NRC·CNRC

NRC Publications Archive
Archives des publications du CNRC

Understanding perceptions: user responses to browser warning messages

Molyneaux, Heather; Kondratova, Irina; Stobert, Elizabeth

For the publisher's version, please access the DOI link below./ Pour consulter la version de l'éditeur, utilisez le lien DOI ci-dessous.

Publisher's version / Version de l'éditeur:
https://doi.org/10.1007/978-3-030-22351-9_11
HCI for Cybersecurity, Privacy and Trust, pp. 164-175, 2019-06-12

NRC Publications Archive Record / Notice des Archives des publications du CNRC :
https://nrc-publications.canada.ca/eng/view/object/?id=97c3a514-69a0-47fe-a454-f96cc9383e2f
https://publications-cnrc.canada.ca/fra/voir/objet/?id=97c3a514-69a0-47fe-a454-f96cc9383e2f

Access and use of this website and the material on it are subject to the Terms and Conditions set forth at
https://nrc-publications.canada.ca/eng/copyright
READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE USING THIS WEBSITE.

L'accès à ce site Web et l'utilisation de son contenu sont assujettis aux conditions présentées dans le site
https://publications-cnrc.canada.ca/fra/droits
LISEZ CES CONDITIONS ATTENTIVEMENT AVANT D'UTILISER CE SITE WEB.

Questions? Contact the NRC Publications Archive team at PublicationsArchive-ArchivesPublications@nrc-cnrc.gc.ca. If you wish to email the authors directly, please see the first page of the publication for their contact information.

Vous avez des questions? Nous pouvons vous aider. Pour communiquer directement avec un auteur, consultez la première page de la revue dans laquelle son article a été publié afin de trouver ses coordonnées. Si vous n'arrivez pas à les repérer, communiquez avec nous à PublicationsArchive-ArchivesPublications@nrc-cnrc.gc.ca.

National Research Council Canada | Conseil national de recherches Canada

Canada

Understanding Perceptions: User responses to browser warning messages

Heather Molyneaux, Irina Kondratova, Elizabeth Stobert

National Research Council, Fredericton NB; Montreal QC

Heather.Molyneaux@nrc-cnrc.gc.ca; Irina.Kondratova@nrc-cnrc.gc.ca; Elizabeth.Stobert@nrc-cnrc.gc.ca

Abstract. With changes in interfaces resulting from the proliferation of IOT devices and new technologies such as self-driving vehicles, user reactions to browser messages may also change. This paper reviews the literature on user reactions to browser warnings, with emphasis on screen size and form factors. The literature indicates that browser warning message design, habituation, awareness of risk and screen size are aspects that effect user perception of risk. This article surveys the findings while noting challenges and proposed solutions to support effective provision of and user compliance with browser security warnings as well as important user study design considerations for future work – in particular, future work on the effect of screen size on user perception of browser warnings.

Keywords: survey; user studies; browser warnings; screen size; form factor; security

1 Introduction

User interfaces are changing. Screen sizes and form factors are, for the most part, shrinking. Smartphone use is growing for not only personal reasons but also for work tasks. Additionally, the proliferation of IOT devices and new technologies such as self-driving cars mean that in the future screens might change again to become larger, smaller or even nonexistent. How do these changes affect how warnings are presented to users? Do these warnings change how users view their own privacy and security? Do people react differently to the same warnings depending on the type of device and the size of the screens on which warnings are displayed? The answers to these questions could have direct implications in designing new interfaces for devices such as driverless cars, to determine appropriate screen sizes for warnings. This study investigates research studies on user perceptions towards browser warnings and outlines best practices for their design. As well, the design for a user evaluation to study screen size and form factor effects in user responses to browser warning messages is presented.

In order to understand the current research we examine the background literature on user reactions to browser warnings and security messages on mobile and desktop computers. There is a gap in the literature whereby the differences between user attitudes

towards browser warnings on mobile compared to desktop or laptop systems are not well examined. As a result, we draw upon the literature review in order to propose a study design that combines observations of any initial differences in a simple user task as well as a self-reported survey asking the same participants to reflect on their mobile vs. desktop and laptop browsing habits and their attitudes towards security and privacy on those devices.

1.1 Background

Improved browser warnings and security indicators can lead to users' improved ability to protect themselves against being cyberattacked online. Phishing and malware attacks are the most prevalent cyberattacks that affect users while Internet browsing, social networking, using online banking services or shopping online. "Phishing refers to use of deceptive computer-based means to trick individuals into disclosing sensitive personal information. Phishing attacks aid criminals in a wide range of illegal activities, including identity theft and fraud. They can also be used to install malware and attacker tools on a user's system" [{1]. Malware is defined by NIST [2] as "A program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system".

To prevent Internet users from falling victim to cybercriminal attacks, W3C's Web Security Context: User Interface Guidelines [3] have prescribed certain best practices for browser security indicators, such as the use of the TLS indicator (https) within the web browser's address bar to indicate secure website. They also give guidelines for designing security warning, caution and danger messages within the browsers, such as:

- Warning messages *must* interrupt the user's current task, such that the user has to acknowledge the message and provide the user with distinct options for how to proceed
- The options *must* be descriptive to the point that their respective meaning can be understood in the absence of any other information contained in the warning interaction
- Danger interactions *must* be presented in a way that makes it impossible for the user to go to or interact with the destination web site that caused the danger situation to occur, without first explicitly interacting with the message.

Borger et al. note that when designing computer warnings the following must be considered: risk needs to be described comprehensively; the warning must be concise and accurate; warnings need to offer users meaningful options; the relevant contextual information must be presented as well as relevant auditing information; and finally, the warning must follow a consistent layout [4].

Borger and colleagues found that browser warnings are an effective way to improve computer security; however there is a need for user studies with larger groups of participants to prove results and improve browser warning effectiveness. Our paper takes a closer look at how people perceive and respond to browser warnings, especially in

the context of limited screen space availability of the mobile world, in order to gather best practices and understand gaps to inform future user studies.

1.2 Methodology: A Subsection Sample

In order to investigate the effect of screen size users' perceptions and interactions with browser warnings, we conducted a literature search on the federal science library (FSL) database. The FSL database provides NRC researchers with access to over a thousand databases. Initial searches were conducted on the FSL database using the search terms "web browser" "warning" and "user." Search results were limited to only items from the last 10 years, including only scholarly material, peer reviewed publications and excluding newspaper articles, book reviews and dissertations. We further limited the results to only those containing user studies and evaluations. This resulted in an initial 16 relevant articles. Further articles were gathered and cited as a result of checking more recent articles citing the initial 16. In total 23 articles with user studies and evaluations are referenced in this paper.

Table 1. Studies included in the literature review.

Authors	Article	Date
Alsharnouby et al.	Why phishing still works: User strategies for combating phishing attacks	2015
Anderson et al.	Your memory is working against you: How eye tracking and memory explain habituation to security warnings	2016
Balebako et al.	The impact of timing on the salience of smartphone app privacy notices.	2015
Böhme & Köpsell	Trained to accept? A field experiment on consent dialogs.	2010
Carpenter, Zhu & Kolimi	Reducing online identity disclosure using warnings	2014
Dong, Clark & Jacob	Defending the weakest link: phishing websites detection by analyzing user behaviors	2010
Fagan et al.	A study of users' experiences and beliefs about software update messages	2015
Fagan et al.	How does this message make you feel? A study of user perspectives on software update/warning message design	2015
Herzberg & Ahmad	Security and identification indicators for browsers against spoofing and phishing attacks	2008
Iuga, Nurse & Erola	Baiting the hook: factors impacting susceptibility to phishing attacks	2016
Jorgensen, et al.	Dimensions of risk in mobile applications: A user study	2015

Junger, Montoya & Overink	Priming and warnings are not effective to prevent social engineering attacks	2017
Kelley & Bertenthal	Attention and past behavior, not security knowledge,, modulate users' decisions to login to insecure websites	2016
Mamonov, Renbunan-Fich	The impact of information security threat awareness on privacy-protective behaviors.	2018
Marforio et al.	Evaluation of personalized security indicators as an anti-phishing mechanism for smartphone applications	2016
Modic & Anderson	Reading this may harm your computer: the psychology of malware warnings	2014
Purkait, Kumar & Suar	An empirical investigation of the factors that influence internet user's ability to correctly identify a phishing website	2014
Redder et al.	An experience sampling study of user reactions to browser warnings in the field	2018
Redmiles et al.	Asking for a friend: evaluating response biases in security user studies.	2018
Schechter, et al.	The emperor's new security indicators: An evaluation of website authentication and the effect of role playing on usability studies	2007
Shah & Patil	Evaluating effectiveness of mobile browser security warnings	2016
Silic & Back	The dark side of social networking sites: understanding phishing risks	2016
Virvillis et al.	Mobile devices: A phisher's paradise	2014

2. Findings

Security and privacy are topics of interest to both computer security experts and novice computer users alike; Jorgenson and colleagues note that security experts and regular users of Android devices have similar concerns about safety and security. Personal information privacy – including personally identifying information, password and login credentials and financial information were seen as of the greatest concern, with general users more concerned about data integrity than monitoring risks [5]. However, it can be tricky for users to protect themselves against online risks. Virvilis and colleagues examined popular web browsers on IOS, Android and desktop systems (Windows platforms) visiting 1400 phishing and 1400 malicious URLs to see if browsers warned users of risk. They found most browsers offered limited protection against threats [6].

Even though many users are interested in protecting their own privacy and security online, users still have difficulty making decisions when faced with browser warnings, app permissions, and software update notifications. Below we summarize the findings

of user studies into four categories on how the following impact user behavior and beliefs about privacy and security alerts and measures: the role of browser warning messages and alert design; habituation; awareness; and screen size and form factor.

2.1 Browser warning messages and alerts: design

Why do participants ignore warnings? In a 2015 study Fagan et al. looked at self-reported ratings of software update messages and warnings. Participants were hesitant to apply updates even when reported they cared about security and privacy. A survey on their opinions and experiences with software was coupled with a study whereby users were shown images and asked to rate perception of aspects of the updates and warnings. Annoyance and confusion over update messages lead users towards non-compliance. Also the study found that the user's opinions of the software and vendors affected their decisions regarding applying an update messages [7].

Timing is an important factor in privacy notices and user recall – what the user remembers seeing and reading. Balebako and colleagues studied recall of privacy notice information as a proxy for participants' attention to and the salience of privacy notices. Participants were shown the privacy notice in the app store, at the startup of the app, during app use and afterwards. Those shown the notice during app use had overall increased recall rates [8].

Another avenue of research is examining how what the message say affects the user. Carpenter et al. found that warnings can be successful for countering user "mindlessness", which runs counter to some research indicating that warnings are not generally successful. In their study they found the wording of the warning made a difference; that the term "hazard" rather than "warning" or "caution" was the most effective wording of a warning message. They found that participants were less likely to disclose their driver license number than email address – perhaps due to heuristic, automatic compliance to a request, or "mindlessness" since people are used to revealing email address information online [9]. For future studies the researchers wonder "Are warnings equally effective in other cyber environments, such as smart phones? [9]"

How can the risks of privacy and security disclosures be mitigated? Two of the articles involved user studies with systems designed to complement existing detection systems. Herzberg and colleagues tested three conditions using the Trustbar browser extension – a certificate-derived identification indicator which is user-customized. Trustbar presents a highly visible indication of the security of websites which significantly improved user detection rates within the researchers' experiments [10].

Dong at al. used a user-based phishing system to complement existing anti-phishing solutions. The system alerts users who are about to submit credential information by monitoring user behavior. When users have never or rarely visited a site and the data being submitted is bound to a website other than the current one an alert is sent to the user. They found that their system could detect pharming attacks – attacks similar to

phishing, where DNS queries are interrupted, replacing legitimate websites with illegitimate versions designed to trick users into disclosing personal information - which were not detected by existing systems. Also their system fills a gap by alerting the user at the stage when they are at a phishing website and could potentially give out personal information. The researchers show that detecting phishing websites through user behavior is an accurate method which can be used to complement existing detection technologies, and their future work will involve user evaluation to inform future development [11].

2.2 Habituation

The role of habituation in user behaviors was a major theme in many of the findings of research papers examining user responses to browser warnings. Many users are accustomed to entering certain personal information on a daily basis for a variety of reasons, or are asked to consent to a variety of consent dialogs, such as end user license agreement (EULA) dialogues. When promoted for information in a way that seems familiar to them users may fill in personal information and consent without knowing first what they are consenting to, and how their information is going to be used.

In general when asked in a research study participants are quick to disclose personal information. Junger et al. surveyed 100 users in a medium sized town in the Netherlands, asking them to disclose their email information, list products recently purchased, the online shops they make these purchases at and the last 9 digits of their bank account. While only 43.3% disclosed the banking information, a high number of participants disclosed the other information even in the group that were primed not to give out personal information. Priming and warnings did not influence the degree to which participants disclosed personal information. Researchers found that the participants lacked knowledge about what constitutes sensitive information and how it can be used and abused by phishers [12].

Social networking sites (SNS) in particular are places in which users run a high risk of being phished. In their 2016 study Silic et al. directed employees to a fake website. Of the 180 visits the fake website, 122 employees filled in all personal information asked for, and an additional 15 filled in some information. The 15 who did not continue were contacted by email and stated that they felt there was an issue with the website (that the site was not a legitimate site). The researchers found that the “liking” influence technique was a strong incentive for people to reveal personal information, a strong first step in deception interaction They concluded that employees are vulnerable to SNS attacks, that organizations need better control over SNS security threats, SNS security policies need to be strengthened and with social engineering attacks SNS can be a security issue [13].

Böhme’s study on online privacy consent dialogs involved showing three type of warnings to 80,000 users. There were three conditions: a neutral condition, a polite request noting a voluntary decision and another condition resembling a typical end-user

license agreement (EULA). They found that being polite and asking for voluntary co-operation decreased the probability of users consenting, whereas the condition resembling a EULA saw higher rates of user acceptance. The researchers attribute this to habituation, noting that more than half the participants took less than 8 seconds – not enough time to read the message. They hypothesize that users are trained to automatically click on "accept" during interruptions typical of EULA – a finding that has repercussions not just with EULAs but also online safety and privacy. The researchers note the importance in interface design in order to prevent habituation of users [14].

However, not all of the research papers pointed to habituation as a major issue in user interactions with browser warnings. Reeder at al. sampled the decisions made by 6,000 Chrome and Firefox users using a browser extension and employing users via Amazon Mechanical Turk – a crowd sourcing marketplace. They found that while users mostly trusted warnings and that habituation was not a major issue, users relied on site reputation, which was a major factor in them proceeding through warnings on trusted sites. They also found that users sometimes downgraded protocols when faced with a warning – proceeding to the site via http when the https site gave them a browser warning [15].

2.3 Awareness

While some of the previously discussed studies noted that awareness of security issues did not seem to have any influence over users prone to habituation, several studies concerned with the susceptibility of users to phishing attacks were interested in seeing if awareness increased user resilience to phishing attacks. These studies had mixed results.

In Alsharnouby et al.'s study participants were asked to identify phishing websites. Only 53% of phishing websites were detected by participants even when users were primed to identify them. The study used eye tracking, and researchers found that users spent little time looking at security indicators – they mainly looked at the content of the website to make their assessment. Gaze time did not correlate with improved detection scores [16]/ The findings of this study seem to indicate that habituation (or at least trust of certain websites or content) has greater influence over user behaviors and opinions on suspicious sites than awareness of potential issues.

In an investigation of susceptibility to phishing attacks Iuga and colleagues examined demographics and ability to detect phishing attacks. They found in their study of 382 users only a small group of participants (25%) were able to detect phishing attacks at rates of 75% of the time or more. The average detection score was 65%, indicating that most people have a high risk of succumbing to phishing attacks. Their results suggest that the user's gender and years of PC usage have a statistically significant impact on the detection rate of phishing. They also found that pop-up phishing attacks have a higher success rate than other tested strategies; and that the psychological anchoring effect can be observed in phishing. The anchoring effect occurs when people rely on

the first piece of information they are presented with, creating cognitive bias. The researchers state that an approach combining detection tools, training and greater awareness could provide users with increased resistance to phishing attacks [17].

Purkait et al. conducted three experimental tasks and administered surveys in order to examine user awareness of phishing, safe internet practices, users' internet usage and internet skills, cognitive levels and demographic factor. Participants were users who were familiar with online banking and shopping tasks. They found that awareness of phishing had the highest positive effect. Internet skill surprisingly did not have a positive effect. They also found that there was a negative impact for those who used the internet frequently for financial activity, which led them to surmise that those who use the internet for online financial transactions tend to not notice the visual cues for phishing and might be more prone to habituation [18].

Mamonov and Benbunan-Fich examine ways in which users can be motivated to protect themselves from privacy and security threats. In an online experiment they exposed users to news stories about security breaches. Users exposed to such stories chose passwords 500x stronger than the control group, who were exposed to general technology news. The treatment group also limited their disclosure on answers to sensitive information within a survey – in particular questions on drug use, drinking and driving and support for the death penalty. Disclosure of non-sensitive information remained the same. This study suggests that "presenting users with narratives highlighting computer security threats may be an effective way to stimulate adherence to using strong passwords." [19]

Another potential avenue to increase user security could be through the deployment of personalized security indicators. As Marforio at al. note, personal indicators on mobile interfaces may be more effective than on PC platforms due to the simplified interfaces on mobile. They found that within their user study phishing attack success rates decreased 50% when adapting personalized security indicators [20].

Users may not even be aware of some currently employed security measures. In Their 2007 study Schechter et al. evaluated user groups' reactions to removing HTTPS indicators, removing the site-authentication image, and replacing the password entry page with a warning. They found that all participants, even in the user group using their own bank account information, ignored the HTTPS indicators and entered their information. In the second condition, with the site-authentication image removed, 92% of those using their own passwords still entered information. Even in the condition where a warning was presented, 36% present of participants still entered their own password information [21].

These articles suggest that greater awareness of phishing threats, through training, or the necessity of stronger passwords could, in conjunction with other methods, such as detection tools, build user resilience to security and privacy threats. Also the narratives and imagery used to deliver training and present alerts are important tools not only to increase awareness but all combat habituation. At the same time, there are specific challenges to training itself – how and when the training is delivered is as important as

the content of that training. There also is a need to be studies of training design and outcomes.

2.4 Screen size and form factor

In addition to human factors that influence the effectiveness of browser security warnings and user compliance, such as user's attention, technical knowledge, past behavior, warning message design, social influence, and memory habituation [22, 23, 24, 25], there some additional factors at play, such as screen size and form factor.

Most of the studies reviewed here are concerned with user interaction on desktop and laptop computers. But the importance of smaller devices, such as smartphones, and user awareness of security risk is a growing concern for cybersecurity researchers. Bitton et al. note that security awareness of personal computers is higher than mobile platform awareness levels, and mobile users require a different set of security awareness skills than those needed for PC [26] At the same time, Goel and Jain note thatusers on mobile devices are three times more vulnerable to phishing attacks. This could be due to a variety of considerations including the smaller screen, awareness issues and lack of user input. Separate techniques are needed to avoid privacy and security attacks on mobile devices [27].

Research demonstrates that the browsers on mobile devices are more limited in availability and visibility of browser security indicators and warnings due to several reasons, including the screen size due to form factor limitations; mobile devices having more limited screen size compared to desktop or laptop computers [28, 29]. For example, in mobile browsers sometimes the edges of pop-ups can extend beyond the side of the display, or buttons can overlap text.

Previous studies of screen size and usability indicate that when the user performs complex tasks, the diminished screen size leads to lower efficiency. Larger device screen sizes are deemed more efficient for information seeking tasks [30]. However, smartphones are increasingly being used for working on the go and social activities, tasks which sometimes require web browsing. With an increase in the use of smartphones for web browsing tasks which involve personal information, such as on SNS sites or financial information, such as online banking, portable devices with smaller screens are becoming more of a target for phishing attacks. Such attacks can lead to identify theft, fraud, and even the installation of malware. Such activities are obfuscated to the user, and due to the limited capacity of some smaller smartphone devices, appropriate countermeasures may not be installed, rendering the user vulnerable.

Research studies indicate that security and privacy can be seen as more of an issue on the smaller screen than a larger screen. In Chin and colleagues' 2012 study of 60 smartphone users it was found that users were more concerned about privacy and connecting to sensitive information on the smartphone compared to a laptop or a desktop, because of fear of physical loss or damage to the device. The users also had concerns over user interface accidents (such as making accidental online purchases), as well as

concerns related to the perception of limited security and privacy properties of their phone [31].

3. Discussion

Researchers note that education and training to increase awareness of security and privacy risks is not enough; software solutions are also necessary [27]. For future work Jorgensen et al. call for an evaluation and development of new risk communication methods– more specifically interfaces that allow users to quickly and accurately assess the security and privacy risks of downloading apps for Android devices [5].

Researchers also highlight the need for increased user studies. User studies are far from straightforward: ecological validity is paramount but ethical issues arise when studying users using their own devices and personal information in real world situations. In lab studies the ethical implications are more limited, especially when users are not using their personal devices or personal data, but in lab settings users are particularly primed for awareness. Redmiles at al. state several benefits and biases of self-reported data in the security field. Self-reported measures, most commonly surveys, are characterized by the ease of which information is collected, the control researchers have over the study and the depth of understanding which can be achieved via user responses. However there are many potential biases inherent in self-reported measures, including users having difficulty remembering past events, as well as users shaping their own answers in order to meet perceived expectations of the audience (i.e. the researchers) [32]. In self-reported accounts of security behaviors, instances of phishing attacks can also be underreported, as users may not even be aware that they have fallen for phishing attacks in the past.

In their study Redmiles and colleagues compared real world behaviors to survey results. They found a systematic relationship between the self-reported data and the real world scenarios which only really "breaks down when survey respondents are required to notice and act on minor details of experimental manipulations." Specific insights are difficult to access within self-reported surveys. The data from the surveys closely mirrored the measurement data but users were prone to over report good behaviors. Attention for message details was more difficult to capture in surveys than real life. The researchers suggest that more security studies should involve interview-facilitated data collection, A/B testing, field observations or lab-observation hybrids [32]. Schechter et al. also note that participants using their own personal account information compared to those given assigned information will be more mindful of security issued in studies, indicating a need for study measures not just following role play participation but also asking questions about real world scenarios [21]. However, having participants use their own personal information in studies puts the participants at greater risk – an ethical complication.

Context also makes a big difference in security studies. Some users might be aware of and responsive to security threats in some areas and not others. Researchers noted that while employees are generally trained on security threats there is a need for better

training and awareness of the security threats SNS pose to employees and companies [13].

4. Future Work

The articles we reviewed raised a variety of issues about privacy and security that could shape future work concerning user behavior on smaller screens, like smartphones, compared to larger screens of laptops and desktops. For example, are users more likely to disclose personal information on their smartphone or using a desktop or laptop? Are users more likely or less likely to engage in financial tasks, like banking and online shopping, on their desktop than the phone, and are users more prone to dismiss browser warnings on smaller screens like mobile phones compared to larger screens?

More work needs to be done in order to examine if users have different security habits on different form factors. Do they feel different devices have different levels of security and how does that affect their own use of the devices? How do users react to security warnings on smaller screen compared to larger screened devices? And what is the role of design, habituation, and awareness on user perceptions of security on the different form factors?

In order to investigate these questions we constructed a research plan that includes observing users' browsing habits in lab during two role-playing tasks, one involving a smartphone and the other involving a laptop. Users will be directed to a website and a researcher will have them think aloud while they complete a task using each of the devices. The researcher will record the actions of the user while paying close attention to what the user does when faced with a browser notification. Afterwards data will be collected about the users' regular smartphone and laptop browsing habits as well as some questions about the task they just completed.

We coupled the task with the survey to encourage the participants to think about how they react to (or are habituated to ignore) different notices on websites in their everyday browsing. Findings from the survey will give us greater insight into what sort of tasks they do as well as their own perceptions of browser warnings on both smaller and larger screens when they are using their own devices in a real world setting.

5. Conclusions

When examining the relationship between the device form factor and user responses to security and privacy warnings, many factors must be considered, including users' past experience with various device form factors, their online habits for each type of the device, and their perceptions of privacy and security in general.

In order to examine users' reactions to browser warnings and gather self-reported measures of users' experiences with browser warnings on smart phones as well as desktop and laptop computers, our future work will involve a user study with multiple user data collection measures, including a two condition task study followed by a survey on users' past practices and experiences. The study will generate new knowledge on users' online behaviors and develop design recommendations to improve the effectiveness of security warnings on mobile devices.

Relatively little attention has been devoted to studying the effect of screen size and the device form factor on users' responses to security warnings. Our future studies will work towards filling this gap.

References

1. Mell, P., Kent, K., & Nusbaum, J. (2005). Guide to malware incident prevention and handling (pp. 800-83). Gaithersburg, Maryland: US Department of Commerce, Technology Administration, National Institute of Standards and Technology.
2. Souppaya, M., & Scarfone, K. (2013). Guide to malware incident prevention and handling for desktops and laptops. NIST Special Publication, 800, 83.
3. W3C (2010). W3C guidelines Web Security Context: User Interface Guidelines, W3C Recommendation 12 August 2010, http://www.w3.org/TR/2010/REC-wsc-ui-20100812/
4. Borger, W., Iacono, L.L. (2015). User perception and response to computer security warnings. Eds. Weisbecker, A., Burmester, M., Schmidt, A. Mensch und computer 2015 Workshopband Stuttgart: Oldenbourg Wissenschaftsverlag, S. 621-646.
5. Jorgensen, Z., Chen, J., Gates, C.S., Li, N., Proctor, R.W., Yu, T. (2015). Dimensions of Risk in Mobile Applications: A User Study. CODASPY'15 March 2-4, 2015, San Antonio, Texas: 49-60.
6. Virilis, N., Mylonas, A., Nikolaos, T. (2015). Security Busters: Web Browser Security vs. Rogue Sites. Computers & Security, n7, v 2
7. Fagan, M., Khan, M., Buck, R. (2015) A Study of User's Experiences and beliefs about software update messages. Computers in Human Behaviour vol. 51.
8. Balebako, R., Schaub, F., Adjerid, I., Acquisti, A., Cranor, L.F. (2015). The impact of timing on the Salience of smartphone app privacy notices. SPSM'15 October 12, 2015. Denver, Colorado: 63-74.
9. Carpenter, S., Zhu, F., Kolimi, S. (2014). Reducing online identity disclosure using warnings. Applied Ergonomics vol. 45 issue 5.
10. Herzberg, A, Jbara, A (2008). Security and identification indicators for browsers against spoofing and phishing attacks. ACM Transactions on Internet Technology vol. 8 issue 4.
11. Dong, X., Clark, J., Jacob, J. (2010). Defending the weakest link: phishing websites section by analysing user behaviours. Telecommunications systems vol 45 issue 2-3.
12. Junger, M., Montoya, L., Overink, F-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. Computers in human behavior. Vol. 66.

13. Silic, M., Back, A. (2016) The dark side of social networking sites: Understanding phishing risks. Computers in human behavior, 60, 35-43.
14. Böhme, R., Köpsell, S. (2010). Trained to Accept? A Field Experiment on Consent Dialogs. CHI 2010 April 10-15, Atlanta Georgia: 2403-2406.
15. Reeder, R., Felt, A., Consolvo, S., Malkin, N., Thompson, C., Egelman, S. (2018) 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. ACM.
16. Alsharnouby, M., Alaca, F, Chiasson, S (2015). Why phishing still works: User strategies for combating phishing attacks. International Journal of Human-Computer Studies no 10 vol 82.
17. Iuga, C., Nurse, J., Erola, A. (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. Human-centric Computing and Information Sciences. Vol. 6 issue 1
18. Purkait, S., Kumar De., S, Suar, D. (2014). An Empirical investigation of the factors that influence internet user's ability to correctly identify a phishing website. Information management & computer security vol. 22, issue 3.
19. Mamonov, S., Renbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. Computers in Human Behavor. 83: 32-44.
20. Marforio, C., Masti, R.J., Soriente, C., Kostianinen, K., Capkun, S. (2016). Evaluation of Personalized Security Indicators as an Anti-Phishing Mechanism for Smartphone Applications. #chiforgood, CHI 2016, San Jose CA, USA: 540-551.
21. Schechter, S., Dhamija, R., Ozment, A., Fischer, I. (2007). The Emperor's New Security Indicators: An Evaluation of Website Authentication and the Effect of Role Playing on Usability Studies. IEE Symposium on Security
22. Kelley, T., & Bertenthal, B. I. (2016). Attention and past behavior, not security knowledge, modulate users' decisions to login to insecure websites. Information & Computer Security, 24(2), 164-176.
23. Fagan, M., Khan, M. M. H., & Nguyen, N. (2015). How does this message make you feel? A study of user perspectives on software update/warning message design. Human-centric Computing and Information Sciences, 5(1), 36.
24. Modic, D., & Anderson, R. (2014). Reading this may harm your computer: The psychology of malware warnings. Computers in Human Behavior, 41, 71-79.
25. Anderson, B. B., Jenkins, J. L., Vance, A., Kirwan, C. B., & Eargle, D. (2016). Your memory is working against you: How eye tracking and memory explain habituation to security warnings. Decision Support Systems, 92, 3-13.
26. Bitton, R., Finkelshtein, A., Sidi, L., Puzis, R., Rokach, L. (2018). Taxonomy of mobile users' security awareness. Computers & Security 73: 266-293.
27. Goel, D., Jain, A.K. (2018). Mobile Phishing attacks and defense mechanisms: state of art and open research challenges. Computers & Security 73: 519-544.
28. Shah, R., & Patil, K. (2016). Evaluating effectiveness of mobile browser security warnings. ICTACT Journal on Communication Technology, 7(3), 1373-1378.
29. Virvilis, N., Tsalis, N., Mylonas, A., & Gritzalis, D. (2014, August). Mobile devices: A phisher's paradise. In Security and Cryptography (SECRYPT), 2014 11th International Conference on (pp. 1-9). IEEE.

30. Raptis, D., Tselios, N., Kjeldskov, J., Skov, M. (2013). Does Size Matter? Investigating the Impact of Mobile Phone Screen Size on Users' Oerceieved Usability, Effectiveness and Efficiency. In Mobile HCI, ACM: 127-136.
31. Chin, E., Felt, A.P, Sekar, V., Wagner, D. (2012). Measuring User Confidence in Smartphone Security and Privacy. Symposium on Usable Privacy and Security (SOUPS), July 11-13, Washington DC: 1- 16.
32. Redmiles, E.M., Zhu, Z., Kross, S., Kuchhal, D., Dumitras, T., Mazurek, M.L. (2018). Asking for a friend: evaluating response biases in security user studies. CCS'18 October 15-19. Toronto ON.