Unpacking Warning Messages: Towards Mitigating Phishing Attacks

Joseph Aneke
Dipartimento di Informatica
Università di Bari Aldo Moro
via Orabona, 4 - 70125 Bari, Italy
joseph.aneke@uniba.it

Carmelo Ardito
Dipartimento di Informatica
Università di Bari Aldo Moro
via Orabona, 4 - 70125 Bari, Italy
carmelo.ardito@uniba.it

Guiseppe Desolda
Dipartimento di Informatica
Università di Bari Aldo Moro
via Orabona, 4 - 70125 Bari, Italy
guiseppe.desolda@uniba.it

***Abstract*— ICT services to citizens are commonly provided through websites. Unfortunately, these sites are often used by hackers to perpetrate phishing attacks against unwitting users. Phishing is a type of fraud designed to steal important sensitive information such as credit card numbers, passwords and bank account data. Despite the notable advances made in the last years by the active warning messages for phishing, this attack remains one of the most effective. In this paper we propose an intelligent warning message mechanism that might limit the effectiveness of phishing attacks and that increase the user awareness about related risks. It implements an intelligent behavior that, besides warning the users that a phishing attack is occurring, explains why the specific suspect site can be fraudulent, thus also acting as a training tool.**

Keywords — Cybersecurity, Phishing, human factors.

I. INTRODUCTION

Phishing is a fraudulent practice that includes an attempt by an attacker to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a dependable entity in an electronic communication. A common phishing attack is (for a phisher) to obtain a victim's authentication information corresponding to one website that is mimicked by the attacker and then use this at another site. This is a successful attack given that many users reuse passwords. Due to the risks associated with cyberattacks, it is crucial for Internet users to be aware of when they are being attacked and to be successfully informed on how to combat them. The recent demography results by Anti-Phishing Working Group 4th quarter report shows that around 45,794 phishing reports have been chronicled [1]. There is no single way or method that can prevent all types of phishing. But different methods applied at different stages of a phishing attack can abort the attempt and properly applied technology can significantly reduce the risk of identity theft [2].

The similarity property of phishing sites has made them difficult for humans to detect, but fortunately, easier for computers. However, the attacker community has proved itself able to quickly adapt to anti-phishing measures mainly warning messages. Different warning messages have been already evaluated during controlled experiments [3, 4]. Besides evaluating the efficacy of different solutions, these experiments provided useful indications on how to design and evaluate phishing warning messages. Despite the notable advances made in the last years by the active warning messages for phishing [3, 4], this attack remains one of the most effective. Indeed, algorithms for detecting phishing attacks are only able to determine the likelihood with which a website can be suspected but without absolute certainty. When the likelihood exceeds a critical threshold the warning messages alert the users about a possible risk and the users must decide to access or not the website. However, current warning messages have large room for improvement, as shown by the high success rate of phishing attacks reported in [5]. One of the first problems is the clickthrough effect [6]: the users tend to skip these alerts because they appear always in the same way, thus pushing most users in neglecting these messages. The second problem is the wrong design of the warning messages in term of colors, words, interaction, as underlined by [3, 4]. Lastly, the users are not experts in cybersecurity, they do not know what a phishing attack is and what are the risks they are exposed to [3]. In order to overcome these limitations, we propose an intelligent warning message mechanism aiming at limiting the effectiveness of phishing attacks and at increasing the user's awareness about related risks. It implements an intelligent behavior that, besides warning the users that a phishing attack is occurring, explains why the specific suspect site can be fraudulent. In smart-cities, Public Administrations and companies can take advantage of the use of smarter warning messages like the ones we propose. Indeed, spear phishing is a specific type of phishing attack where the emails are carefully designed to target particular users, which are often workers and employees of Public Administrations and companies.

II. A POLYMORPHIC USER INTERFACE AGAINST PHISHING ATTACKS

An example of the polymorphic user interface we propose to warn users about phishing attacks is reported in Fig. 2. In addition to addressing the design guidelines and lesson learnt in [3, 4], this prototype shows three panels that explain the reasons why the target website can be fake.

In this example, the panel on the left specifies that the URL of the target website (www.paypaI.com) looks similar to the original one but the "l" letter has been replaced by capital "I", thus confusing the users. The panel in the center reports that the suspect website was created three weeks ago, an age typical of phishing websites. The last box reports information about the HTTPS certificate of the suspect website, explaining that even if the "safe navigation" icon is shown in the browser toolbar, the certificate is self-signed, thus there is no guarantee that the site behavior is legitimate. It is worth remarking that the three panels show different information

according to the suspect website, thus different reasons would be reported with different phishing websites.
Thank to this intelligent warning message, we address three important goals, i.e.:

1. Prevent user habituation: a polymorphic message decreases the clickthrough effect caused by the user habituation [6];
2. Provide explanation about the attack: useful information about the causes of the phishing attacks support the users in deciding if the website is (or not) a phishing attack;
3. Train the users on cyberattacks and related risks: a long-term training of the users on phishing attacks is performed since they understand the reasons for this attack.

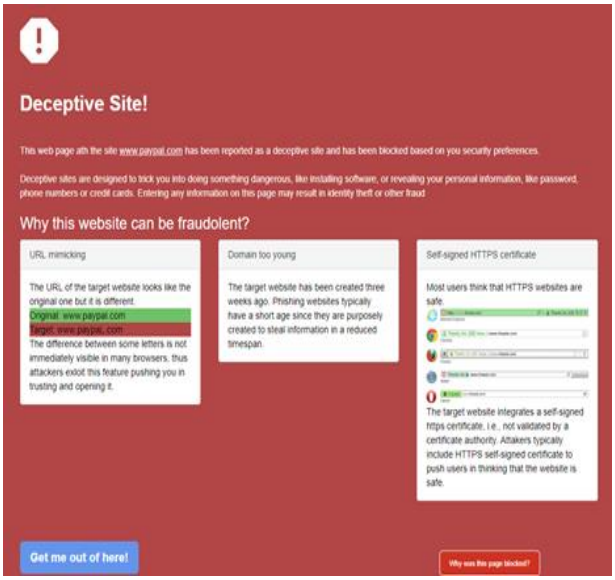

Figure 2. A Prototype of intelligent warning message for phishing attack.

In our approach, we start from the assumption that the browser can detect the phishing website through its internal algorithm, or that we use an API to detect malicious sites. Regardless of which of the two solutions we adopt, when a phishing website is detected, instead of displaying the traditional warning messages implemented in the browser, we show the intelligent UI proposed in this paper (see Fig. 2). To provide users with information that explain the reasons of the phishing attacks, our approach consists of two main steps, i.e., 1) the computation of a set of indicators that can reveal phishing websites and 2) the use of machine learning approaches to select the most important indicators. The three most important indicators will be shown and explained to the user, as shown in the example above.

In our work we are not interested to classify phishing websites, as this has been already addressed in the literature (see, for example, [7-9]). We start from the assumption that the browser can detect the phishing website through its internal algorithm, or that we use an API to detect malicious sites. Regardless of which of the two solutions we adopt, when a phishing website is detected, instead of displaying the traditional warning messages implemented in the browser, we show the intelligent UI proposed in this paper (see Fig.2).To provide users with information that explain the reasons of the phishing attacks, our approach consists of two main steps, i.e., 1) the computation of a set of indicators that can reveal phishing websites and 2) the use of machine learning approaches to select the most important indicators. The three most important indicators will be shown and explained to the user, as shown in the example above.

III. Conclusion

In this paper, we discussed the current trend of phishing attack from an HCI perspective. We aimed at revealing to the user some schema phishers use. We agree with [3] that users need to understand and use systems warnings correctly in order to guarantee the efficacy of any security strategy that has been implemented. An intelligent user interface is presented aimed at training users, improving the effectiveness of warning messages and prevent habitation.

Acknowledgment

This work is partially supported by the Italian Ministry of University and Research (MIUR) under grant PRIN 2017 “EMPATHY: Empowering People in dealing with internet of Things ecosystems”.

References

[1] APWG Anti Phishing Working Group. *Phishing Attack Trends Report - 4Q 2018*. 2018.

[2] Emigh, A. *Online identity theft: Phishing technology, chokepoints and countermeasures. ITTC Report on Online Identity Theft Technology and Counter measures*. 2014.

[3] Reeder, R.W., Felt, A.P., Consolvo, S., Malkin, N., Thompson, C., and Egelman, S.: ‘An Experience Sampling Study of User Reactions to Browser Warnings in the Field’. Proc. ACM SIGCHI Conference on Human Factors in Computing Systems (*CHI '18)*, 1-13.

[4] Egelman, S., Cranor, L.F., and Hong, J.: ‘You've been warned: an empirical study of the effectiveness of web browser phishing warnings’, in Editor (Ed.)^(Eds.): ‘Book You've been warned: an empirical study of the effectiveness of web browser phishing warnings’ (ACM, 2008, edn.), pp. 1065-1074

[5] IBM. *IBM X-Force Threat Intelligence Index 2018*.

[6] Felt, A.P., Ainslie, A., Reeder, R.W., Consolvo, S., Thyagaraja, S., Bettes, A., Harris, H., and Grimes, J.: ‘Improving SSL Warnings: Comprehension and Adherence’. Proc. ACM Conference on Human Factors in Computing Systems (*CHI '15)*, 2893-2902.

[7] Varshney, G., Misra, M., and Atrey, P.K.: ‘A survey and classification of web phishing detection schemes’, Security and Communication Networks, 2016, 9, (18), pp. 6266-6284.

[8] Abu-Nimeh, S., Nappa, D., Wang, X., and Nair, S.: ‘A comparison of machine learning techniques for phishing detection’. Proc. Anti-phishing working groups 2nd annual eCrime researchers summit (*eCrime '07)*, 60-69.

[9] Almomani, A., Gupta, B.B., Atawneh, S., Meulenberg, A., and Almomani, E.: ‘A Survey of Phishing Email Filtering Techniques’, IEEE Communications Surveys & Tutorials, 2013, 15, (4), pp. 2070-2090.