ELEKTROTEHNIŠKI VESTNIK 87(1-2): 31–38, 2020
REVIEW SCIENTIFIC PAPER

A literature survey of security indicators in web browsers

Luka Jelovčan[1], **Simon L. R. Vrhovec**[1], **Anže Mihelič**[1,*]

[1] *University of Maribor, Faculty of Criminal Justice and Security*
Kotnikova 8, 1000 Ljubljana, Slovenia

[*] *E-mail: anze.mihelic@um.si*

Abstract. The web browser security indicators are one of the main tools helping users to identify fraudulent (e.g., phishing) websites. The research in detection of phishing websites focuses predominantly on automated solutions for blocking potentially harmful websites and only rarely considers other measures such as security indicators that help users to recognise phishing websites and human factors associated with them. To gather the key findings on the efficiency of the security indicators and human factors affecting it, a systematic survey of the literature in major scientific databases has been conducted. The survey reveals that the security indicators may help users to recognise the phishing websites, however, the users often fail to consider them while evaluating the websites' authenticity. The key potential factors are the lack of users' knowledge, poor design and inappropriate placement of the security indicators in web browsers. Additional challenges stem from searching for the balance between the visibility and discretion of the security indicators as an intrusive design or placement may induce the users' annoyance.

Keywords: security indicator, phishing, web browser, internet browser, fraudulent website, fake website, browser security

Pregled literature o varnostnih kazalnikih v spletnih brskalnikih

Varnostni kazalniki v spletnih brskalnikih spadajo med pomembnejša orodja, ki so v pomoč uporabnikom pri prepoznavi zlonamernih dejanj spletnih strani, kot je zvabljanje. Raziskave o prepoznavi tovrstnih strani se pretežno osredotočajo na rešitve za samodejno prepoznavanje potencialno škodljivih spletnih strani, redkeje pa na druge ukrepe, kot so varnostni kazalniki in z njimi povezani psihološki dejavniki. Da bi zbrali ključne ugotovitve o učinkovitosti varnostnih kazalnikov, smo izvedli sistematičen pregled literature. Ugotovitve kažejo, da varnostni kazalniki sicer pomagajo pri prepoznavanju potencialno škodljivih spletnih strani, vendar so uporabniki pogosto tisti, ki jih pri ocenjevanju legitimnosti pogosto spregledajo ali ne upoštevajo. Glavni dejavniki te težave so pomanjkanje znanja uporabnikov, slaba zasnova kazalnikov in njihova neprimerna postavitev v brskalnikih. Dodatni izzivi izvirajo iz iskanja ravnovesja med opaznostjo in diskretnostjo varnostnih kazalnikov, saj bi lahko vsiljivi zasnova in postavitev pri uporabnikih vzbudili nelagodje.

1 INTRODUCTION

Phishing attacks are on the rise again. The Anti-Phishing Working Group (APWG) [1], [2], [3], [4], [5] reports that there were 785,921 detected phishing websites in 2018, i. e. an almost 19 percent increase from 662,615 in 2017. Phishing is one of the most popular techniques used by online scammers and also one of the most costly for the company, as a single data record lost can cost a company up to $100 [6]. Fraudulent websites are a common component for phishing attacks that are comprised of two phases. In the e-mail phase, phishing e-mails are sent to the victims to lure them to a fraudulent website. In the website phase, victims are persuaded to submit their personal information to a fraudulent website. Victims may be particularly vulnerable to phishing websites if they do not pay a special attention to the website authenticity and especially when they are familiar with a certain website [7].

Our paper focuses on the efficiency of the security indicators in desktop web browsers for detecting fraudulent websites and human factors associated with them. The security indicators are the last line of defence that users have when deciding on the website authenticity [8]. If web browser users do not recognise a fraudulent website, they can give away their personal information to a potentially harmful entity. The focus of our survey is on the passive security indicators, as the active security indicators are directly related to an automated phishing detection of web browsers. The number of the detected phishing websites grows every year [1], [2], [3], [4], [5]. This is not necessarily a problem, as this could mean that users have learned to recognise phishing websites better. The problem is that the majority of detected

Received 28 November 2019
Accepted 7 January 2020

phishing websites is detected by trained individuals who then report the website to APWG [2]. Thus, we can assume that there are more phishing websites created every year. Also, unskilled users still fail to recognise them. Automated web browser solutions block up to 92 percents of the phishing websites that users open [9] and they seem to be effective. The problem appears to lie with users who fail to detect fraudulent websites by themselves and the security indicators which fail to help the users. Despite all measures, the users still fall victim to phishing websites. That is why our aim is to determine the state-of-the-art in the field of the security indicators' effectiveness and its impact on users. We also want to fill the gap in the literature since, to the best of our knowledge, our literature survey is the first focusing on the security indicators effectiveness in detecting phishing websites in web browsers and human factors associated with it.

In our survey, we examine research papers to determine the state-of-the-art of the security indicators effectiveness. For the survey to be comprehensive, the examined research papers are from different research areas approaching the issue from different perspectives as the security indicators in their current form appear to be ineffective. We also emphasize the deficiencies concerning the design of the security indicators and their placement in individual web browsers.

The paper is structured as follows. Section 2 provides a theoretical background. Section 3 presents the used methods. Section 4 presents results of our study. Section 5 provides a discussion with theoretical and practical implications. Section 6 draws conclusions.

2 Theoretical Background

2.1 Security indicators

The security indicators are present every time a user opens the web browser. However, an average internet user rarely notices them and may not understand their meaning [8], [10], [11], [12], [13]. The security indicators in web browsers are visual cues which help users to identify fraudulent websites. They are most often divided into two groups: passive and active security indicators. The passive security indicators indicate an impending danger by providing a certain textual information, changing colours, or through other means without interrupting the user's online activity, while the active security indicators force the user to take notice of the warnings by interrupting the user's main online activity [8].

Authors do not always agree, on which visual cues should be considered as the security indicators and which not, as different papers include different cues. In general, most authors consider three main cues as the security indicators: URL bar, https indicators (SSL/TLS) and digital certificate indicators. There are also some other indicators that users can take into consideration when determining the website authenticity, such as cipher selection [14], quality of the website content [15], extended validation (EV) certificates [16], [17], [18], favicon [16], [19] and certificate warnings [16].

2.2 Phishing websites

The main goal of using the security indicators is to inform the user if the website that he or she is visiting is fraudulent or not. The fraudulent websites are usually posing as legitimate online sources of information, goods, product and services [20], however, their main purpose is to prey on victims and propagate fraud [21]. An example of misusing the websites for a fraudulent purpose are phishing websites. The phishing websites have a similar look as the legitimate websites owned by organizations such as banks, credit unions, and governments. Phishers download pages of legitimate websites and modify some of their parts. In particular, they modify the elements that contain forms to be filled out by end users. These modifications cause victims to submit their information to repositories accessible by attackers [22]. Phishing attacks take advantage of the users' inability to distinguish the legitimate websites from the fraudulent ones [23]. Visually deceptive texts, images that mask the underlying text, windows that mask the underlying windows and deceptive looks are just a few clues that a website might not be trustworthy [10]. Bartoli et al. [24] propose a metric for a visual comparison of the similarity between a fraudulent website and its real version. Although fraudulent websites differ significantly from real websites, users may still find them sufficiently similar. They most often judge the website authenticity based on the websites content and not on other more relevant signs of authenticity [25]. Following the above, the conclusion is that users need some sort of help when judging the website authenticity.

3 Methods

Our systematic literature survey has been conducted to assess the effectiveness of the security indicators in their current form. We first determined the field of our interest, then defined our inclusion and exclusion criteria and finally collected the literature. Our literature survey took place between the 21st of March 2019 and the 19th of April 2019.

The research papers were searched in two databases: Web of Science and Scopus. The same combinations of the keywords were used in both databases. When choosing the keywords,the papers from two key research fields were targeted: the security indicators in web browsers and the user's detection of fraudulent websites. The following combinations of the keywords were used:

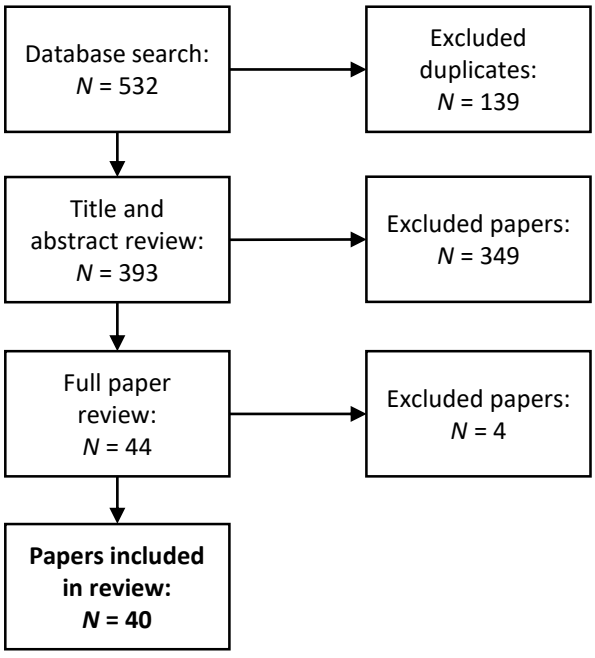
Table 1. Inclusion and exclusion criteria

Inclusion criteria	Exclusion criteria
Article is available in English	Article is not available in English
Article suits a chosen topic	Article does not suit the chosen topic
Article focuses on phishing websites	Article focuses on phishing e-mail
Article focuses on human factors	Article focuses on automatic anti-phishing mechanisms
Article focuses on desktop web browsers	Article focuses on mobile web browsers

web browser, security indicators; phishing, security indicators; website, security indicators; website, trust indicators; web browser, trust indicators; phishing, human behaviour; phishing, psychology; phishing, human factor. To from the keyword combinations, the Boolean operator OR was used. No other filters were chosen. Our search resulted in 532 papers combined (213 in Web of Science and 319 in Scopus). The papers not suiting our topic and the papers on automated mechanical solutions to detect phishing websites were excluded. Our inclusion and exclusion criteria are presented in Table 1.

After reviewing the titles and abstracts, 488 papers were excluded based on our exclusion criteria. Most of them failed to meet the human factors criterion. The abstracts of selected papers were then thoroughly examined and four more papers not meeting our inclusion criteria were excluded. Some papers propose automated solutions but were nevertheless included because they present findings on human factors and security indicators necessary for the development of automated solutions. As presented in Figure 1, 40 papers ($N = 40$) were included in our literature survey after full paper review.

Figure 1. Results of literature review



4 RESULTS

The results of our literature survey are given in Table 2. The source, methodology, sample size, and key findings of the papers included in the survey are presented.

Experiments made in a controlled environment show that the security indicators may have a positive impact on user's decisions [16], [15], [26], [27], however, not all the users use them to assess the website authenticity. The main problem is that users fail to consider them when judging the website authenticity [28], [16], [15], [10], [29], [30], [31], [32], [33], [34], [19]. The reasons for such behavior are several. First, users are not educated about the security indicators and therefore do not understand them [10], [11], [12], [8], [13]. Second, the familiarity with the website decreases the likelihood to check the security indicators [35]. Third, impulsive individuals show significantly less brain activity when assessing website authenticity and are thus less likely to check the security indicators [36].

Using the security indicators depends on the user's noticing and correctly interpreting them [37]. It is important to understand that because social engineering attacks take advantage of the predictable human behaviour and psychological triggers [38], users will be often asked to make security decisions against best-practice recommendations on security indicators [7]. Security is not the users' primary goal when browsing the internet [39], [13] and therefore users do not pay attention to the security indicators [37].

Another problem are the security indicators themselves as they are not designed properly to catch the users' attention [40], [25] and are easily spoofed [10], [41], [33]. Attackers who create phishing websites rely on building the trust, so that their victims believe that they are in contact with a trustworthy entity. The attackers might use tricks, persuasion, visceral influence, and/or any other technique to gain users' trust [42]. The problem with the security indicators is that they do not catch the users' attention if they are too subtle.

However, if they are too obtrusive, there is a risk that users will ignore the security altogether, either because they become annoyed or they grow too accustomed to the security indicators [40]. Performing additional security tasks does not improve the phishing website detection and leads to a greater annoyance [43]. Customization of the security indicators is one of the most

suggested solutions, but its efficiency is not clear as some studies suggest that customized security indicators better catch users' attention [44] and some do not [43]. Timing of displaying the security indicators is also an important option. A study suggests that users make different decisions depending on the timing a certain information is displayed [45].

5 Discussion

The users' assessment of the website authenticity should be smart and the security indicators are there to help. Or are they? With both the automated web browser solutions and visual clues for the website security identification, the users should be safer now than ever. Our survey reveals that the security indicators in their current form are not sufficiently effective. Although our study focuses on the effectiveness of the security indicators in web browsers, the conclusion we drew is similar to the ones in the surveyed literature covering a broader field of the security indicators [12], [17], [37], [46] associated with the human behaviour [11], [41], [46], design of the security indicators [13], [18], and user-indicator interaction [15], [10], [26], [36]. Our survey shows that not knowing and understanding the applied security indicators, as well as the inadequacy of their current design and placement in web browsers, are the main reasons for their inefficiency. Even though the users' factors in detecting the security indicators are thoroughly examined, the studies on how to make the security indicators more appealing and easier to understand for the user seem to be particularly scarce. There is no universal answer to how to make the security indicators more effective for everyone. As every user perceives a certain website differently than others, the only solution would be customization of the security indicators to meet the needs of every individual. In 2010, the World Wide Web Consortium (W3C) published the User Interface Guidelines [47] and set the guidelines for the security indicators implementation in web browsers. Even though in 2012 the security indicators in the desktop web browsers met most of these criteria [48], this research may be outdated due to the rapid evolution and development of web browsers in recent years and an update would be therefore beneficial. W3C has not published any new guideline since 2010 and it does not appear there is any other standard or guideline regarding the security indicators. Setting the standards and/or guidelines to implement the security indicators in web browsers should be one of the top priorities. This way, when users use different browsers on different devices, they also see the same security indicators and are thus not confused about their meaning. The standards should also guarantee that the displayed security indicators are created to be effective at catching the user's attention and helpful at the same time.

Even though the desktop web browsers are effective in automated detecting and blocking phishing websites [49], none of them has a perfect block rate. The security indicators serve as an assistance for users to distinguish between fraudulent and real websites. If automated mechanisms for detecting phishing websites fail, the security indicators are the last line of defence that users have. The research shows that the security indicators are effective when users take them into consideration [16], [15], [26], [27] but even at this point they may fail to make the right choice when faced with well-designed phishing websites in the vast majority of cases [10]. A single entry of a personal information can have serious consequences for the user. Because the security indicators are easy to falsify, users are likely to make wrong decisions even when considering them. Even if users are educated about the security indicators and take them into consideration when making their decisions about visiting a certain site, continuing their visit or even entering personal information, they cannot trust them completely since they may be faked. Even though the security indicators (as they are at this moment) are the only solution that helps users when judging the authenticity of a website, their low impact on the users' decisions and susceptibility to spoofing shows the need to start a debate about new forms of informing users about the potential threats.

This paper provides several useful theoretical and practical observations. First, our survey of different research papers combining and analysing various findings shows that security indicators are insufficiently effective. Several studies research the human factors affecting detection of the security indicators, however, the problem is not due to the users' lack of knowledge. Some studies [40], [25] suggest that the security indicators are not sufficiently well designed and thus fail at catching the users' attention. Second, the design of the security indicators is inadequately dealt with in the literature. The design and placement of the security indicators in web browsers is a largely unexplored field and needs to be examined to improve the security indicators' effectiveness. Also, there is no up-to-date recommendation or guideline that would set standards on the design and placement of the security indicators in the desktop web browsers. Third, there is a scarcity of research in effectiveness of the security indicators in specific web browsers. Since the design of the security indicators varies from browser to browser, it is important for users to know which browser to choose for the best results.

Our survey shows that the effect of the security indicators in web browsers is insufficient and therefore the reason why users fail to follow them. To our mind, the factors importantly affecting the users' decision-making are the users' familiarity with the website, users' knowledge about the security indicators and phishing, type

Table 2.: Literature review

Source	Methodology and sample size	Key findings
[42]	Systematic literature review	Establishing trust is very important for the attackers and users mostly rely on their experience and trusting the entity.
[28]	Experiment, 50/120 participants	Users are bad at recognising phishing websites. Most of them do not pay attention to security indicators.
[16]	User study, 21 participants	Users spend only 6% of their time looking at the security indicators when evaluating the website authenticity and 85% of their time at the website content. There is a positive correlation between the time spent looking at the security indicators and recognising the phishing websites.
[44]	Experiment, 62 participants	Users get habituated to security messages after constantly seeing them and start to ignore them.
[50]	Experiment, 19 participants	Users with a better computer knowledge look more at the security indicators. Those using a single sign-on are more vulnerable to phishing as they do not understand how it works.
[38]	Systematic literature review	Phishing takes the advantage of the predictable human responses to psychological triggers.
[51]	Experiment, 1201 / 811 participants	Users intolerant of a risk are more likely to recognise legitimate websites as phishing.
[15]	Experiment, 36 participants	90% of the users rely on the domain name as a legitimacy indicator of a website. The website design affects the user's decision in web browsers.
[10]	Experiment, 22 participants	23% of participants ignore the security indicators, which are easy to spoof. Users are bad at recognising phishing websites.
[41]	Systematic literature review	System designers should improve the security indicators because they are easy to spoof.
[45]	Experiment, 89 participants	Displaying the privacy indicators at a right moment has affects the users' decision to access the website.
[37]	Systematic literature review	Web browsers provide an insufficient defence mechanism against phishing. For the website security, it is important to acknowledge URL, padlock and HTTPS indicators.
[52]	Experiment	The security indicators alone are not enough to prevent phishing. The proposed new security indicators improve the phishing website detection rates.
[11]	Systematic literature review	Despite doubting about the website authenticity, users will access it, because they want benefit from it.
[29]	User study, 382 participants	Users ignore the security indicators. Spending more time to determine the website authenticity does not always mean they make better decision.
[7]	Experiment, 173 participants	The more the users are familiar with the website, the lesser is the possibility that they are going to check the security indicators. The knowledge of the security indicators increases the phished site recognition, while the familiarity with it decreases it. Users with a higher technical knowledge, are better at detecting the spoofed websites.
[30]	Experiment, 123 participants	EV certificate is the main trust indicator. When in a dilemma, users rather stay on the website than leave it.
[35]	Experiment, 173 participants	People with a security knowledge are more likely to acknowledge the security indicators. The security indicators can be misleading when an encryption is present on a faked website.
[12]	Systematic literature review	Education alone is not enough to prevent a phishing attack. Better user interfaces are needed for warning deliverance.

Source	Methodology and sample size	Key findings
[23]	Systematic literature review	The existing online anti-phishing training tools are not sufficient. The current practice of sending out a security notice is ineffective.
[43]	Experiment, 482 participants	Security images have a low impact on the users' choice to enter personal information. Performing additional tasks to log in does not lead to a significantly greater effectiveness but can lead to a greater annoyance.
[31]	Experiment, 24 participants	Users do not distinguish between different types of the certificates. Only 11% of the users know what certificates are.
[26]	Experiment, 23 participants	The average error when users only check the content is 32.4%, compared to 13.5% when they also check security indicators. The accuracy of the users' falling for phishing based on their eye movement is 79.3% accurate.
[27]	Experiment, 23 participants	Checking the address bar improves the users' recognition of the phishing websites.
[32]	Experiment, 100 participants	Users do not spend enough time looking at security indicators. Users may detect phishing attacks better if they are trained to exercise attention control.
[36]	Experiment, 25 participants	Users do not recognise the clues for the website authenticity. Malware warnings are more efficient than the security indicators.
[53]	Experiment, 275 participants	Vulnerability and perceived net benefit are the key factors when deciding whether to access a website.
[8]	User study, 137 participants	The security indicators' design is not intrusive enough. It should be placed into an immediate users' eye range or else it is not effective.
[39]	Systematic literature review	Neither the server-side security indicators nor the client-side toolbars and warnings are successful in preventing the vulnerable users from being deceived.
[33]	Experiment	The Web browser's security indicators are easy to spoof.
[17]	Systematic literature review	Users do not spot the security indicators. They are only cautious on the login site and not after it. When users know a website, they won't be cautious. They do not understand the security indicators, they find them confusing.
[34]	Experiment, 67 participants	Users enter their credentials despite the website's security indicators. Site-authentication images may cause users to disregard other important security indicators.
[54]	Experiment, 1001 participants	People who are aware of the risk, fall for less phishing websites. Educators need to teach users how to distinguish between real and fake websites.
[18]	User study, 15 participants	The security indicators visually fail to protect users from falling for phishing. Users expect the security indicators to be eye-catching but not obtrusive.
[40]	User study, 28 participants	The security indicators should take more place in the browser's chrome to be more effective.
[19]	Case study, 125 websites	Only five websites avoid all misleading security indicators. Users are being educated to ignore the security indicators.
[55]	Systematic literature review	Overconfidence, higher trust disposition, peripheral information processing and habits are the reason for falling for phishing. Anti-phishing education is not effective. Anti-phishing recommendations should be more specific for specific groups of users.
[25]	User study, 17 participants	Too much security can cause the website to be ineffective. The security indicator's design matters. Users find personalised indicators more trustworthy.
[46]	Systematic literature review	Users do not focus on URL enough.
[13]	Experiment, 30 participants	Users fail to continuously check the browser's security indicators, since maintaining the security is not the user's primary goal. Users do not know how to interpret signs of the security indicators.

of the users' personality, and visual presentation of the security indicators and their placement in a web browser. These factors should be taken into consideration when designing security indicators. Second, the insight into insufficient effectiveness of the current security indicators provides the basis for creating standards and guidelines for the design and placement of the security indicators in web browsers in order to increase the users' awareness of the importance of the efficient security indicators. The standards imposed on the design and placement of the security indicators in web browsers are important because of their generalising of the security indicators in different web browsers and thus reducing the confusion on the users' side when faced with the security-indicators issues.

6 Conclusion

A systematic literature survey is conducted to assess the effectiveness of the current security indicators in desktop web browsers. To the best of our knowledge, this is the first survey of this kind. It combines different approaches to the security indicators' effectiveness ranging from the psychological to neurological ones. The conclusion of our survey is that the security indicators in their current form are insufficiently effective because of their failure to draw the users' attention and, moreover, the users do not understand them. Also, as the security indicators are easy to fake, users can not absolutely rely on them when facing a potentially phishing website. In the literature, the design of the security indicators and their placement in specific web browsers does not seem to be of a great concern. Our future work should be towards improving the current state-of-the-art, i.e. to advance the web browsers security and the users' safety as well as to promote adoption of advanced standards responsive and adaptable to the current and evolving states in the field of the security indicators in desktop web browsers.

References

[1] Anti-Phishing Working Group, "Phishing Attack Trends Report - 1Q 2018," pp. 1–14, 2018.

[2] ——, "Phishing Attack Trends Report - 2Q 2018," pp. 1–9, 2018. [Online]. Available: https://docs.apwg.org//reports/apwg_trends_report_q2_2018.pdf

[3] ——, "Phishing Activity Trends Report 1st Half 2017," pp. 1–12, 2017. [Online]. Available: https://www.antiphishing.org/apwg-news-center/

[4] ——, "Phishing Attack Trends Report - 3Q 2018," pp. 1–11, 2018. [Online]. Available: https://docs.apwg.org//reports/apwg_trends_report_q3_2018.pdf

[5] ——, "Phishing Attack Trends Report - 4Q 2018," pp. 1–13, 2019. [Online]. Available: https://docs.apwg.org//reports/apwg_trends_report_q4_2018.pdf

[6] M. Korolov, "Report: average cost per record breached is 58 cents, discovery times are down," 2015. [Online]. Available: https://www.csoonline.com/article/2909613/report-average-cost-per-record-breached-is-58-cents-discovery-times-are-down.html

[7] T. Kelley and B. I. Bertenthal, "Tracking Risky Behavior On The Web: Distinguishing Between What Users 'Say' And 'Do'," in *Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015)*, no. HAISA, 2015, pp. 204–214.

[8] E. A. Oghenerukeybe, "Customers perception of security indicators in online banking sites in Nigeria," *Journal of Internet Banking and Commerce*, vol. 14, no. 1, 2009.

[9] M. Dhanraj and L. Rojo, "NSS Labs Web Browser Security Phishing Comparative Report," Tech. Rep., 2017.

[10] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Conference on Human Factors in Computing Systems - Proceedings*, no. April, 2006, pp. 581–590.

[11] A. E. Howe, I. Ray, M. Roberts, M. Urbanska, and Z. Byrne, "The psychology of security for the home computer user," in *Proceedings - IEEE Symposium on Security and Privacy*, 2012, pp. 209–223.

[12] M. Khonji, Y. Iraqi, and A. Jones, "Phishing detection: A literature survey," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 4, pp. 2091–2121, 2013.

[13] M. Wu, R. C. Miller, and S. L. Garfinkel, "Do security toolbars actually prevent phishing attacks?" in *Conference on Human Factors in Computing Systems - Proceedings*, 2006, pp. 601 – 610.

[14] C. Amrutkar, P. Traynor, and P. C. Van Oorschot, "An Empirical Evaluation of Security Indicators in Mobile Web Browsers," *IEEE Transactions on Mobile Computing*, vol. 14, no. 5, pp. 889–903, 2015.

[15] A. Darwish and E. Bataineh, "Eye tracking analysis of browser security indicators," in *2012 International Conference on Computer Systems and Industrial Informatics, ICCSII 2012*, 2012, pp. 1–6.

[16] M. Alsharnouby, F. Alaca, and S. Chiasson, "Why Phishing Still Works," *International Journal of Human-Computer Studies*, vol. 82, pp. 69–82, 2015.

[17] N. A. Rana and T. Hayajneh, "Reevaluating the effectiveness of visual cues for website security," in *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2017*, vol. January, 2018, pp. 451–457.

[18] P. Shi, H. Xu, and X. L. Zhang, "Informing security indicator design in web browsers," in *ACM International Conference Proceeding Series*, 2011, pp. 569–575.

[19] D. Stebila, "Reinforcing bad behaviour: the misuse of security indicators on popular websites," in *Proceedings of the 22nd Conference of the Computer- ...*, no. November, 2010, pp. 248–251. [Online]. Available: http://dl.acm.org/citation.cfm?id=1952275

[20] A. Abbasi and H. Chen, "A Comparison of Tools for Detecting Fake Websites," *Computer*, vol. 42, no. 10, pp. 78–86, 2009.

[21] M. Maktabar, A. Zainal, M. A. Maarof, and M. N. Kassim, "Content based fraudulent website detection using supervised machine learning techniques," *Advances in Intelligent Systems and Computing*, vol. 734, pp. 294–304, 2018.

[22] H. Shahriar and M. Zulkernine, "Trustworthiness testing of phishing websites: A behavior model-based approach," *Future Generation Computer Systems*, vol. 28, no. 8, pp. 1258–1271, 2012. [Online]. Available: http://dx.doi.org/10.1016/j.future.2011.02.001

[23] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching Johnny not to fall for phish," *ACM Transactions on Internet Technology*, vol. 10, no. 2, pp. 1–31, 2010.

[24] A. Bartoli, A. De Lorenzo, E. Medvet, and F. Tarlao, "How Phishing Pages Look Like?" *Cybernetics and Information Technologies*, vol. 18, no. 4, pp. 43–60, 2018.

[25] A. Tsow, Y.-K. Lim, M. Jakobsson, A. Shah, and E. Blevis, "What Instills Trust? A Qualitative Study of Phishing," *FINANCIAL CRYPTOGRAPHY AND DATA SECURITY*, vol. 4886, pp. 356–361, 2007.

[26] D. Miyamoto, G. Blanc, and Y. Kadobayashi, "Eye can tell: On the correlation between eye movement and phishing identification," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9491, pp. 223–232, 2015.

[27] D. Miyamoto, T. Iimura, G. Blanc, H. Tazaki, and Y. Kadobayashi, "EyeBit: Eye-Tracking Approach for Enforcing Phishing Prevention Habits," in *3rd International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, BADGERS 2014*, 2016, pp. 56–65.

[28] M. Aburrous, M. A. Hossain, K. Dahal, and F. Thabtah, "Experimental Case Studies for Investigating E-Banking Phishing Techniques and Attack Strategies," *Cognitive Computation*, vol. 2, no. 3, pp. 242–253, 2010.

[29] C. Iuga, J. R. Nurse, and A. Erola, "Baiting the hook: factors impacting susceptibility to phishing attacks," *Human-centric Computing and Information Sciences*, vol. 6, no. 1, 2016.

[30] T. Kelley, M. J. Amon, and B. I. Bertenthal, "Statistical models for predicting threat detection from human behavior," *Frontiers in Psychology*, vol. 9, no. APR, pp. 1–17, 2018.

[31] M. E. Maurer, A. De Luca, and T. Stockinger, "Shining chrome: Using web browser personas to enhance ssl certificate visualization," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6949 LNCS, no. PART 4, pp. 44–51, 2011.

[32] A. Neupane, M. L. Rahman, N. Saxena, and L. Hirshfield, "A Multi-Modal Neuro-Physiological Study of Phishing Detection and Malware Warnings," in *CCS'15: PROCEEDINGS OF THE 22ND ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY*, no. 1, 2015, pp. 479–491.

[33] S. Purkait, "Phishing counter measures and their effectiveness - Literature review," *Information Management and Computer Security*, vol. 20, no. 5, pp. 382–420, 2012.

[34] S. E. Schechter, R. Dhamija, A. Ozment, and I. Fischer, "The Emperor's New Security Indicators," in *2007 IEEE SYMPOSIUM ON SECURITY AND PRIVACY*, 2007, pp. 51–65.

[35] T. Kelley and B. I. Bertenthal, "Attention and Past Behavior, not Security Knowledge, Modulate Users' Decisions to Login to Insecure Websites," *Information and Computer Security*, vol. 24, no. 2, pp. 164–176, 2016.

[36] A. Neupane, N. Saxena, J. O. Maximo, and R. Kana, "Neural Markers of Cybersecurity: An fMRI Study of Phishing and Malware Warnings," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 1970–1983, 2016.

[37] A. Herzberg, "Why Johnny can't surf (safely)? Attacks and defenses for web users," *Computers and Security*, vol. 28, no. 1-2, pp. 63–71, 2009. [Online]. Available: http://dx.doi.org/10.1016/j.cose.2008.09.007

[38] N. Benias and A. P. Markopoulos, "Hacking the human: Exploiting primordial instincts," in *South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference, SEEDA_CECNSM 2018*, vol. 26, no. 4. TEI OF WESTERN MACEDONIA, 2018, pp. 1–6.

[39] S. Purkait, "Examining the effectiveness ofphishing filters against DNS based phishing attacks.pdf," *Information and Computer Security*, vol. 23, no. 3, pp. 333 – 346, 2015.

[40] J. Sobey, R. Biddle, P. C. Van Oorschot, and A. S. Patrick, "Exploring user reactions to new browser cues for extended validation certificates," in *13th European Symposium on Research in Computer Security*, vol. 5283 LNCS, 2008, pp. 411–427.

[41] X. Dong, J. A. Clark, and J. Jacob, "Modelling User-Phishing Interaction," in *2008 CONFERENCE ON HUMAN SYSTEM INTERACTIONS*, 2008, pp. 633 – 638.

[42] H. Abroshan, J. Devos, G. Poels, and E. Laermans, "Phishing Attacks Root Causes," in *12th International Conference on Risks and Security of Internet and Systems (CRISIS)*, vol. 10694. Springer International Publishing, 2018, pp. 35–40. [Online]. Available: http://link.springer.com/10.1007/978-3-319-76687-4

[43] J. Lee, L. Bauer, and M. L. Mazurek, "The effectiveness of security images in internet banking," *IEEE Internet Computing*, vol. 19, no. 1, pp. 54–62, 2015.

[44] B. B. Anderson, A. Vance, C. B. Kirwan, D. Eargle, and J. L. Jenkins, "How users perceive and respond to security messages: A NeuroIS research agenda and empirical study," *European Journal of Information Systems*, vol. 25, no. 4, pp. 364–390, 2016. [Online]. Available: http://dx.doi.org/10.1057/ejis.2015.21

[45] S. Egelman, J. Tsai, L. F. Cranor, and A. Acquisti, "Timing Is Everything? The Effects of Timing and Placement of Online Privacy Indicators," in *CHI2009: PROCEEDINGS OF THE 27TH ANNUAL CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS*, 2009, pp. 319 – 328.

[46] P. A. Watters, "Why do users trust the wrong messages? A behavioural model of phishing," in *2009 eCrime Researchers Summit, eCRIME '09*, 2009.

[47] T. Roessler and A. Saldhana, "Web Security Context: User Interface Guidelines," 2010. [Online]. Available: https://www.w3.org/TR/2010/REC-wsc-ui-20100812/

[48] C. Amrutkar, P. Traynor, and P. C. Van Oorschot, "Measuring SSL indicators on mobile browsers: Extended life, or end of the road?" *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, pp. 86–103, 2012.

[49] N. Virvilis, A. Mylonas, N. Tsalis, and D. Gritzalis, "Security Busters: Web browser security vs. rogue sites," *Computers and Security*, vol. 52, pp. 90–105, 2015. [Online]. Available: http://dx.doi.org/10.1016/j.cose.2015.04.009

[50] M. Arianezhad, L. J. Camp, T. Kelley, and D. Stebila, "Comparative eye tracking of experts and novices in web single sign-on," in *Proceedings of the 3rd ACM Conference on Data and Application Security and Privacy*, no. October, 2013, pp. 105 – 116.

[51] Y. Chen, I. YeckehZaare, and A. F. Zhang, "Real or bogus: Predicting susceptibility to phishing with economic experiments," *PLoS ONE*, vol. 13, no. 6, pp. 1–18, 2018.

[52] A. Herzberg and A. Jbara, "Security and identification indicators for browsers against spoofing and phishing attacks," *ACM Transactions on Internet Technology*, vol. 8, no. 4, pp. 1–36, 2008.

[53] K. D. Nguyen, H. Rosoff, and R. S. John, "Valuing information security from a phishing attack," *Journal of Cybersecurity*, vol. 3, no. 3, pp. 159–171, 2017.

[54] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions," in *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10*, 2010, p. 373. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1753326.1753383

[55] A. Tambe Ebot, "Using stage theorizing to make anti-phishing recommendations more effective," *Information and Computer Security*, vol. 26, no. 4, pp. 401–419, 2018.

Luka Jelovčan is an undergraduate student at Faculty of Criminal Justice and Security, University of Maribor. His research interest are in human factors in cybersecurity, cyber warfare, internet privacy and internet voting.

Simon L. R. Vrhovec is an Assistant Professor at the University of Maribor, Slovenia. He received his PhD degree in Computer and Information Science from the University of Ljubljana in 2015. He co-chaired the *Central European Cybersecurity Conference* (CECC) in 2018 and 2019. Since 2019, he is a steering committee member of the *European Interdisciplinary Cybersecurity Conference* (EICC) and a member of the *Journal of Cyber Security and Mobility* editorial board. His research interests are in human factors in cybersecurity, agile methods and secure software development, resistance to change, and medical informatics.

Anže Mihelič is a doctoral candidate at two faculties at the University of Ljubljana, Faculty of Computer and Information Science, and Faculty of Law. He is an Assistant at the University of Maribor, Faculty of Criminal Justice and Security, and a Researcher at the University of Hagen, Faculty of Mathematics and Computer Science. His primary interests include privacy law, social and psychological aspects of cybersecurity, secure software development with agile methods, and steganography.