Alerting Users About Phishing Attacks

Giuseppe Desolda[1(✉)], Francesco Di Nocera[2], Lauren Ferro[3], Rosa Lanzilotti[1], Piero Maggi[2], and Andrea Marrella[3]

[1] Department of Computer Science, University of Bari Aldo Moro, Bari, Italy
{giuseppe.desolda, rosa.lanzilotti}@uniba.it
[2] Department of Psychology, University of Roma "La Sapienza", Rome, Italy
{dinocera, piero.maggi}@uniromal.it
[3] Department of Computer, Control, and Management Engineering, University of Roma "La Sapienza", Rome, Italy
{lsferro, marrella}@diag.uniromal.it

Abstract. Cyber attacks are emerging as problems caused not only by technological aspects but also by human factors neglected when designing interactive systems. In this paper, we show how one of the most popular attacks on the Web, phishing, is very much related to UI aspects and how a wrong UI design determines a greater vulnerability of users. We performed a heuristic evaluation to assess the most recent applications such as browsers and mail clients that adopt warning messages as prevention of phishing attacks. The results highlighted that different aspects of UI should be better designed to limit phishing attacks. In addition, as a prevention of cyber attacks, we described an ongoing work of a questionnaire that aims to make users aware of the risks of cyber attacks.

Keywords: Usable security · Cyber security · Phishing · Design patterns

1 Introduction

Cyber attacks are growing very much in recent years. According to the Symantec Annual Threat Report published for 2018, the total number of Web threats were more than 1 Billion, which was 400% more than in 2014 [29]. For example, in 2018 the number of new malware variants increased by 92%, the coinminer detection grew by 8500%, attacks against IoT devices increased by 600%, the malware variants in mobile devices increased by 54% and the number of new vulnerabilities increased by 13%. According to a new report by the Center for Strategic and International Studies (CSIS) and McAfee [21], cybercrime now costs the world almost $600 billion, or 0.8% of global GDP. This problem touches two-thirds of people who use online services (more than two billion individuals), of which have had their personal data stolen or compromised.

Despite these problems appearing to relate to obsolete technologies or to the scarce adoption of preventions (e.g., antivirus, firewall, etc.), close to 95% of all security incidents are due to human errors, as reported by the IBM latest Cyber Security Intelligence Index Report [17]. Wrong human behaviors can and have led to a range of issues from users becoming a victim of phishing attacks to the disclosure of sensitive information.

A. Moallem (Ed.): HCII 2019, LNCS 11594, pp. 134–148, 2019.
https://doi.org/10.1007/978-3-030-22351-9_9

The causes of these cyber attacks inevitably push HCI researchers, as well as companies, to investigate additional aspects related to users' vulnerabilities. Such areas include the user interface and user interaction, which are at the basis of these attacks. Therefore, if we can improve these areas, we can dramatically decrease the number of attacks, with obvious advantages for people, companies and any organization. Consequently, methods and methodologies defined by the HCI research to create successful and pleasurable interfaces must be revised in order to consider the security aspect.

The research work described in this paper focuses one of the most widespread attacks, i.e. phishing. Phishing is a technique used to collect personal information by and/or sending fraudulent emails that appear to be from a reputable or known source to users to induce them to reveal sensitive information (e.g. passwords, bank account details). Moreover, it is important to note that this is an attack that relies on exploiting people via carefully crafted social engineering campaigns. As a result, the dynamic nature of phishing attacks makes it difficult to implement algorithms that automatically detect phishing scams. Therefore, in case of suspicious phishing attacks, specific software (e.g. antivirus, alerts) and system tools (e.g. firewalls) use warnings to alert users. As demonstrated in [10], the design of warning notifications heavily affects the right identification of a phishing attack by users and, consequently, the system's security.

This paper describes an analysis performed on various applications that provide warning messages for phishing attacks to their users.

2 Related Work

The user interface has an influence on aspects of human behaviors, and thus, are the main causes of security incidents. A study conducted by 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 [30]. By analyzing more than 300 security incidents, Hosteler found that human error is one of the first cause of cyberattack (37%) [2]. Furthermore, the simplest and fastest way to start an attack is by means of phishing and social engineering attacks, where 91% of all cyber attacks start with some kind of phishing email that manipulates users to provide sensitive information via various methods of social engineering [14]. Because of the risks associated with cyber attacks, 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.

Usable security is a research area that in the last 10 year has been addressing such issues. Areas of password creation, demographic and workplace culture, security and trade-offs, and real-time assistance, all influence on a user's practice of good cybersecurity and ultimately contribute to their level of online security.

Security issues may increase also when technology is perceived as an obstacle. In such a case, the user may feel overwhelmed, or may not trust the warnings from the system, thus dismissing them [24]. In several contexts security tools are inherently complex, because they rely on knowledge of concepts such as cryptography, access keys, and digital signature. Therefore, securing a system may be not enough if users do not know how to properly use it. For example, firewalls, anti-viruses, and all the other

means to reduce vulnerabilities will protect the system as far as it has been activated and properly configured. Password management is a clear example of this tradeoff: strong but complex passwords are easily forgotten, whereas easy but weak passwords are easily remembered and, generally speaking, more convenient [18]. Usability of those systems is a critical security determinant [28] and can make the difference between system security and letting the user be the weakest link in system security [18]. This problem can be considered as a security-usability tradeoff, indeed, security and usability are perceived as mutually exclusive and the user is asked to tradeoff between them [5]. A user-centered approach to security design is therefore needed [23].

An additional area of consideration when it comes to phishing is how cybersecurity is perceived and practiced depending on the demographic and workplace culture of users. With the ubiquity that global offices afford, it is important to consider the cultural differences that influence the attitudes of users' security, especially when it comes to that of eastern and western culture and norms [6]. For example, the location of work environments that exist in areas that are more vulnerable to phishing scams (e.g. financial businesses) should be treated differently than those that are not given the different motivations and cultural aspects that are fueling attacks. In a study conducted by Henshel et al. [16] they explored the addition of a human factor component to Hofstede's [22] cultural dimensions. This sought to explore variations in cultural behavior among six dimensions and how to integrate them within the Human Factors Framework and Ontology to identify cybersecurity risk assessment metrics. The potential of a framework like this can greatly influence the design of solutions towards issues such as phishing since a one size fits all approach will only address a small part of a larger problem that requires tailored solutions. Hence, researchers can use this for modeling to facilitate additional experimentation. In addition, Henshel et al. assert that culture is a key factor with respect to the human element that has been understudied in cybersecurity risk literature and is key to enhancing and exploring areas of concern within cybersecurity of several fronts such as training, adversaries' cultural framework, and cyber defender/operator [27]. This same approach requires exploration within a workplace environment, given that work environments now are multicultural and thus contain a mix of individualistic and collectivist societal cultures (and various degrees between), which inevitably provide context for individual behaviors and norms for groups [27].

In addition to culture, many aspects of the user interfaces that can expose systems to vulnerabilities have been investigated. One of the most critical aspects regards the warning messages for phishing. Since this is a semantic attack that relies on confusing people, it is difficult to implement an algorithm to automatically detect these attacks [14]. Thus, in case of suspicious phishing attacks, tools use passive or active warnings to alert users to potential phishing sites. Passive indicators are typically implemented as toolbars in a web browser and show security-related information about a website to help users detect phishing attacks. However, they often fail because users do not notice them or do not trust them [33]. Active indicators, available in newest web browsers, typically are pop-up windows that force users to notice the warnings by interrupting their navigation. Even if they are more effective than passive approaches, as in [10], the design of warning message communicates the right identification of a phishing attack on users. A recent investigation [26] reports the results of a large-scale study on web

browser security warnings, which involved over 6,000 Chrome and Firefox users. They concluded that warnings of these browsers have improved that their effectiveness can be increased by examining contextual factors and a wider variety of users' concerns. Their results also suggest that habituation plays a smaller role in user decision making than previously thought. These results are in line with the one reported in [13] where 7,225 undergraduate students received (benign) phishing emails to elicit either the fear of losing something valuable (e.g., course registrations, tuition assistance) or the anticipation of gaining something desirable (e.g., iPad, gift card, social networks). The study results revealed that contextualizing messages to appeal to recipients' psychological weaknesses increased their susceptibility to phishing. The fear of losing or anticipation of gaining something valuable increased susceptibility to deception and vulnerability to phishing.

3 Analyzing Some Warnings in Current Applications

Many popular and recent applications like desktop browsers, mobile browsers or email clients nowadays include active phishing warnings. Despite in recent years important indications have emerged on how to improve such warning messages [10, 26], all of them still lack effectiveness, since phishing still remains the most widespread and effective cyber-attack [17, 21, 29].

In this section, we report on a review of some active warning messages implemented by the most popular Web browsers, both for PCs and mobile devices and by some email clients. In order to assess their effectiveness, we carried out an expert evaluation based on the heuristics reported in [10, 26].

3.1 Active Warning Messages Review

We started our review by analyzing three types of applications that implement warning messages for phishing attacks, i.e., desktop Web Browsers, mobile Web browsers and email clients.

Figure 1 reports four warning messages related to the desktop Web browsers we selected, i.e., *Google Chrome*, *Mozilla Firefox*, *Windows Edge* and *Opera*. All of them are active warning, i.e., when the browser detects a potential phishing site, instead of opening the Web page, it stops the users task flow by showing a message that reports information to help the users to decide if they can safely continue or if they have to return to the previous (safe) website.

The main differences between them are: the background color, the alert icon, the text of the message, the place/size/type of the button they must click on if they want to go on the phishing site. Regarding the background color, all of them, except Opera, use varying shades of red to warn the users about the potential fraud. In addition, the alert icon involves a different approach where all the browsers present different icons, which express a different meaning. For example, Google Chrome and Mozilla Firefox use two icons inspired by road symbols, a triangle containing an exclamation point and a circle having a horizontal bar, respectively. The last one appears to be stronger since it indicates a prohibition of access. MS Edge uses a rounded shield with an "X" inside it,

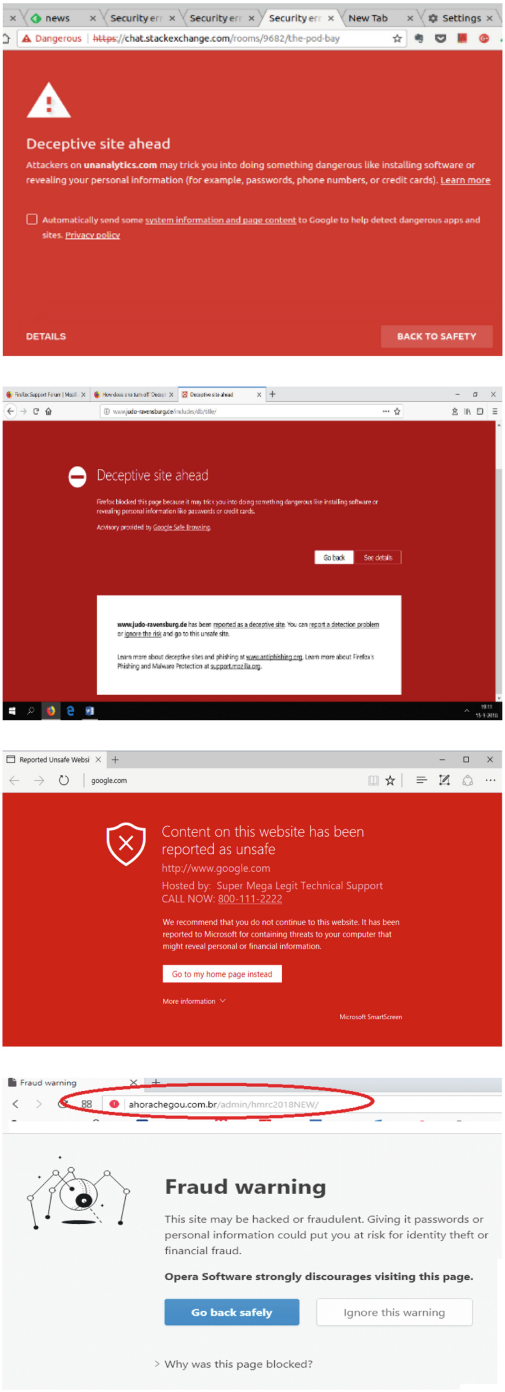

Fig. 1. Warning messages visualized by. (a) Google Chrome, (b) Mozilla Firefox, (c) Microsoft Edge, and (d) Opera. (Color figure online)

while Opera uses a robotic spider. All the messages also include a text reporting additional information about the alert, like the URL of the phishing site (the URL is missing in Opera) or what the consequences could be if the users land on to the phishing site. The last aspect is the button that the users must click on to open the phishing site. Except for Opera, all the warning messages hide this button inside a section that the users can reveal by clicking a button (Details, See details, Additional Information). In this way, it requires that the user takes the time to locate the button before accessing the potentially dangerous website.

Figure 2 shows the warning messages implemented by the browsers for mobile devices we chose, i.e., *Mobile Chrome*, *Opera Mobile*, *CM Browser*, *Internet Samsung*, *Edge mobile*, and *Firefox mobile*. Like desktop browsers, all of them implement active warnings and their peculiarities are the background color, the alert icon, the text of the message, the place/size/type of the link they must click in case they want to go on the phishing site. Only three of them, i.e., Mobile Chrome, CM Browser, and Firefox use a different shade of red as a background color. Mobile Chrome and Firefox do not use any icon to enrich the warning, while the other browsers visualize a triangle (or a circle in case of Internet Samsung) with an exclamation point inside. All the warnings also report additional information about the alert, like the URL of the phishing site (missing information in Mobile Chrome, Opera and Firefox mobile) or text explaining the risk to open a phishing site. The last aspect is the link the users must click on to open the phishing site. Mobile Chrome, Opera and Firefox mobile show this link in the main page, while the other browsers include it in a section that the users can reveal by clicking a button (Details, See details, Additional Information).

The last type of warning messages we considered are the ones of e-mail clients like *MS Outlook*, *Windows Mail app*, *Gmail*, and *Thunderbird,* which are shown in Fig. 3. Unlike the ones analyzed so far, these are passive warning messages, i.e., when the application detects a potential phishing email, it only shows a message, which informs the users that the email can contain suspicious content, like links or attachments. In this case, the main differences between them are the background color, the text of the message, the action the users can do on suspicious contents, the alert icon, and the place/size/type of the button they must click on if they trust the email.

Regarding the first aspect, different background colors are used, like light red on Outlook, orange on Windows mail app, light gray on Gmail and light gray on Thunderbird. The message texts always specify, in different ways, that the email has been detected as potentially unsafe. For example, Outlook says that all the suspicious content are disabled and that the users have to click on a link in the text if they want to enable such contents. The alert icon is used by Windows Mail app, Thunderbird and Gmail. The first two adopt a warning triangle with an exclamation point inside, while Gmail uses a hexagon with an exclamation point indicating the stop. Regarding the button the users must click on to activate the email content, except Gmail, all the warning messages show a link in the text message, while Gmail hides this link inside a section that the users can reveal by clicking the “View Details” button.

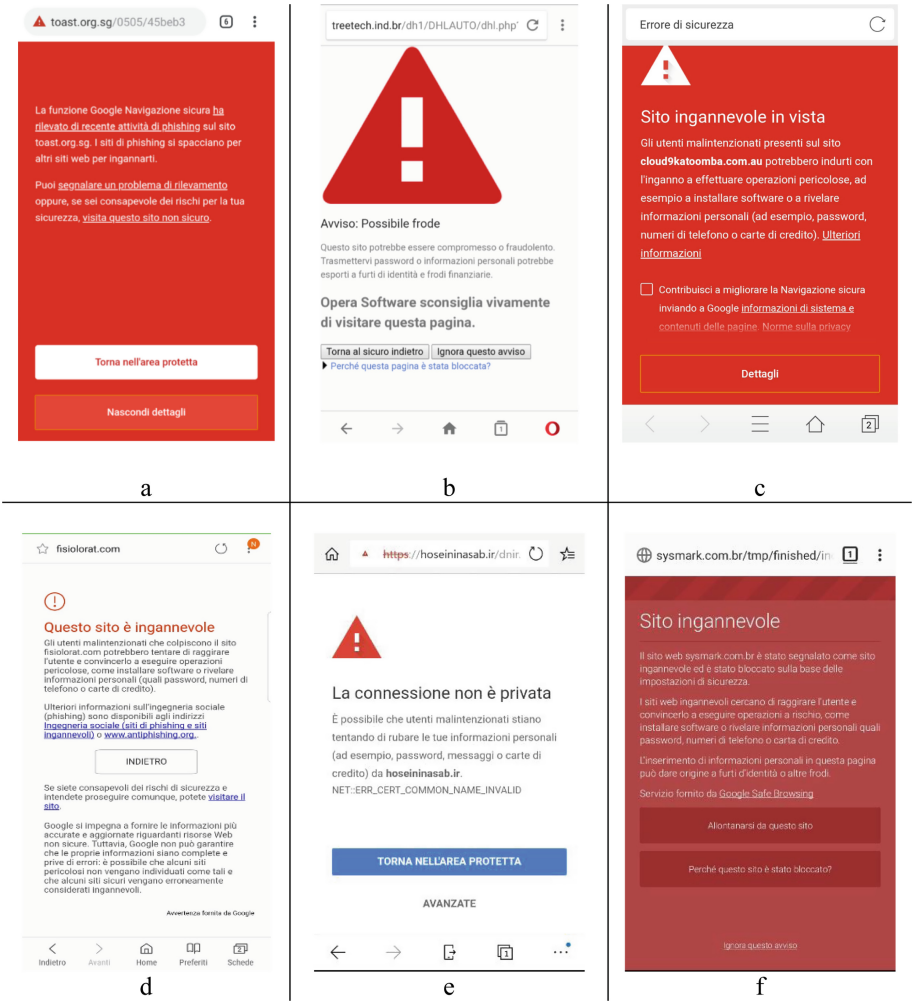

Fig. 2. Warning messages visualized by (a) Mobile Chrome, (b) Opera Mobile, (c) CM Browser, (d) Internet Samsung, (e) Edge mobile, and (f) Firefox mobile. (Color figure online)

3.2 Evaluation of Warning Messages

Different warning messages have been already evaluated during controlled experiments [10, 26]. Besides evaluating the efficacy of different solutions, these experiments provided useful indications on how to design and evaluate phishing warning messages. In this paper, given the large number of applications that we considered, rather than doing a controlled experiment, we performed a heuristic evaluation driven by the lessons learned distilled by the previous studies. The aim of our evaluation is to

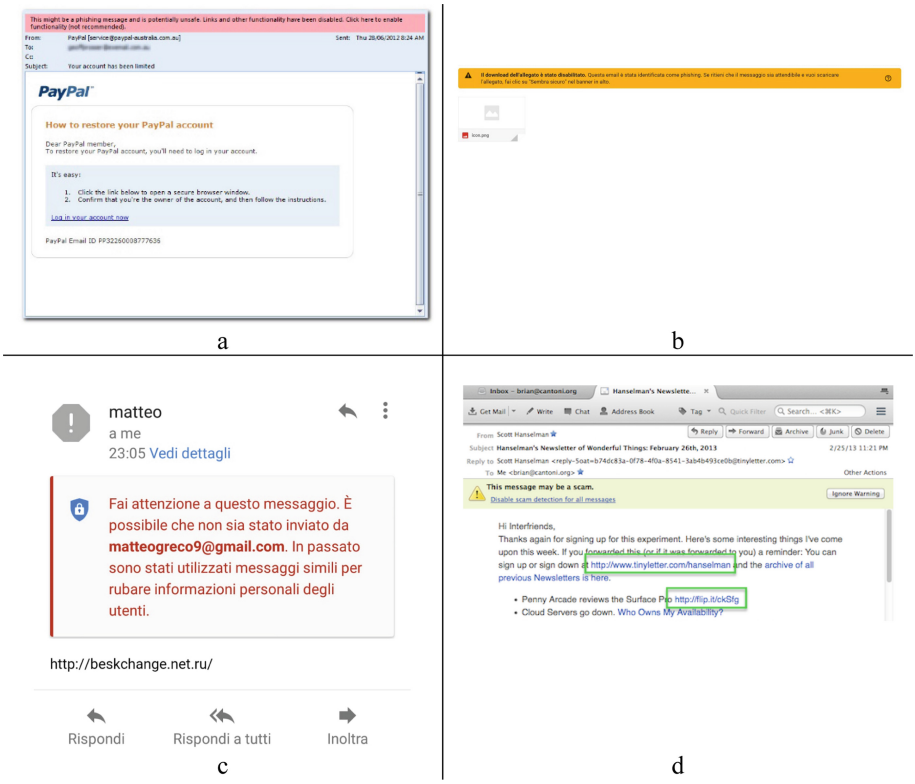

Fig. 3. Warning messages visualized by. (a) MS Outlook, (b) Windows Mail app, (c) Gmail, and (d) Thunderbird.

(*i*) assess the design of a broad spectrum of warning messages, and (*ii*) identify those aspects that still deserve even more attention. This evaluation was driven by two set of heuristics [10, 26]. In the following, we report the list of heuristics used by the evaluators, also specifying the paper they are related to:

1. *Providing clear choices* [10]—Phishing indicators need to provide the user with clear options on how to proceed, rather than simply displaying a block of text. For example, active warnings present choices and recommendations which were largely heeded.
2. *Failing safely* [10]—Phishing indicators must be designed so that users can only proceed to the phishing website after reading the warning message. For instance, active warning prevents users from accessing the page without reviewing the warning's recommendations.
3. *Preventing habituation* [10, 26]—Phishing indicators need to be distinguishable from less serious warnings and used only when there is a clear danger. Polymorphic messages can be adopted to minimize this factor.

4. *Altering the phishing website* [10]—Phishing indicators need to change the original look and feel of the website such that the user does not place trust in it. This can be accomplished by altering its look or simply not displaying it at all.
5. *Comprehension* [26]—Unfortunately, just because people make different choices when faced with the warning, it is not guaranteed that these are well-informed decisions.
6. *Site Reputation, History, and Trust* [26]—Participants' apparent willingness to proceed through a warning because they trust a site or have an account or visit history with a site may be in need of correction. It may help if warnings make it clearer that when a warning appears on a trusted site, it's a good time not to proceed.

A team of 5 HCI experts evaluated all the warning messages that are reported in Sect. 3.1. After an individual evaluation of all the messages, they discussed their results merging them in a single report summarized in Table 1. A discussion of the detected issues is reported in the following section, also including a proposal of three different warning messages, one for each type of application, that ideally satisfy all the heuristics considered.

Table 1. Report that summarizes all the identified problems. Each problem is described in term of severity, violated heuristic, details about the problem and a possible solution.

Application	Heuristic	Severity (1–5)	Problem	Possible solution
All applications	Preventing habituation	4	The error message is always the same	Change the message layout, text, without losing meaning
	Altering website	4	The applications do not change the look and feel of the website	The applications change the look and feel of the website
	Providing clear choices - Site reputation	3	The application does not show the URL of the mimicked site, sometimes only the URL of the fake site	The applications show both the URL so that the users can make more informed decisions by taking advantage of original site reputation
	Comprehension	3	The examples reported in the text are often too vague and general	More concrete examples can be reported, for example depending by the type of phishing site
Edge	Comprehension	3	Text of the message to come back to the previous and safe website is not so clear	Change this text by using a clearer text

(*continued*)

Table 1. (*continued*)

Application	Heuristic	Severity (1–5)	Problem	Possible solution
Opera desktop – Opera mobile	Site reputation	2	It does not allow to report false positive Web sites	A function to report false positive should be introduced
	Comprehension	5	The background color and the used icon are not adequate for this type of message	The background color should be changed by using the color red; the icon should be replaced with a more effective one
	Failing safely	5	It is possible to ignore the message without reading it. Indeed, the 'Ignore this warning' button is not adequately hidden. It also has the same emphasis of the 'Go back safely' button	The 'Ignore this warning' button should be placed in an internal section, for example in the one the users open by clicking on 'Why was this page blocked'. It should be also changed by using a link instead of a button, to reduce its importance
Opera mobile	Comprehension	4	The message layout and look and feel is very poor	A more professional look and feel can improve the credibility of the message
Internet Samsung	Comprehension	3	Too much information in the same screen, the users will be more prone to avoid reading the text	Short and optimize the text
	Comprehension	5	The background color is not adequate for this type of message	Use the color red as background
Edge mobile	Comprehension	5	The background color is not adequate for this type of message	Use the color red as background
	Comprehension	4	Technical details about the error message are shown and can confuse the users	Remove technical details, in order to speak a language closer to no-technical users
Firefox mobile	Failing safely	5	It is possible to ignore the message without reading it as for Opera browsers	Same suggestion of Opera browsers
All email clients	Failing safely	5	It is possible to ignore the message without reading it	When a phishing email is read, an active warning should be used
	Preventing habituation	5	Phishing indicators are not significantly distinguishable from less serious warnings	More emphasis should be given to these messages

3.3 Discussion

The heuristic evaluation highlighted that there is still much room for improvement to limit a greater number of phishing attacks with more effective warning messages. All the applications we analyzed share some problems.

Desktop browsers are mainly affected by these problems, but Opera also suffers from further critical issues, like the background color that appears not to effectively communicate a danger message, or, more importantly, the link to the phishing page has the same emphasis of the link to go back to the previous and safe site. This last aspect has proven to be crucial for this type of messages since users tend to read the warning messages quite fast and in-turn click on an option that seems more adapt to skip the message, like the button to go on.

Mobile browsers present further critical problems, beyond the ones that we have presented here. For example, Opera mobile has all the problems underlined for the desktop version, but in addition, it also presents a poor look&feel that reduces the users trust. The problem of the background color also affects Samsung Internet and Edge Mobile. In addition, Samsung Internet also reports a long text that can discourage the users in reading it and understand their risks, while Edge mobile shows technical details about the error message, which typically should be included in a hidden section to avoid confusing the users. Another critical problem was detected for Firefox mobile where, like the Opera browser, it is possible to ignore the message without reading it. This situation becomes more dramatic if we consider that most of the Internet access today take place by using mobile phone.

A more problematic situation was highlighted for the email clients. Indeed, all of them are passive warning messages, and it has been proven for over 10 years that they are not very effective for phishing attacks. In addition, their design is not adequate due to the adopted colors, text messages and icons.

In the following, we propose some design indications that could be useful for creating effective warning messages. Polymorphic messages are a solution that is strongly recommended to prevent users from habituation. If warning messages were visualized every time in a slightly different way, changing their content (e.g., the text) and their layout could result in the users being more likely to pay attention to what the message says without skipping it.

Another communal problem regards the information that guides the users in deciding if the suspicious site is dangerous. Users could decide easier if they can see both the URL of the mimicked site and the URL of the fake site, however, none of the applications adopts this strategy, showing only the fake URL. More significant and concrete examples could be used, eventually relate to the exploitation that the phishing attack is trying to initiate (e.g., data or money theft) rather than saying that the phishing site can steal personal data or money. In addition, pictures can be introduced to quickly explain the possible consequences of the attacks, because users often do not read text warning.

4 Toward a Questionnaire to Make Users Aware of Security Issues

Users' vulnerability to cyber-attacks, rather than a matter of tools and policies, is a matter of knowledge about the need of those tools and policies as well as the awareness about the possibilities of intrusions by hackers. This is demonstrated by several cybersecurity breaches (WannaCry ransomware affecting 150 countries is a recent

example) in contexts where tools and policies are highly implemented. These breaches rely on social engineering rather than computer science. Enhancing users' awareness and skills on cybersecurity may be a solution to effectively integrate tools and policies with the human factor. In a recent survey regarding the level of risk associated with home users, Furnell et al. [11] found that many responders still lack awareness about cyber-risks. In particular, IT novices, lack the knowledge to protect themselves from Cyber attacks despite they are aware of the fact that they are responsible for.

Empowering users by giving them a better understanding of security issues, possible threats, and how to avoid them is the goal of many intervention programs [7, 19]. This problem has been approached by the military, banking and financial industries and recently it became a priority in healthcare with the adoption of health information technology. Generally speaking, the protection of certain vulnerable groups, for example children, is a societal responsibility [32], but assessing vulnerability is also a crucial variable in cybersecurity research. This area of investigation, tough recognizing in many cases the role of the human factor, has almost exclusively considered demographic and personality factors. Although Rahim et al. [25] reported that the assessment of cybersecurity awareness is not new, to our knowledge no validated, recognized, and general purpose instrument exists for classifying users in terms of cybersecurity awareness.

Some authors of this paper are currently developing an inventory of behavioral markers of the vulnerability to Cyber attacks (CAIN: Cybersecurity Awareness INventory) in a form a questionnaire, which is aimed at investigating both general knowledge about cyber risks and knowledge about specific types of Cyber attacks (such as phishing emails). In this way, it will be possible to use it both in the public and in the private sector and possibly identify specific vulnerabilities. Self-report measures are easy to use, inexpensive, and very useful for obtaining meaningful information from the users that would be inaccessible otherwise. The rating scale will be used for classifying users and correlate the vulnerability score to behavioral outcomes and security threats.

CAIN items are based on scientific and technical literature as well as anecdotal evidence about risky situations for the users. Examples of items are: "My webcam can be accessed by a malicious user", "Permission I have granted to apps on my phone can be exploited by a malicious user", "I use different passwords for different accounts".

A preliminary version of the questionnaire will be administered to a large sample ($N > 300$) to assess its psychometric properties (reliability and validity). Data will be analyzed using factor analysis to understand whether the scale is mono- or multi-dimensional. The multi-dimensional nature of the questionnaire is very likely as people may cognitively represent threats and secure behaviors differently according to, for example, the type of technology (e.g. desktop vs. mobile). The final version of the questionnaire will retain only those items mostly contributing to the measure of the construct and to the overall reliability. To assess its validity, CAIN will be administered along with other measures in a series of experiments in which the user will face cybersecurity threats. People scoring high on cybersecurity awareness should perform significantly better than the others. This index should provide information about people awareness of cyber risks and about their skills in providing the correct behavior in risky situations. Users need to understand and use systems correctly in order to guarantee the

efficacy of any security strategy that has been implemented [11]. Moreover, the possibility to evaluate the level of knowledge and experience that the user has about cybersecurity issues is useful in many ways. In fact, this information could be used to set the right level of security within a system by forcing an inexperienced user to comply with certain protocols, which are necessary for the protection of sensitive information and, at the same time, allowing experienced users to interact with optimized and faster systems.

5 Conclusions and Future Work

In this article, we discussed the problem of cyber security from the perspective of HCI. In particular, we focused on phishing, one of the most effective and widespread cyber attacks that affect the majority of Internet users. We carried out a heuristic evaluation that revealed that warning phishing messages implemented in modern browsers and email clients still lacks in preventing phishing attacks. We also presented an ongoing work on a questionnaire that will make users more aware of the risks of the network.

One of the long-term goals of our research is to define a set of new behavior-based design patterns that support designers by providing indications on how to manage the interface design related to the security aspects. Design patterns have been used in different domains. In computer science, they have used in the design of computer systems of various types [15], including hypertext design [3, 12], e-learning systems design [1, 9], and interaction design [4, 31]. Some authors of this paper have defined a usability evaluation method that uses evaluation patterns [20]. Based on this expertise, a further long-term goal will be to identify evaluation patterns addressing usable security, for traditional systems and more advanced technological solution devoted to web exploration, like mobile cross-device interaction [8] or IoT.

Acknowledgements. The authors are members of ECoNA, an inter-university center for research and services. This collaboration started during the ECONA Workshop that was a Satellite Event of AVI 2018. The authors are grateful to Prof. Tiziana Catarci and Prof. Maria Francesca Costabile for their valuable and constant support.

References

1. Avgeriou, P., Papasalouros, A., Retalis, S., Skordalakis, M.: Towards a pattern language for learning management systems. Educ. Technol. Soc. **6**(2), 11–24 (2003)
2. Is Your Organization Compromise Ready? Data Security Incident Response Report (2016). https://www.bakerlaw.com/files/uploads/Documents/Privacy/2016-Data-Security-Incident-Response-Report.pdf. Accessed 30 Jan 2019
3. Bernstein, M.: Patterns of hypertext. In: Proceedings of ACM Conference on Hypertext and Hypermedia: Links, Objects, Time and Space (HYPERTEXT 1998). ACM, pp. 21–29 (1998)
4. Borchers, J.O.: A pattern approach to interaction design. AI Soc. **15**(4), 359–376 (2001)

5. Braz, C., Seffah, A., M'Raihi, D.: Designing a trade-off between usability and security: a metrics based-model. In: Baranauskas, C., Palanque, P., Abascal, J., Barbosa, S.D.J. (eds.) INTERACT 2007. LNCS, vol. 4663, pp. 114–126. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74800-7_9
6. Chang, C.-C., Hsueh, W.-Y., Cheng, T.-F.: An advanced anonymous and biometrics-based multi-server authentication scheme using smart cards. Int. J. Netw. Secur. **18**(6), 1010–1021 (2016)
7. de Bruijn, H., Janssen, M.: Building cybersecurity awareness: the need for evidence-based framing strategies. Govern. Inform. Q. **34**(1), 1–7 (2017)
8. Desolda, G., Ardito, C., Jetter, H.-C., Lanzilotti, R.: Exploring spatially-aware cross-device interaction techniques for mobile collaborative sensemaking. Int. J. Hum.-Comput. Stud. **122**, 1–20 (2019)
9. Dimitriadis, Y., Goodyear, P., Retalis, S.: Using e-learning design patterns to augment learners' experiences. Comput. Hum. Behav. **25**(5), 997–998 (2009)
10. Egelman, S., Cranor, L.F., Hong, J.: You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In: Proceedings of SIGCHI Conference on Human Factors in Computing Systems (CHI 2008). ACM, New York, pp. 1065–1074 (2008)
11. Furnell, S.M., Bryant, P., Phippen, A.D.: Assessing the security perceptions of personal internet users. Comput. Secur. **26**(5), 410–417 (2007)
12. Garzotto, F., Paolini, P., Schwabe, D.: HDM—a model-based approach to hypertext application design. ACM Trans. Inform. Syst. (TOIS) **11**(1), 1–26 (1993)
13. Goel, S., Williams, K., Dincelli, E.: Got phished? Internet security and human vulnerability. J. Assoc. Inform. Syst. **18**(1), 22 (2017)
14. Gupta, B.B., Tewari, A., Jain, A.K., Agrawal, D.P.: Fighting against phishing attacks: state of the art and future challenges. Neural Comput. Appl. **28**(12), 3629–3654 (2017)
15. Helm, R., Johnson, R.E., Gamma, E., Vlissides, J.: Design Patterns: Elements of Reusable Object-Oriented Software. Braille Jymico Incorporated, Quebec (2000)
16. Henshel, D., Sample, C., Cains, M., Hoffman, B.: Integrating cultural factors into human factors framework and ontology for cyber attackers. In: Nicholson, D. (ed.) Advances in Human Factors in Cybersecurity. Advances in Intelligent Systems and Computing, vol. 501, pp. 123–137. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-41932-9_11
17. IBM X-Force Threat Intelligence Index (2018). https://microstrat.com/sites/default/files/security-ibm-security-solutions-wg-research-report-77014377usen-20180329.pdf. Accessed 30 Jan 2019
18. Johnston, J., Eloff, J.H.P., Labuschagne, L.: Security and human computer interfaces. Comput. Secur. **22**(8), 675–684 (2003)
19. Kritzinger, E., von Solms, S.H.: Cyber security for home users: a new way of protection through awareness enforcement. Comput. Secur. **29**(8), 840–847 (2010)
20. Lanzilotti, R., Ardito, C., Costabile, M.F., De Angeli, A.: Do patterns help novice evaluators? A comparative study. Int. J. Hum.-Comput. Stud. **69**(1–2), 52–69 (2011)
21. The Economic Impact of Cybercrime—No Slowing Down Executive Summary. https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf. Accessed 30 Jan 2019
22. Mintu, A.T.: Cultures and organizations: software of the mind. J. Int. Bus. Stud. **23**, 362–365 (1992)
23. Muñoz-Arteaga, J., González, R.M., Martin, M.V., Vanderdonckt, J., Álvarez-Rodríguez, F.: A methodology for designing information security feedback based on user interface patterns. Adv. Eng. Softw. **40**(12), 1231–1241 (2009)

24. Pfleeger, S.L., Caputo, D.D.: Leveraging behavioral science to mitigate cyber security risk. Comput. Secur. **31**(4), 597–611 (2012)
25. Rahim, N.H.A., Hamid, S., Mat Kiah, M.L., Shamshirband, S., Furnell, S.: A systematic review of approaches to assessing cybersecurity awareness. Kybernetes **44**(4), 606–622 (2015)
26. 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: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI 2018), pp. 1–13. ACM, New York (2018)
27. Sample, C., Cowley, J., Hutchinson, S., Bakdash, J.: Culture + cyber: exploring the relationship. In: Nicholson, D. (ed.) AHFE 2017. AISC, vol. 593, pp. 185–196. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-60585-2_18
28. Schultz, E.E., Proctor, R.W., Lien, M.-C., Salvendy, G.: Usability and security an appraisal of usability issues in information security methods. Comput. Secur. **20**(2001), 620–634 (2001)
29. Symantec 2018 - Internet Security Threat Report. https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf. Accessed 30 Jan 2019
30. Insider Threat Report. https://go.thalesesecurity.com/ESG-Insider-Threat-WP.html. Accessed 30 Jan 2019
31. Tidwell, J.: Designing Interfaces: Patterns for Effective Interaction Design. O'Reilly Media, Inc., Newton (2010)
32. Von Solms, R., Van Niekerk, J.: From information security to cyber security. Comput. Secur. **38**, 97–102 (2013)
33. Wu, M., Miller, R.C., Garfinkel S.L.: Do security toolbars actually prevent phishing attacks? In: Proceedings of SIGCHI Conference on Human Factors in Computing Systems (CHI 2006), pp. 601–610. ACM, New York (2006)