Towards Understanding Phishing Victims' Profile

Ali Darwish
College of Information Technology
Zayed University – UAE
Email: ali.darwish@zu.ac.ae

Ahmed El Zarka and Fadi Aloul
Computer Engineering Department
American University of Sharjah – UAE
Email: {b00022890, faloul}@aus.edu

Abstract — **Today it is known that the weakest link in the cyber security chain is the computer user. Social engineering attacks are commonly used to deceive computer users to perform actions that could leak private information. Such attacks psychologically manipulate the computer users to reveal his/her confidential information. Therefore, the computer user has been carefully studied by security researchers to understand the relationship between cyber security incidents and the victim background. In this paper, we present a breadth-first survey of recent studies that aim to understand the relationship between victims' backgrounds and phishing attacks. We summarize the characteristics of the phishing victims, following a review of their demographic and personality traits.**

I. INTRODUCTION

Phishing is defined as a form of social engineering attack in which phishers, i.e. attackers, trick the victim to fraudulently obtain private information [1]. The common phishing attack scenario starts by the phisher sending an email to the victim. The email appears to come from a legitimate website, e.g. a bank or a university, asking the victim to login and update some private information. A warning message is typically added to the email to persuade the victim to believe the email and reply immediately. The email typically has a URL link that appears to be legitimate but directs the victim to a fraudulent website that looks identical to the legitimate website. Once the victim enters the private information, e.g. username and password, into the fraudulent website, the data is sent to the phisher and the victim is redirected to the legitimate website in order not to detect the attack.

While phishing attacks have been known since 1996, these attacks have been on the rise in the past few years [2]. Phishers are commonly using them to target banks, e-commerce, and social networking websites to steal thousands if not millions of dollars. Phishing attacks are continuously improved to deceive even the best security-aware computer users.

According to RSA security solution, the number of phishing attacks in September 2011 increased by more than 100 percent to reach 38,970 attacks compared to 16,247 attacks in September 2010 [3]. Losses incurred from phishing attacks alone during the period of the second half of 2010 through the first half of 2011 reached nearly $1 billion [3]. The recent significant increase in the number of phishing attacks is an indication of the effectiveness of the attack and the high number of potential phishing victims.

This paper addresses the question of what are the computer user susceptibility factors to being victims of phishing attacks. We summarize and analyze a collection of research studies that were recently conducted to understand the user's susceptibility to fall for phishing attacks. By determining such susceptibility factors, we can assist in the development of security solutions that are based on a *user-centric* design rather than the traditional *technology-centric* design. Furthermore, understanding the phishing victims' demographics, personalities, and backgrounds can help improve the security awareness and reduce the effectiveness of phishing attacks.

The rest of this paper is organized as follows. In Section II we present some of the common techniques used in phishing attacks. Section III describes some of the commonly used protection methods against phishing attacks and their effectiveness. Section IV discusses the recent studies conducted to understand the relationship between the victims' backgrounds and phishing attacks. Section IV also summarizes the characteristics of victims that are likely to fall victims to phishing attacks. We conclude in Section V.

II. PHISHING ATTACK TECHNIQUES

Recent years have seen an increase in phishing attacks due to the increase in online financial transactions and e-commerce websites. New phishing attack techniques, such as spear phishing and pharming, are continuously developed to fool the best security-aware computer users. This section summarizes some of the effective phishing attack methods.

A. Phishing Toolkits

One of the growing means of setting up a phishing attack is by using free online phishing toolkits. The toolkits help automate and customize the creation process of the phishing website. However, an interesting study in [4] showed that there is no such thing as a free phishing toolkit. This was proven in the study which analyzed a large number of freely available phishing tool kits. The study found that the original authors of the toolkits developed backdoors in their toolkits which would send them back all the information that the users of these phishing kits illegally collect. That was a clever way for these authors to collect illegal information without being directly involved in the attack process; hence they reduce the risk of being caught while the attackers who are using their

978-1-4673-5157-7/13/$31.00 ©2013 IEEE

free phishing toolkits put themselves in risk of being caught by the authorities.

B. Related Domain Names

It is common for an organization before it launches its business to reserve a domain name for their main website. Phishers typically reserve domain names that are relatively similar to the legitimate domain name. The idea is to host a phishing website that is identical to the original website using the similar domain names. Users will most likely not carefully check the all characters in the phishing website domain name and end up falling victim to the phishing attack. An example would be to buy the fraudulent domain name *www.citiibank.com* to replicate the original bank domain name *www.citibank.com*.

In a study by Dhamija et al. on why phishing works [5], it was proven how a small but clever change in the domain name can cause a large number of users to fall for a phishing attack. In the study the domain name *www.bankofthewest.com* was changed *www.bankofthevvest.com*. The only difference was replacing the letter "*w*" with two instances of the letter "*v*". 91% of the participants in the study fell for the phishing website, which was due to the fact that the domain name was slightly changed and a fast scan through it would not be enough to recognize the change.

C. Visual Deception

A carefully designed phishing website can attract more victims. In a phishing study presented by Dhamija et al. on 22 participants from different backgrounds yielded that good phishing websites can fool even users who have good security backgrounds [5]. The phishing website they constructed fooled 90% of the study participants. Some phishers use high quality visual contents like animated images and flash media to be able trick careful users into their scam. The study also found that a lot of the participants fell for web pages that were simply "good looking". Participants fell for a number of phishing websites thinking it is legitimate and gave the following reason, "fake websites could never be this good" or thinking that a video in the link showed legitimacy "because that would take a lot of effort to copy". The study proved how distracting the users with a well-designed website could easily fool the users or even turn the users away from paying attention to alerts or the domain name.

D. Pharming

Pharming or DNS poisoning is considered one of the most difficult to detect phishing attacks. The attack involves injecting fraudulent entries to the organization's DNS server which redirects the users to the fraudulent IP address while the browser is displaying the original domain name. Hence, even if the user checks the domain name, it will match the legitimate domain name.

E. Anti-Phishing Filter Evasion

Since security filters rely on text mining to discover suspicious keywords and patterns, some phishers tend to use images instead of text to bypass the filters. When anti-phishing filters fail to detect the phishing email or website, users are responsible for identifying the security threat.

F. Spear Phishing

Spear phishing is a type of phishing attack that targets specific users. Rather than mass emailing the phishing message, the phisher will carefully select a small number of users that are not aware of phishing attacks and email them the phishing message. Emailing the phishing message to many users will most likely have them alert the authorities and shut down the phishing website.

III. Combating Phishing Attacks

Several technologies and tools have been proposed to combat phishing. These technologies can be categorized as:

1) Web browser security toolbars
2) Anti-phishing filters
3) Anti-phishing honeypots

Web browsers use security toolbars that are designed to show security-related information about a visited website like the availability of a legitimate digital certificate and SSL encryption. When the toolbar detects the absence of the digital certificate it issues a warning message since the visited website could be fraudulent [6]. Some studies evaluated anti-phishing toolbars to test their effectiveness in combating phishing and found them to be ineffective in protecting users from phishing attacks. Phishing warning messages were overlooked by some users due to their lack of awareness about phishing attacks [7][8].

Phishing filters typically work by checking the domain name of the visited website against a list of reported phishing domain names. If a match is found the filter blocks the website or triggers a warning message. Such filters can be bypassed using *pharming* attacks [9].

Honeypots are widely deployed to detect phishing emails and identify phishing websites [10]. The idea hasn't been heavily researched and there are no clear indications of the effectiveness of honeypots in blocking phishing attacks. Furthermore, honeypots will likely need time to detect and block the phishing websites which will leave users vulnerable for a period of time.

IV. Understanding The Phishing Victim's Background

Several phishing studies have been conducted over the past few years, most of which are based on role-play studies. Role-play studies enable researchers to analyze the effectiveness of phishing attacks without conducting an actual phishing experiment. The method of role-play is based on giving the users a questionnaire to assess a possible security scenario. The users' answers are analyzed and summarized to draw conclusions about the potential phishing victim backgrounds [11][12]. Other researchers studied the effectiveness of phishing attacks by running "controlled" phishing experiments, in which the users receive a real phishing email

that directs them to a phishing website, but the phishing website doesn't collect or store any of the private information [2][12][13][14][15]. The website keeps track of the number and possibly the usernames of the victims. The data can be used to assess the security awareness among the users and improve future security trainings.

In the sections below, we describe some of the identified characteristics of potential phishing victims based on various conducted studies.

A. *Victim's Age*

Age plays an important role in identifying potential phishing victims. Most phishing studies found that age correlates with the likelihood to fall for phishing deception. Among internet users that are computer literate, older ones were less likely to fall prey for phishing; while younger users, particularly between the age of 18-25 or younger, were consistently more vulnerable to phishing attacks [11][12][13].

Sheng et al. performed a role-play survey to study demographics and phishing susceptibility; they found that participants' age linearly predicts their susceptibility to phishing; the younger the age the higher the risk for falling prey for phishing [11]. An empirical study by researchers from Carnegie Mellon University tested different age groups in a phishing experiment. The study was based on sending phishing emails to a group of 515 participants. They found that 62.3% of users from the age group of 18-25 fell for the phishing email whereas 41.1% of the users from the age group of 26 years or older fell for the same phishing email [13]. Later, the researchers conducted a new phishing experiment in an extended study which included 5,182 participants from all age groups and found that younger users are more vulnerable to phishing attacks [12].

B. *Victim's Gender*

Probably one of the most studied susceptibility factors in phishing attacks is gender differences. Most studies showed that women are more likely to fall for phishing attacks than men [11][12][14].

Jagatic et al. conducted a real phishing attack experiment on 1731 students from Indiana University. Their results showed that 77% of female students fell for the spear phishing attacks while 65% of the male students fell for the same attack [14].

Sheng et al. conducted a phishing role-play and found that 53.1% of the women fell for phishing attacks while 41% of the men did [11]. Another study that is focused on the increased role of phishing awareness and anti-phishing education yielded that men were more likely than women to correctly distinguish between phishing and legitimate websites. The study found that 75.5% and 64.4% of the women and men, respectively, who participated in the study fell for phishing attacks [12].

Nevertheless, the study by Kumaraguru et al. contradicted the hypothesis of gender differences in falling for phishing attacks. The study conducted to test the anti-phishing training effect in preventing users from falling for phishing attacks did not find significant differences in gender among the phishing victims [13].

C. *Victim's Anti-Phishing Education*

Security awareness and specifically anti-phishing training can play an important role in protecting the users from social engineering attacks. Several researchers evaluated the effectiveness of anti-phishing training in reducing the possibility of users falling victims to phishing attacks [11][12][13][15].

Kumaraguru et al. evaluated *PhishGuru* which is an embedded anti-phishing training system with 515 participants in a real world study which analyzed responses over a course of 28 days [13]. They provided different groups of participants with different training methods to find out the best practice of anti-phishing training approach and concluded that: (1) People with anti-phishing training are less vulnerable to phishing. (2) Providing intense anti-phishing training gives better result in identifying phishing risks. (3) Users gain better experience and retain their knowledge after a short-period of time compared to long periods. (4) Anti-phishing training radically reduced vulnerability to phishing attacks but some users still did fall for the phishing attacks. Figure 1 shows the difference in the number of victims in day 2 and day 28.

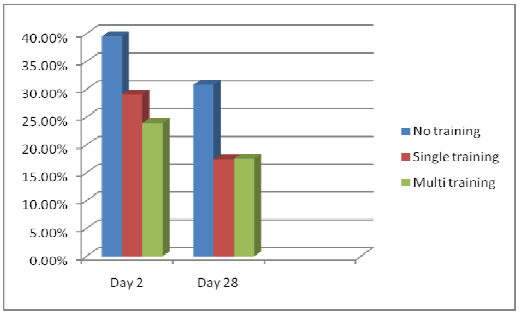

Figure 1. Percentage of participants who clicked on phishing links and gave information on the first day (day 2) and the last day of the study (day 28) [13].

Kumaraguru et al. extended their study to include 5,182 internet users to measure the effectiveness of an anti-phishing interactive game. They demonstrated that after playing the anti-phishing game, people were able to distinguish phishing websites more accurately and in general performed at least 50% better in protecting themselves from phishing attacks [12].

To support the previous findings, Dodge et al. conducted an experiment that focused on the retention level of acquired anti-phishing knowledge [15]. The study targeted 892 students and simulated a phishing attack. The phishing attack was classified into 3 categories; each category targeted a group of users however, different feedback was provided. The first group got a server-error message, without informing them that they were victims of a phishing attack; the second group users' were informed that they were targeted by a phishing attack; and the last group received an anti-phishing training.

To test the knowledge retention level, a second phishing email was sent 10 days later. The results are shown in Figure 2. Users from the three different groups became more aware of phishing attacks. However, "no feedback" and "feedback" group users responded to the phishing scam during the second round more than the "training" group users. This indicates that the knowledge retention between the first and the second round of the experiment was slightly better in those who received training after the first phishing scam.

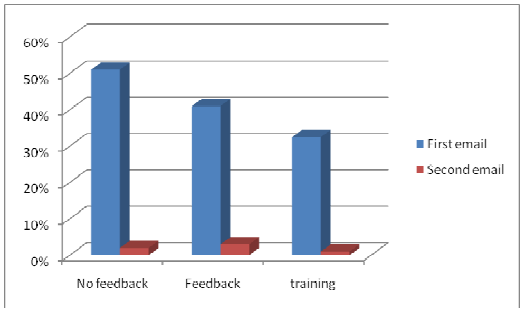

Figure 2. Response results between the first phishing email and the second one [15].

D. *Victim's General Educational*

Users with IT knowledge are expected to be more aware of phishing attacks. Nevertheless, a study reported by Kumaraguru et al, showed that users with computer science backgrounds performed slightly better than users with other backgrounds when being attacked by phishing. This is shown in Figure 3.

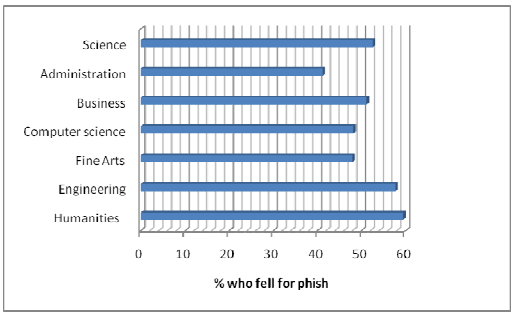

Figure 3. Percentage of phishing attack victims by major [13].

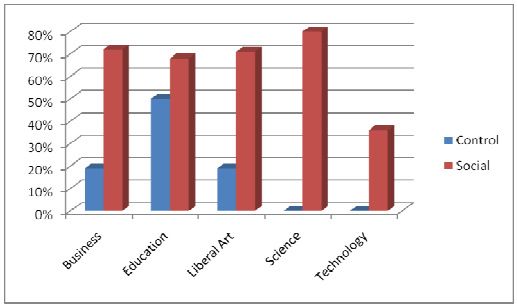

Figure 4. Success rate of phishing attack by major. Control indicates a regular phishing email. Social indicates a spear phishing email [14].

Jagatic et al. evaluated the effectiveness of *regular* phishing emails and *spear* phishing emails among students enrolled in different colleges [14]. As shown in Figure 4, Science and Technology students were invulnerable to regular phishing emails, while Business, Education, and Liberal Art students did fall victims for regular phishing emails. However, students from all colleges fell victims to the spear phishing attacks with no exceptions. Interestingly, the highest percentage of spear phishing victims was Science students.

E. *Anti-Phishing Training Delivery Method*

The delivery method of the anti-phishing training can play an important role in reducing phishing incidents. A study performed by Kumaraguru et al. evaluated two training methods: embedded and non-embedded training [16][17]. In the *embedded* training method users were sent a controlled phishing attack and trained after they fell victims for the attack. In the *non-embedded* training method users were given the phishing training without experiencing the controlled phishing attack. The study showed that: (1) Users learned more effectively when the training material was presented after they fell victims for the phishing experiment, i.e. the embedded method. (2) Users can retain and transfer more knowledge when taught with embedded training.

F. *Victim's Personality*

Recently, researchers at the university of Arkansas and Louisiana Tech studied the "Big-Five" personality traits to relate phishing attacks with the victims' personalities [18]. The five board of personality domains are: Neuroticism, Extraversion, Openness, Agreeableness and Conscientiousness [18]. People who are classified with *Neuroticism* tend to be sad and sometimes hot tempered. *Extraversion* is the tendency to be energetic, active and love to socialize with others. *Openness* describes those who are less anxious and more open to different ideas and beliefs. Those who exhibit high levels of openness revel in fantasy and have high sense of art and nature. *Agreeableness* measures the level of relationships with others. Those who exhibit high level of agreeableness are cooperative because they think that in general others have good intentions. The fifth personality domain is *conscientiousness*, it focuses on self-discipline, respect for rules and dutifulness. Conscientiousness people typically have high common sense.

Users who are at a high rate of security risk possess high levels of *agreeableness* and *extraversion*. Whereas, *conscientiousness* users who are more mature and always show a respect for standards and procedures usually have a lower security risk rate [19].

Young users were shown earlier to be more vulnerable to phishing attacks. Young users are known to have a high level of *agreeableness* which correlates with their high susceptibility to fall victims for phishing attacks [20].

Female users were also shown earlier to be more vulnerable to phishing attacks than male users. A study conducted by Costa et al. classified females to be more *agreeable* than males which also correlates with why woman have a higher chance of falling for phishing attacks [21]. Users

with *agreeable* personalities are known to trust and can be easily exploited by attackers to lure them to clicking on a phishing link and revealing their private information [11]. Men naturally are more antagonistic and suspicious which puts them at a lower security risk [17].

G. Victim's Internet Usage Behavior

While the internet usage between male and female is relatively equally distributed, a study by Abraham et al. showed that women are more likely to shop online than men [22]. The study indicated that in 2010 women generated 58% of the e-commerce dollars globally. Therefore, women are more likely to be targeted by phishing attacks. The internet usage behavior can play a role in attracting or deterring phishing attacks.

Table 1 summarizes all the factors we found to be correlated with susceptibility to phishing attacks.

Table 1. Summary of characteristics of potential phishing victims.

	Highly Susceptible	**Less Susceptible**
Age	18-24 years old or less	25 years old or more
Gender	Female	Male
Anti-phishing Training	No training	Anti-Phishing trained
Education	Humanities	Computer Science
Training Delivery Method	Non-embedded	Embedded
Personality	Agreeableness	Consciousness
Internet Usage Behavior	E-commerce & Online Banking	E-mails and simple browsing

V. CONCLUSION AND FUTURE WORK

As the present review demonstrates, users' demographic and personality traits are valuable factors for social engineering studies and other social security research. The user factor can provide quantitative measures for social-cyber security, and a valuable component that moderates the Human Computer Interaction (HCI) with cyber security. Previous studies showed that young users are more likely to fall for phishing attacks. Furthermore, users with agreeable personality trait are likely to be lured by phishing scam more than other users. It is also shown that women are more likely to provide their personal and financial details to phishing emails and websites. This casual relationship between gender and social engineering is influenced by the internet usage behavior. Our future work is two-fold, to build a machine learning model for predicting users' vulnerability to phishing, and to assess current deployable approaches to combat social engineering threat at the technology front. Both pathways investigate broader class of solutions than seen in the past.

VI. REFERENCES

[1] A. Martino and X. Perramon, "Phishing Secrets: History, Effects, and Countermeasure," in *International Journal of Network Security*, 12(1), pp. 37–45, January 2011.

[2] F. Aloul, "The Need for Effective Information Security Awareness," in *Journal of Advances in Information Technology* (JAIT), 3(3), pp. 176-183, 2012.

[3] "Cyber Security Awareness Month Fails to Deter Phishers," *RSA The security division of EMC, Bedford, Massachusetts, Fraud Rep.*, October 2011.

[4] M. Cova, C. Kruegel and G. Vigna, "There is No Free Phish: An Analysis of "Free" and Live Phishing Kits," in *Proc. of the 2nd USENIX Workshop on Offensive Technologies*, 2008.

[5] R. Dhamija, J. Tygar and M. Hearst. "Why Phishing Works," *in Proc.of the Conference on Human Factors in Computing Systems* (CHI), p. 581-590, 2006.

[6] Y. Zhang, S. Egelman, L. Cranor and J. Hong, "Phinding Phish: Evaluating Anti-Phishing Tools." in *Proc. of the 14th Annual Network & Distributed System Security Symposium* (NDSS), February 2007.

[7] M. Wu, R. Miller and S. Garfinkel, "Do Security Toolbars Actually Prevent Phishing Attacks?" in *Proc. of the Conference on Human-Computer Interaction* (CHI), New York, pp. 601-610, 2006.

[8] S. Egelman, L. Cranor and J. Hong, "You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings," in *Proc. of the Conference on Human-Computer Interaction* (CHI), Florence, Italy, pp. 1065-74, 2008.

[9] G. Ollmann, "The Pharming Guide: Understanding and Preventing DNS-related Attacks by Phishers," NGS Secure, 2005. Available at: *www.infosecwriters.com/text_resources/pdf/ThePharmingGuide.pdf*

[10] L. Shujun and R. Schmitz, "A novel anti-phishing framework based on honeypots," in *Proc. of the eCrime Researchers Summit*, pp.1-13, September 2009.

[11] S. Sheng, M. Holbrook, P. Kumaraguru, L. Cranor, and J. Downs, "Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions," in *Proc. of the Conference on Human-Computer Interaction* (CHI), Atlanta, Georgia, 2010.

[12] T. Jagatic, N. Johnson, M. Jakobsson and F. Menczer, "Social Phishing," in *Proc. of the Communications of ACM,* 50(10), pp. 94-100, October 2007.

[13] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong. "Teaching Johnny Not to Fall for Phish", in *Proc. of the ACM Transactions on Internet Technology,* 10(2), pp. 1-31, May 2010.

[14] P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. A. Blair, and T. Pham, "School of Phish: A Real-World Evaluation of Anti-Phishing Training,"in *Proc. of the 5th Symposium on Usable Privacy and Security,* pp. 1-12, 2009.

[15] R. Dodge, E. Rovira, R. Zachary, and S. Joseph, "Phishing Awareness Exercise," in *Proc. of the 15th colloquium for Information Systems Security Education*, Fairborn, Ohio, June 13-15, 2011.

[16] P. Kumaraguru Y. Rhee, S. Sheng, S. Hasan, A. Acquisti, L. F. Cranor, and J. Hong, "Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer," in *Proc. of the 2nd Annual eCrime Researchers Summit,* pp. 70-81, New York, 2007.

[17] J. Parrish, J. Bailey and J. Courtney, "A Personality Based Model For Determining Susceptibility To Phishing Attacks," *Southwestern Decision Sciences Institute*, February 2009.

[18] S. Gosling, P. Rentfrow, and W. Swann, "A Very Brief Measure of the Big-Five Personality Domains," in *Journal of Research in Personality*, vol. 37, pp. 504-528, 2003.

[19] I. Weiner and R. Greene, "Handbook of Personality Assessment. Hoboken, New Jersey, John Wiley & Sons, Chapter 10, pp. 315-340, 2008.

[20] S. Srivastava, O. P. John, S. D. Gosling, and J. Potter, "Development of Personality in Early and Middle Adulthood: Set Like Plaster or Persistent Change?" in *Journal of Personality and Social Psychology*, vol. 84, pp. 1041-1053, 2003.

[21] P. Costa, A. Terracciano and R. McCrae, "Gender Differences in Personality Traits Across Cultures: Robust and Surprising Findings," in *Journal of Personality and Social Psychology*, vol.18, pp. 322-331, 2001.

[22] L. B. Abraham, M. P. Morn and A. Vollman, "Women on the Web: How Women are Shaping the Internet", June 2010. Available at: *www.iab.net/media/file/womenontheweb.pdf*