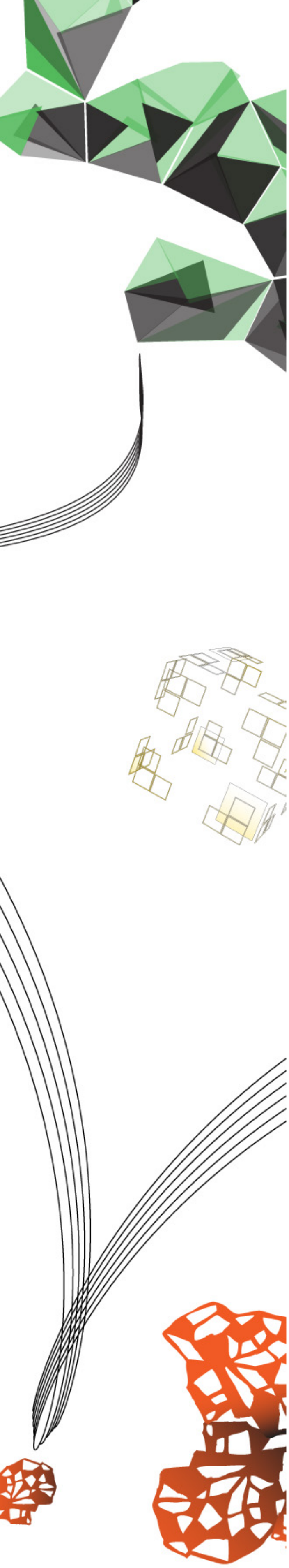


NURUL AKBAR

TITLE WILL GO HERE

Put somethingHERE

HERE

HERE & HERE

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

UNIVERSITEIT TWENTE.

TITLE WILL GO HERE

NURUL AKBAR

UNIVERSITY OF TWENTE.

Put subtitle here

August 2014 – version 1

Appear weak when you are strong, and strong when you are weak.
— Sun Tzu, The Art of War

There is nothing more deceptive than an obvious fact.
— Arthur Conan Doyle, The Boscombe Valley Mystery

ABSTRACT

Short summary of the contents in English…

ZUSAMMENFASSUNG

Kurze Zusammenfassung des Inhaltes in deutscher Sprache…

PUBLICATIONS

Some ideas and figures have appeared previously in the following publications:

Put your publications from the thesis here. The packages `multibib` or `bibtopic` etc. can be used to handle multiple different bibliographies in your document.

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

Put your acknowledgments here.

This is example ackowledgments

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

Put Introduction here

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 attack could be done by social engineering. Phishing is a form of social engineering that aim to retrieve credential from online users by mimicking trustworthy and legitimate institutions [23]. 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?

In the real world, phishing has a similar basic principle as 'fishing'. Instead of fish, online users are lured by authentic looking communication and hooked by authentic looking websites. Phishing is a malicious technique to manipulate online users into sharing their sensitive information by masquerading as legitimate and trustworthy institutions. Phishing attack also is a form of online criminal activity by using social engineering technique [23]. An individual or a group who uses this technique is called *Phishers*. After successfully gain 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 [24]. A fraudulent website is designed in such a way that it would be very identical to its legitimate target.

2.2 HISTORY OF PHISHING

The first time the term "phishing" was published by the American Online (AOL) UseNet Newsgroup on January 2, 1996 and began to expand in 2004 [50]. Since then, phishing development in cyberspace unfortunately was a great achievement 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 [16]. Jakobsson, et al. mentioned that in the early years of 90's (according to [50] it was around 1995) many hackers would create bogus AOL user accounts with automatically generated fraudulent credit card information [23]. 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 [23]. Hackers would masquerade themselves as AOL's employees asking to other users for credit card information through AOL instant messenger and email system. At this point, we believe the term of phishing attack has been born. 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 [50]. At the present day, phishing attacks have evolved not only aim to AOL users, but also any online users motivated by financial gain. Consequently, large number of legitimate institutions such as PayPal and eBay are being spoofed.

2.3 FORMAL DEFINITION OF PHISHING

Before we begin to dig deeper understanding of phishing attacks, 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 [23, 24, 54, 6, 48, 22, 9]. 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. We will take a look of one particular phishing definition from various 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"* [24]

> *"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"* [54]
>
> *"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"* [6]
>
> *"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"* [48]

It is noteworthy that the definition described by James, et al, Tally, et al, and Clayton, et al. [24, 54, 6] 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 [10, 11, 56] 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. Therefore, We follow the definition of phishing by Lastdrager [31] which stated:

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

The definition presented above is developed in a comprehensive way by using existing definitions as input and combined them. 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 [31] that this definition addresses all the essential elements of phishing and we will adopt it as universally accepted terminology throughout our research.

2.4 ECONOMICS IMPACT CAUSED BY PHISHING

It is non-trivial task to find a real cost from phishing damage in term of money or direct cost. This due to phishing economy is consistent with black market economy and does not advertise its successes [23]. On this section, brief explanation of direct cost on phishing attack will be illustrated based on literature reviews.

The difficulty of assessing the damage on phishing attack is caused by unwillingness of many users to share to acknowledge that they have been victimized by phishing attacks. This happens might be because of fear of humiliation, financial loses, or legal liability [23]. However, studies estimate the damage ranging from $61 million [19] to $3 billion per year [33] of direct losses to victims in the US only [20]. 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 [33]. By the 2007, it escalated to more than $3 billion loss [41]. 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]. Moreover, figure [num] illustrated the direct cost of phishing in 2013 by the same companies. <still in progress>

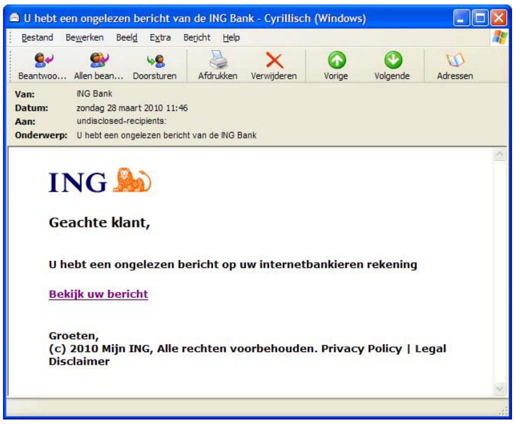
2.5 PHISHING MODUS OPERANDI

As we mentioned earlier, Phishing attack is a form of cybercrime. The technique of the attack usually carried out firstly by creating a replica/clone of a legitimate website such as financial website with almost 100% similar. 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. With the information obtained, they will try to steal money from their victims. 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. Typically, 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 at the end, we will present our own phase.

Based on the example scenario explained earlier, we believe that phishing attacks may consist of several phases. J. Hong [20] argued that there are three major phases:

1. Potential victims receive a phish.

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



U hebt een ongelezen bericht van de ING Bank - Cyrillisch (Windows)

Van: ING Bank
Datum: zondag 28 maart 2010 11:46
Aan: undisclosed-recipients:
Onderwerp: U hebt een ongelezen bericht van de ING Bank

ING

Geachte klant,

U hebt een ongelezen bericht op uw internetbankieren rekening

Bekijk uw bericht

Groeten,
(c) 2010 Mijn ING, Alle rechten voorbehouden. Privacy Policy | Legal Disclaimer

Figure 1: Example of fake ING logo in phishing email

2. The victim may take a suggested action in the message.
3. The phisher monetizes the stolen information.

Frauenstein, et al. [17] suggested that typically there are five main processes are used to perform phishing attack based on the perpective of the attacker. On the first process, a phisher usually will do some reconnaissance on how would the attack is executed and what information would be obtained from the victim. The first process is called planning. On the second process, a phisher typically deliver its message via 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 1 illustrates the example of fake ING bank logo in a phishing email to create "legitimate" feel[2].

On the third process, phisher fabricate 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, security enhancement, etc. so that the victim would feel obliged to be informed. This technique is commonly known as reverse social engineering. Moreover, we believe this process also corresponds with Cialdini [5] that suggested reciprocation as one of the technique to persuade people. 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. This process also corresponds with the theory of persuasion called authority [5]. The last process involved with fraudulent website that has been created by the phisher. Users may falsely believe to the message given in the

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

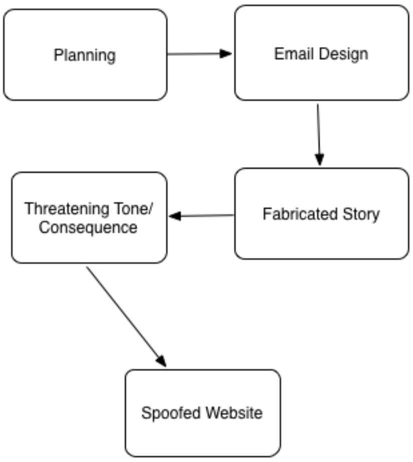


Figure 2: Phishing processes based on Frauenstein[17]

email and may click a Uniform Resource Locator (URL) that is embedded in the email. Subsequently, the URL would redirect users to this fraudulent 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 Cialdini's six basic tendencies of human behavior in generating positive response to persuasion [5] in a later section. To make a better understanding, we have created a diagram of these processes based on Frauenstein's typical five main processes [17] in Figure 2.

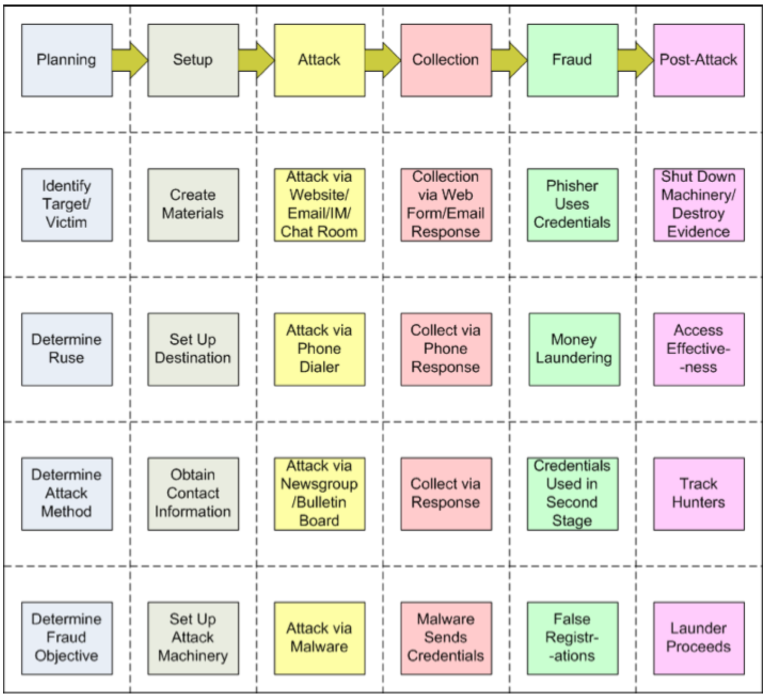
Considering that phishing attack is a process, Wetzel [58] suggested a taxonomy to make sense of the complex nature of the problem by mapping out a common attack lifecycle, and a possible set of activities attackers engage in within each phase. The taxonomy is illustrated in Figure 3. We believe it is analogous with Frauenstein's main phishing processes [17], however the differences is that Wetzel has added several phases like *Collection*, *Fraud* and *Post-attack*. The taxonomy is depicted as phases in the perspective of the phisher 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



Planning	Setup	Attack	Collection	Fraud	Post-Attack
Identify Target/ Victim	Create Materials	Attack via Website/ Email/IM/ Chat Room	Collection via Web Form/Email Response	Phisher Uses Credentials	Shut Down Machinery/ Destroy Evidence
Determine Ruse	Set Up Destination	Attack via Phone Dialer	Collect via Phone Response	Money Laundering	Access Effective- -ness
Determine Attack Method	Obtain Contact Information	Attack via Newsgroup /Bulletin Board	Collect via Response	Credentials Used in Second Stage	Track Hunters
Determine Fraud Objective	Set Up Attack Machinery	Attack via Malware	Malware Sends Credentials	False Registr- -ations	Launder Proceeds

Figure 3: Phishing attack taxonomy and lifecycle[58]

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.

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.

A study suggest that there are several phases involved in phishing attack based on the attacker's point of view:

> "1. The attacker obtains E-mail addresses for the intended victims. These could be guessed or obtained from a variety of sources.
>
> 2. The attacker generates an E-mail that appears legitimate and requests the recipient to perform some action.
>
> 3. The attacker sends the E-mail to the intended victims in a way that appears legitimate and obscures the true source.
>
> 4. Depending on the content of the E-mail, the recipient opens a malicious attachment, completes a form, or visits a web site.
>
> 5. The attacker harvests the victim's sensitive information and may exploit it in the future." [54]

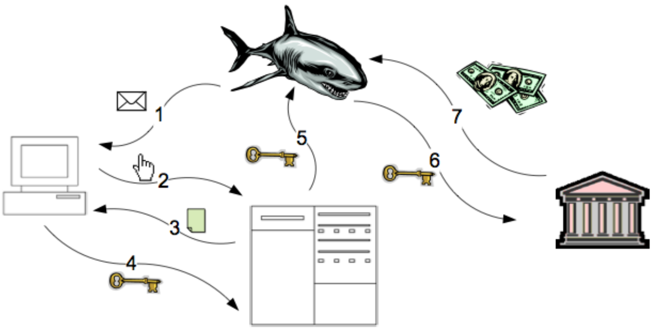


Figure 4: Flow of information in phishing attack [15]

The phases described by [54] are also analogous with the information flow explained by [15] represented in Figure 4.

Quoted from Emigh [15], the information flow of phishing attack is described by the following phases without countermeasures part:

> "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." [15]

Phishing attack steps performed by the phisher are also addressed by Nero, et al [45]. 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" [45]

As we can see from the earlier phases, there is a high amount of similarity between each other. We believe our phases are also analogous with other earlier studies. We thereby present our own phases of phishing attack and its categorization such as the lure, the hook and the catch. From Figure 5, we believe that the phishing attack phases based on the attacker point of view are generally characterized in the following way:

- The lure

1. Phishers prepare the attack
2. Deliver initial payload to victim
3. Direct spoofed website

- 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

2.6 TYPE OF PHISHING

In January 2014, 8300 patients data are being compromised in medical company in the US[3]. 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, phisher has successfully stole US$163,000 from US public school based on Michigan[4]. 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[5]. The attack was carried firstly with incoming email asking for opening document hosted at Google docs. Users that have clicked on

[3] http://www.scmagazine.com/medical-staffers-fall-for-phishing-emails-data-on-8300-compromised/article/340590/

[4] http://www.scmagazine.com/phishing-scam-targets-michigan-public-schools/article/343177/

[5] http://www.scmagazine.com/phishing-scam-aimed-at-google-docs-drive-users/article/338369/

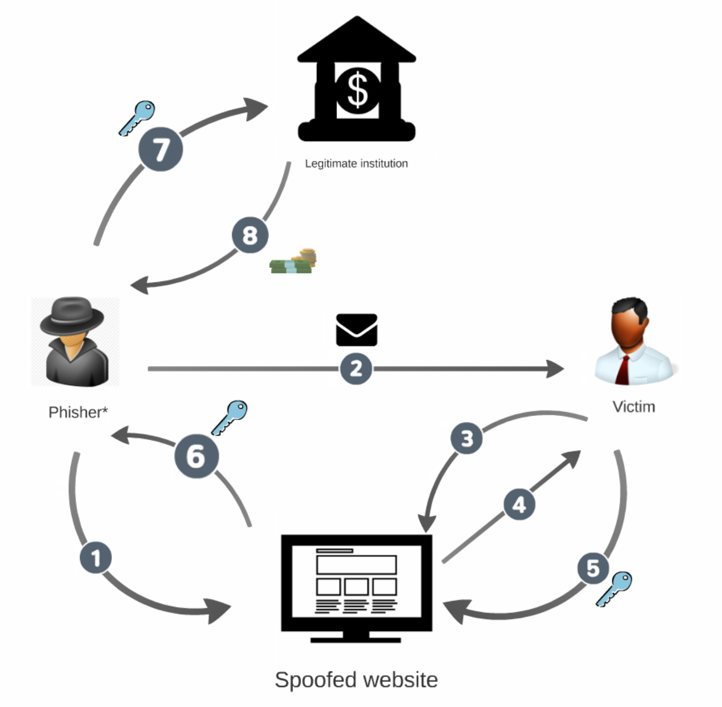


Figure 5: Information flow phishing attack

the link are taken to fraudulent Google login page prompted Google users credentials. Interestingly, the URL seems very convincing because it hosted on Google secure servers. We believe 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? The threat of phishing attacks is still alarming until today, and will be evolving in the future with more sophisticated technique of attacks. For this reason, we believe that it is necessary to provide a brief insight on popular variants of phishing that currently exist.

2.6.1 *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 [23]. 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".

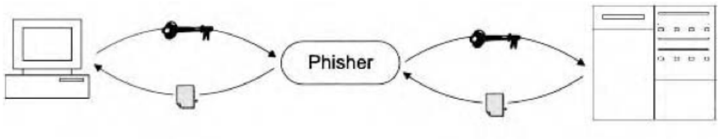


Figure 6: Man in the middle phishing[23]

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.

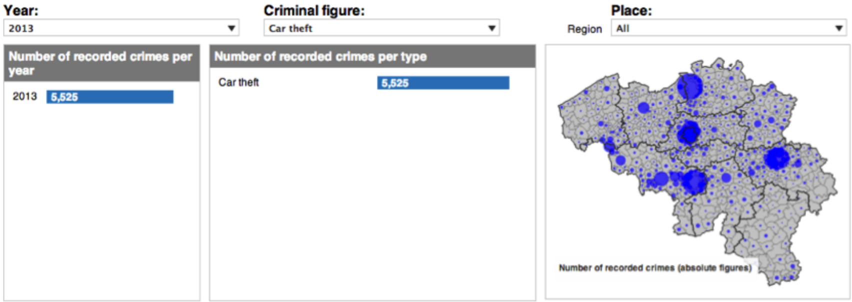
Another type of deceptive phishing scheme is rock-phish attacks. They held responsible for half a number of reported incidents worldwide in 2005 [42]. These attacks evade email filters by utilizes random text and GIF images which contain the actual message. Rock phish attacks also utilize a toolkit that 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.

2.6.2 *Malware-based phishing*

Generally, malware based phishing refers to any type of phishing which involves installing malicious piece of software onto users' personal computer [23]. 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.

2.6.3 *Man in the middle phishing*

Man-in-the-middle phishing attacks refer to the phishers that positioned in the middle between a legitimate institution and an end user [23]. The objective of these attacks is to make end users and legitimate institution (eg. Internet banking website) believe that they are truly communicating with each other. According to Jakobsson, et al.[23], Figure 6 illustrates the information flow of this type of attacks. Confidential information intended for legitimate site will be passed to the phishers before they can forward it to the legitimate site. Similarly, information from legitimate site to end-users will be passed to



Year: 2013

Criminal figure: Car theft

Place: Region All

Number of recorded crimes per year

2013 5,525

Number of recorded crimes per type

Car theft 5,525

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

the phishers first before the phishers can forward it to them. Unfortunately, man-in-the-middle attacks are also capable to exploit two-factor authentication system (sometimes called two steps verification) that ensures the authenticity of sender and recipient (Eg. Popular ABN Amro case in 2007[6]).

2.7 BAD NEIGHBORHOODS ON PHISHING

In the real world, there are parts of certain area that have higher crime rates than others (eg. Bronx in the US). Evidently, it is statistically more likely that a crime will occur compared to other locations [44]. To better illustrate this analogy, the police department in Belgium[7] 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[8]. The data is not necessarily based on cities, it can be based on the residential area within a city. This 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, the existence of bad neighborhood phenomenon also occurs in the Internet world called "Internet bad neighborhoods". 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 [44] which states:

[6] http://www.theregister.co.uk/2007/04/19/phishing_evades_two-factor_authentication

[7] http://www.polfed-fedpol.be/

[8] http://www.polfed-fedpol.be/crim/crim_statistieken/app_crimestat/app_crimestat_dashboard_crimfig_misdrijven_nl.php

> *"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 [51, 7, 2]. A dissertation study argues 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) [44]. 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) [44]. This suggests that phishing sites are required to have more reliable hosts in term of availability, while spams are not. We will see on section [num] our preliminary analysis on phishing Badhoods.

2.8 CURRENT COUNTERMEASURES OF PHISHING ATTACKS

There are various types of phishing countermeasures. However, since all the approaches reviewed so far all are preventive in nature, we believe phishing detection also aims to prevent user's confidential information to be successfully transmitted onto the wrong hands. A study suggests that phishing detection can be classified into two types; user training approach and software classification approach [47]. Parmar, et al. suggested a diagram and a table that summarize phishing detection as countermeasures in a broad view. In their study, Figure 8 categorizes the current countermeasures that presently developed. They also argued the advantages and disadavantages of each category in Table 1 [47]. However, as our research is specifically analyze the phishing attacks' method via emails, we will not give a complete wide range literature survey on all available phishing countermeasures. We will only discuss our result of literature reviews on Phishtank as a blacklist and machine learning classification, and anti-phishing training as prevention.

2.8.1 *Phishing detection*

2.8.1.1 *Phishtank*

One of the common approaches to detect phishing attack is blacklisting. 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. Phishtank stores phishing URLs in its database and the data is widely available for use by other companies. Some of the big companies that are using Phishtank's data in-

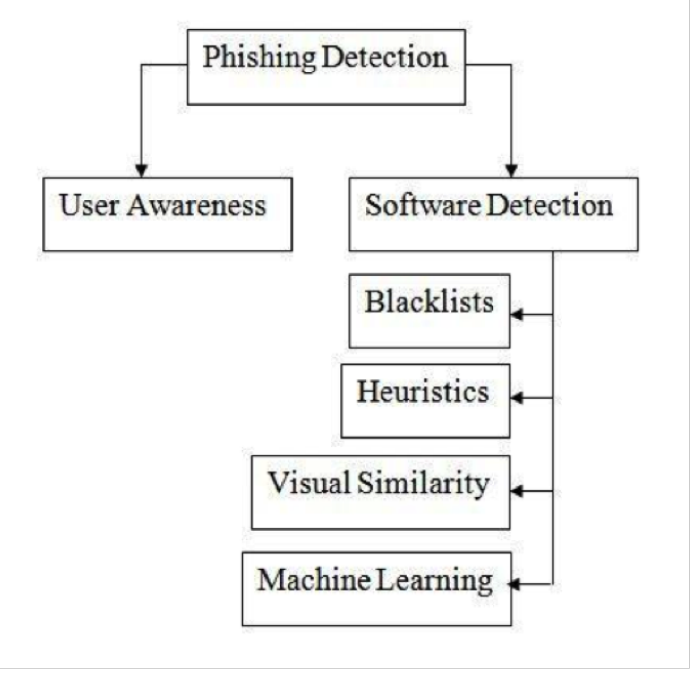


Figure 8: Phishing detection[47]

Detection techniques	**Advantages**	**Disadvantages**
Blacklist	• Requiring low resources on host machine • Effective when minimal FP rates are required	• Mitigation of zero hour phishing attack • Can result in excessive queries with heavily loaded servers
Heuristics and visual similarity	• Mitigate zero hour attacks	• Higher FP rate than blacklists • High computational cost
Machine Learning	• Mitigate zero hour attacks • Construct own classification model	• Time consuming • Costly • Huge number of rules

Table 1: Advantages-disadvantages detection technique[47]

cludes; 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 the data provided by Phishtank. Table 2 summarizes the papers selected and its relevancy with Phishtank. It is noteworthy that literatures selected do not represent all studies available that relevant with phishtank, we aim to only analyzed how crowd-sourced phishing detection such as phishtank works with the help of these literatures.

Table 2: Summary phishtank studies

Paper title	**First author**	**Country**	**Relevancy with phishtank**
Evaluating the wisdom of crowds in assessing phishing website [43]	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 [4]	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 [34]	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 [59]	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 [62]	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 [21]	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 [18]	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 [14]	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 [3]	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 [57]	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 URL, for that reason a study aims to evaluate the wisdom of crowd provided by Phishtank [43]. The study finds 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 [30]. Power law also applies to a system when large is rare and small is common [9]. 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 [43] between Phishtank and closed proprietary anti-phishing feeds[10]. 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 like Phishtank is that the distribution of user participation

[9] http://kottke.org/03/02/weblogs-and-power-laws

[10] The author did not specify 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	

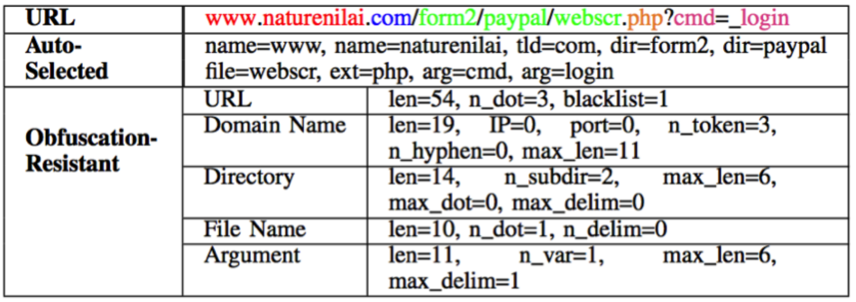
Table 3: Comparison summary [43]

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

2.8.1.2 *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



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 9: Example lexical features [32]

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, phishing 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, support vector machine, etc.. 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. We analyze three features: lexical feature, host-based feature and site popularity feature. Each of these features will be introduced briefly as follows.

1. Lexical features

Lexical features (URL based features) are based on the analysis of URL structure without any external information. A study suggest that the structure URL of phishing may "looks" different to experts [38]. These features include how many dots exist, the length, how deep the path traversal do the URL has, if there any sensitive words present in a URL, etc.. 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 9 shows the example analysis of lexical features in a phishing URL [32].

We believe lexical features analysis has a 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 [32]. A study also performed evaluation of lightweight classification that includes lexical features and host based features in

Haotian Liu, et al. [35]	Guang Xiang, et al. [61]
• 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 [35, 61]

its model [14]. 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 by two different studies [61, 35]. However, [61] 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 [61], 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 [61], 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 [14].

2. Host based features

Justin Ma, et al.[38, 37]	**Haotian Liu, et al. [46][35]**	**Guang Xiang, et al. [61]**
• 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 [38, 37, 35, 61]

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 [38]. Table 5 shows the host-based features from two studies that are currently used in machine learning phishing detection. The two studies are selected only for example comparison.

Each of these features does matter for phishing detection. However, we will not describe each of these features in detail. 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 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 [37, 38]. 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.

Guang Xiang, et al. [61]	Haotian Liu, et al. [35]
• 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 [61, 35]

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.

During our preliminary analysis, we will show that we could add reverse IP address lookup to find bad neighborhoods within the same IP address or domain.

4. 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 [61], some of the features indicated in Table 6 are well performed when incorporated with machine learning system.

1. Page in top search results: this feature originally used by [63] 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 [61]. 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 [61], 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 [35] 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 [61] and the latter feature can be obtained from amazon.com [35].

2.8.2 *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 [17]. Figure 10 illustrates where human factor takes part on phishing threats [17]. User's awareness of phishing has been explored by several studies [24, 17, 15, 28, 25, 12] as preventive measure against phishing attack. According to ISO/IEC 27002 [8], 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. A study suggests that users often ignore security indicators thus makes them ineffective [9]. 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 [27]. Evidently, another study also argued that 53% of their study participants were still attempting to provide their confidential information, even after their task was interrupted by strong security warning [52]. 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 [15]. 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 [39]. To do this, simulated phishing attacks often performed internally in an organization. Figure 11 shows a simulated phishing email and website carried out by Kumaraguru, et al. from PhishGuru [29]. As a result, this scenario puts them in the ultimate teachable

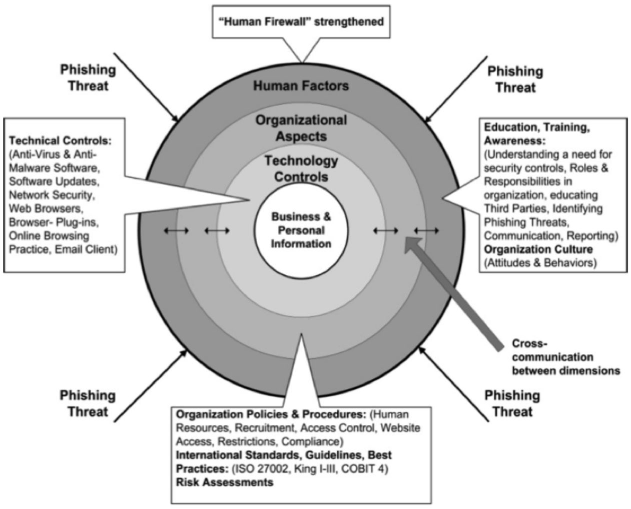
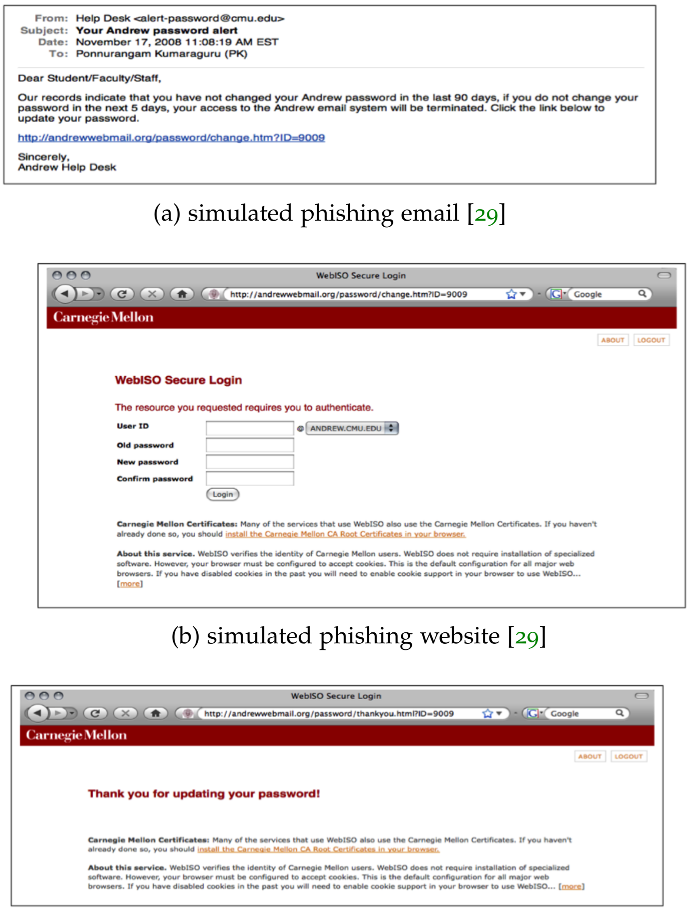

"Human Firewall" strengthened
Phishing Threat
Phishing Threat
Human Factors
Organizational Aspects
Technology Controls
Business & Personal Information
Technical Controls: (Anti-Virus & Anti-Malware Software, Software Updates, Network Security, Web Browsers, Browser- Plug-ins, Online Browsing Practice, Email Client)
Education, Training, Awareness: (Understanding a need for security controls, Roles & Responsibilities in organization, educating Third Parties, Identifying Phishing Threats, Communication, Reporting) Organization Culture (Attitudes & Behaviors)
Cross-communication between dimensions
Phishing Threat
Phishing Threat
Organization Policies & Procedures: (Human Resources, Recruitment, Access Control, Website Access, Restrictions, Compliance) International Standards, Guidelines, Best Practices: (ISO 27002, King I-III, COBIT 4) Risk Assessments

Figure 10: Holistic anti-phishing framework [17]

moment if they fall for these attacks, which is arguable an effective education.

Phishguru is one of the leading providers of cyber security training that educate online users to have some sort of security awareness . They argued that they provide more effective training than traditional training as it is designed to be more engaging. Figure 12 illustrates how embedded phishing training was presented by PhishGuru.

A study investigates the effectiveness of embedded training methodology in a real world situation [29]. They find 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 [29]. This suggests that user training strategy as an effective phishing education in order to improve phishing awareness especially in organizational environment.



From: Help Desk <alert-password@cmu.edu>
Subject: **Your Andrew password alert**
Date: November 17, 2008 11:08:19 AM EST
To: Ponnurangam Kumaraguru (PK)

Dear Student/Faculty/Staff,

Our records indicate that you have not changed your Andrew password in the last 90 days, if you do not change your password in the next 5 days, your access to the Andrew email system will be terminated. Click the link below to update your password.

http://andrewwebmail.org/password/change.htm?ID=9009

Sincerely,
Andrew Help Desk

(a) simulated phishing email [29]

WebISO Secure Login

http://andrewwebmail.org/password/change.htm?ID=9009

Carnegie Mellon

ABOUT LOGOUT

WebISO Secure Login

The resource you requested requires you to authenticate.

User ID @ ANDREW.CMU.EDU
Old password
New password
Confirm password
Login

Carnegie Mellon Certificates: Many of the services that use WebISO also use the Carnegie Mellon Certificates. If you haven't already done so, you should install the Carnegie Mellon CA Root Certificates in your browser.

About this service. WebISO verifies the identity of Carnegie Mellon users. WebISO does not require installation of specialized software. However, your browser must be configured to accept cookies. This is the default configuration for all major web browsers. If you have disabled cookies in the past you will need to enable cookie support in your browser to use WebISO... [more]

(b) simulated phishing website [29]

WebISO Secure Login

http://andrewwebmail.org/password/thankyou.html?ID=9009

Carnegie Mellon

ABOUT LOGOUT

Thank you for updating your password!

Carnegie Mellon Certificates: Many of the services that use WebISO also use the Carnegie Mellon Certificates. If you haven't already done so, you should install the Carnegie Mellon CA Root Certificates in your browser.

About this service. WebISO verifies the identity of Carnegie Mellon users. WebISO does not require installation of specialized software. However, your browser must be configured to accept cookies. This is the default configuration for all major web browsers. If you have disabled cookies in the past you will need to enable cookie support in your browser to use WebISO... [more]

(c) simulated phishing message [29]

Figure 11: Simulated phishing attack [29]

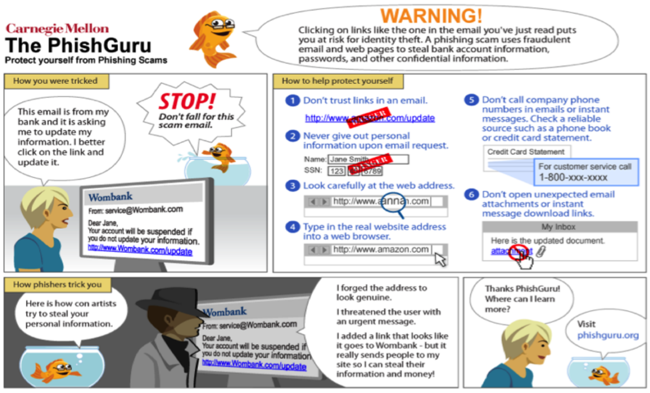

Carnegie Mellon
The PhishGuru
Protect yourself from Phishing Scams
WARNING!
Clicking on links like the one in the email you've just read puts you at risk for identity theft. A phishing scam uses fraudulent email and web pages to steal bank account information, passwords, and other confidential information.
How you were tricked
This email is from my bank and it is asking me to update my information. I better click on the link and update it.
STOP! Don't fall for this scam email.
Wombank
From: service@Wombank.com
Dear Jane,
Your account will be suspended if you do not update your information.
http://www.Wombank.com/update
How to help protect yourself
1 Don't trust links in an email.
http://www.amazon.com/update
DANGER
2 Never give out personal information upon email request.
Name: Jane Smith
SSN: 123 45 6789
DANGER
3 Look carefully at the web address.
http://www.aannan.com
4 Type in the real website address into a web browser.
http://www.amazon.com
5 Don't call company phone numbers in emails or instant messages. Check a reliable source such as a phone book or credit card statement.
Credit Card Statement
For customer service call 1-800-xxx-xxxx
6 Don't open unexpected email attachments or instant message download links.
My Inbox
Here is the updated document.
attachment
How phishers trick you
Here is how con artists try to steal your personal information.
Wombank
From: service@Wombank.com
Dear Jane,
Your account will be suspended if you do not update your information
http://www.Wombank.com/update
I forged the address to look genuine.
I threatened the user with an urgent message.
I added a link that looks like it goes to Wombank - but it really sends people to my site so I can steal their information and money!
Thanks PhishGuru! Where can I learn more?
Visit phishguru.org

Figure 12: Embedded phishing training [29]

3 PRELIMINARY ANALYSIS

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 examination. These tools includes:

- 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 which were valid and online in sequence 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 the phishing URLs separately in Table 8 the appendix section.

Table 7: Phishtank URL analysis

URL ID	**TLD**	**TL-IP**	**No. Domain found**	**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
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	No known domains hosted on this IP	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	No known domains hosted on this IP	No known domains hosted on this IP	Russia	124
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	No known domains hosted on this IP. 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. 3 of them are hacked domain (10%) while 11 domains (35%) have the possibilities of harmful instances. It makes 17 domains (55%) do not have the possibilties of bad neighborhoods. In conclusion, while there are some possibilities of bad neighborhood, there are much more legitimate domains attributed from a phishing domain as well.

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 [40] 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 [40]. Moreover, the tables of the database is already explained by Maurer on his website [40].

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 [36], 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 [36].

- 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 [26, 36].

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 find 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 != ’unde-
fined’){PAYPAL.core.Navigation.init(); }</script>
```

For the sake of simplicity, we put a detailed of differences table of 20 phishing webpage vs original webpage in the Section A.1 Table 9. Based on our manual analysis, we found out that most of the HTML sources are tampered while maintaining the looks of legitimacy. The alteration includes, 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. The details of modification can be seen in Table 9.

4 RESEARCH QUESTION

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

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

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

In our coding 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 [55]. 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 [46]. Based on this conception, phishers may also have applied the same principle and as a dominance principle of all other principles. This leads to our second research question below. Therefore, hypotheses are established accordingly to answer **RQ1** (**H1, H2, H6, H11**).

RQ2: How dominance authoritative principle in the dataset?

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 [49]. 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 link 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 [13]. 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 association 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 [53]. 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 [60]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 link 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 that 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 hyperlink in the email, phishers do not necessarily obfuscates the real URL with something else. Logically, such phishers do not aim to make a high quality of bogus email, rather they aim to take chances in getting potential victims that are very careless. This leads to our hypothesis that say

H8: Phishing emails that include hyperlink 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 hyperlink or attachment in the body of the email and also they may request unsuspecting victim to click the hyperlink or to open the attachment. This leads us to two hypotheses which state

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

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 [5]. 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 H14, it is sensible if a phishing email which contains account related reason such as reset password or security update, may tend to have a hyperlink 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 phishing emails need immediate action greater than other reasons. Therefore, phishers may likely to include a hyperlink 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 hyperlinks

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 have document related reason will likely targeting government sector

---

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

---

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

5.1 RESEARCH METHODOLOGY

As we illustrate in Figure 13, 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 gathered from fraudehelpdesk.nl by my supervisor, Elmer Lastdrager MSc. in the form of phishing emails which were reported between august 2013 and december 2013. 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

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:

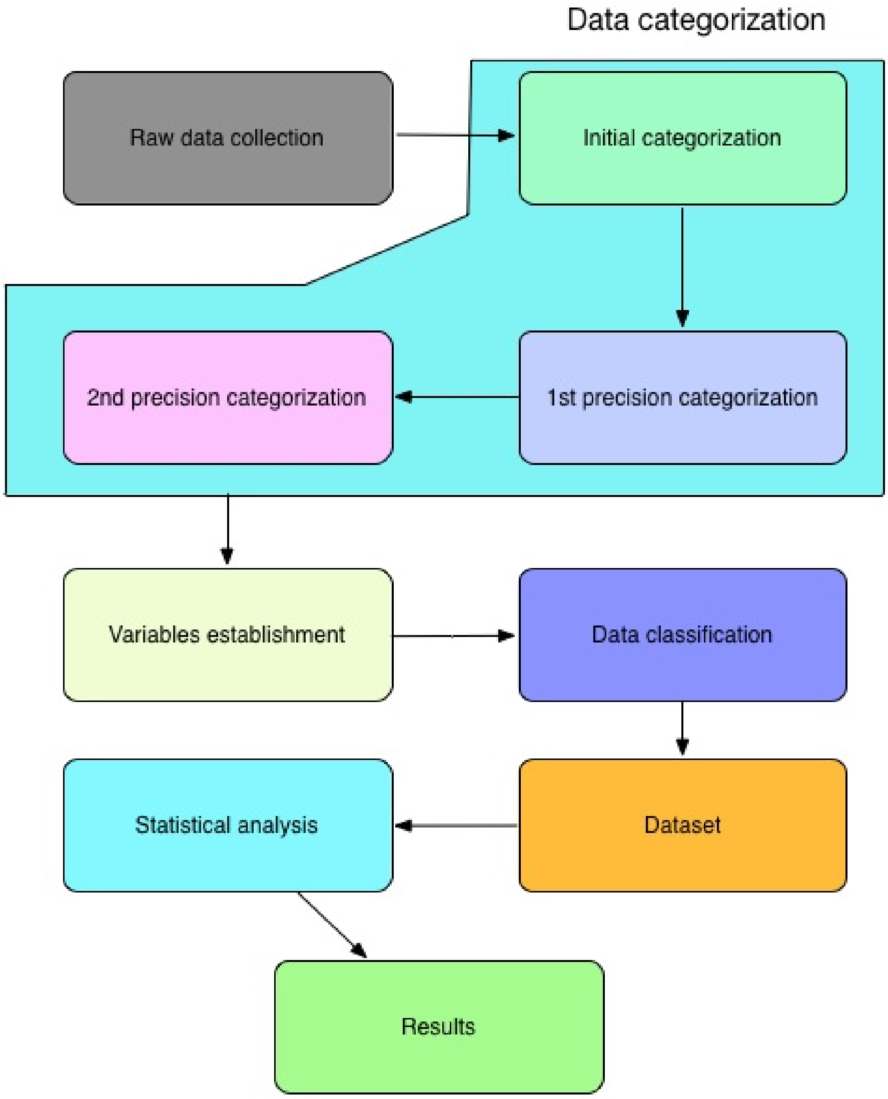


Figure 13: Research methodology diagram

- 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.

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

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 [5].
2. Consistency: Public commitment. Where people become psychologically become vested in a decision they have made [60].
3. Social proof: Where people model the behavior of their peer group, role models, important others or because it is generally "fashionable" [60].
4. Likeability: Where 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 [60].
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 [60].
6. Scarcity: based on the principle of reactance, where people respond to perceived shortages by placing greater psychological value on perceived scarce items [60].

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

High level flowchart in Figure 14 is made to illustrate our integration of cialdini's principles with the dataset.

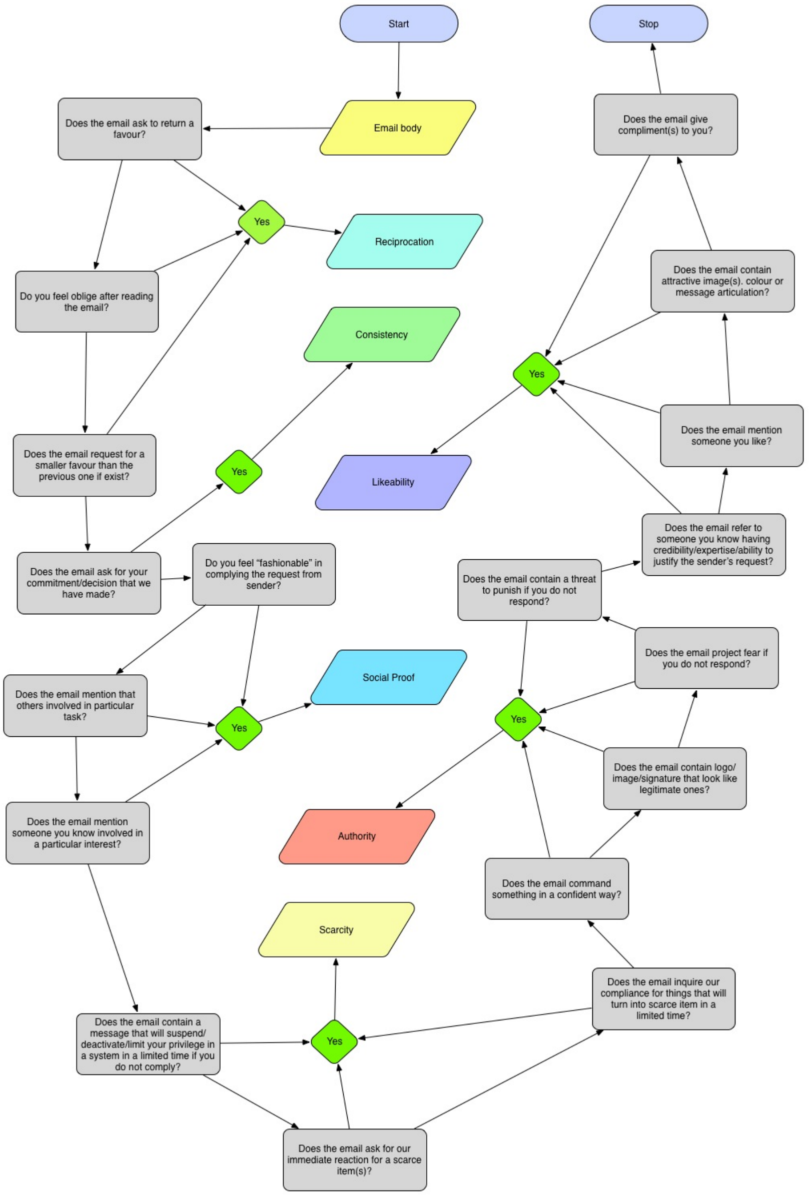

Start
Stop
Email body
Does the email ask to return a favour?
Yes
Reciprocation
Do you feel oblige after reading the email?
Does the email request for a smaller favour than the previous one if exist?
Consistency
Yes
Does the email ask for your commitment/decision that we have made?
Do you feel “fashionable” in complying the request from sender?
Does the email mention that others involved in particular task?
Yes
Social Proof
Does the email mention someone you know involved in a particular interest?
Does the email give compliment(s) to you?
Does the email contain attractive image(s). colour or message articulation?
Yes
Likeability
Does the email mention someone you like?
Does the email refer to someone you know having credibility/expertise/ability to justify the sender’s request?
Does the email contain a threat to punish if you do not respond?
Does the email project fear if you do not respond?
Yes
Authority
Does the email contain logo/ image/signature that look like legitimate ones?
Does the email command something in a confident way?
Scarcity
Does the email inquire our compliance for things that will turn into scarce item in a limited time?
Does the email contain a message that will suspend/ deactivate/limit your privilege in a system in a limited time if you do not comply?
Yes
Does the email ask for our immediate reaction for a scarce item(s)?

Figure 14: Integration flowchart of cialdini’s principles

A

APPENDIX TEST

A.1 APPENDIX PRELIMINARY ANALYSIS

Table 8: 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=54cc48e97ad73aaa2519dbb379719301FpG7mo2DssMkja2121545487KJJ9ecd33e80218623592ca5d52281eb16eHHG5548782
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&amp;amp;amp;amp;amp;amp;amp;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

Table 9: 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>&lt;img src="//paypal.112.2O7.net/b/ss/paypalglobal/1/H.6–NS/0?pageName=NonJavaScript" height="1" width="1" border="0" alt="" /&gt;</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&amp;dispatch=5885d80a13c0db1f998ca054efbdf2c29878a435fe324eec2511727fbf3e9efcd8" 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> </div> • 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&amp;dispatch=5885d80a13c0db1f998ca054efbdf2c29878a435fe324eec2511727fbf3e9efcd8" 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 &gt; 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"><a href="https://yahoo.com">Einloggen</a></li>
	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	

A.2 ANOTHER APPENDIX SECTION TEST

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 16.)

[2] 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 14.)

[3] 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 17.)

[4] 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 16.)

[5] Robert Cialdini. The science of persuasion. *Scientific American Mind*, 2001. ISSN 1555-2284. (Cited on pages 6, 7, 37, and 43.)

[6] 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 pages 3 and 4.)

[7] 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 14.)

[8] Organización Internacional de Normalización. *ISO/IEC 27002: Information Technology, Security Techniques, Code of Practice for Information Security Management*. ISO/IEC, 2005. (Cited on page 23.)

[9] 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 3 and 23.)

[10] Oxford Dictionaries. Phishing. URL `http://www.oxforddictionaries.com/definition/english/phishing`. (Cited on page 4.)

[11] Collins English Dictionary. Phishing. URL http://www.collinsdictionary.com/dictionary/american/phishing. (Cited on page 4.)

[12] 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 23.)

[13] 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 35.)

[14] 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 17 and 20.)

[15] Aaron Emigh. Online identity theft: Phishing technology, chokepoints and countermeasures. *ITTC Report on Online Identity Theft Technology and Countermeasures*, 3, 2005. (Cited on pages ix, 9, and 23.)

[16] 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 3.)

[17] Edwin Donald Frauenstein and Rossouw von Solms. *An Enterprise Anti-phishing Framework*, pages 196–203. Springer, 2013. (Cited on pages ix, 6, 7, 23, and 24.)

[18] Gaurav Gupta and Josef Pieprzyk. Socio-technological phishing prevention. *Information Security Technical Report*, 16(2):67–73, 2011. ISSN 1363-4127. (Cited on page 17.)

[19] 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 page 5.)

[20] Jason Hong. The state of phishing attacks. *Communications of the ACM*, 55(1):74–81, 2012. ISSN 0001-0782. (Cited on page 5.)

[21] 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 17.)

[22] Markus Jakobsson. Modeling and preventing phishing attacks. In *Financial Cryptography*, volume 5. Citeseer. (Cited on page 3.)

[23] 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 ix, 2, 3, 4, 5, 11, and 12.)

[24] Lance James. *Phishing exposed*. Syngress, 2005. ISBN 0080489532. (Cited on pages 2, 3, 4, and 23.)

[25] K Jansson and R Von Solms. Phishing for phishing awareness. *Behaviour & Information Technology*, 32(6):584–593, 2013. ISSN 0144-929X. (Cited on page 23.)

[26] 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 31.)

[27] 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 23.)

[28] 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 23.)

[29] 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 ix, 23, 24, and 25.)

[30] Willy Lai. Fitting power law distributions to data. (Cited on page 17.)

[31] Elmer Lastdrager. Achieving a consensual definition of phishing based on a systematic review of the literature. 2014. (Cited on page 4.)

[32] 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 ix and 19.)

[33] Avivah Litan. Phishing victims likely will suffer identity theft fraud. *Gartner Research Note (May 14, 2004)*, 2004. (Cited on page 5.)

[34] 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 16.)

[35] Haotian Liu, Xiang Pan, and Zhengyang Qu. Learning based malicious web sites detection using suspicious urls. . (Cited on pages ix, 20, 21, 22, and 23.)

[36] 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 31.)

[37] 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 ix and 21.)

[38] 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 ix, 19, and 21.)

[39] Steve Mansfield-Devine. Interview: Joe ferrara–fighting phishing. *Computer Fraud & Security*, 2013(7):17–20, 2013. (Cited on page 23.)

[40] 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 30.)

[41] Tom McCall. Gartner survey shows phishing attacks escalated in 2007; more than $3 billion lost to these attacks. *Stephane GALLAND*, 2007. (Cited on page 5.)

[42] Tyler Moore and Richard Clayton. An empirical analysis of the current state of phishing attack and defence. In *WEIS*. Citeseer. (Cited on page 12.)

[43] Tyler Moore and Richard Clayton. *Evaluating the wisdom of crowds in assessing phishing websites*, pages 16–30. Springer, 2008. ISBN 3540852298. (Cited on pages ix, 16, 17, and 18.)

[44] Giovane César Moura. *Internet bad neighborhoods*. Giovane Cesar Moreira Moura, 2013. ISBN 9036534607. (Cited on pages 13 and 14.)

[45] 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 page 9.)

[46] National Plant Diagnostic Network. Types of social engineering. URL http://www.npdn.org/social_engineering_types. [Online; accessed 16-July-2014]. (Cited on page 34.)

[47] 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 pages ix, 14, and 15.)

[48] Bryan Parno, Cynthia Kuo, and Adrian Perrig. *Phoolproof phishing prevention*. Springer, 2006. ISBN 3540462554. (Cited on pages 3 and 4.)

[49] 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 34.)

[50] Phishing.org. History of phishing. URL http://www.phishing.org/history-of-phishing/. (Cited on pages 2 and 3.)

[51] 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 14.)

[52] 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 23.)

[53] Henri Tajfel and John C Turner. The social identity theory of intergroup behavior. 2004. (Cited on page 35.)

[54] Gregg Tally, Roshan Thomas, and Tom Van Vleck. Anti-phishing: Best practices for institutions and consumers. *McAfee Research, Mar*, 2004. (Cited on pages 3, 4, 8, and 9.)

[55] 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 34.)

[56] Merriam Webster. Phishing. URL http://www.merriam-webster.com/dictionary/phishing. (Cited on page 4.)

[57] 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 17.)

[58] Rebecca Wetzel. Tackling phishing. *Business Communications Review*, 35(2):46–49, 2005. (Cited on pages ix, 7, and 8.)

[59] 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 16.)

[60] 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 35 and 43.)

[61] 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 ix, 20, 21, 22, and 23.)

[62] 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 16.)

[63] 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 page 22.)

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/

DECLARATION

Put your declaration here.

Enschede, August 2014

Nurul Akbar