Towards Intelligent User Interfaces to Prevent Phishing Attacks

Joseph Aneke, Carmelo Ardito and Giuseppe Desolda
Università degli Studi di Bari Aldo Moro Via Orabona,
4 – 70125 – Bari, Italy
joseph.aneke@uniba.it, carmelo.ardito@uniba.it, giuseppe.desolda@uniba.it

Abstract

Phishing is a type of fraud designed to steal important sensitive information such as credit card numbers, passwords and bank account data. The fraudulent website is graphically very similar to the original one and invites the users to enter some personal information then used to steal the identity of the person who takes the scam. Other times, the website injects malicious code in the user's computer. 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 might 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.

Keywords

Usable Security · Intelligent User Interfaces · Cybersecurity.

How to cite this book chapter:
Aneke, J., Ardito, C. and Desolda, G. 2020. Towards Intelligent User Interfaces to Prevent Phishing Attacks. In: Loizides, F., Winckler, M., Chatterjee, U., Abdelnour-Nocera, J. and Parmaxi, A. (eds.) *Human Computer Interaction and Emerging Technologies: Adjunct Proceedings from the INTERACT 2019 Workshops*. Pp. 279–288. Cardiff: Cardiff University Press. DOI: https://doi.org/10.18573/book3.ak.

1 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 – whether in verbatim or with only slight changes. This attack is typically carried out by e-mail or instant messaging, and often directs users to enter details at a fake website [1]. A common example is "we need you to confirm your account details or we must shut your account down". The reason why an individual falls prey to this type of trap is that the message, which appears as the victim expects, and therefore legitimate, directs the user to visit fake webpages whose look and feel is similar or identical to the legitimate one. This phishing modality is also known as context-aware attack and is becoming increasingly common. Fig. 1 shows an example of a phishing attack sent to a user by email. The email appears genuine from a trusted sender, i.e. "uniba.it" which is the email service provider of the user. However, visualizing the details of the sender's identity reveals that it was masquerading to get the user to fill a form.

The effectiveness of phishing techniques, and more in general of cyberattacks, is not only related to the obsolescence of software and hardware. Federal Computer Week reports that almost 59% of security incidents that involve human errors are the result of simple mistakes as opposed to intentional malicious actions [2]. Hosteler found that human error is one of the first cause of cyberattacks (37%) [3]. Furthermore, the simplest and fastest way to start an attack is by means of phishing and social engineering attacks, where 91% of all cyberattacks starts with some kind of phishing email that manipulates users to provide sensitive information via various methods of social engineering [4].

Because of the risks associated with cyberattacks, it is crucial for Internet users to be aware of when they are being attacked and to be successfully

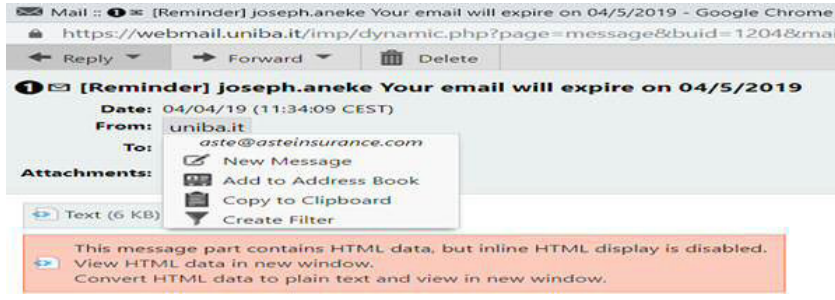

Fig. 1: Example of phishing attack sent by email.

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 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 [5]. Different approaches are already proposed to automatically detect phishing websites [6–8]. These methods and algorithms determine the likelihood that a website can be suspect but without absolute certainty. When the resulting likelihood exceeds a critical threshold, typically the users are informed about the potential risk of phishing attacks. This is done through a visual warning message that should help users in deciding to access or not the suspect website. Despite the significant advances of current warning messages, this attack still remain very effective since the users often is not able to take the right decision.

There is a direct need for us to design such a remedy which can address the above problem and stand out from the traditional warning messages available. In this paper, we report on an ongoing work about an intelligent warning message that might limit the effectiveness of phishing attacks and that might increase the user awareness about the related risks. The proposed solution implements an intelligent behavior that explains why the specific suspect site can be fraudulent. It is well-known that explaining the reasons about a fact helps the user being aware of the danger and taking more conscious and adequate decisions [9].

2 Literature Review

Successful security depends on systems, technology and people (including users) collaborating to identify threats, weaknesses, and solutions. However, many initiatives today focus on systems and technology, without addressing well-known user-related issues. In fact, users have been identified as one of the major security weaknesses in today's technologies, as they may be unaware that their behavior while interacting with a system may have security consequences. The user interface is where the human users interact with the computer systems. It is where the user's intention transforms into the system operation. It is where the semantic gap arises [10]. And this is the aspect that needs more attention to further limit the effectiveness of cyberattacks.

One typical anti-phishing approach is to use visual indicators, for example an informative toolbar, to differentiate legitimate messages from phishing messages [11]. This approach tries to bridge the semantic gap by unveiling to human users the system model and expects them to make a wise decision under phishing attacks. User studies in [12] show that the tested anti-phishing toolbars fail to effectively prevent high quality phishing attacks. Many subjects failed to constantly pay attention to the toolbar's messages; others disregarded the warnings shown in the toolbar if the web page content looked legitimate. The studies also

found that many subjects did not understand phishing attacks or realize how sophisticated such attacks can be.

In [13], the authors sought to determine if user's education was a possible solution to prevent phishing attacks. They explored the impact of both specific users' characteristics (age, gender, education, knowledge about phishing) and of their Internet usage habits on their ability to correctly identify e-mail messages. Quantitative data was collected by showing to participants e-mail messages and quizzing their ability to correctly categorize them. The results show the variables listed above did influence the participant's ability to correctly identify email messages.

A study to determine the impact that communicating to users different security policies has on mitigating phishing attacks is discussed in [8]. The research results reveal that a security policy that contains an explanation of the impact of an attack or a statement indicating an evaluation for non-compliance or a statement from a direct authority provides no significant impact on mitigating phishing attacks [14]. The use of online games to teach users good habits to help them avoid phishing attacks is investigated in [15]. The authors explore the relationship between demographics and phishing susceptibilities, and the effectiveness of several anti-phishing educational materials. Results suggest that women are more susceptible to phishing than men and participants between the ages of 18 and 25 are more likely to be a victim of a phishing attack than other age groups.

A new anti-phishing approach which uses training intervention for phishing web sites detection is discussed in [16]. The results of this work show that technical ability has minimal effect whereas phishing knowledge has a positive effect on phishing web site detection. A system called PhishGuru incorporating an embedded training methodology and learning science principles is proposed in [17]. Author evaluates the proposed methodology through laboratory and field studies. Results show that people trained with the proposed system retain knowledge even after 28 days. A major drawback is that the system will need to be trained and updated regularly. Robert W et al [18] found that web browser warnings should help protect people from malware, phishing, and network attacks. Adhering to these warnings keeps people safer online. They further demonstrated that recent improvements in warning designs have raised adherence rates, but they could still be higher. And prior work suggests many people still do not understand them. Thus, two challenges remain: increasing both comprehension and adherence rates. The authors in [18] suggested that further improvements to warnings will require solving a range of smaller contextual misunderstandings.

Most phishing sites are simply copies of real sites with the above mentioned feature slightly distorted or in some cases masqueraded [19]. This 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. Differ-

ent warning messages have been already evaluated during controlled experiments [18, 20]. 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 [18, 20], this attack remains one the most effective. Indeed, algorithms for detecting phishing attacks are only able to determine the likelihood with which a website can be suspect but without absolute certainty. When the likelihood exceeds a critical threshold the warning messages alert the users about a possible risk and the users have to 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 [21]. One of the first problems is the clickthrough effect [22]: 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 [18, 20]. 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 [18].

In order to overcome these limitations, in the following section we propose an intelligent warning message mechanism that might limit the effectiveness of phishing attacks and that might 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.

3 A Polymorphic User Interface to Warn Users about Phishing Attacks

An example of polymorphic user interface to warn users about phishing attacks is reported in Fig. 2. In addition to addressing the design guidelines and lesson learned proposed in [18, 20], this prototype shows three panels that explain the reasons why the target website can be a fake. In this example, the first panel specifies that the URL of the target website (www.paypaI.com) looks similar to the original one but the l has been replaced by capital I, thus confusing the users. The second panel 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 users see safe navigation in the browser toolbar, with a self-signed certificate they are not guaranteed 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.:

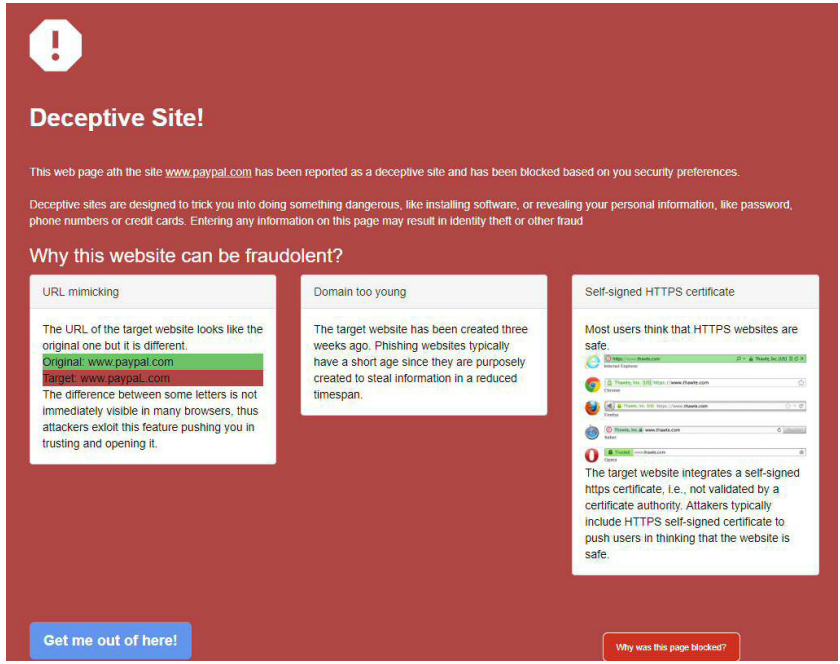

Fig. 2: A prototype of intelligent warning message for phishing attacks.

1. *Prevent user habituation*: a polymorphic message decreases the click-through effect caused by the user habituation [22];
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.

In our work we are not interested to classify phishing websites [6–8]. 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.[1] 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

[1] https://safebrowsing.google.com.

important indicators will be shown and explained to the user, as shown in the example above.

According to our goal and a literature review [6–8], we are considering indicators for the suspect web sites like:

- *URL*: phishing sites typically have URLs containing more than 2/3 number of digits or "-". In addition, they often try to mimic the original URL changing character that looks similar, for example, "l" with "I";
- *Server location*: phishing websites are often hosted by a web server located in countries where there are not strict laws against cyberattacks;
- *Alexa or search engine rank*: phishing website typically appear after the first 1 million Alexa top results, or in the last positions of search engines like Google Search;
- *Timelife*: this cyber-attack is usually concentrated in a limited time span, thus the suspect website is typically created few days/weeks before the attack;
- *Top level domain*: attackers typically use free domains to host phishing web sites; one of the most popular is freenom.com, thus domains like ".cf", ".gq", ".ml", ".tk" and ".ga" are common among phishing web sites;
- *Name length*: Attackers may create domains using a specific template, such as random strings of a given length;
- *Archived domain*: a domain archived on the "Wayback Machine" is more likely to be legitimately owned, and vice versa;
- *Self-signed https certificate*: the suspect websites often integrate a self-signed https certificate, i.e., not validated by a certification authority. Including this certificate, attackers confuse users who see safe navigation in the browser toolbar, but without any guarantee about the web site behaviour.

We defined different metrics to calculate each indicator for the suspect website. For example, Alexa rank can be obtained through its API; the Wayback Machine APIs are used to get information about website archiving; SSL certificate is inspected to see if a trustable certification authority signed it. Those indicators, resulting in a numeric value, are normalized in a 0–1 interval using a min-max function, with min and max values obtained calculating each indicator on all the phishing websites available in the *PhishTank* database and selecting for each indicator the min and max value.

After the computation of the indicators, we use a decision tree model to select the most important indicators. In particular, we adopted the C4.5 algorithm to generate our decision tree. This algorithm was developed by Ross Quinlan [23] and it is an extension of Quinlan's earlier ID3 algorithm. The decision trees generated by C4.5 can be used for classification, and in our case to classify the suspect website. However, we are not interested to understand if it is a phishing site, since we already know it. We only exploit this tree to select those three nodes that positively contribute in determining it as phishing. In other words, we use it to filter the indicators that are more influential in the classification process.

After the selection of the three most important indicators, we dynamically create three panels that are visualized in the warning message and properly adapted if necessary. For example, if a panel has to report the information on the URL, it is customized with the URL of the suspect website and the URL of the Website that is mimicked.

4 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 [18] 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.

Acknowledgments

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). Available at: http://docs.apwg.org/reports/apwg_trends_report_q4_2018.pdf
2. Thales: Insider Threat Report. Available at: https://go.thalesesecurity.com/ESG-Insider-Threat-WP.html
3. BakerHostetler: Is Your Organization Compromise Ready? 2016 Data Security Incident Response Report (2016). Available at: https://www.bakerlaw.com/files/uploads/Documents/Privacy/2016-Data-Security-Incident-Response-Report.pdf
4. Gupta, B.B., Tewari, A., Jain, A.K., Agrawal, D.P.: Fighting against phishing attacks: state of the art and future challenges. Neural Computing and Applications 28(12), pp. 3629–3654 (2017)
5. Emigh, A.: Online identity theft: Phishing technology, chokepoints and countermeasures. ITTC Report on Online Identity Theft Technology and Counter measures (2014). Available at: http://www.anti-phishing.org/Phishingdhs-report.pdf
6. Varshney, G., Misra, M., Atrey, P.K.: A survey and classification of web phishing detection schemes. Security and Communication Networks 9(18), pp. 6266–6284 (2016)

7. Abu-Nimeh, S., Nappa, D., Wang, X., Nair, S.: A comparison of machine learning techniques for phishing detection. In: Anti-phishing working groups 2nd annual eCrime researchers summit (eCrime '07). pp. 60–69. ACM, New York, NY, USA (2007)
8. Almomani, A., Gupta, B.B., Atawneh, S., Meulenberg, A., Almomani, E.: A Survey of Phishing Email Filtering Techniques. IEEE Communications Surveys & Tutorials 15(4), pp. 2070–2090 (2013)
9. Biran, O., Cotton, C.: Explanation and justification in machine learning: A survey. In: IJCAI-17 workshop on explainable AI (XAI '17), (2017)
10. Wu, M.: Fighting phishing at the user interface. Massachusetts Institute of Technology (2006)
11. Department of Justice Federal Bureau of Investigation: FBI Says Web Spoofing Scams Are a Growing Problem (2003). Available at: http://www.fbi.gov/pressrel/pressrel03/spoofing072103.htm
12. Wu, M., Miller, R.C., Garfinkel, S.L.: Do security toolbars actually prevent phishing attacks? In: ACM SIGCHI Conference on Human Factors in Computing Systems (CHI '06). pp. 601–610. ACM, New York, NY, USA (2006)
13. Martin, T.D.: Phishing for Answers: Exploring the Factors that Influence a Participant's Ability to Correctly Identify Email. Capella University, Minneapolis, MN (2008)
14. McNealy, J.E.: Angling for Phishers: Legislative Responses to Deceptive E-Mail. Communication Law & Policy 13(2), pp. 275–300 (2008)
15. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., Downs, J.: Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In: ACM SIGCHI Conference on Human Factors in Computing Systems (CHI '19). pp. 373–382. ACM, New York, NY, USA (2010)
16. Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M.A., Pham, T.: School of phish: a real-world evaluation of anti-phishing training. In: Symposium on Usable Privacy and Security (SOUPS '09). pp. 1–12. ACM, New York, NY, USA (2009)
17. Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F., Hong, J.: Teaching Johnny not to fall for phish. ACM Trans. Internet Technol. 10(2), pp. 1–31 (2010)
18. Reeder, R.W., Felt, A.P., Consolvo, S., Malkin, N., Thompson, C., Egelman, S.: An Experience Sampling Study of User Reactions to Browser Warnings in the Field. In: ACM SIGCHI Conference on Human Factors in Computing Systems (CHI '18). pp. 1–13. ACM, New York, NY, USA (2018)
19. Afroz, S., Greenstadt, R.: PhishZoo: Detecting Phishing Websites by Looking at Them. In: IEEE International Conference on Semantic Computing (ICSC '11). pp. 368–375, (2011)
20. Egelman, S., Cranor, L.F., Hong, J.: You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In: ACM

SIGCHI Conference on Human Factors in Computing Systems (CHI '08), Florence, Italy. pp. 1065–1074. ACM, New York, NY, USA (2008)
21. IBM: IBM X-Force Threat Intelligence Index 2018. Available at: https://microstrat.com/sites/default/files/security-ibm-security-solutions-wg-research-report-77014377usen-20180329.pdf
22. Felt, A.P., Ainslie, A., Reeder, R.W., Consolvo, S., Thyagaraja, S., Bettes, A., Harris, H., Grimes, J.: Improving SSL Warnings: Comprehension and Adherence. In: ACM Conference on Human Factors in Computing Systems (CHI '15). pp. 2893–2902. ACM, New York, NY, USA (2015)
23. Quinlan, J.R.: C4.5: programs for machine learning. Morgan Kaufmann Publishers Inc. (1993)