Perception of Risk and Precautionary Behavior in CyberSecurity: Hints for Future Research

Eliza Oliveira[1[0000-0002-3518-3447]] and Vania Baldi[1[0000-0002-7663-3328]]

[1] CIC-DIGITAL/Digimedia, Department of Communication and Arts, University of Aveiro
Aveiro, Portugal
elizaoliveira@ua.pt, vbaldi@ua.pt

Abstract. People are using the internet each day more and more, being exposed to the risk of harms in the cyberspace. Thus, it's necessary to identify how individuals perceive those risks and what are the safety behaviors they take to avoid them. However, while risk perception is not a recent area of study and a plethora of cyberthreats frequently emerge, little attention has been given to these kinds of risks in the academy field. The goal of this paper is to present a literature review of the studies concerning risk perception and precautionary behavior associated with the use of digital technologies. To accomplish this, a survey in the multidisciplinary data basis of Science Direct and Web of Science was conducted, focusing in publications after 2016. Seven articles have been analyzed. The small number of studies proves that risk perception concerning cyber-security is still underexplored so that only a few authors commonly have published in this area. Methodological limitations will be noted, as well as other issues, regarding the conducted experiments and data analysis. Additionally, significant gaps to be fulfilled in the next investigations will be pointed out, to provide hints for future researches. Studies in this area provide a dataset for policy-makers, directing educational efforts and predicting public responses to technologies, making this subject-matter highly significant.

Keywords: Cyber-security, risk perception, precautionary behavior, survey.

1 Introduction

In recent years, the whole world has testified an incredible evolution of the digital technologies, highly associated with the feasibility of the global communication and the power of penetration of the information in everyone's life. In this direction, humanity has been living an age of great success concerning to technological advances. In this context, people communicate through the cyberspace, being able to use different kinds of technological devices and being able to connect anytime and anywhere they wish [1]. With this fast development and the lower cost in Information and Communication Technologies (TICs), people are using technological solutions each day more [2]. While this progress has provided countless advantages for internet users, digital technologies bring a series of hazards related to the use of TICs, such as risks related to information-sharing security and privacy in the network [3]. Moreover, despite its advantages, the fact of data and information be easily moved, shared, copied and stored in digital media, cyber threats are frequently forged, being the cyberspace continuously a dangerous environment for sharing personal information [4][2]. These include identity thief, virus, spyware, user surveillance and cyberbullying [5].

While everyone is exposed to risks, young people tend to be more vulnerable to cyber-attacks. Simultaneously, recent studies have verified that university students are lax about the use of technology, more specifically in terms of mobile devices [2].

According to [2], risk scenario regarding the use of TICs leads to the obligation of the person to be aware of risks to which they are exposed online to protect its personal information on the internet [2]. For [6], those risks immediately brings up the subject of awareness, being risk perception directly related to this issue, as well as the precaution of individuals when facing risks.

Risk perception can be defined as an intuitive risk judgement by individuals [7]. Risk perception is an interdisciplinary field and has been widely studied by different areas, including geography, anthropology, social sciences and psychology. Some studies were conducted to find out how people perceive risks related to different kind of hazards such as nuclear waste, chemical risks and automobile safety defects [8]. Also, some of the major challenges in risk science has been the attempt to identify user's risk perception and security behavior regarding the use of technologies. However, as different hazards frequently appear with the use of digital technologies, recently little attention has been given to these kinds of risks in the academy field.

The main goal of this paper is to present a literature review based in recent research publications that show studies related to risk perception and precautionary behavior in the cyber-security domain. Other objectives are identifying gaps to be fulfilled in the next researches and analyze methodological and procedure possible issues.

This article is organized as follows. Next section (2) will present the state of art regarding the meanings of risk, risk perception and precautionary behavior. Also, relevant studies will be highlighted. The methodology associated to the survey is presented in section 3. Results will be described in section 4, as well as the discussion. Finally, section 5 provides the most relevant conclusions and considerations for future works.

2 Background Theory

Throughout the history of the humankind, people always suffered and survived to the inherent risks of each period. Although risks always exist, its meanings have suffered changes over time, as well as the way people perceive and deal with it. In spite studies of risk have begun during the Renaissance, it remains a lack of consensus about the etymology and the meaning of risk in literature nowadays [9][10]. According to [10], some historicist agree that the term came from the Arabic word *risq* which refers to acquisition of wealth and good fortune, while some others believe that "risk" derives from the Latin, *risco*, and it was used primarily by the sailors when entering in uncharted waters [10]. Moreover, the author Peter Bernstein [9] points out that the word risk derives from the earlier Italian, *risicare*, and it means "to dare", defending that risk is a choice rather than a fate. The author also says that "The actions we dare to take, which depend on how free we are to make choices, are what the story of risk is all about" (Bernstein, 1998, p. 29).

Concerning risk perception, Paul Slovic [7], relates the term to intuitive daily risk judgments in which the majority of citizens rely on to evaluate typical and catastrophic hazards. For the author, "The ability to sense and avoid harmful environmental conditions is necessary for the survival of all living organisms. Survival is also aided by an ability to codify and learn from past experience. Humans have an additional capability that allows them to alter their

environment as well as respond to it. This capacity both creates and reduces risk." (Slovic, 2000, p. 220). In this text, Paul Slovic [7] correlate the human capacity of identifying and perceiving risks to the survival, defending that individuals have the unique quality of learning with the environment, facing it and changing it according to their own benefits. This significative adaptation capacity can be notice in everyday life, in which people develop personal safety techniques as a habitual daily activity [10]. In this sense, the perception of risk, as well as the way people will respond to the hazards, is strictly related to personal characteristics, such as the individual's experience, cultural and societal background and the subject interpretation of the risks [11]. Consequently, risk is culturally and socially dependent, varying the way different people perceive it and behave to avoid it [10].

Perception of risk, as well as the risks itself, has been suffered changes throughout the ages, presenting different contours formatted according to social construction and technological development of the historical epochs. In Pre-Enlightenment, Christian understandings of human existence typically perceived the risks and dangers as fate, as an unpleasant but inevitable aspect of life [10]. In the Post- Enlightenment era, dominant religious methods for explaining risk have given rise to technical and scientific rationality [10]. Ulrich Beck presents the science as a driving force behind the definition of risk and claim that the transition from religion to technical and scientific rationality was reflected by the emergence of a distinct institutional form, which should protect citizens from potential dangers of the time. In this period, novel methods of risk assessment linked to mathematics and probability theory have been developed, rising what's called calculation of risk [10]. Therefore, the emergence of risk assessment led to a different mode of perceiving risks, from the lenses of logic and probability. For example, in this period of history, actuarial insurance systems have emerged to determine the likelihood of accidents occurring [10].

In contemporary western society the manufactured threats increase, creating "serial risks", which reproduce to such an extent that risk management mechanisms become insufficient. These "serial risks" bring with them peculiar features: neither institutions nor even scientists hold the knowledge about all the risks associated with new technologies or the repercussions of their dangers to the population. Therefore, the very use of technology itself represents a risk for people, who begins to distrust politicians and regulated organizations [11]. Lash [12] presents that in contemporary times there is a significant intensification in the perceived risks by population, which comes from the dissemination of information through media and the increase of interpersonal communication using digital technologies. For the author, contemporary society introduces an overwhelming flow of judgements, since images, sounds and narratives are brought under the lens of media. Concerning this state of affairs, Wildavsky [13] commented as follows:

"How extraordinary! The richest, longest lived, best protected, most resourceful civilization, with the highest degree of insight into its own technology, is on its way to becoming the most frightened. Is it our environment or ourselves that have changed? Would people like us have had this sort of concern in the past?… Has there ever been, one wonders, a society that produced more uncertainty more often about everyday life? Today, there are risks from numerous small dams far exceeding those from nuclear reactors. Why is the one feared and not the other? Is it just that we are used to the old or are some of us looking differently at essentially the same sorts of experience?" (Wildavsky, 1979, p, 32).

During the last decades, few investigations have been an attempt to answer these questions by identifying the opinion of individuals about hazardous activities, substances and technologies, developing technics and methods for assessing the opinions about several kinds of risks [7]. For [7] the basic assumption underlying risks studies is those promoted and regulated by health and safety needs, to understand the way people think and respond to risk, improving communication between politicians and the public, directing efforts to new risk management strategies (e.g warning labels, regulations, substitute products).

In the next subsection, major significant works carried out in the risk perception and precautionary behavior area will be presented.

2.1 Relevant Studies

Historically, the bulk of empirical studies related to risk research has been conducted in the United States [7]. In this context, the majority of the earlier researches in risk perception utilized the psychometric paradigm as a methodological approach, seeking out to probe behavioral intentions in hypothetical situations and access the decision making progress [10]. Previous study has proposed several risk dimensions as a predictor of perceived risks [14][15]. Starr [15] underlines two categories: those in which the individual is involved on a voluntary basis and those in which the participation is involuntary, imposed by society. His findings show that voluntary activities are perceived as less risky. Following this perspective, Slovic [14] presented nine dimensions which influence risk perceptions, such as immediacy of the effects, the severity of consequences and knowledge about risk. The empirical study evaluated 30 different activities (e.g smoking, alcoholic behaviors) and technologies (e.g X-ray, nuclear power). The outcomes of the indicated dimensions proved to be effective predictors of the perception of risk, risk acceptance and perceived benefits. Other studies conducted by the author proved that, in general, people feel themselves to be immunity from risks related to familiar activities, individuals overestimate the risk presented by atypical but remarkable events, whilst underestimate typical daily risks [16] and that immediacy has a positive impact in risk perception, since they are more likely to provoke anxiety [17].

Kahneman [18] discovered that the more voluntary people believe exposure to the risks associated with phishing is, the less risky they perceive phishing to be. In addition, [18] presented that when positive consequences are immediate and negative repercussion of an activity are not, perceived risk is reduced. Other relevant findings include the reduction of risk perception when individuals feel they are in control, understand about the risks and when they are experts [19].

Despite the fact that the majority of the works related to cyber-security focus on protection and security of the systems, and that studies related to individual's awareness and behavior regarding the use of information systems are limited [2], some works are worth to be mentioned. In this sense, [19] and [20] analyzed a set of hazard (21 and 15, respectively) on internet in terms of risk perception and other risk dimensions. The authors concluded that severity of consequences, accident history, voluntariness, duration of impacts, understanding and possibility of exposure were significant positive predictors of risk [19]. In [20] outcomes showed that voluntariness, knowledge to science, controllability, newness, dread and severity were significant predictors of risk.

Concerning precautionary behavior, [21] proposed a new model to assess user's computer security behavior specifically, susceptibility perception, severity perception and cues to action, together with the component of effective risk management, suggesting that individual's security behavior is strictly related to the perception of threat and evaluation of the behavior to resolve the threat. The authors state that security behavior demands the user to take additional steps towards avoiding security accidents (e.g the use of strong passwords and conduct regular backups) and conclude, that, practices and behaviors related to cyber-security could be considered as protective approaches and as preventive actions. After presenting the grounded theory, the next section details the methodology used in this survey, encompassing all the steps taken in the process of finding and choosing the articles in the data basis.

3 Methodology

Literature review has become an increasingly significant aspect of research for gathering advanced knowledge regarding a specific area and has been detailed previously [22]. The first stage towards conducting the survey was the definition of the appropriate databases to find research articles associated with risk perception and precautionary behavior related to cyber-security. In this direction, as perception of risk and precautionary behavior is an interdisciplinary area, the databases chosen for the research of the articles were the Web of Science and Science Direct. These data aggregate systems are a multidisciplinary research tool that grants easy access to a wide range scientific literature since they encompass publications in physical sciences and engineering, biological sciences, health sciences and social and human sciences. Following this stage, the correspondent keywords must be defined. In this scope, three keywords were designed to find articles correlated with this paper's subject: risk perception, cyber-security and precautionary behavior. Papers and proceedings published before 2016 have been excluded, as well as papers related to workshops, courses, book and book chapter. The year-based exclusion criterion took into account the fact that there is one relevant review published in 2015 [23]. The inclusion criteria were: being original research articles, being published after 2016 and present empirical work respecting the previously mentioned keywords. It is important to emphasize that papers which present studies related to only one of the principal topics (i.e works that provide studies related to perception of risk or precautionary behavior) were also accepted. However, all papers should approach cyber-security issues.

The steps for the selection of the papers used in this survey were the following ones: first, the titles were analyzed. At this point, it has been excluded those papers which do not fit the inclusion criteria of this study. After, a pre-selection was done through the reading of the abstract. Next, all the selected papers were fully read to select the documents that effectively illustrate relevant research that should be considered in this literature review.

As a consequence of the search in the previously mentioned databases, 13 articles were found in Science Direct and only one, repeated article, has been found in Web of Science. Thus, 13 research articles were considered as possible to use in this survey, although only seven were selected as they comply with the inclusion criteria. The next following section presents these selected works.

4 Results

As previously said, seven articles were selected for this survey as they fulfil the inclusion criteria of the study. According to the analysis, the first four main regions dealing with cyber-security problems include the United Kingdom, The Netherlands, The USA and Ireland. The following Table 1 lists the authors and year of publications, the study conducted, and principal contributions of the approaches contemplated in each document. Considering the year of publication, two papers were published in 2019, two in 2018, two in 2017 and only one in 2016. Also, among the seven selected works, four were written by the same author, showing that only few researches have focused on cyber-security studies. Issues related to cyber-security were similar across studies, emphasizing the aspect related to the protection of personal data by individuals, namely regulation of the user's information-sharing and only one measured security and privacy regarding social media.

In respect to the methodological approaches, all works carried out quantitative empirical study with internet users, conducting an online survey. In addition, participants were chosen through different methods, but all through online recruitment such as through Mechanical Turk [24], an invitation sent by Toluna [25], using recruitment services of online panels [26][5], recruitments by e-mail [3][27] and selection as a sample [2].

Table 1. General information of the studies contemplated for this review.

Authors / Year of Publication	Conducted Study	Main Result
Bavel et. al (2019) [25]	Online experiment with a sample of 2024 internet users from several countries. Explored the effects of notifications (message advised and threat appeal) on security behavior when purchase in a mock e-commerce store.	Both of kinds of notifications increased security behavior, but coping message more so.
Jansen & Schaik (2019) [26]	Online experiment with 786 Dutch internet users. Examined the impact of fear appeal messages on user cognitions, attitudes and security behaviors against phishing attacks.	Positive effects on cognition, attitudes and security behaviors.
Cain et. al (2018) [24]	Online experiment with 268 internet users from different countries. Explore the user's knowledge and behavior regarding cyber hygiene, such as the use of antivirus, firewall and providing name in social media.	Gender and age are determinants in user's behavior and knowledge regarding cyber hygiene.
Schaik et. al (2018) [5]	Online study with 201 UK non-student internet users. Examined risk perception, other risk dimensions and precautionary behavior related to set of hazards that correspond with security and privacy settings of the Facebook.	Perception of risk was highest for cyberbullying and information sharing.
Schaik et. al (2017) [3]	Online study with 436 UK and US college students. Examined risk perception and precautionary behavior of a set of internet security hazards, including phishing, identity thief, keylogger and cyberbullying.	Risk Perception was higher for identity thief, keylogger and cyberbullying.
Jeske & Schaik (2017) [27]	Online study with 323 college students of US and UK. Examined the familiarity of users about 16 online threats, internet attitudes and security behavior, including phishing, identity thief, keylogger and cyberbullying.	Three different clusters of knowledge were labeled, which influences in security behavior and internet attitudes.
Ögütçü et. al (2016) [2]	Online study with a total of 881 (169 academic, 317 administrative and 395 college students) individuals from Turkey Examined levels of awareness toward information security in terms of perception and behavioral aspects, using four elaborated scales.	Results show significant differences within samples and habits of internet usage

Measurements data were collected using the Psychometric Paradigm by the administration of Likert scales [2][27][3][5][26][24] in six studies. Therefore, only one research article presented a distinct strategy for obtaining outcomes, determined by the decisions made by participants during the experiment with the mock online purchase [25].

In addition, the numbers of participants were different in all research studies, with a minimum of 201 individuals in [5] and a maximum of 2024 parties in [25]. Crosscultural works was conducted by [3][25][27]. The sample was different in all studies: In [25] the mean age was 40.8 years with 50.3% of females with 40.84% with upper secondary education. In [26] the age range was 19-76 years with 50.6% females and 52.5% with high education. Participants of paper [24] presented age range of 18-55+ years with 142 females, being 38.06% with a 4-year degree, while the sample of [5] have an average age of 42 years with 92 females and 55% with an undergraduate degree. In [3] the mean age of participants was 23 with 336 females. Finally, participants of paper [27] presented an age range equal to 18-60 years, with 74% female and [2] had a mean age of 28.1, being 70% undergraduate. Additionally, all participants in papers [3] and [27] were US or UK college students.

4.1 Discussion

Given the characterization of the selected articles, some observations can be made. Thus, this subsection will provide a general discussion encompassing procedure concerns, methodological limitations, measurement methods and data analysis. Results will not be detailed in this section since the goal is to point out opinions and comments to improve future research in the cyber-security field. However, considerations will be made concerning variables, such as age and multinational approach always where such data are important to be mentioned.

Since the use of internet in countries of Europe and in the US are quite intense, studies in cyber-security shows to be highly significant. Thus, in order to grant a safe use of technologies, citizen's security behavior and awareness must be considered.

Two papers selected in this review utilized theory models that are currently used in health interventions. In this sense, both papers, [26] and [25], used the Protection Motivation Theory in order to accomplish their goals. These two studies presented similar objectives related to the use of copying and threat appeal messages to measure improvements in security behavior. Thus, these were the only works which intervened with participants. Other studies have no intention to intervene with individuals. They only investigate risk perception and security behavior. This ups on to new future works possibilities, since it is important, not only to determine people's awareness regarding the use of technologies but also to improve it.

In regard to methodological approaches used by the researchers, only one work did not use the Psychometric Paradigm to collect data [25]. Therefore, this is one of the methodological limitations of the analyzed works, which utilizes quantitative methods to achieve the purpose of the study. Therefore, there is a lack of qualitative data concerning perception and precautionary behavior in cyber-security domain. This is highly significant, since the perception of risk and precautionary behavior are both dependent on subjective and cultural factors. In addition, all the works were conducted through the online environment, which makes difficult to reach a qualitative personal opinion of the participants with respect to cyber-security issues. Also, the

recurrence of the same authors in the papers makes the theme centralized and little explored. The centralization of publications leads to the recurrent use of only one methodological strategy. The results and contributions are thus limited. Mythen [10] presents a critique of the use of the psychometric paradigm in research on risk perception by social sciences, arguing that risk perception and Internet security behavior are culturally and subjectively constructed. In this sense, should be analyzed through qualitative measures which include interviews and focus group.

Since the whole world has been suffering a significant transformation in human's habits, changing the physical environment to the virtual one, where the construction of online interpersonal relations become natural and all the daily activities seem to migrate too, many contributions can be achieved by conducting a cross-cultural study. [2] obtained interesting outcomes by people of different countries, being Polish and Spanish people's behavior the most insecure among the other countries (UK, German, Sweden). Other findings highlight the way that individual decision-making strategies differ across countries and the author suggests the need to adopt a multi-national approach in studies such as his, especially if the aim is to produce policy options that are generalizable across contexts.

The age is another point to be discussed. Works with a wide range of age found that security behavior tends to be higher by the older individuals. One of the findings of [2] is that students (between the ages of 18 and 30) seem to be the most at-risk group. The reason for this may be the high use of the Internet, especially the social networks and social media. Another reason may be the low possibility that the youth had a negative experience with Internet/information security or technology and that they are less controlled by parents. In article [25] the relationship between age and cyber-security is highly complex. For example, older adults are more vulnerable than younger adults to certain types of phishing attack but less vulnerable to others. Both younger and older adults are likely to modify their security behaviors following a warning of some kind, but older adults are particularly affected by trust violations. Also, Cain et. al (2018) present that, although it is commonly believed that age has an impact on cyber hygiene behaviors, older users tended to behave more securely than younger users. According to the author, this finding was counterintuitive because younger people are believed to have the most know-how about technology. Is important to highlight that studies which encompass a wide range of ages are more likely to identify disparities in the behaviors of people who present themselves in different age groups. Thus, future works must provide information among individuals, in order to provide behavioral comparisons between different ages.

In conducting studies that address individuals' awareness of risk perception and precaution, the authors agree that data security and privacy in the online environment is primarily the responsibility of individuals. Paper [2] points out that the overall success of both software and hardware security mechanisms are based on the effective behavior of users of the IS specification. Also, [10] highlights that in contemporaneity, with the technological improvements, people are more enlightened about the risks they are exposed to and how to prevent or to behave more securely. However, since the risk exposure are each day bigger and the cyber threats are more and more prominent, it is important to conduct training concerning the secure use of the internet and other TICs.

Regarding the perception of risk, in the two works published by Schaik [3] and [5] the particular hazards/activities that were judged to be most risky were cyberbullying, sharing telephone

number, sharing e-mail address and failing to receive login notifications about the Facebook user. Additionally, the same author, in [3], identified that keyloggers, identity theft and cyberbullying have higher perceptions of risk.

Finally, the works address issues regarding, predominantly, with the security of information-sharing on the internet, while topics related to online aggression are not presented. This gap provides hints for future works since cyberbullying threats has been widely studying in literature and the incident has been each day more intense in the entire world. Is also important to highlight the importance of studies regarding risk perception and precautionary behavior for providing a dataset for policy-makers, directing educational efforts and predicting public responses to technologies, making this subject-matter highly significant. This will give significative insights for the production of future commercial product's release in regard cyber-security, such as better protective software and hardware.

5 Conclusion and Future Work

This paper presents a literature review regarding risk perception and precautionary behavior concerning cyber-security threats. Additionally, with the analysis of the papers is possible to conclude that work's majority focus is on cyber-security related to security of personal information, being others significant subjects like cyberbullying and online harassment not addressed by the researchers. Finally, future works should address alternative subject-matters, such as precautionary behavior and risk perception regarding online aggression. In addition, intervention with users in order to educate them for better use of TICs should be considered to be conducted.

Future works should take into account that cross-cultural studies provide contributions to the literature since they enable comparisons and analysis between different countries and cultures. Upcoming researches should be made using alternative methodologies, in order to cover qualitative data of cultural and subjective determinants for perception of risk and security behavior. Information about these subjects will provide great information concerning how the risks are perceived be cultural and societal individuals.

Finally, as previously said, Studies in this area provide a dataset for policy-makers, directing educational efforts and predicting public responses to technologies, making this subject-matter highly significant.

References

1. Baldi, V., Oliveira, E.: A queda do império Facebook: uma análise sobre os motivos que levam ao afastamento da rede social. In: Educación y comunicación mediada por las tecnologías. pp. 41–60. EGREGIUS Ediciones, Sevilha (2018).
2. Öıütçü, G., Testik, Ö.M., Chouseinoglou, O.: Analysis of personal information security behavior and awareness. Comput. Secur. 56, 83–93 (2016).
3. Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., Kusev, P.: Risk perceptions of cyber-security and precautionary behaviour. Comput. Human Behav. 75, 547–559 (2017).

4. Loon, J. van: Risk and Technological Culture: Towards a Sociology of Virulence. Routledge, London and New York (2003).
5. Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., Kusev, P.: Security and privacy in online social networking: Risk perceptions and precautionary behaviour. Comput. Human Behav. 78, 283–297 (2018).
6. Assailly, J.-P.: The psychology of risk. Nova Science Publisher, INC, New York (2010).
7. Slovic, P.: Perceptio of Risk. In: The Perception of Risk. p. 511. Taylor & Francis Group; Routledge, Nova York (2000).
8. Kahan, D.M.: Handbook of Risk Theory. (2011).
9. Bernstein, P.: Against-the-Gods-The-Remarkable-Story-of-Risk. John Wiley & Sons, INC, New York (1996).
10. Mythen, G.: A critical introduction into the risk society. Pluto Press, Londres (2004).
11. Adam, B., Beck, U., Loon, J.: The Risk Society and Beyond: Critical Issues for Social Theory. Crit. Issues Soc. Theory. 232 (2000).
12. Lash, S.: Risk Culture. In: The Risk Society and Beyond: Critical Issues for Social Theory. pp. 47–63. SAGE Publications Inc, Londres (2000).
13. Wildavsky, A.: No Risk Is the Highest Risk of All. Am. Sci. 67, 32–37 (1979).
14. Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., Combs, B.: How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. Policy Sci. 9, 127–152 (1978).
15. Starr, C.: Social benefit versus technological risk. What is our Society Willing to Pay for Safety. Science (80-.). 1232–1238 (1969).
16. Slovic, P., Fischhoff, B., Lichtenstein, S., Roe, F.J.C.: Perceived Risk: Psychological Factors and Social Implications. Proc. R. Soc. A Math. Phys. Eng. Sci. 376, 17–34 (1981).
17. Slovic, P.: Perception of Risk: Reflections on the Psychometric Paradigm. In: Krimsky and D. Golding (ed.) Social Theories of Risk Westport. pp. 117–52. Praeger, New York (1990).
18. Kahneman, D.: Thinking, Fast and Slow. Routledge, New York (2017).
19. Huang, D.L., Rau, P.L.P., Salvendy, G.: Perception of information security. Behav. Inf. Technol. 29, 221–232 (2010).
20. Garg, V., Camp, J.: End User Perception of Online Risk Under Uncertainty. In: Proceedings of 45th Hawaii International Conference on System Sciences. pp. 3278– 87. , Manoa (2012).
21. Ng, B.Y., Kankanhalli, A., Xu, Y. (Calvin): Studying users' computer security behavior: A health belief perspective. Decis. Support Syst. 46, 815–825 (2009).
22. Gough, D., Oliver, S., Thomas, J.: An Introduction to Systematic Reviews. SAGE Publications Inc, London (2017).
23. Quigley, K., Burns, C., Stallard, K.: "Cyber Gurus": A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. Gov. Inf. Q. 32, 108–117 (2015).
24. Cain, A.A., Edwards, M.E., Still, J.D.: An exploratory study of cyber hygiene behaviors and knowledge. J. Inf. Secur. Appl. 42, 36–45 (2018).
25. Van Bavel, R., Rodríguez-Priego, N., Vila, J., Briggs, P.: Using protection motivation theory in the design of nudges to improve online security behavior. Int. J. Hum. Comput. Stud. 123, 29–39 (2019).
26. Jansen, J., Van Schaik, P.: The design and evaluation of a theory-based intervention to promote security behaviour against phishing. Int. J. Hum. Comput. Stud. 123, 40–55 (2019).
27. Jeske, D., Schaik, P. Van: Familiarity with Internet threat: Beyond a wareness. 66, 129– 141 (2017).