeanna N Matthews, and John L Stacy. A method for the automated detection phishing websites through both site

characteristics and image analysis. In *SPIE Defense, Security, and Sensing*, pages 84080B–84080B–11. International Society for Optics and Photonics. (Cited on page 21.)

[79] Michael Workman. Wisecrackers: A theory - grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, 59(4):662–674, 2008. ISSN 1532-2890. (Cited on pages 5, 9, 10, 41, and 49.)

[80] Guang Xiang, Jason Hong, Carolyn P Rose, and Lorrie Cranor. Cantina+: a feature-rich machine learning framework for detecting phishing web sites. *ACM Transactions on Information and System Security (TISSEC)*, 14(2):21, 2011. ISSN 1094-9224. (Cited on pages xiii, 25, 26, and 27.)

[81] Huiping Yao and Dongwan Shin. Towards preventing qr code based attacks on android phone using security warnings. In *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*, pages 341–346. ACM. ISBN 1450317677. (Cited on page 21.)

[82] Yue Zhang, Serge Egelman, Lorrie Cranor, and Jason Hong. Phinding phish: Evaluating anti-phishing tools. ISOC, . (Cited on page 2.)

[83] Yue Zhang, Jason I Hong, and Lorrie F Cranor. Cantina: a content-based approach to detecting phishing web sites. In *Proceedings of the 16th international conference on World Wide Web*, pages 639–648. ACM, . ISBN 1595936548. (Cited on pages 2 and 27.)

COLOPHON

This document was typeset using the typographical look-and-feel `classicthesis` developed by André Miede. The style was inspired by Robert Bringhurst's seminal book on typography *"The Elements of Typographic Style"*. `classicthesis` is available for both LaTeX and LyX:

http://code.google.com/p/classicthesis/

Happy users of `classicthesis` usually send a real postcard to the author, a collection of postcards received so far is featured at:

http://postcards.miede.de/

Final Version as of August 23, 2014 (`Nurul Akbar` version 1).

DECLARATION

Put your declaration here.

Enschede, August 2014

Nurul Akbar