Phishing: Social Engineering in the Digital Age

Brenda S. Izquierdo
School of Computing and
Information Sciences
Florida International University
Miami, FL
bizqu002@fiu.edu

***Abstract*—This paper elaborates on a widespread cybercrime known as phishing. Phishing is an information privacy violation in which a target is contacted by email by an attacker posing as a legitimate institution or person to lure the individual into providing sensitive data over the Internet such as personally identifiable information, banking and credit card numbers, and passwords. The information is then used to access important accounts and can result in identity theft and financial loss. Email use has become ubiquitous, increasing the number of potential victims of a phishing scam. This work will touch on many topics related to phishing within a social engineering context such as the modus operandi of the cybercriminals, and the detection, and countermeasures that email users can take. The focus of this paper is on email phishing but it also throws light upon voice, mobile, and website phishing techniques from a social perspective.**

***Index Terms*—Cybersecurity, Phishing, Email Phishing, Social Engineering**

I. Introduction

We live in a digital world where widespread written communication between people across great distances has never been so easier nor faster. In medieval times, professional messengers who delivered the news in person or carried the message with them were employed to perform this service. Modernity brought with it the idea of a mail service, leading to the eventual creation of post offices, and together with the electric telegraph, it launched a new era of personal messaging, which culminated in the first electronic mail being sent on the latter half of the next century. But it was the explosion of Internet use in the 1990s that turned the email into a legitimate and necessary message channel between two or more people. By the turn of the millennium, having an email address became a societal expectation similar to having a phone number. Even though the email made personal communication an effortless task, it also brought privacy concerns. Email phishing is one of them.

But, what is phishing in the first place? It is "a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion" [1]. Electronic communications are vast; we can have voice phishing, mobile phishing, website phishing, and email phishing. The last one is the focus of this research paper.

II. Social Engineering

In the context of information security, social engineering "is the psychological manipulation of people in order to make them divulge their confidential information or perform activities which can be harmful for security and privacy" [2]. The appellation "social engineering", is an umbrella term for a widespread scope of malicious pursuits accomplished through means of communication and interaction. Social engineers use psychological tricks to fool people into providing sensitive information that can be used for the profit of the manipulator [3].

To talk about social engineering is to talk about deception. A social engineer is someone "who uses deception, influence, and persuasion" against others [4]. The practice has existed since the beginning of the world; one good example of social engineering is described in Homer's Iliad during the mythological war between Greece and Troy. After a grueling and fruitless ten-year siege to the city of Troy, the Greeks built a colossal wooden horse and hid inside it a small force. That night they pretended to have sailed away from the city, leaving that horse as a piece offering to the mighty Trojans, who unsuspectingly brought the horse inside the city and celebrated the flight of their enemies. As the long worn out Trojan soldiers surrendered themselves to a night of debauchery after having fought so hard to hold on to their fortress for the past ten years, the Greek armies sailed back surreptitiously and surrounded the city. At midnight, the men who were hidden inside the horse went down and opened the door to their fellow soldiers. Troy was in ruins long before the first rays of the sun touched the horizon.

Surprisingly, researchers have shown that the same human interaction principles that take place when malicious agents are trying to extract information also take place in our daily life when communicating with family and friends. Social engineering can occur in human-only interactions, but it can also be combined with technical attacks [5]. Social engineering is different from other security breaches because it relies on human error rather than software or hardware malfunction. Mistakes made by a person are hard to predict, thus security products and regulations cannot identify them and take preventive measures [3].

Regardless of the communication means, social engineering occurs in a four-level predictable chain: information gather-

ing, establishing relationship and rapport, exploitation, and execution. The order of these stages changes from attack to attack and some phases can be repeated. The success of the attack depends on the first step. Factors like getting to know the target, and preparing convincing justifications are paramount. In the second phase, the attacker establishes a 'working' relationship with the victim; this is the opportunity for the intruder to size up his victim, map out his weaknesses and devise a plan of attack. The scope of the relationship can vary. For example, some attackers are satisfied with a simple acquaintanceship with the victim through Facebook where they can gather general facts, while others prefer a full-blown cyberstalking of their victim until they are sure it is safe to make their move. The third step, exploitation, is when the attacker actively uses the resources he has gathered in the two previous steps while still maintaining a friendly facade. The last step is execution, which is when the attacker deals his last blow to the target and covers all traces. "A well planned and smooth exit strategy is the attacker's goal and final act in the attack" [6].

Some examples of social engineering attacks are:

- **Pretexting**: The attacker creates a false social scenario. It consists of an elaborated lie that may include the date of birth, Social Security number, or last bill amount to deceive the target into providing more information without doubting the legitimacy of the criminal's intentions [7].
- **Diversion theft**: It is used to deceive courier or transport companies into delivering their packages to wrong addresses [7].
- **Water holing**: A technique that embeds the attack in a legitimate website. A careful person may think twice before clicking on a link that appears in an email from an unknown sender, but the same person could probably click on a link that appears in a website they visit regularly without a second thought [7].
- **Baiting**: This is the Trojan horse of social engineering assaults. An attacker may leave a USB, CD, or floppy disk that contains malware in a conspicuous place. Even though there are conscientious individuals who might report it to the nearest lost and found office or simply ignore the device, most people would connect it to a computer and examine the contents out of mere curiosity, thus installing malware into their own devices [7].
- **Quid Pro Quo**: It means "something for something". The assailant gives something to the victim in order to make a security breach. For example, an attacker makes random phone calls impersonating a customer service agent returning a call for help from a client until an unsuspecting user takes the bait. The attacker then 'helps' the user while making him enter commands that grant system access to the criminal or that install malware in his device [7].
- **Tailgating**: An attacker breaks into a restricted area manipulating others inside. For example, a person might infiltrate an ATM without swiping his card in the entrance by coming in right behind someone else or at the same time that a user is leaving. Out of courtesy, ATM patrons may be holding the door open for an attacker without knowing it [7].

The examples just listed are typical illustrations of social engineering, but there is another one called 'phishing', which is arguably the most representative and commonplace of all social engineering attacks.

III. Phishing

According to the Oxford English Dictionary, phishing is "the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers" [8]. Although phishing is not limited to emails, most phishing attacks befall through this electronic means of communication.

A. History

To speak about the history of phishing in general we need to go back to the decade of 1990-2000 and to American Online Inc., better known as AOL. During the last ten years of the past century, AOL was for America what Google is now for the world. An early pioneer of the Internet, a web portal, a web browser, an online service provider, AOL was the most recognized brand on the web in the United States [9]. But pirate software was on its rise at the same time, and challenged the system security of AOL. Black hat hackers lost no time perpetuating "credit card fraud and other online crimes". Consequently, AOL sought to counteract the onslaught by detecting symbols, words, and sequences in the AOL chat rooms that triggered an alarm. The only term that could not be filtered by the AOL security team was '<><' because it was the generic tag of HTML for all conversations and as such, it was bound to appear in every interaction. "The symbol <>< was replaced for any wording that referred to stolen credit cards, accounts, or illegal activity" that managed to avoid the prying eyes of AOL security. Members of the team soon noticed the resemblance of '<><' to a fish, so they coined the new term as 'phishing' [10].

Another theory regarding the origin of the sobriquet 'phishing' is that since criminals dangled a bait that users took, one could say that the criminals were fishing for victims [11]. Whatsoever the origin of the appellative, phishing attacks became an almost permanent fixture of AOL services. In early 1995, the infamous AOHell, "a program designed to hack AOL users by allowing the attacker to pose as an AOL staff member, and send an instant message to a potential victim, asking him to reveal his password" was released, becoming the first phishing-specialized software product. The success that AOHell met was so vast that AOL had to include the following line in all chat rooms: "no one working at AOL will ask for your password or billing information". Yet as AOL declined in popularity, phishing went on to become extremely commonplace [10].

B. Types of Phishing Attacks

1) By communication means:

- **Voice phishing**: Also referred as 'vishing', a combination of the words voice and phishing. It is the criminal practice of using social engineering over the telephone to gain access to the personal and financial information of a second party for the purpose of monetary gain. "Voice phishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals" [12].
- **Mobile phishing**: In a mobile phishing attack, an intruder usually sends an SMS message that contains links to websites or applications that request the user to enter credentials, credit card numbers, and other data. Website and email phishing attacks can also take place through this means [13].
- **Website phishing**: Website phishing is the act of luring unsuspecting users by counterfeiting a legitimate company's website. Attackers recreate the logo, copyright statements, and fonts of a legitimate business and thus deceive customers into submitting credentials and other information [14].
- **Email phishing**: Email phishing is the act of contacting users through email pretending to be a legitimate organization or individual in order to trick recipients to install malware, share private information or redirect them to a counterfeit website where they can fall into those two traps [15].

2) By target:

- **Spear phishing**: A spear phishing attack is one that is targeted to a specific individual or business. Before establishing contact with the victim, the attacker had already gathered some data about him or her. "In a typical case, spear phishing emails appear to be coming from accounts within the same company or coming from a coworker or a friend" [16].
- **Whaling**: "Whaling employs spear phishing tactics, but is intended to go after high-profile targets such as an executive within a company" [17]. The word 'whaling' is a play upon phishing; rather than go for a small target, the criminal goes for the big fish.
- **Clone phishing**: "Clone phishing is a type of phishing attack whereby a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email. The attachment or link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender" [10].

C. Email Phishing

"Email phishing is the act of impersonating a business or other entity for the purpose of tricking the recipient of email into giving up sensitive personal information. Data gleaned from phishing often is used to commit identity theft or to gain access to online accounts" [15]. Anyone with an email account is a potential victim of a phishing scam. State-of-the-art email phishing attacks can be classified into one of these three scenarios:

1) The email contains a link to an apparently legitimate website where the victim is deceived into entering sensitive data such as credentials, a credit card number, or a Social Security number, etc.
2) The email tricks the victim into entering commands that allow system access to the criminal.
3) The email contains a link, instructions or an attachment that installs malware in the victim's device.

Email phishing is a roaring business, almost an art, one that becomes more and more sophisticated. Today's phishing scams are a far cry from how they began in the 1990s. Early phishing emails were easy to detect due to their poor grammar and spelling, and lack of official logos and fonts. Email users could easily spot a phishing email because it was clear that no legitimate company would ever send an email to a customer that was ridden with errors or without a logo, so cybercriminals changed their modus operandi. Not only emails are now most persuasive and well-written, they are also highly personalized, addressing the recipient by name and including some personal information such as home address, workplace name, work address, phone number, etc. Moreover, the emails now convey a sense of legitimacy by replicating the look and feel of an authentic email: fonts, footers, logos, and copyright statements [18].

The effect of being scammed depends on what the scammer set out to get. Some criminals may not be after money but after a Social Security number, passport information, a driver's license number, etc. so they can steal the victim's identity. They may also be trying to phish usernames and passwords to break into an online account. The target's predicament aggravates if he or she re-uses the same credentials for other accounts [19].

IV. Protective Measures

The following is a list of details that betray an email phishing scam attempt. Users should beware of:

- *False email addresses*: Sometimes an email inbox only displays the first part of the sender's email address. Users should bear in mind that an authentic business owns the domain name, which is either the name of the company or its initials. If the email comes from a generic source like "secure.com", it is most likely a phishing scam [20].
- *Urgent requests*: "Invoking a sense of urgency or fear is a common phishing tactic" [20]. For example, an email from an unknown sender offering a user a free membership for one month or a free gift only if they fill

a registration form or a survey within 10 minutes is most likely a phishing attempt. Other examples can be emails that ask users to immediately update their accounts in order to receive an unexpected refund, or the old "click here to order your free gift now (this link will expire within 1 minute)" which usually ends with the user's device being infested with malware [21].

- *Unexpected refunds and payments*: Attackers masquerade their emails to make it seem like they come from Amazon, PayPal, etc. or even government agencies such as the IRS offering the victim a refund or a payment. The emails include links to fake company websites or that install malware [21].
- *Emails from high-level executives*: The attacker tries to recreate the context of an email from a legitimate person of authority in the company the user works for. Usually this is an executive whom the employee is not in constant touch with. "These emails play on our respect for these individuals and take advantage of the lack of formality that sometimes accompanies their requests" [21].
- *Dubious content*: Corporations and companies "are pretty serious about email. Legitimate messages usually do not have major spelling mistakes or poor grammar". Phishing emails can be spotted by the salutation too, some attackers do not take time to prepare a spearing assault so the email's subject is a vague greeting addressed to a "Valued Customer"; legitimate businesses strive to send personalized greetings that contain the name of the client. Regarding financial scams, users need to bear in mind that "companies will never ask for personal information via email" especially if the information is sensitive. Email users should also beware of emails that appear to come from companies or organizations that do not include a phone number or an address. "Legitimate businesses always provide contact details" [20].

Some recommendations to avoid phishing attacks in general:

- *Set spam filters to high*: Every email inbox has spam filters. It is recommendable to set these to high, even if the user has to check them from time to time to ensure that no legitimate email has fallen there [5].
- *Secure computing devices*: Up-to-date anti-virus software and firewalls should always be installed and turned on respectively. If possible, the user should set the computer's operating system to automatically update, but if not, then it should be done manually. The same for smartphones. Another recommendation is to add an anti-phishing tool to browsers to receive alerts of potential attacks [5].

V. Summary

Phishing is a cybercrime that due to the extensive use of electronic communication devices nowadays and the lack of a strong cybercrime legislation has grown to become a real threat in the digital world and a roaring business for cybercriminals. Phishing, as well as all social engineering attacks, aims to deceive users into parting with highly sensitive information, personal and financial, or to mislead them into installing malware or granting access to their devices. These exceedingly effective, pervasive attacks can be carried on through most electronic communication means. In this paper we discuss the most prevalent of them, which is email phishing, including a historical review in the context of social engineering and phishing in general, as well as recommendations to avoid being a victim of an email phishing scam.

References

[1] M. Jakobsson and S. Myers, *Phishing and countermeasures: understanding the increasing problem of electronic identity theft*. Wiley-Interscience, 2007.

[2] V. Ahuja and S. Rathore, *Multidisciplinary perspectives on human capital and information technology professionals*. IGI Global, 2018.

[3] "Social engineering." [Online]. Available: https://www.incapsula.com/web-application-security/social-engineering-attack.html

[4] K. D. Mitnick, *The art of deception: controlling the human element of security*. Wiley, 2003.

[5] "What is social engineering?" [Online]. Available: https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering

[6] "The social engineering framework." [Online]. Available: https://www.social-engineer.org/framework/attack-vectors/attack-cycle/

[7] "Social engineering (security)." [Online]. Available: https://en.wikipedia.org/wiki/Social_engineering_(security)

[8] "phishing — definition of phishing in english by oxford dictionaries." [Online]. Available: https://en.oxforddictionaries.com/definition/phishing

[9] "Aol," Jun 2018. [Online]. Available: https://en.wikipedia.org/wiki/AOL

[10] "Phishing." [Online]. Available: https://en.wikipedia.org/wiki/Phishing

[11] "What is a phishing email and how do i spot the scam?" [Online]. Available: https://www.webroot.com/us/en/resources/tips-articles/what-is-phishing

[12] "Voice phishing." [Online]. Available: https://en.wikipedia.org/wiki/Voice_phishing

[13] H. Shahriar, T. Klintic, and V. Clincy, "Mobile phishing attacks and mitigation techniques," Jun 2015. [Online]. Available: https://pdfs.semanticscholar.org/60aa/7348b1730aef6400e5e23c0b864ea94b1b36.pdf

[14] O. Akanbi, A. Abunadi, and A. Zainal, "Phishing website classification: A machine learning approach," Jun 2015. [Online]. Available: https://www.researchgate.net/publication/271647530_Phishing_Website_Classification_

[15] "What is email phishing and spoofing?" [Online]. Available: https://consumer.findlaw.com/online-scams/what-is-email-phishing-and-spoofing-.html

[16] M. Almgren, V. Gulisano, and F. Maggi, *Detection of Intrusions and Malware, and Vulnerability Assessment 12th International Conference, DIMVA 2015, Milan, Italy, July 9-10, 2015, Proceedings*. Springer International Publishing, 2015.

[17] D. Barrett, *CompTIA security SY0-301 practice questions*. Pearson Education, 2012.

[18] M. Levinson, "How to tell if an email is a phishing scam," Apr 2012. [Online]. Available: https://www.cio.com/article/2397353/security0/how-to-tell-if-an-email-is-a-phishing-scam.html

[19] J. Regan, "What is phishing? avoid phishing emails, scams & attacks," Feb 2018. [Online]. Available: https://www.avg.com/en/signal/what-is-phishing

[20] E. Derouet, "10 tips on how to identify a phishing or spoofing email," Dec 2015. [Online]. Available: https://blog.returnpath.com/10-tips-on-how-to-identify-a-phishing-or-spoofing-email-v2/

[21] C. Johnson, "15 examples of phishing emails from 2016-2017," Jul 2017. [Online]. Available: https://www.edts.com/edts-blog/15-examples-of-phishing-emails-from-2016-2017