Chapter 9

An Exploration of the Design Features of Phishing Attacks

Jingguo Wang
Information Systems and Operations Management, College of Business, The University of Texas at Arlington, Arlington, TX 76019, USA

Rui Chen
Department of Information Systems and Operations Management, Miller College of Business, Ball State University, Muncie, IN 47306, USA

Tejaswini Herath
Finance, Operations and Information Systems, Faculty of Business, Brock University, St. Catharines, Ontario L2S 3A1, Canada

H. Raghav Rao
Management Science and Systems, School of Management, State University of New York at Buffalo, Buffalo, NY 14260-4000, USA

Abstract

Phishing is a growing phenomenon, which has not only caused billions in losses, but also has eroded consumer confidence in online transactions. To develop effective countermeasures, we need to understand how phishing e-mails exploit human vulnerabilities. We develop a framework to explore phishing from the perspective of victims. The framework helps understand different features that are utilized by phishers in designing e-mails and websites. We further explore the design patterns of phishing attacks. We collect 195 phishing records from the antiphishing work group website. Using content analysis and two-step cluster analysis, we examine those attacks for the presence of design features identified through our framework. We find that phishing attacks in different time periods present different characteristics, and the quality of phishing attacks have advanced consistently over time. Finally, on the basis of the location of the phishing hosts, we group the
Phishing attacks into four groups: USA, Asia, Europe, and South America. We find interesting patterns among the phishing attacks worldwide and pinpoint the major similarities and differences.

1 Introduction

Phishing is a new form of deception appearing over the Internet in recent years. In a typical phishing scheme, a phisher sends a forged e-mail to a recipient, falsely mimicking a legitimate establishment in an attempt to scam the recipient into divulging personal information such as personal name, bank account and passwords, credit card numbers, social security numbers, and other sensitive information. In most of the cases, the e-mail will request the user to visit a web site to fill in the information. Different from many other types of deception widely carried out through use of rich media such as face-to-face conversations or telephone communication, phishing e-mail lacks the availability of dynamics of face-to-face interaction. Phishers only rely on e-mail/website to deceive the targeted consumers. Garfinkel and Cranor (2005) provided an excellent description of phishing examples.

Phishing has caused billions of dollars in losses. Although estimates of losses due to phishing vary, Gartner estimated that phishing attacked 57 million Americans in 2003 and based on responses from 5000 online adults reported that phishing e-mails successfully deceived more than half of the recipients (Litan, 2004). Phishing also erodes the consumer's trust in online communication and transactions. The erosion drives the consumer from an online business (such as an online bank) to more expensive and labor-intensive channels, such as telephone call centers or "bricks and mortar" branch offices. Fighting phishing is an urgent task for the health of e-commerce (Garrity et al., 2004).

Phishing is a form of cognitive hacking. It manipulates a user's perception and relies on the user's changed actions to carry out attacks (Cybenko et al., 2002). In this study, we look at various features presented in phishing attacks to understand how phishing exploits human vulnerabilities through so called "interface illusions," in which a criminal attacks people via user interfaces (Levy, 2004). Guided by the elaboration likelihood model (ELM) (Petty and Cacioppo, 1986) and research in e-commerce, we first develop a framework and identify a set of features which are used by phishers to exploit consumers' vulnerabilities. We then explore the design patterns of the phishing e-mails collected from the antiphishing work group (APWG) (http://www.antiphishing.org) using content analysis and cluster analysis. Finally, we group the phishing attacks based on their hosting location into four groups: USA, Asia, Europe, and South America. On the basis of the analysis, we identify the major similarities and differences.
The contribution of this study is threefold. First, we examine the users' information processing and decision-making process during phishing attacks through theory informed approaches (e.g., activity theory and ELM). Second, we identify a set of phishing design features employed for deception purpose, which provide the research community with an opportunity for further development of attack taxonomy and antiphishing instruments. Third, we design and carry out content analyses to study the evolution of phishing attacks. Using the phishing design framework, we provide a comprehensive and vivid illustration of the phishing phenomena along with greater details on development trends and patterns than the prior phishing research offers. Last, we find interesting patterns among the phishing attacks worldwide and we pinpoint the major similarities and differences among phishing website hosted in USA, Asia, Europe, and South America. Although recently, new vectors such as spyware/adware or other malware are also used in phishing attacks, we focus on phishing that uses e-mail/webmail as the attack vector.

This chapter is organized as follows. In Section 2, we introduce the relevant theoretical foundations and explore the phishing design features. We introduce our research methodology for the exploration of the design pattern of phishing attacks in Section 3 and discuss evolvement of phishing in Section 4. In Section 5, on the basis of the traced-back IP address of hosting website, we group the hosts into four: Asia, USA, Europe, and South America. We compare the differences in their design patterns using statistical analysis. Finally, we conclude the chapter with the discussion of avenues for future research in Section 6.

2 Design features in phishing attacks.

In a classical phishing attack, a phisher first sets up a spoofed website and then sends an e-mail bait to a group of targeted consumers. Recipients read bait, and might click the spoofed link presented in the e-mail following the instructions of the bait. The link leads to the spoofed website mimicking a legitimate establishment that might be of the recipients' interest. Some recipients enter personal information and fall victim. Activity theory provides a general framework for us to understand the phishing process (Fig. 1). Activity theory describes human activity in terms of elements such as an actor who is using a tool to manipulate an object such as users via executing a plan (Nardi, 1996). The actor goes through a process to achieve

![Fig. 1. The activity theory framework.](image-url)
a certain outcome. In our case, the actor is the phisher. The tool is e-mail and website (user-interface). The objective of a phisher is to manipulate and scam recipients into divulging personal information, such as personal identity, financial accounts, etc. The process is sending out the e-mails to a target population and luring the recipients release their personal information. The potential outcome of a phisher is to obtain the recipient's information and gain the financial benefits. E-mail recipients are active agents in the process of making choices on clicking the spoofed link and further entering their personal information. The phisher may do all that is possible to lure recipients to release their information. In this study, we make an effort to understand how recipients might be influenced by forged e-mails and websites via different design features based on previous studies in psychology and e-commerce.

2.1 An elaboration likelihood model (ELM) perspective

Dual-process theories expounded in prior psychology research have examined the role of influence in shaping human perception and behavior. The theories postulate two sets of processes underlying human reasoning: a process that is associative, automatic, unconscious, parallel, and fast based on heuristic cues, and a process that is rule-based, controlled, conscious, serial, and slow based on effortful processing of judgment-relevant information (Schneider and Shiffrin, 1977; Shiffrin and Schneider, 1977). Dual-process theories also specify conditions under which each of the two alternative processes are likely to be invoked. We take the perspective of the ELM (Petty and Cacioppo, 1986), one of the often used dual-process theories, to understand how phishing might explore human vulnerabilities. We consider that the underlying influence process in phishing (via cues in phishing e-mail/website) and the recipients information process can be directly related to ELM (Bhattacherjee and Sanford, 2006; Petty and Cacioppo, 1986).

The flow of phishing attack initiates at the moment a conned e-mail reaches the target population. As the recipient examines the persuasive arguments and the heuristic cues conveyed, he or she may be influenced or persuaded to give out valuable information and fall victim to the attack. ELM posits two basic routes for persuasion: the central route and the peripheral route. The routes differ in the amount of thoughtful information processing or "elaboration" needed. The central route involves message elaboration. In this route, a recipient carefully thinks about issue-related arguments contained in the phishing e-mail and inspects all available information. In the phishing context, such arguments may refer to the description of a dramatic event/scenario, response actions requested in the e-mail and its justification, potential benefits of following the instruction in the e-mail and the potential cost of not acting as requested. The peripheral route processes the message without any active thinking about the
attributes of the issue, and requires less cognitive efforts. The recipients rely on a variety of cues to make quick decisions, such as the appearance of e-mail/web page, rather than the content in the message. In summary, the central and peripheral routes differ in at least two aspects: first, different types of information processed (message-related arguments via heuristic cues); second, the cognitive effort involved in information processing (higher in the central route than in the peripheral route). The central and peripheral routes of attitude change are typically operationalized in ELM using the argument quality and peripheral cue constructs, respectively. Note that ELM does not imply that people persuaded via the central or peripheral routes will experience different outcomes.

The recipients may vary widely in their motivation and ability to elaborate the e-mail, which in turn moderate how a given influence impacts the attitude formation (Petty and Cacioppo, 1986). ELM captures the ability and motivation to elaborate in terms of levels of elaboration likelihood. The recipients that experience high elaboration likelihood are more likely to be persuaded via the central route, and the recipients that experience low elaboration likelihood are more likely to be persuaded via the peripheral route. If recipients view an e-mail as being important and relevant, they are more likely to elaborate the content, and inspect the content. If the recipient thinks the message is not such important or relevant, he may just rely on cue-based heuristics for framing his/her perceptions. By examining the peripheral cues (e.g., e-mail and website appearance), the recipient forms his attitudes and may still be persuaded without carefully examining the quality of the argument. Although a phisher may not be able to anticipate the ability of an individual recipient, he may manipulate the relevance of a phishing message applying more contextual information (Jakobsson, 2005). Although recipients’ motivation and ability are critical to their attitude formation, in this research we will only consider the features that are purposely presented in phishing attacks to scam the recipient into divulging private information. Message relevance and recipients’ ability are beyond the scope of study.

ELM posits that the central route and peripheral route together account for all the changes in persuasive communication (Petty and Cacioppo, 1986). When it is applied in the phishing context, however, we find that the ELM may be insufficient to capture the dynamics of recipient’s propensity unless it recognizes the media embedded in the phishing scenario. Consumers consider Internet involves more uncertainty and risk compared with the traditional communication channels. Consumers’ risk perception serves as additional sources of influence; and they may even offset the favorable propensity changes from argument quality or information credibility. An individual who is persuaded by the phishing e-mails may not necessarily submit his or her sensitive information over the Internet, in case he or she perceives high levels of risk. Consequently, we argue that, in addition to the influences from central/peripheral route, perceived risk may have an impact on the recipient’s propensity.
Table 1
Key design features of phishing attacks

<table>
<thead>
<tr>
<th>Dimensions</th>
<th>Number of features</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail argument quality</td>
<td>7</td>
<td>Event, impact, urgency, courtesy, justification, response action requested, penalty</td>
</tr>
<tr>
<td>E-mail title</td>
<td>3</td>
<td>Impact, urgency, company name</td>
</tr>
<tr>
<td>Message appearance</td>
<td>8</td>
<td>Authentic looking e-mail sender, e-mail signatory, personalization, media type, typo, third party icon for trustworthiness, copyright, company logo</td>
</tr>
<tr>
<td>Website appearance</td>
<td>5</td>
<td>Consistent links, consistent appearance theme, third party icon for trustworthiness, copyright, company logo</td>
</tr>
<tr>
<td>Assurance mechanisms</td>
<td>7</td>
<td>Third party icon for assurance, antifraud/privacy statement, SSL padlock, general security lock, help link/feedback mechanisms, authentication mechanisms, https link</td>
</tr>
</tbody>
</table>

2.2 The key features in phishing attacks

In this section, we employ ELM along with research in e-commerce to identify the key features that play roles in the phishing attacks. We further examine interdependencies among the involved entities as well as their interactive dynamics. By synthesizing and extending the related work into a coherent body, we identify key design features as summarized in Table 1. In this study, we will explore the design features of phishing attacks. We will examine the effects of those features empirically in our future study.

2.2.1 Message argument quality: central route of persuasion

ELM literature suggests that the message argument quality affects the attitude change of the message recipient. The argument quality refers to the persuasive strength of arguments embedded in an informational message (Bhattacherjee and Sanford, 2006). Arguments presented with these features are stronger in the persuasion effectiveness and are the primary drivers of message acceptance. Information quality also impacts the customer’s willingness to pay (or fall for the scam) (Chung et al., 2006).

We use a grounded approach to generate the measurement from data since there are no existing measurements for argument quality in phishing e-mails. We employ a computer-aided text analysis tool called CATPAC™ to investigate the underlying components (patterns) of e-mail content. CATPAC is a self-organizing artificial neural network computer program, which is optimized for analyzing text. It is able to identify the most important words in a text and determine their patterns of similarity
As CATPAC does not require pre-coding or linguistic assumptions, it has been widely used in the text analysis research (Gay and Hembrooke, 2002; Kim et al., 2005a). On the basis of the CATPAC analysis results, we identified seven argument components: event, impact, justification, response action requested, penalty, urgency, and courtesy. Figure 2 demonstrates the interactions among the components and the roles they play to convey a strong influence on persuasion. These seven components are consistent with the prior research findings discussed and they systematically contribute to the quality of the argument as a coherent group. Any argument with missing features, justification for example, may be perceived as flaw of logic and fail to convey strong persuasion consequently.

2.2.2 Message and website appearance: peripheral route of persuasion

Perceived credibility of the message plays a major role in the peripheral route to impact persuasion (Petty and Cacioppo, 1986). At its simplest, credibility can be defined as “believability” (Wathen and Burkell, 2002). The appearance and the background credentials of the e-mail/website have a persuasive impact regardless of how the message itself argues. In this section, we examine the e-mail heuristic cues that may contribute to the perceived credibility of information presented in phishing attacks.

Among others, the source (sender) credentials have long been recognized for their impact on perceived credibility (Schneider and Shiffrin, 1977; Shiffrin and Schneider, 1977). It is suggested that reputation and legitimacy are two pivotal credentials for effective communication. The words from a reputable authority may be perceived as of higher credibility than to those from an unknown identity. For communication media such as e-mails, the features such as designation of the signatory, company logo, and copyright may be manipulated to enhance the credentials of the messenger senders and to improve the perceived credibility of the e-mail consequently. The third party icon for trustworthiness (such as “FDIC Member”, “Trust.e”)
also presents a high level of business integrity and reputation of the seal receivers. The icons, therefore, serve as effective artifacts to convey the credibility of the sender as well as that of the information (Hu et al., 2003).

Credibility of message also considers the message formation and layout, suggesting that the e-mail is well-written, well-produced, and well-organized. In contrast with well-presented e-mail, poorly presented e-mails such as one with typos (including grammar errors) may detract from the credibility of the source. Furthermore, IS literature finds that rich-media content improves data quality and perceived credibility (Kim et al., 2005b). The e-mails presented in rich html format with pictures and animations, therefore, may lead to a greater level of perceived credibility than those written in plain text.

Recent studies have identified personalization as an influential component in communication (Tam and Ho, 2005). When the personalization (tailoring) matches the preference of the recipient, he or she may perceive higher credibility of the information. In the context of e-mail communication, we therefore argue that the personalization (e.g., using the recipient’s name) may enhance the information credibility perceived.

On the basis of the earlier discussion, eight features are proposed to measure the information credibility (or lack of it) presented in the phishing e-mails. They include authentic looking sender e-mail address, e-mail signatory, personalization, e-mail media type, lack of typos, third party icon for trustworthiness, copyright, and company logo.

After evaluating the phishing e-mail in terms of its content and peripheral cues, the recipient may follow the links given in the e-mail and visit the phishing website. Through the manipulation of website designs, the phishers may enhance the credibility and deceive the victims through such cues as third party icon for trustworthiness, copyright, and company logo consistent with the e-mail body (Kim et al., 2005a; Wathen and Burkell, 2002). As the website visitors have already viewed and read the e-mail, it is important for both media (i.e., e-mail and website) to remain consistent. A recipient would expect to witness the same visible URL and appearance themes between the e-mail and website. Appearance themes may include page layout, color scheme, and font types. A lack of consistency during information process may greatly reduce the perceived information credibility. We summarize these features for Website as consistent links, consistent appearance themes, third party icon for trustworthiness, copyright, and company logo.

2.2.3 E-mail title: motivation

ELM suggests that the effects of argument quality and information credibility are moderated by the recipient’s motivation. The psychology literature defines motivation as “an internal state or condition, sometimes described as a need, desire, or want, that serves to activate or energize behavior and give it direction” (Kleinginna and Kleinginna, 1981). For a communication channel such as e-mail, subject line (e-mail title) is identified as a motivating factor for e-mail comprehension (Mackenzie, 2000). With
regard to the motivation effect, however, a detailed measurement for e-mail title is missing in prior literature. Following a grounded approach, for e-mail argument quality, we identified three measurements for the title based on the CATPAC analysis that include (1) urgency which portrays the emergency of the situations, (2) impact which depicts the threats and potential losses of one's personal interest, and (3) company name which may be stated in the e-mail titles to draw reader attention.

By describing an emergency situation, the urgency attracts user attentions. By conveying the sense of threat and loss, the impact may successfully raise the cognitive needs for motivation and also introduce a high level of relevance. Meanwhile, the company name of reputable business entities may arouse favorable affective needs for motivation and encourage the recipient to process the e-mail with more effort. The proposed measurements, therefore, are consistent with and supported by the motivation research findings.

2.2.4 Assurance mechanisms: decision making under risk

IS research suggests that online users are skeptical about Internet as a secure channel and they worry about the potential risks from attacks, losing private information, and losing monetary information (Lee and Rao, 2007). This perceived risk may discourage individuals to submit sensitive information (such as credit card number and SSN) over the Internet. In the context of phishing attacks, such perceived risks are even more salient since the recipients are requested to give out their information and to submit online. Counter-risk approaches, therefore, may be exploited by the phishers to reduce the perceived risks by the potential victims. In line with the e-commerce findings, we expect that the perceived risk may have a negative impact on the recipient's propensity to release requested information.

Studies have proposed information assurance mechanisms, which may address the risk concerns. Extending these into the phishing phenomenon, we summarize seven assurance mechanisms, which may reduce the perceived risks involved in the attacks. The mechanisms include: third party icon for assurance (security and privacy), antifraud/privacy statement, SSL padlock, general security lock, help link/feedback mechanism, authentication mechanism, and Https links. These components represent the typical information assurance mechanisms that have been widely exercised in e-commerce nowadays. The presence of these features, therefore, may help the recipients lower the perceived risks involved in giving out sensitive information during phishing attacks.

Typical information that is requested in the attacks may be described as (1) personal information such as date of birth, (2) nonfinancial information which refers to online service accounts rather than real banking accounts, (3) financial information which refers to credit card, debit card, and banking accounts, (4) social security numbers, and (5) other information which could not be otherwise categorized. Besides those, we are also
interested in studying the targeted industry. As industries of different types may vary in their information assurance practices and in the types of information involved with customers, we wish to examine whether such differences hold in phishing attacks. We identify four industry types in this study: (1) financial service (banking and credit card), (2) retail and auction, (3) ISP, and (4) miscellaneous.

3 Methodology

In this section, we discuss our methods for data collection. We employ content analysis. The data collected will be used in the statistical analysis presented in Sections 4 and 5.

3.1 Sample

We collected the samples of phishing records from the phishing archive maintained by the APWG. APWG is the leading organization in fighting e-mail frauds and phishing. It provides comprehensive information on phishing statistics, attack documentations, and business solutions. When we carried out the study, 210 phishing e-mail records spanning from September 2003 to July 2005 were kept in its archives. Each record contains the related phishing e-mail, phishing website, and a brief summary. The phishing archive provides a representative sample set within which the general phishing themes and patterns are reserved. The bias of the sample set, though inevitable, is recognized as a limitation of this study.

3.2 Content analysis

To extract the desired information from multiple data formats such as text and images, we employed both human- and computer-based coding in content analysis. A codebook and corresponding code sheet were developed for human-based coding. The computer software VBPro (http://www.textanalysis.info/VBPRO.pdf) was used with custom dictionaries for computer-based coding. The first two dimensions presented in Table 1 (e-mail argument quality and e-mail title) were computer coded, whereas the next three dimensions (message appearance, website appearance, assurance mechanisms) and information requested were human coded.

Two graduate students who were unaware of the research questions were hired to perform human-based coding. This practice allows blind coding and thus reduces the biasing effect of coder knowledge of variables extraneous to the content analysis (Neuendorf, 2002). We captured the coding protocol into a codebook and corresponding code spreadsheet. The codebook defined the features and gave coding instructions. The coding
options for each item were designed to be mutually exclusive for validity and reliability concerns.

We developed the coding protocol through multiround revisions in accordance with the coder training process. The coders were first instructed to fully understand the coding protocols. Next step involved a consensus building among the coders. The feedback from the coders was obtained to update the codebook and the code sheet accordingly. Next, a pilot coding was carried out and the Cohen’s $\kappa$ (Krippendorff, 1980) indicating the intercoder reliability was above 0.76 for each individual coding item. The coding codebook was revised for the inconsistencies. The Cohen’s $\kappa$ in final coding was above 0.81 for each coding item. As Kappa is an overly conservative test for reliability, the results of over 0.81 is considered as an excellent agreement, given the fact that many of the items, with only two options, have chance agreements at 0.5 (Benerjee et al., 1999).

For computer-based coding, we employed VBPro, a powerful content analysis program, to process the dataset with word as the unit of analysis. A set of custom dictionaries were developed to precisely measure the features of interest. Owing to the lack of research in phishing, we were not able to find related dictionaries and had to build them. We constructed dictionaries based on the findings from CATPAC analysis. These dictionaries were then screened by a panel of seven experts from academia, FBI, and industry. The dictionaries were modified and finalized with keywords that are closely related to the features under investigation. A sample of custom dictionary keywords is illustrated in Table 2. The computer-coding analysis is based on a single keyword and raises possibility of false errors since the analysis ignores the contexts where the keywords are

<table>
<thead>
<tr>
<th>Table 2</th>
<th>Example of custom dictionaries</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dimensions</strong></td>
<td><strong>Features</strong></td>
</tr>
<tr>
<td>E-mail title</td>
<td>Urgency</td>
</tr>
<tr>
<td></td>
<td>Impact</td>
</tr>
<tr>
<td></td>
<td>Company name</td>
</tr>
<tr>
<td>E-mail argument quality</td>
<td>Event</td>
</tr>
<tr>
<td></td>
<td>Impact</td>
</tr>
<tr>
<td></td>
<td>Justification</td>
</tr>
<tr>
<td></td>
<td>Response action</td>
</tr>
<tr>
<td></td>
<td>Penalty</td>
</tr>
<tr>
<td></td>
<td>Urgency</td>
</tr>
<tr>
<td></td>
<td>Courtesy</td>
</tr>
</tbody>
</table>
presented. It is a limitation that is common to computer-based content analysis studies.

Fifteen phishing records were eliminated from the study as they are not properly achieved and had more than 5 features (out of 35) that cannot be exactly coded. The missing data in the rest of the records were replaced with the most frequently occurring values in the corresponding features. We, therefore, had 195 valid phishing records for final analysis. 127 of these were targeted at the financial services sector, 43 targeted the retail and auction industry, whereas 23 targeted ISPs.

4 Evolution analysis of phishing attacks

In this section, we analyze the evolution of phishing attacks in terms of its design patterns and changes. This study is enabled by two-step cluster analysis (Bapna et al., 2006; Okazaki, 2006), which discovers three clusters in the entire sample size with each cluster representing phishing attacks in a different era.

4.1 Cluster analysis

The two-step cluster analysis starts with a precluster phrase where sequential clustering approaches are employed to build a modified cluster feature (CF) tree (Zhang et al., 1996). The goal of preclustering is to reduce the size of the matrix that contains distances between all possible pairs of sample cases. During the construction of CF tree, each case may be emerged to the existing preclusters or may create a new precluster, using a likelihood distance measure as the similarity criterion. Upon the completion of the precluster phrase, standard hierarchical clustering algorithm such as agglomerative (Johnson, 1967) is performed on the preclusters to group them into desired number of clusters. In our study, we use SPSS v13 and employ the clustering criteria of Schwarz’s Bayesian inference criterion (BIC) (Schwarz, 1978), a well-known and default criteria, to calculate the cluster number automatically by finding the largest increase in distance between the two closest clusters in each hierarchical clustering stage. In addition, we standardized the continuous variables and treated the outliers with noise handling in the clustering process.

As in Table 3, three clusters are identified through two-step cluster analysis. Interestingly, the compositions of each cluster, in terms of the occurrence year and industry, are quite different from one another. In the whole sample, 10% occurred in 2003, 68% in 2004, and 22% in 2005. If the clusters are uniformly drawn from the whole sample, a distribution of the occurrence year in each cluster would be expected to be similar. However, the results demonstrated that the three clusters are represented in
Table 3
Composition of three clusters

<table>
<thead>
<tr>
<th>Cluster</th>
<th>Number of e-mails</th>
<th>Year composition</th>
<th>Industry composition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>2003</td>
<td>2004</td>
</tr>
<tr>
<td>The whole sample</td>
<td>195</td>
<td>10</td>
<td>68</td>
</tr>
<tr>
<td>1 (maps to early-stage)</td>
<td>40 (20%)</td>
<td>35</td>
<td>55</td>
</tr>
<tr>
<td>2 (maps to mid-stage)</td>
<td>81 (42%)</td>
<td>4</td>
<td>77</td>
</tr>
<tr>
<td>3 (maps to late-stage)</td>
<td>74 (38%)</td>
<td>4</td>
<td>65</td>
</tr>
</tbody>
</table>

Note: Grayed cells represent individual cluster compositions that are greater than those in the whole sample composition. For example, composition of 2005 is 31% in Cluster 3, which is greater than that (22%) in the whole sample.

different years. In cluster 1, 35% occurred in 2003, together with 55% in year 2004, accounting for 90% of the cluster. In cluster 2, there is a dominant percent for year 2004 (77%), which is far above 68% in the whole sample. In cluster 3, 31% occurred in 2005, which is greater than 22% as in the whole sample. And years 2004 and 2005, accounts for 96% of that cluster.

Because of the way the clusters congregate in terms of year composition and time spanning of the clusters, we use the following names for the three clusters hereafter: “early-stage” for cluster 1 which primarily consists of phishing attacks occurred in 2003 and 2004, “mid-stage” for cluster 2 which primarily consists of attacks in 2004, and “late-stage” for cluster 3 which primarily consists of attacks in the 2004 and 2005. The sample clusters, therefore, in general reveal the evolution of the phishing attack.

We observed that the distributions of the target industry across the three clusters are quite different. The early-stage (cluster 1) has a strong interest in the financial service industry, the middle-stage (cluster 2) shifts the interest toward retail and auction and ISP, and the late-stage (cluster 3) returns to the financial service as their major target. This trend suggests the financial service as the most threatened industry. The shift of target industry between financial service and retail and auction and ISP may also indicate that phishers are altering their targets to avoid an increased public awareness and to raise their perceived benefits, resulted by the excessive attacks in the selected industries. We discuss other results in detail in the following subsections. An overview of the findings is presented in Table 4.

Using the design framework developed earlier, we investigated the design patterns and changes in the three clusters. An illustration of the findings is
Table 4
Summary of discussion

<table>
<thead>
<tr>
<th>Cluster</th>
<th>Major occurrence year</th>
<th>Attack quality</th>
<th>Target industry</th>
<th>Information focus</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>E-mail/ website feature presence</td>
<td>Assurance mechanism</td>
<td>E-mail content E-mail title</td>
</tr>
<tr>
<td>Early-stage</td>
<td>2003, 2004</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Mid-stage</td>
<td>2004</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Late-stage</td>
<td>2004, 2005</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

presented in Fig. 3. We discuss the detailed findings in the rest of this section.

4.2 Information requested

Spoofing people to give out information is the ultimate goal of the phishing attacks. The information requested in the attacks may vary over time. In this section, we explore the three clusters to examine the trend of the requested information and to learn the patterns embedded.

Figure 3(a) compares the three clusters through the five types of information requested. For example, in personal information, among the whole sample of 195 phishing records, 41% of the attacks requested this specific type of information. When the individual clusters are concerned, however, 8% attacks in the early-stage, 68% attacks in the middle-stage, and 30% attacks in the late-stage requested this information, respectively.

As we can see from Fig. 3(a), overall the early-stage cluster requests much less information except for the nonfinancial account. The middle-stage cluster has high proportions for each type of requested information. The late-stage cluster is much more focused and it concentrates on the nonfinancial account information and financial information. This is also in line with the target industries for late-stage cluster attacks.

4.3 E-mail and website appearance

The e-mail message appearance features are examined across the three clusters and the results are illustrated in Fig. 3(b). Among the eight features, seven are categorical values, whereas the eighth typo is continuous.
Consider the feature, *authentic looking sender e-mail* as an example. 86% of the attacks presented this feature in their phishing e-mails in the whole sample, 93% in early-stage cluster, 79% in mid-stage cluster, and 92% in late stage. The number of typo is a reverse measurement of the message appearance. In the whole sample, the average number of typos reaches 0.88, which means that there is almost one typo in every phishing e-mail. It is worthy to mention that typos may exist, which are rendered invisible,
through appropriate HTML design techniques, to the e-mail recipients. They are injected into the e-mails so as to elude spam or phishing filters. They are discarded in this research due to the zero-impact on information processing of the recipients. Nevertheless, further research on typos may be
important for the development of effective phishing filters. Fig. 3(b) shows that the early-stage cluster has the lowest percent of desirable features presented in e-mail appearance, and highest of the number of typos. The mid-stage cluster presents a great improvement over the early-stage cluster.
However, the late stage is even better crafted. It outranks the mid-stage in seven out of eight features. The late-stage also has better features than the whole sample. The sharp difference in the use of message features suggests that the attacks realized the importance of e-mail and website appearance, and improved those features consistently. The presence of website features demonstrates the similar patterns (Fig. 3(c)).

4.4 Assurance mechanism features

The three phishing clusters differ greatly in the features of assurance mechanisms (Fig. 3(d)). Generally speaking, the early-stage cluster has the lowest percentage of e-mails/website featured with the assurance mechanisms. It, however, has a highest level presence of the authentication mechanisms than that of the whole sample. This may be because that the cluster requests the relative high level of nonfinancial account information. Each authentication procedure presents an opportunity for the phishers to harvest the user accounts. The mid-stage cluster demonstrates an improvement over the early-stage cluster in other features than authentication. It has two of eight features above the presence percentage of the sample, whereas the late-stage cluster has six features. It demonstrates that phishers consistently have an intension to take advantage of assurance mechanisms over the time.

4.5 E-mail content

Unlike the previous analysis, the e-mail content analysis reveals the frequency of the words used in the e-mail composition. With the information on the average word usage among the entire sample, we found that the phishing e-mails highly value the importance of impact, for which about 6.60 words are used to describe the impact. The phishing attacks also values the roles of courtesy, justification, and response action. Surprisingly, we found that the penalty is not well utilized in the phishing e-mails. This may suggest that the phishers are expecting that the individuals are willing to cooperate with requests from the “legitimate looking” companies. The analysis results are illustrated in Fig. 3(e). The three clusters have similar patterns. The early-stage cluster used the least amount of the words except for the justification. The mid-stage cluster presents a higher level of manipulation on the keywords. It has three out of seven features that have a frequency above that of the sample average, whereas the late-stage cluster is most effective and have all seven features with a frequency above that of the sample average.
4.6 E-mail title

Owing to the fact that the e-mail title is short in length with only two to five words in most cases, the analysis of the e-mail title does not reveal too much new findings on the cluster patterns. We found similar patterns across the three clusters (Fig. 3(f)). The early-stage cluster has a lowest level of all title features and the levels are all below the sample average. Both the mid- and late-stage have two features above the sample average. However, the late-stage is better than the mid-stage in two out of three features. Within the whole sample, the usage frequencies of the three features are all below one, which may suggest further improvement to the custom dictionary and new features to be identified.

5 Host-based analysis of global attack difference

Recent literature suggests that cyber crimes committed from different regions across the world would differ due to differences in regulative, normative, and cognitive legitimacy as well as hacking skills relative to the availability of economic opportunities (Kshetri, 2006). Other differences such as language skills, technology skills, and cultural influences may also play a role in a way how a criminal activity is carried out. In general, drawing from insights of cultural studies, "cultural criminology" stream of research has considered various influences of culture on image, representation, and style of crime (Ferrell, 1999).

We examine whether the attacks worldwide are homogeneous in attack design. To do this, we categorized the attack records into geographic groups based on their corresponding hosts (i.e., web server) of phishing websites. We are aware of the fact that several phishers mount their attacks from hijacked legitimate websites, but we have not considered that aspect in our analysis. Although this is a limitation, we also believe that the exercise conducted in this chapter has useful implications with regard to the forensic process. We believe the findings in this chapter will help forensic analysts to comprehend regional development patterns in phishing attacks and to recognize their similarities and differences.

Prior research suggests that USA and Asia are among the top regions where phishing attacks are initiated (Wolfer, 2005). Studies have also found that Europe and South America are becoming more and more active in the online phishing and other cyber crimes recently (Weiss, 2006). Accordingly, we consider the attack origins as USA, Asia, Europe, and South America, attempting to explore their attack design similarities and differences. The categorization process was facilitated through the analyses (www.ip2location.com) of IP addresses of the phishing website that were used in the attacks. Despite the typical criticisms that website hosts may include offshore providers and zombie networks, the above categorization process
is followed by antiphishing research leaders, such as APWG, as the best known approach so far. After leaving out 32 records with unknown sources (such as missing data or hijacks), we categorized USA (67 cases), Asia (60 cases), Europe (20 cases), and South America (16 cases).

Among the design features, 24 out of 35 are recorded in our data set using nominal value. These design features are message appearance (other than "typo"), website appearance, assurance information, and information requested. The rest of the design features, mainly e-mail argument and e-mail title, are recorded using ratio values. For design features of nominal values, we conducted $\chi^2$ tests using SPSS v13. $\chi^2$ test is able to detect whether the attack regions and attack designs are dependent on each other, that is, whether the attack design patterns are homogenous across the four attacks regions. Once we found that the attack regions significantly differ on a particular design feature, we conducted additional $Z$ tests. It is noticed that each design feature may be implemented using a variety of options. For example, phishers may choose from different options, for example, "no visible https link," "visible https link with false looking address," and "visible https link with true looking address" in designing Https Link feature (Chandrasekaran et al., 2006; Drake et al., 2004; Fette et al., 2007). The $Z$ test allows us to examine the four attack regions on each one of the design options for a given design feature under question. As in Fig. 4, the $Z$ test compares two groups (the attack regions in this study) with their proportions of utilizing one specific design option. To facilitate our discussion, we compare Asia, Europe, and South America with USA as it has been well known as the world leader in high technology development and its related crimes. By comparing with USA (one tail $Z$ test), we are interested to explore whether the phishers worldwide have grown as mature as those in USA.

Meanwhile, we employed analysis of variance (ANOVA) and multivariate analysis of variance (MANOVA) to examine the phishing designs whose data is recorded by ratio values. ANOVA is used to analyze the design feature of e-mail typo, whereas MANOVA is exercised on e-mail argument quality and e-mail title dimensions. MANOVA provides several advantages over ANOVA test such as it protects against type I error of multiple ANOVA. For phishing designs on which the four attack regions significantly differ, we conducted additional post hoc analysis (Scheffe and

$$z_1 = \frac{\hat{p}_1 - \hat{p}_2}{\sqrt{\frac{\hat{p}_1(1-\hat{p}_1)}{n_1} + \frac{\hat{p}_2(1-\hat{p}_2)}{n_2}}}$$

where $\hat{p}_1$, $\hat{p}_2$ are the proportions of group 1 and 2 respectively while $n_1$ and $n_2$ are the two corresponding group size.

Fig. 4. $Z$ test for homogeneity of group proportions.
Tukey), which compares all pairs of the attack regions to explore their similarities and differences for given design features.

5.1 E-mail message appearance

The e-mail message appearance dimension consists of design feature such as authentic looking e-mail sender, e-mail signatory, personalization, media type, typo, third party icon for trustworthiness, copyright, and company logo. For these design features (except typo), the $\chi^2$ test found that the four attack regions marginally differ in their use of copyright feature (Table 5).

To find any patterns that were embedded, we conducted a follow-up Z tests. As illustrated in Table 6, 89.55% of all Phishing attacks originated in USA are designed with copyright information appearing in the phishing e-mails, whereas only 10.45% of them do not. The Z test indicated that, compared with USA, Asia, Europe, and South America attacks represent significantly lower proportions of e-mails designed with copyright information. That is, 78.33% of Asian phishing e-mails, 70% of European e-mails, and 68.75% of South American e-mails are designed with copyright information shown up. As copyright information is likely to enhance the recipient's perception of e-mail authenticity, the results suggest that phishers in USA are more sophisticated in crafting e-mails.

Table 5
\(\chi^2\) test for e-mail copyright

<table>
<thead>
<tr>
<th></th>
<th>Value</th>
<th>df</th>
<th>p-value (two-sided)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pearson (\chi^2)</td>
<td>6.589</td>
<td>3</td>
<td>.086*</td>
</tr>
<tr>
<td>Likelihood ratio</td>
<td>6.703</td>
<td>3</td>
<td>.082</td>
</tr>
<tr>
<td>Linear-by-linear association</td>
<td>6.059</td>
<td>1</td>
<td>.014</td>
</tr>
<tr>
<td>Number of valid cases</td>
<td>163</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Significant at 0.1 level.

Table 6
Homogeneity of group proportion test for copyright

<table>
<thead>
<tr>
<th>Design option/region</th>
<th>USA (%)</th>
<th>Asia (%)</th>
<th>Europe (%)</th>
<th>South America (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Without copyright information</td>
<td>10.45</td>
<td>21.67**</td>
<td>30**</td>
<td>31.25**</td>
</tr>
<tr>
<td>With copyright information</td>
<td>89.55</td>
<td>78.33**</td>
<td>70**</td>
<td>68.75**</td>
</tr>
</tbody>
</table>

**Significant at 0.05 level.
regions of the world. Intellectual property literature suggests that USA is a world leading nation in protecting intellectual property rights and USA has established a rich volume of related regulations including Copyright Act and US Digital Millennium Copyright Act (Analytics, 2005). USA also dominates the world economy with respect to trade in copyright-based goods and it plays a dominant role in developing worldwide intellectual property regulations such as WTO Trade-Related Aspects of Intellectual Property Rights (TRIPs) agreement (Canada, 2003). The use of copyright has therefore become an accepted social norm in the society of USA; phishers are therefore more likely to add copyright signs when they are crafting phishing designs.

For e-mail typo (ratio value), the ANOVA test reveals that the four attack regions differ significantly on the number of typos appeared in the phishing e-mails (Table 7). Post hoc analysis found that there is no significant difference between USA and the other three attack regions. The differences mainly stems from the fact that Asia (0.47 typo per e-mail) has a significantly lower number of typos than Europe (1.95 typo per e-mail). Studies have shown that Asia has a much larger population practicing English than European countries (Wikipedia, 2007). As most of the European countries (e.g., Russia and Romania) in our data sample do not have English as their first language, the observed discrepancy in typo numbers is consistent with the known differences in English levels.

5.2 Website appearance

The website appearance dimension includes design features of consistent links, consistent appearance theme, third party icon for trustworthiness, copyright, and company logo. The $\chi^2$ analysis found that the four regions follow similar design patterns.

5.3 Assurance mechanisms

Assurance mechanisms consist of following design features: third party icon for assurance, antifraud/privacy statement, SSL padlock, general

<table>
<thead>
<tr>
<th>Table 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANOVA test for e-mail typo</td>
</tr>
<tr>
<td>Sum of squares</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>Between groups</td>
</tr>
<tr>
<td>Within groups</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

**Approximately significant at 0.05 level.
security lock, help link/feedback mechanisms, authentication mechanisms, and https link. The $\chi^2$ analysis found that the four attack regions follow similar design patterns.

5.4 Information requested

The information requested dimension consists of personal information, nonfinancial account information, financial information, social security number (SSN), and other information such as mother's maiden name. The $\chi^2$ test found that the four attack regions marginally differ in their requests of SSN (Table 8).

The follow-up Z test reveals the following analysis results. As in Table 9, 28.36% of phishing e-mails from USA requested SSN information. Compared with USA, Asia and Europe have marginally higher proportions of e-mails requesting SSN. On the contrary, South America phishers have a marginally lower proportion in this regard. These findings suggest that both Asian and European phishers may be more aggressive than those in USA, in part because they reside in countries where phishing-related regulations are less mature. The findings also suggest that South American attackers are likely to be less aggressive in their pursuit of extremely sensitive information such as SSN; they are more focused on other types of information (e.g., credit card number) that can be quickly and easily cashed in.

Table 8
$\chi^2$ test for SSN

<table>
<thead>
<tr>
<th></th>
<th>Value</th>
<th>df</th>
<th>p-value (two-sided)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pearson $\chi^2$</td>
<td>6.917</td>
<td>3</td>
<td>.075*</td>
</tr>
<tr>
<td>Likelihood ratio</td>
<td>7.425</td>
<td>3</td>
<td>.060</td>
</tr>
<tr>
<td>Linear-by-linear association</td>
<td>.026</td>
<td>1</td>
<td>.871</td>
</tr>
<tr>
<td>Number of valid cases</td>
<td>163</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Significant at 0.1 level.

Table 9
Homogeneity of group proportion test for SSN

<table>
<thead>
<tr>
<th>Design option/region</th>
<th>USA (%)</th>
<th>Asia (%)</th>
<th>Europe (%)</th>
<th>South America (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSN not requested</td>
<td>71.64</td>
<td>58.33*</td>
<td>55*</td>
<td>87.50*</td>
</tr>
<tr>
<td>SSN requested</td>
<td>28.36</td>
<td>41.67*</td>
<td>45*</td>
<td>12.50*</td>
</tr>
</tbody>
</table>

*Significant at 0.1 level.
5.5 E-mail argument

E-mail argument quality consists of design features such as event, impact, urgency, courtesy, justification, response action requested, and penalty. The MANOVA test found that the four attack regions share similar design patterns except their use of penalty in the phishing e-mails (Table 10).

The follow-up post hoc test revealed that there is no significant difference between USA and the rest (Asia, Europe, and South America) in terms of their e-mail penalty design. Rather, Asia (1.52 penalty keywords per e-mail) significantly differ from South America (0.5 penalty keywords per e-mail) when e-mail penalty is concerned. The fact that Asian culture has a high use and tolerance of punishment may account for the preceding difference (Kwok and Tam, 2005). This belief is consequently reflected in the phishing attacks.

5.6 E-mail title

The e-mail title dimension consists of design features such as company name, urgency, and impact. The MANOVA test found that the four attack regions significantly differ in their design of impact feature (Table 11).

The follow-up post hoc tests revealed that there is significant difference between USA (0.82 impact keywords per e-mail title) and South America (0.38 impact keywords per e-mail title) in their utilization level of impact keywords in e-mail title design. This difference is consistent with the fact that openness is a typical personality in USA. The phishers may therefore tend to explicit the impact information more frequently than the others.

Table 10
MANOVA test for e-mail argument quality

<table>
<thead>
<tr>
<th>Source</th>
<th>Dependent variable</th>
<th>Type III sum of squares</th>
<th>df</th>
<th>Mean square</th>
<th>F</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
<td>Courtesy</td>
<td>16.259</td>
<td>3</td>
<td>5.420</td>
<td>1.462</td>
<td>.227</td>
</tr>
<tr>
<td></td>
<td>Event</td>
<td>47.987</td>
<td>3</td>
<td>15.996</td>
<td>1.925</td>
<td>.128</td>
</tr>
<tr>
<td></td>
<td>Impact</td>
<td>46.930</td>
<td>3</td>
<td>15.643</td>
<td>.791</td>
<td>.501</td>
</tr>
<tr>
<td></td>
<td>Urgency</td>
<td>5.346</td>
<td>3</td>
<td>1.782</td>
<td>.700</td>
<td>.553</td>
</tr>
<tr>
<td></td>
<td>Justification</td>
<td>100.212</td>
<td>3</td>
<td>33.404</td>
<td>1.536</td>
<td>.207</td>
</tr>
<tr>
<td></td>
<td>Response act</td>
<td>39.721</td>
<td>3</td>
<td>13.240</td>
<td>1.807</td>
<td>.148</td>
</tr>
<tr>
<td></td>
<td>Penalty</td>
<td>16.009</td>
<td>3</td>
<td>5.336</td>
<td>2.393</td>
<td>.070*</td>
</tr>
</tbody>
</table>

*Significant at 0.1 level.
Table 11 MANOVA test for e-mail title

<table>
<thead>
<tr>
<th>Source</th>
<th>Dependent variable</th>
<th>Type III sum of squares</th>
<th>df</th>
<th>Mean square</th>
<th>F</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
<td>Company name</td>
<td>.349</td>
<td>3</td>
<td>.116</td>
<td>.358</td>
<td>.783</td>
</tr>
<tr>
<td>Urgency</td>
<td></td>
<td>.652</td>
<td>3</td>
<td>.217</td>
<td>.542</td>
<td>.654</td>
</tr>
<tr>
<td>Impact</td>
<td></td>
<td>3.286</td>
<td>3</td>
<td>1.095</td>
<td>2.856</td>
<td>.039**</td>
</tr>
</tbody>
</table>

**Significant at 0.05 level.

6 Conclusion

In this chapter, we understand phishing based on ELM and studies in e-commerce. Key features in phishing attacks are identified. We found that the quality of the crafted e-mails and websites (user-interfaces) are improving over the time. The current research is explorative in nature and lays the foundation for the future research effort to leverage the findings in this chapter. Several future research streams are suggested as follows.

We found that there was at least one typo in every phishing e-mail in our sample and there were significant differences in number of typos per e-mail among the four regions evaluated in this study. Our intuition tells us that perhaps the typos may be due to the language differences existing in countries from which the phishing attacks are carried out. Also, the corporate e-mails will most probably be cautious about typo and grammatical errors in their communication. It would be interesting to analyze if there are differences in normal e-mails and phishing e-mails in future.

The evolutionary nature of phishing attacks has also resulted in enrichment of the phishing attack design framework. For example, new phishing e-mails have incorporated emerging attack designs such as "Re:" in the title of some SPAM e-mail, which increases message relevance and helps elude e-mail filters.

An investigation into the human factors with their impacts on the individual's tendency toward acceptance of the phishing persuasion calls for an experiment-based study. A theoretical development of how various factors of the phishing e-mail and websites influence persuasion process can be developed based on the framework introduced in this chapter. Factors such as motivation, ability/skills (it is likely that e-mail recipients have become wiser over time), and risk perceptions are likely to affect elaboration and persuasion. ELM posits the moderating role on the effects of central and peripheral routes of persuasion on the attitude formation. In a similar vein, recipient awareness regarding phishing e-mail as well as recipient's risk perception can be evaluated. These related inquiries can be investigated in laboratory experiments. In addition to the role of motivation
considered by ELM, role of awareness and risk perception can be evaluated in the extended framework.

It is also worthy of mention that, although conventional wisdoms such as "cultural criminology" may still be existent, the results of this chapter show that differences, even if they exist are no longer significant across the globe and hence will prove less helpful for forensic analysis. The attacks worldwide are evolving toward a high level of homogeneity in most parts. Although the findings may be biased to certain extent, it certainly highlights the pending challenges to the forensic research in the new era of Internet.

7 Suggested questions

1. Discuss the new trends in phishing attacks with the help of information available on current Internet statistics, cyber threats, and internet crimes.
2. Discuss various approaches recommended to fight phishing attacks such as phishing-fighting software tools available in market as well as techniques promoted by awareness campaigns.

Acknowledgment

The research of H. Raghav Rao was supported in part by NSF under grant 0548917 and 0705292. The usual disclaimer applies.

References


**Online resources**

- Anti-Phishing Working Group—http://www.antiphishing.org/
- Indiana University—http://www.indiana.edu/~phishing/
- Security Focus—http://www.securityfocus.com/infocus/1745

**Suggested readings**