An interdiscplinary study of phishing and spear-phishing attacks.

Robin Gonzalez and Michael E. Locasto
University of Calgary

1. INTRODUCTION

In a world where spear-phishing is one of the most common attacks used to steal confidential data, it is necessary to instruct technical and non-technical users about new mechanisms attackers can use to generate these attacks. We want to focus on *phishing* attacks, where a social engineer communicates a deceitful message to their victims in order to obtain some confidential information, because of recent advancements in the field. Nowadays, with all the information most users provide online along with the advancements of fields such as data mining, it is more difficult for users to distinguish between malicious and benign communication. If the attack is designed to target a specific user with the knowledge of his or her information it is called *spear-phishing*. Spear-phishing attacks tend to be more successful than other attacks due to their targeted nature.

Recent studies by Intel suggest that 97% of people cannot identify phishing emails[1]. Therefore, as educators we find the need to instruct users about the structure, purpose, and power of these attacks. In this investigation we propose the construction of a body of knowledge for phishing and spear-phishing attacks. Our motivation is the increasement of accuracy, success, and scale of these attacks in the last decade. The body of knowledge we propose provide a corpus of what we think are the main components of phishing attacks: psychology, computation, and sociology. Studying these aspects of phishing attacks can help future generations of computer science students to better understand how to defend against them.

As a community, we need to provide a better definition for the set of vulnerabilities social engineers use to exploit their victims. We propose to expand the curriculum for these types of attacks and to include interdisciplinary areas such as psychology and sociology in future courses that relate to social engineering. More precisely, we aim to educate students on the aspects we argue are involved in the evaluation of phishing attacks with usable privacy. We believe that interdisciplinary methods are necessary to study social engineer attacks. Computer science students need to learn more about the psychological and sociological vulnerabilities social engineers use to exploit their victims. This could increase the percentage of success when identifying these attacks as well as a better future construction of research experiments.

There are many investigations that study phishing defenses and attacks. There are also many courses that focus in their computational technicalities. However, we argue that the best approach to teach computer science students about phishing and other social engineering attacks is with a course that combines the aforementioned three fields of study. We want students to learn about the psychological manipulation, or exploitation of emotions, scammers commonly look to include when they build their attacks. This can be done by studying real life cases of targeted communications (such as the ones described below) as well as famous cases of con-artists. We also want students to learn about the sociological vulnerabilities that social groups or user segments have.

From the sociological point of view, attackers can exploit multiple users at the same time by grouping them in segments. Users who share similar interests belong to a specific user segment and are susceptible to a specific type of attack. Our intentions are to instruct computer science students how to be able to identify a communication that intends to hide its true purpose using aspects from psychology and sociology. We also look to teach graduate and senior students how to conduct research about social engineering since it usually involves the deception of users as well as the avoidance of certain biases.

2. VULNERABILITIES TO DISCUSS

2.1 Computational

The computational vulnerabilities of phishing attacks are well understood by the community and computer science students. One could argue that the most notable characteristic of phishing attacks is that, most of the time, they do not require an in-depth technical knowledge for attackers to create them. In fact, nowadays anyone with access to a social network profile (e.g., Facebook, Twitter, Instagram) can manually generate a message to send as a phishing attack.

Our approach does not focus on the content of the phishing attack itself (i.e., the malicious content) but rather the communication (between sender and receiver) that leads to

[1]http://securityaffairs.co/wordpress/36922/cyber-crime/study-phishing-emails-response.html

the user trusting and, consequently, falling for the attack. As an example, [6] designs a targeted phishing to attack a social group (i.e., students from a university). They, however, only focus on the impact of a single attack and how many students fall for the attack. In our approach we study instead how phishing attacks can be automated to increase their scope and effectiveness and how attackers can automatically create different attacks for different social groups.

This brings us to a new set of approaches to study techniques adversaries could use to design better phishing attacks [7, 2]. Jakobsson et al. [7] study the feasibility of context-aware phishing where the adversary creates an online persona to manipulate the context of another online persona (i.e., the victim) so the user expects the attack. Sites such as Ebay offer a rich context that could help adversaries in the design of more effective phishing messages. As an example, adversaries can obtain the email address of a "currently winning" Ebay auctioneer then they can send them a congratulation email that falsely indicates the Ebayer as a winner of the auction. The email would contain a phishing attack that further obtains confidential information from the user.

As a different, but related, example the large-scale phishing on Indiana University [6] also uses online personas' context (email of their university) as part of the attack. We study the feasibility of the automation of two steps of this type of context-aware attack (1) its context-awareness or analysis of an online persona and (2) its automatic design or construction. Another experiment done by Ferguson [1] results that over 80% of cadets fall for phishing attacks if they are directed from a colonel. In this investigation, however, there are two factors that justify the high results of their attack. First, the attack was targeted because it was specifically designed to cadets that study in the same university as the colonel. Second, the sender has a higher degree of power than other experiments since he/she is not a peer of the receiver (as in [6]). These increase the trust the receiver has on the sender and thus the probabilities that the phishing attack is successful.

2.2 Sociological

In social sciences, it is common to talk about an interest-oriented action when they refer to the influence of interests in human beings. There seems to be a lot of discrepancy, however, in the discipline about the topic [9]. In contrast, other fields such as political and economical sciences assume that action is oriented primarily to pursue interests [11]. We can see each concept separately from the perspectives of the sender and receiver. From the sender's perspective we can argue there exists an interest-oriented action where the sender expects the receiver to act according to his or her interests. From the receiver's pespective we can argue the opposite because the receiver acts according to his or her interests.

It seems to be the case that a lot of questions arise in sociology when we talk about interests, primarily abouts the definition of "interests". In this investigation we define interests as any page that is liked by a user on Facebook. Therefore, as an example if a user likes a movie we say the user is interested on the movie. Moreover, he is also potentially interested in any movie that shares attributes (e.g., genre, producer, actors) with that movie. We can compare our work to a certain extent with Feld's [4] where he studies how social networks are inter-connected with activities, interactions, and sentiments. We study these networks from an interest-based perspective instead.

We argue that these sociological aspects are vulnerabilities social engineers could exploit in a large scale.

2.3 Psychological

There is some work proposed in [8] that studies the psychological or human side of phishing attacks to help users prevent future attacks. URLs are not, however, the only medium to steal information or place malicious code in phishing attacks. Phishers can also use, for example, attachments to attack users and thus it is necessary to defend against all possible mediums a phisher can use to steal information. Other psychological issues involved in phishing studies is correspondence bias and .

There has been many real-life cases where security experts can argue of invasion of privacy for marketing or business use. Perhaps the most infamous case about targeted advertising happened in 2012 when the company Target sent pregnancy advertisements by mail to a high school girl before her parents knew about her pregnancy [5]. Companies such as Facebook, Google, and Amazon use their users' data for target advertise them with their interests, hobbies, and passions. From these companies, Amazon has an advantage over their users with targeted advertisements since they have data on users' browse history and purchases of millions of items. Facebook and Google, however, also possess valuable data since we use Google for problem-solving, emails, and social networks (Google Plus) – all of which can be further used for the inference of users' interests.

It is unnecessary in today's world to explain what users often do with Facebook but it includes many social interactions human subjects do in real life plus some that only online social networks offer (e.g., liking photos or text, filling surveys, playing games, communicating with celebrities). Viewing someone's profile is the equivalent of browsing around 11 years (since Facebook was founded) of some of their online and real-life activities. In fact, people tend to forget the publicity of their online activities to the point were they say things they shouldn't say (e.g., political activism in countries where it is illegal, advertisement of illegal products and goods) and are later used against them [10, 3].

3. REFERENCES

[1] A.J., F. Fostering E-mail Security Awareness: The West Point Carronade. In *Educause Quarterly 1* (2005), pp. 54–57.

[2] Aycock, J., and Friess, N. Spam Zombies from Outer Space. In *EICAR* (2006), pp. 164–179.

[3] CNET. Facebook Scans Chats and Posts for Criminal Activity, 2012. `http://www.cnet.com/news/facebook-scans-chats-and-posts-for-criminal-activity/`.

[4] Feld, S. L. The Focused Organization of Social Ties. *American Journal of Sociology 86*, 5 (1981), 1015–1035.

[5] Forbes. How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did, 2012. `http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her`

[6] Jagatic, T. N., Johnson, N. A., Jakobsson, M., and Menczer, F. Social phishing. *Commun. ACM 50*, 10 (Oct. 2007), 94–100.

[7] Jakobsson, M. Modeling and Preventing Phishing Attacks. In *Proceedings of the 9th International Conference on Financial Cryptography and Data Security* (Berlin, Heidelberg, 2005), FC'05, Springer-Verlag, pp. 89–89.

[8] Liu, G., Xiang, G., Pendleton, B. A., Hong, J. I., and Liu, W. Smartening the crowds: Computational techniques for improving human verification to fight phishing scams. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (New York, NY, USA, 2011), SOUPS '11, ACM, pp. 8:1–8:13.

[9] Martinelli, A. Rational Choice and Sociology. In *Self, Social Structure, and Beliefs: Explorations in Sociology* (2004), 73 (5), pp. 82–102.

[10] Mashable. 8 Dumb Criminals Caught Through Facebook, 2012. `http://mashable.com/2012/12/12/crime-social-media/`.

[11] Uusitalo, L. Beyond self-interest: J. mansbridge (ed.), the university of chicago press, chicago, il, 1990. pp. 392. [uk pound]11.95 (pb.), [uk pound]42.50 (hb.). *Journal of Economic Psychology 12*, 3 (1991), 547–550.