Relationship between Phishing Techniques and User Personality Model of Bangkok Internet Users

Chat Chuchuen* and Pisit Chanvarasuth

ABSTRACT

This paper discusses the relationship between user personality types and several phishing techniques. Since personality type is known to have an impact on trust, in this analysis it is posited to also have an impact on effective phishing attempts. This paper tests the relationships between four phishing approaches (link manipulation, filter evasion, website forgery, and spear phishing) and four personality traits (dominance, influence, steadiness, and conscientiousness). A questionnaire including 15 items from the DISC personality scale and 20 items addressing phishing techniques was distributed to a sample size of 400 in the Bangkok area using convenience sampling. The study found that users had varying levels of understanding of phishing techniques, with link manipulation being the least understood and spear phishing being the most understood in every personality group. The study also found that each personality type was susceptible to techniques at a different level. This study supported the idea that user personality types influence vulnerability to different phishing techniques.

Keywords: web fraudulent, user vulnerability, internet scam, DISC model, trust

บทคัดย่อ

การศึกษานี้กล่าวถึงความสัมพันธ์ระหว่างลักษณะบุคลิกภาพของผู้ใช้งานและเทคนิคการหลอกลวงทางอินเทอร์เน็ตที่ส่งผลกระทบกับกลุ่มผู้ใช้งานในแต่ละกลุ่ม ในการวิเคราะห์นี้ได้แสดงถึงสิ่งที่เกิดขึ้นและผลกระทบต่อความพยายามใช้เทคนิคหลอกลวงทางอินเทอร์เน็ต งานวิจัยนี้ได้ทำการทดสอบความสัมพันธ์ระหว่างเทคนิคการหลอกลวงทางอินเทอร์เน็ต 4 ประเภทได้แก่ การหลอกลวงโดยใช้ลิ้งค์ การหลอกลวงโดยสร้างเว็บไซต์ปลอม การหลอกลวงโดยใช้รูปภาพร่วม และการหลอกลวงแบบที่มีกลุ่มเป้าหมายชัดเจน กับ ลักษณะบุคลิกภาพของผู้ใช้งาน 4 ประเภทตามตัวแบบ DISC คือ กลุ่มกล้าได้กล้าเสีย กลุ่มชอบเข้าสังคม กลุ่มที่มีความอดทนสูง และกลุ่มที่หัวโบราณ สำหรับแบบสอบถามที่ใช้ในครั้งนี้ประกอบไปด้วยคำถามเกี่ยวกับลักษณะบุคลิกภาพของผู้ใช้งานจำนวน 15 คำถามและคำถามเกี่ยวกับเทคนิคการหลอกลวงทางอินเทอร์เน็ตจำนวน 20 คำถาม โดยทำการสำรวจกับกลุ่มผู้ใช้อินเทอร์เน็ตในเขตกรุงเทพมหานครโดยวิธีการเลือกแบบตามสะดวกจำนวน 400 ราย ผลการศึกษาพบว่าความเข้าใจในเทคนิคการหลอกลวงทางอินเทอร์เน็ตของผู้ใช้งานอินเทอร์เน็ตมีค่อนข้างหลากหลาย โดยจากการศึกษาชี้ให้เห็นว่าการหลอกลวงโดยใช้ลิ้งค์เป็นรูปแบบที่ผู้ใช้งานอินเทอร์เน็ตมีความเข้าใจน้อยที่สุด

School of Management Technology, Sirindhorn International Institute of Technology, Thammasat University, Pathum Thani 12000, Thailand.

* Corresponding author, e-mail: chat318@hotmail.com

ส่วนการหลอกลวงแบบที่มีกลุ่มเป้าหมายชัดเจนเป็นรูปแบบที่ผู้ใช้งานในทุกๆกลุ่มมีความเข้าใจมากที่สุด การศึกษาในครั้งนี้ยังพบว่าลักษณะบุคลิกภาพของผู้ใช้งานแต่ละประเภทจะถูกล่อลวงโดยเทคนิคการหลอกลวงทางอินเทอร์เน็ตในระดับที่ต่างกัน สุดท้ายนี้จากการวิจัยนี้ได้สนับสนุนแนวคิดที่ว่าลักษณะบุคลิกภาพของผู้ใช้งานมีความอ่อนไหวต่อเทคนิคการหลอกลวงทางอินเทอร์เน็ตนั่นเอง

คำสำคัญ: การหลอกลวงทางเว็บไซต์ ความอ่อนไหวของผู้ใช้งาน การหลอกลวงทางอินเทอร์เน็ต โมเดล DISC ความไว้วางใจ

INTRODUCTION

Local and global communication has become possible through the use of the Internet. Spatial barriers have been remedied or eliminated by using this mode of communication. The convenience and spatial indifference of the Internet has allowed for unprecedented levels of global communication and interaction. However, this high level of interaction has also resulted in an increasing risk of interpersonal interactions that are dangerous or fraudulent. Types of fraud like advance fee fraud have become increasingly prevalent. Perhaps more dangerous, however, is the increasing assumption on the part of users that emails are a trusted means of communication. The usual examples of threats in security on the Internet such as hacking, virus attacks, malware, spyware, and other techniques are well known. However, one of the lesser known crimes of security on Internet transactions is " phishing". Phishing is defined as the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication (Danuvasin, 2011; Downs, Holbrook, & Cranor, 2006; McCombie & Pieprzyk, 2010; McFredries, 2004; Olivo, Santin, & Oliveira, 2011; Shahriar & Zulkernine, 2012). The effects of phishing in cyberspace have continuously grown. It can affect the operation of business firms, especially in the financial and e-commerce businesses (APWG, 2011). What is unique about phishing compared to other methods of gaining private information is that it relies on existing institutional trust in banks or firms that the individual has already done business with in order to gain access to private information. Rather than examining the visual signs in the browser (such as security indicators or even the URL), many users base their trust in the spoofed site on the visual appearance and expected behavior of the site (Dhamija, Tygar, & Hearst , 2006). Some forms of phishing, such as 'social' phishing, take this effect even further, deliberately encouraging personal contact in order to gain access to even more information (Jagatic, Johnson, Jakobsson, & Menczer, 2007). Phishing attacks cost billions of dollars in losses to many organizations and worldwide end users (Geer, 2005). The worldwide report of the Anti-Phishing Work Group (APWG, 2014) showed the number of phishing sites detected jumped almost 30 percent from 38,110 in June 2013 to 49,480 in July 2013, and stayed at the higher rate through the third quarter. The total number of phishing incidences observed in the third quarter 2013 was 143,353 which was a 20 percent increase over the second quarter of 2013. The most targeted websites were for payments and financial services. In Thailand, phishing situations have become a major concern because the financial loss from the damage can be very large. There has been especially strong concern by the industries that utilize computers and the Internet, such as the financial sector and e-commerce business (ThaiCert, 2007). The number of phishing cases in Thailand more than doubled from 2012 to 2013 (ThaiCert, 2014). However, phishing does not work on everyone, suggesting there are personal characteristics also in play. Personality traits are one known factor in predicting the formation of trust (Dohmen, Falk, Huffman, & Sunde, 2008), which can make users more susceptible to phishing attempts.

This study investigated the relationship between phishing techniques and user personalities. The objectives of this study were: 1) to understand the current situation of phishing and types of phishing techniques; and 2) to investigate whether there are significantly different impacts of phishing techniques among different user's personalities. The contribution of this study is to develop guidelines of a policy to protect people, by knowing differences in personality types, from the vulnerability of phishing to gain their trust.

LITERATURE REVIEW

Phishing

The term "phishing" first emerged in 1996, but the technique was described in 1987 (Jagatic et al., 2007). The term alludes to bait which is used in order to "catch" sensitive information, such as financial data and passwords. McFredries (2004) defines the term *phishing* as a way of presenting a misleading web page to deceive people into submitting their personal information, such as passwords and financial information. The practice of phishing is fairly new compared to other forms of fraud. One of the first reported instances was an attempt to collect Internet users' passwords in the USA in the mid-1990s. Stallings (1995) reported that worms were another tool used in phishing at the time, since email was not yet ubiquitous. For example, some Internet users were deceived into believing that their software, such as Microsoft Windows®, had nearly expired. They were then offered software that will "update" their existing software. This resulted in some users giving their credit card numbers to sources or entities without care or regard to the legitimacy of the recipient. In this way, worms attempted to dupe users into handing over credit card information while posing as either a Microsoft Windows® expiration notice or a PayPal application (Levy, 2004).

Based on this information, phishing can be defined as a fraudulent process used to gain access to sensitive information through an electronic communication that appears credible to the user. It may appear to originate from email, auction sites, social networking sites, commercial businesses, or banks (Downs, Holbrook, & Cranor, 2006; McCombie & Pieprzyk, 2010; McFredries, 2004; Olivo, Santin, & Oliveira, 2011; Shahriar & Zulkernine, 2012; Turban, Leidner, McLean, & Wetherbe, 2008). The most common channels are likely to be email or instant messages, though phone calls may also be used (Jagatic et al., 2007). For example, users may receive an email that appears to be from their bank, asking them to update their personal information via a link provided in the email. This link takes them to a site that looks like (but is not) their bank. The phishing attempt can be highly sophisticated, with many users finding it difficult to actually identify whether or not there is something wrong with the site they are directed to, and in some extreme cases can even use hijacked parts of a real website in order to lend the attempt credibility. The typical target of the phishing attempt is personal and financial information, including account numbers, passwords, credit card numbers, or other sensitive information. However, other identity information, like the address and social security number, may also be sought for the purposes of more comprehensive identity theft attempts (Lininger & Vines, 2005). The economic cost of phishing is high, with attacks alone estimated to cost $687 million in the first half of 2012 (RSA, 2012).

Previous research has shown that many individuals may be highly susceptible to phishing. For example, a large number of the studies conducted showed that individuals did not notice or pay attention to critical details that suggested that the email they received or the sites they visited may not be legitimate, such as security toolbars or lock icons (Dhamija et al., 2006; Friedman, Hurley, Howe, Felten, & Nissenbaum, 2002; Wu, Miller, & Garfinkel, 2006; Whalen & Inkpen, 2005). The use of lock icons appears to be particularly problematic, as users either do not notice these or do not realize

that these icons may be spoofed; the users may never actually click on the icon in order to determine what it indicates, making it a less useful means of identifying a safe site. According to Dhamija, Tygar, & Hearst (2006), many users do not actually have enough knowledge about computer systems or the Internet to actually understand what these symbols mean or what to look for. For example, they may not actually be able to tell how a lock icon is forged, which Whalen & Inkpen (2005) note is a potential risk. In addition to the technical risks involved, there is also the problem of social trust and involvement. For example, one study found that around 80 percent of users were likely to believe an email that came from a friend, despite evidence to the contrary (Jagatic et al., 2007). Some users looked for the wrong cues, such as focusing on either IP addresses or subdomains, both of which can indicate a phishing attempt (Jakobsson & Ratkiewicz, 2006). The findings were not highly optimistic about the potential for users to effectively identify a phishing attempt unless they have previously seen one like it, with up to 80 percent of users becoming victims (Downs, Holbrook, & Cranor, 2006; Jagatic et al., 2007).

Statistics and trends of phishing

A report of phishing taking place during January–December 2011 submitted to the Anti-Phishing Working Group (APWG) shows that the number of occurrences fell steadily between January and July, and then there was a large rise in December. The number increased from 18,388 in August to 32,979 in December. This is a 44.24 percent increase in only 5 months (APWG, 2011). There is strong evidence that phishing is on the rise. A more recent study on the prevalence of phishing by RSA (2012) indicated that there was an average of 32,581 global phishing events reported in the first half of that year. This was an increase of 19 percent over the previous half-year, and 32 percent over the same period in 2011 (RSA, 2012). This report also indicated that the USA, UK, and Canada were the most heavily targeted regions, with most reports being focused on bank brands from these countries (RSA, 2012). Additionally, the volume of phishing attacks (the number of emails sent in a single attack) has been rising, with the volume up 400 percent in Canada. However, companies have also become more adept at suppressing phishing attacks, which has led to a reduction in the potential loss to these attacks by 31 percent (RSA, 2012). Recently, spear phishing (with specific high-value individuals being targeted with personalized attacks) has also increased, as have phishing attacks directed through online games and social media (Hong, 2012). The increasing prevalence of phishing has brought it to the forefront of online security, although there are still issues involved in detecting and fighting it, especially given user involvement.

A large number of people fall victim to phishing techniques for various reasons. First, they may not have enough knowledge to deal with this kind of threat (Leyden, 2006; Miller, 2006). Second, they may not have the sufficient technical sophistication or support to help them know whether their received emails or visited web pages are from a legitimate source (Evers, 2007; Dunn, 2007). Finally, they may be lax in their online security because they often ignore or overlook signs of risk, which warn them about phishing (Gooden, 2007).

Phishing techniques

Summarized from previous studies (e.g. Krebs, 2006, Lininger & Vines, 2005, Mutton, 2006), phishing techniques can be classified in four main types, while each applies diverse approaches to attract Internet users as shown in Table 1.

DISC personality model

DISC is an acronym for Dominance, Influence, Steadiness, and Conscienciousness which are the model's four personality types and is a four aspects behavioral model based on Marston and Moulton (2013) that explored an individual's behavior within an environment or particular event.

Table 1 Phishing techniques

Link manipulation	Filter evasion	Website forgery	Spear phishing
In most attempts of phishing, the criminals will apply some technical deception forms that are designed to create a link in spoofed websites and emails that seem to be owned by the genuine organization (Lininger & Vines, 2005). The common tricks are misspelling of URLs (Uniform Resource Identifier) and the applying of subdomains that phishers use to appear as legitimate.	Phishers in some way may use images in text to replace the more difficult to detect common text (by the anti-phishing filters) as used in phishing e-mails (Mutton, 2006). More fraudsters have applied new approaches to create undetectable phishing sites through general security measures like firewalls and web proxies content filtering. Some textual content can be replaced by similar-looking images on the phishing page, and fraudsters can make this even more difficult to detect by the automated security systems or the presence of such “PayPal” and “credit card” keywords.	An attacker can even make flaws in the trusted website’s scripts (Krebs, 2006). These attacks are called cross-site scripting or XSS and are specifically problematic since the users will be directed to sign on their own webpage of a bank or service, where all the web address and security certificates show in the correct form. The link to the website is actually crafted to carry the attack and make it hard to detect without expert knowledge. This flaw type was applied to attack PayPal in 2006 (Mutton, 2006).	Spear phishing is a newer tactic of phishing that employs phishing emails to the targeted users known to engage with a particular firm, and the individual users (Lininger & Vines, 2005). Spear phishing refers to an increase in response rates through adding legitimate email appearance. Spear phishers will send e-mails that seem genuine to members and employees of particular firms, government agencies, groups, and organizations. Messages look like they were sent from colleagues and employers and may include requests for passwords and usernames. In a spear phishing experiment, 80 percent of 500 West Point cadets that were sent a fake email, were tricked into revealing their personal information (Bank, 2005).

The focuses are on the preferences and styles as observed by such behavior. The DISC personality model was applied in this study to itemize, detail, and distingish the Internet users’ personalities. Below, we will explain the details of the DISC personality model as well as its categories. As noted by Vrba (2008), These personality type characteristics are defined in Table 2.

Relationship between personality and phishing techniques

Each of the four identified phishing techniques relies on a different approach to gain the trust of the user and make them likely to respond. For example, link manipulation relies on users not noticing (or not being equipped to notice) slight differences from the expected link, such as a

Table 2 User personality model (DISC model)

Dominance (the 'D' trait)	Influence (the 'I' trait)	Steadiness (the 'S' trait)	Conscientiousness (the 'C' trait)
The Dominant personality characteristics include those that are directed, decisive, driven, self-starting, forceful, demanding strong-willed, egocentric, ambitious, aggressive, and initiating. The Dominant personality is complicated. Good results are achieved with strong levels of organizational skills, time management, with tough challenges. The Dominant personality can be perceived as sharp, demanding, or interfering by others, but viewed as highly effective as well.	'I' people are prominent in the sense of preferring to handle people, and love to gain attention. Usually, they are charismatic leaders that can take control over a crowd and motivate them to a particular objective. 'I' people prefer to be fun and love parties as those who have high "I" scores manipulate others in their activity and talk, which is emotional. They can be explained with terms such as magnetic, enthusiastic, convincing, persuasive, warm, affectionate, credible, political, and cheerful.	'S' people are stable, steady paced, extremely loyal, secure, and do not prefer change. 'S' people are more passively perceived in comparison to 'D' and 'I' people. Moreover, they may appear reserved, and they tend to listen more than speaking. They are friendly and understanding. 'S' people seem to have a small group of close friends. When it comes to demands, the 'S' trait friend seems to lend the helping hand. People with high 'S' are relaxed, calm, patient, predictable, protective, intentional, unwavering, and consistent, and tend to be poker faced and unemotional.	'C' people usually can be explained as the compliant, controlled, and correct. They will be your compliance, quality control, and analyst people. 'C' people are accurate in details and systematic, and usually neat in appearance. It is simple to spot 'C' people in the workplace. Just walk through and observe clean and neat work desks —they usually belong to 'C' trait people. 'C' people's decisions are usually based on figures and facts. People with high 'C' follow regulations, rules, and structure. They love quality work right from the start. They are cautious, careful, neat, exacting, accurate, diplomatic, and sensitive.

Source: (Marston & Moulton, 2013; Vrba, 2008)

misspelling or subdomain (Lininger & Vines, 2005). Many users may not recognize an error like "payapl.com" or may not realize that "paypalpayments.com" is not legitimate. Similarly, filter evasion relies on users viewing text in HTML format and not noticing that text has been replaced with images (Mutton, 2006). Website forgery relies on users not investigating the site they visit (such as clicking on locks that seem to indicate security), or on technical vulnerabilities in the site itself (Mutton, 2006). Finally, spear phishing relies on a presumed connection to the user that encourages trust, such as by using known sites or even directly using names (Lininger & Vines, 2005). This suggests there will be differences in what types of users are vulnerable to various attacks. There are no existing studies that use the DISC personality model to understand differences in vulnerability to specific phishing attacks. However, other studies have identified factors that can generate such a connection. For

example, one study found that urgency clues (such as time limits or indications that an account is locked) will reduce attention to other clues that the email may not be legitimate (Vishwanath, Herath, Chen, Wang, & Rao, 2011). This can mean that personality types more prone to completing tasks immediately, like those with primarily Dominance traits (Vrba, 2008), can be more susceptible to these types of attacks. However, those with primarily Conscientious traits, who may be more inclined to take their time and examine the entire email, identifying issues and spotting problems with it, may not be susceptible.

The personality types themselves point to some potential differences in vulnerability. For example, Influential types may be more susceptible to spear phishing, particularly highly targeted attempts. This susceptibility stems from their desire to be recognized and to be the center of attention (Vrba, 2008), which can reduce their ability to identify a phishing attempt. Those with a dominant trait of Steadiness, on the other hand, may be less comfortable with personal recognition. Having fewer, closer relationships with individuals, they may be more likely to be able to identify phishing attempts that claim to come from close friends. Those who have a primarily Dominance trait may be susceptible to phishing attempts in general, due to their prompt approach to getting things done. Conscientious types may also be driven to take care of seeming demands from banks or other important financial partners rapidly, but they may be less vulnerable because of more attention to detail.

Research model and hypothesis

We have developed a research model by integrating the DISC personality model (Vrba, 2008) and the four identified phishing techniques. It is hypothesized that the efficacy of the four phishing techniques will vary depending on the dominant personality type shown by the user. This is a general statement because there has been relatively little research into the role of personality type on the efficacy of phishing techniques or vulnerability to them. This means that identifying directionality or the extent of vulnerability for specific personality types is as yet a matter of speculation. Under these conditions, it would be inappropriate to speculate about the direction or strength of the relationship; instead, it is simply argued that there is likely to be one.

Figure 1 shows the research framework that was used in the primary research in this study. From the research framework, the hypothesis of the study is posed as follows. There are significant differences in the vulnerability to phishing techniques depending on the user's DISC personality type. The hypothesis was tested using a quantitative survey as described in the section below, to determine the strength and direction of these relationships.

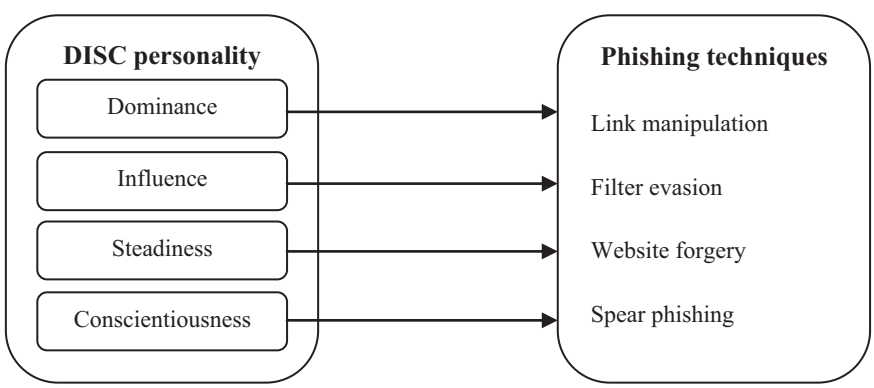

Figure 1 Conceptual Model showing the relationship between DISC personality models and phishing techniques

Research methodology

In this research, a questionnaire was the main tool used to gather data from people about their personality and their phishing knowledge. The set of items on the questionnaire was developed and the data were compiled by: 1) studying the techniques of phishing and DISC personality in order to create a guideline for questionnaire items; and 2) formulating items about phishing techniques using the DISC personality model.

The completed questionnaire consisted of four parts. The first and second parts were used to collect demographic information as well as information about the personality of each individual. The third part contained general questions about phishing. The last part focused more specifically on different phishing techniques. The main items used in the questionnaire were: 1) 15 nominal scale items on DISC personality; and 2) 20 Likert Scale items on phishing techniques which consisted of understanding the phishing techniques.

The level of analysis for this research was the individual. A sample size of 400 was randomly acquired from Bangkok Internet users by the convenience technique. When the questionnaires were returned from respondents, an initial analysis was conducted based on their responses. This step also made connections in the relationship between different groups/types of personalities and the relative correspondence to phishing techniques.

The descriptive analysis in this study included frequency and percentage, mean, and standard deviation, as appropriate based on the data. The inferential statistics in this study consisted of Analysis of Variance (ANOVA) and post-testing using the Least Significant Difference (LSD) technique.

RESULTS AND DISCUSSION

Table 3 shows the demographic and personality information collected from the users. The gender distribution was not significantly different from a uniform distribution ($\chi^2 = 0.490$, $p = .484$), and 43 percent of the users were aged between 18 and 25 years. This is not representative of the Thai population, but it is consistent with a study conducted in a university environment, as this one was. The high rate of degree attainment (73% of the sample with Bachelor degree or higher) is also consistent with a university environment. This is also shown in the occupation, where almost half (49.25%) of participants were either pre-university students or undergraduate or graduate university students.

The second area of descriptive statistics is the dominant DISC personality type. These types were calculated using the DISC personality inventory (the first 20 items in the questionnaire). This showed that the most frequent dominant personality type was Influence (33.5%), followed by Steadiness (26.5%). Dominance (21.5%) and Conscientiousness (18.5%) were less common. A chi-square test ($\chi^2 = 20.640$, $p = .0001$) showed that this is statistically different from a uniform distribution, indicating that some personality types are more common than others in the sample.

The second part of the analytical results was the inferential statistics. There were two dimensions in the questions in this research. The first dimension represented the relationship between the DISC personality model and an Internet user's understanding of phishing techniques. The other dimension represented the relationship between the DISC personality model and an Internet user's vulnerability to phishing techniques. Table 4 shows the level of understanding of phishing techniques based on personality types using the mean and standard deviation. This shows that there are differences in the mean understanding of various techniques based on personality type. Spear phishing had the highest level of understanding compared to other phishing techniques, following by filter evasion, website forgery, and link manipulation. When considering the relationship between respondent personalities and level of

understanding phishing techniques, it was found that for every group in the DISC, the lowest level of understanding was for link manipulation. In other words, link manipulation had the highest level of vulnerability with respect to phishing techniques. However, spear phishing had the highest level of understanding for phishing, for each personality. The level of understanding of phishing for every technique was moderate to quite low with any personality group

Table 3 Demographic and personality information

(n = 400)

	n	%
Gender		
Male	207	51.75
Female	193	48.25
Age		
Lower than 18	53	13.25
Between 18 and 25	172	43.00
Over 25	175	43.75
Education level		
Under Bachelor's degree	108	27.00
Bachelor's degree	224	56.00
Over Bachelor's degree	68	17.00
Occupation		
Student (below College level)	62	15.50
Undergraduate, graduate	135	33.75
Employed	144	36.00
Housewife, unemployed, retired	11	2.75
Business owner	43	10.75
Other	5	1.25
DISC Personality		
Dominance	86	21.50
Influence	134	33.50
Steadiness	106	26.50
Conscientiousness	74	18.50

Table 4 Analysis between DISC personality and understanding in phishing techniques

Understanding in phishing techniques	DISC characteristic			
	Dominance	Influence	Steadiness	Conscientiousness
	$\bar{x}$	$\bar{x}$	$\bar{x}$	$\bar{x}$
1. Link manipulation	2.14	2.16	2.06	2.07
2. Website forgery	2.30	2.28	2.10	2.09
3. Spear phishing	2.66	2.64	2.50	2.65
4. Filter evasion	2.35	2.51	2.28	2.38

To determine whether the differences in understanding of techniques were relevant, an ANOVA test was used to compare the outcomes. A significance level of $p < .05$ was chosen for significance testing. LSD testing was used as a post-testing approach to determine differences between groups.

In terms of the relationship between the DISC personality model and vulnerability to phishing techniques on specific dimensions of phishing techniques, the results from Table 5 and 6 indicate that the Influence (I) personality group was the most "at risk" group in terms of phishing. However, only spear phishing and filter evasion were statistically significant based on the one-way ANOVA test, with link manipulation being at the edge of the significance range. The analysis showed that the Influence (I) personality group is at risk from fraud by the two techniques more than the Dominance personality group (D) and Conscientiousness personality group (C). With regard to spear phishing, the Steadiness personality group (S) was more vulnerable than the Dominance personality group (D). This result is shown in Table 5.

In summary, the Influence personality group was more at risk from spear phishing and filter evasion than the Dominance and Conscientiousness groups, while the Steadiness personality group was also more vulnerable than the Dominance group (though not significantly different from the Conscientiousness group). Link manipulation and

Table 5 Results from ANOVA

Phishing technique		Sum of squares	df	Mean Square	F	*p*
1. Link manipulation	Between Group	0.9884	3	1.663		
	Within Group	251.2000	396	0.634	2.621	.050
	Total	256.1880	399			
2. Website forgery	Between Group	3.662	3	1.221		
	Within Group	266.259	396	0.672	1.816	.144
	Total	269.922	399			
3. Spear phishing	Between Group	9.253	3	3.084		
	Within Group	186.202	396	0.470	6.560	.000*
	Total	195.456	399			
4. Filter evasion	Between Group	7.887	3	2.629		
	Within Group	265.278	396	0.670	3.924	.009*
	Total	273.164	399			

* $p < .05$

Table 6 Comparative results between the DISC personality and phishing techniques

Phishing technique	DISC Characteristic			
	Dominance	Influence	Steadiness	Conscientiousness
	$\overline{x}$	$\overline{x}$	$\overline{x}$	$\overline{x}$
1. Link manipulation	2.36	2.63	2.44	2.38
2. Website forgery	1.91	2.14	1.97	1.96
3. Spear phishing	2.18	2.54	2.45	2.22
4. Filter evasion	1.86	2.19	2.08	1.88

website forgery did not show significant differences. However, the fact that these techniques are rarely used in isolation means that it is possible that any phishing email may trick any personality type.

As noted above, there is relatively little information available in the literature about the relationship between personality types and phishing techniques. However, there is some interesting literature on the relationship between decision-making techniques that could reflect on this area. For example, differences in decision information and urgency can influence how vulnerable users are (Vishwanath et al., 2011). It is particularly noticeable that urgency indicators can reduce the attention paid to the other indicators (Vishwanath et al., 2011). This could help explain the lack of difference between the groups for link manipulation and website forgery. Simply, inclusion of urgency indicators can increase the vulnerabilities of all groups to phishing techniques. Since link manipulation and website forgery techniques are the foundation of all phishing efforts (Lininger & Vines, 2005), this is particularly important. It suggests that there is a shared vulnerability to the most frequent techniques.

The finding that the Influence group was more vulnerable to spear phishing than the other groups is not surprising, given the characteristics of the Influence group. Specifically, the Influence group prefers personal attention and being the center of attention (Vrba, 2008). This makes them strong leaders, but it also makes them vulnerable to flattery and other techniques that spear phishing may involve. Although social phishing was not considered as one of the dominant techniques (since it remains in the minority), the personal focus of this technique (Jagatic et al., 2007) may also make Influence group members more vulnerable to it as well.

The Dominance group was found to be one of the less vulnerable groups, which was not necessarily expected, given their take-charge personalities (Vrba, 2008). However, the Dominance group is also highly detailed-oriented (though not as much as the Conscientiousness group), which can make them more likely to identify problems with the email and identify issues like filter evasion techniques that use images instead of texts. The Conscientiousness group is also more likely to recognize these issues.

CONCLUSION

This research studied the relationship between phishing techniques and the user personality model (DISC model). Each user personality was studied based on the DISC model to investigate risk types of phishing techniques, to investigate the riskiest types of phishing techniques, and to investigate what type of user personality appears to be the most regularly cheated (Bonnstetter, CPCM, & CPCA 2006; Scarbecz, 2007; Sugerman, 2009). The findings can be summarized as follows.

Having considered the evidence, the Internet users who are identified with Influence and Steadiness personalities are likely to become victims of the aforementioned phishing techniques. In addition, when we focus on phishing techniques, link manipulation is the most serious problem for all personality groups. Upon being exposed to the topics and being shown how to analyze a message for phishing characteristics, Internet users are able to correctly identify most of the threats.

More work remains to be done. Given the increasing availability of tools to fight phishing, it is expected that future attacks will continue to become more and more refined in user and event specificity. The validity in the context of predicting an individual's susceptibility to various forms of phishing attacks is still unclear and will require further research. This paper attempted to provide structure to help users be aware of phishing attacks and to identify reasons why susceptibilities need to be identified before effective measures can be implemented to mitigate those vulnerabilities.

The results of this study are limited to the data provided by the questionnaires. Thus to determine whether the information on the questionnaire has any broader relevance will take some time to fully study the effects on the results. In addition, the sample data were collected from a population in a limited area only. For future study, a broader approach to data collection should be used and possibly in different dimensions to provide more beneficial results for both practitioners and academics.

In the future, the results from the above analysis can be used to construct a model to prevent the typical Internet user from phishing attacks. This will decrease the online crime commitment rate. In addition, this study could be used by organizations responsible for Internet usage at any level so that these organizations can be more aware of this problem and can find ways to solve related problems. This study can also be used for research in the future by adapting it to subjects that are related to the Internet in general and online business transactions.

REFERENCES

APWG. (2011). *The statistics of a phishing report received H12011 and H22011, an APWG survey*, Retrieved from http://www.antiphishing .org/

APWG. (2014). *Phishing activity trends report 3rd quarter 2013* Retrieved from http://docs.apwg. org/reports/apwg_trends_report_q3_2013.pdf

Bank, D. (2005). *Spear phishing' tests educate people about online scams* Retrieved from http: //online.wsj.com/news/articles/SB 112424042313615131

Bonnstetter, B., CPCM, C., & CPVA, T. (2006). *Information that adds to the art of selection for the financial industry*. Retrieved from http:// www.sayitcommunications.com/Portals/ 175357/docs/billscornerfinancialindustry.pdf

Danuvasin, C. (2011). Phishing: A field experiment. *International Journal of Computer Science and Security (IJCSS), 5*(2), 277–286.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *Proceedings of the SIGCHI conference on Human Factors in Computing Systems* (CHI 006) April 22 - 27, 2006 Montréal, Canada 2006: 581–590.

Dohmen, T., Falk, A., Huffman, D., & Sunde, U. (2008). Representative trust and reciprocity: Prevalence and determinants. *Economic Inquiry, 46*(1), 84–90.

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. *Proceedings of the Second Symposium on Usable Privacy and Security* (SOUPS) July 12-14, 2006 Pittsburgh, PA, USA 2006: 79–90 .

Dunn, J.E. (2007). *Do-it-yourself phishing kit*. Retrieved from http://www.pcworld.in/news/ index.jsp/artId=4915203

Evers, J. (2007). *New tools enables sophisticated phishing scams*. Retrieved from http:// zdnetindia.com/ news/security/stories/167392. html

Friedman, B., Hurley, D., Howe, D. C., Felten, E., & Nissenbaum, H. (2002). Users' conceptions of web security: A comparative study, pp 746–747. *Paper presented at the CHI'02 extended abstracts on Human Factors in Computing Systems(*CHI 2002*)* April 20-25, 2002 Minneapolis, MN.

Geer, D. (2005). Security technologies go phishing. *Computer, 38*(6), 18–21.

Gooden D. (2007). *Man hijacks 90 eBay accounts*. Retrieved from http://www.theregister.co.uk / 2007/03/21/ebay_hijack_plea

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM, 55*(1), 74–81.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94–100.

Jakobsson, M., & Ratkiewicz, J. (2006). Designing ethical phishing experiments: a study of (ROT 13) rOnl query features, pp 513–522. *Proceedings of the 15th international*

conference on World Wide Web (WWW '06) May 23–26, 2006 Edinburgh, Scotland, UK. ACM Press, New York, NY.

Krebs, B. (2006). Flaws in Financial Sites Aid Scammers. *Security Fix*.

Levy, E. (2004). Criminals become tech savvy. *Security & Privacy, IEEE, 2*(2), 65–68.

Leyden, J. (2006). *Phishing fraudsters offer cash reward*. Retrieved from http://play.tm/wire/click/824881

Lininger, R., & Vines, R. D. (2005). *Phishing: Cutting the identity theft line*. Retrieved from www.wiley.com.

Marston, W. M., & Moulton, M. W. (2013). *Emotions of normal people* (Vol. 158). Hoboken, NJ.: Taylor and Francis.

McCombie, S., & Pieprzyk, J. (2010). Winning the phishing war: a strategy for Australia. *Cybercrime and trustworthy computing workshop (CTC), 2010 Second* (IEEE), 79–86.

McFedries, P. (2004). *Word spy: The word lover's guide to modern culture.* New York : Broadway Books.

Miller, R. (2006). *Chinese bank'sserver used in phishing attacks on US banks*. Retrieved from http://news.netcraft.com/archives/2006/03/12/chinese_banks_server_used_in_ phishing_attacks_on_us_banks.html.

Mutton, P. (2006). Paypal security flaw allows identity theft. *Netcraft, news. netcraft. com/archives, 6*, 16.

Olivo, C. K, Santin, A. O., & Oliveira, L. S. (2011). Obtaining the threat model for e-mail phishing. *Applied Soft Computing, 13*(12), 4841–4848.

RSA. (2012). *Phishing in season: A look at online fraud in 2012*. Retrieved from http://blogs.rsa.com/phishing-in-season-a-look-at-online-fraud-in-2012

Scarbecz, M. (2007). Using the DISC system to motivate dental patients. *The Journal of the American Dental Association, 138*(3), 381–385.

Shahriar, H., & Zulkernine, M. (2012). Trustworthiness testing of phishing websites: A behavior model-based approach. *Future Generation Computer Systems, 28*(8), 1258–71.

Stallings, W. (1995). *Network and internetwork security: Principles and practice*. Englewood Cliffs, NJ.: Prentice-Hall.

Sugerman, J. (2009). Using the DISC® model to improve communication effectiveness. *Industrial and Commercial Training, 41*(3), 151–154.

ThaiCert. (2007). ThaiCERT's handled incident response summary. Retrieve from http://www.itu.int/ITD/cyb/events/2008/brisbane/docs/jirawannakool-thaicert-brisbane-july-08.pdf.

ThaiCert. (2014). *ThaiCERT incident statistic report 2012–2013.* Retrieve from https://www.thaicert.or.th/statistics/statistics-en.html

Turban, E., Leidner, D., McLean, E., & Wetherbe, J. (2008). *Information Technology for Management.* Hoboken, NJ.: John Wiley & Sons.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51*(3), 576–586.

Vrba, A. M. (2008). *Relationship between follower behavior style and perception of effective leadership characteristics in adult learners*. *ProQuest.*

Whalen, T., & Inkpen, K. M. (2005). Gathering evidence: Use of visual security cues in web browsers, pp 137–144. *Proceedings of Graphics Interface 2005 (GI 05)* May 9-11, 2005 Canadian human-computer communications society. Victoria, BC, Canada.

Wu, M., Miller, R. C., & Garfinkel, S. L. (2006). Do security toolbars actually prevent phishing attacks? pp 601–610. *Proceedings of the SIGCHI conference on Human Factors in computing systems*(CHI 006) April 22–27, 2006. Montréal, Quebec, Canada.