COMPUTERS AND INFORMATICS
2757-8259 2021, Volume 1 Issue 1
Research Article

Development of an online learning system about information security

Onur Ceran
Gazi University, Computer and Instructional Technology Department, Ankara, Turkey, onur.ceran@gazi.edu.tr
Serçin Karataş
Gazi University, Computer and Instructional Technology Department, Ankara, Turkey, sercin@gazi.edu.tr

Submitted: *01.11.2020*
Accepted: *07.12.2020*
Published: *28.02.2021*

Abstract:

With the increase in people's access to information and communication technologies, threats to information security have developed in the same direction. It is seen that the measures to be taken with technical devices or services are not sufficient alone. For this reason, it becomes evident that the end users, who seem to be the weakest targets, should be trained on the subject. Since the size of the target audience to be trained may consist of everyone who even uses a smartphone, it was concluded that the most suitable environment for information security education is online learning systems. This study aims to develop an online learning system for information security education. To achieve this goal, the design-based research method and rapid prototyping instructional design model were used in the study. After initializing the first prototype of the learning environment examining the related literature, the final version of the prototype was emerged following the opinions received from experts from different but related disciplines.

Keywords: *Information security, Online learning, Rapid prototyping*

Cite this paper as: Ceran, O. & Karataş, S. Development of an online learning system about information security, *Computers and Informatics*, 2021, *1*(1), 26-35.

1. INTRODUCTION

With the incremental development of internet and mobile technologies, people can execute many processes, in which the result maybe even in a different continent, using just one mouse click. According to "We Are Social" international digital report [1] while 60% of the world population is internet users, 70% of them are using smart devices with an increase of 10% compared to the previous year. Although these emerging technologies make transactions to be done easier, on the other hand, they also cause criminal cases to be committed [2].

Statistics and reports show that precautions about information security are tried to be provided through the medium of hardware or software-based solutions in general [3, 4]. However, the percentage of people facing information security breaches and the amount of money which is lost seems to be increasing incrementally [5, 6]. The report of the European Union Agency for Cybersecurity [7] indicates that end users are unaware of the confidentiality of the data sent through their smart devices and how they prevent it by changing settings even though settable features exist, which creates the riskiest situation of unawareness about information security. Similarly, the study of [8] showed that end users are unaware of the risks of installing applications acquired from unknown resources and the occurrence of social engineering attacks. Notwithstanding that organizations allocate their information technology budget on high-tech devices and technology producer firms provide end users with individual protective solutions about information security, attackers generally choose untrained, uninformed, and untracked users as a target, which shows the importance of information security awareness.

1.1. Information Security Awareness

When two words "education" and "training" are translated in to Turkish Language they have the same meaning. However, these two words have different meanings when they are used in the context of information security. Within the literature, despite not being agreed upon concepts that have small differences have emerged when information security and education/training are handled together. [9] summed up this distinction in their study as follows:

1. Information Security Education (ISE): This caption consists of not only technical but also administrative information set. It aims to guarantee information security triad of CIA which are confidentiality (the state of keeping the information private, to prevent unauthorized access), integrity (the state of keeping information as a whole, to make information reliable and trustable) and accessibility (state of keeping information available, to make information accessible when it is needed). It is generally intended for people whose work needs expertise on information security or information security professionals.
2. Information Security Training (IST): It is intended for staff within an organization or firm to equip them with information security behaviors for carrying out their specific duties. Generally, practical methods such as seminars and workshops are chosen for this purpose.
3. Information Security Awareness (ISA): It is intended for every end user of information technologies, in order to engage their attention to information security, make them aware of any concerns about the issue, adapt to precautions, and change behavior in that manner.

Especially, the departments in the universities such as computer engineering, software engineering, informatics, and information systems, which aim to create expertise on information and communication, have a curriculum in accordance with the information security triad of CIA. [10] emphasized that programming, networking, human-computer interaction, database systems, and web-based systems are the key five pre-request subjects mandatory for information security curriculum. In this context, it is obvious that this kind of education is related to a small size target in addition to those whose mission is to develop new technology and provide information security service. [11] in their study indicated that the researches are carried out generally according to technologies and firewalls for information security

professionals. And they also criticized that these researches do not include end-user opinions and experiences. Thus information security awareness becomes a subject that should be studied. [12] mention that Turkey and the rest of the world have been trying to create policies in technical, procedural, methodological, and statutory terms to ensure information security. However, the expected problems and their negative impacts continue to gradually increase instead of decreasing with the help of such policies. They also emphasized that for information security, awareness of end users should have a priority over technological investments. According to this context, "information security awareness (ISA)" comes to the fore about providing information security. Related literature shows that everybody who uses an information system including just a smartphone or a database management system is a candidate that may face information security breaches, hence every end user regardless of their education, income level, gender, or background should be trained about information security awareness.

2. METHOD

With this study, it was aimed to develop an online learning system about information security to make a massive amount of people aware of possible security breaches. In order to achieve this aim, the design-based research method, which is generally used for developing a service, product, or system, in addition, producing a product as an application of a theory or education [13], and the rapid prototyping instructional design method, which enables designing instruction for small courses rather than designing the entire curriculum [14], were preferred and used.

"Design" is defined as a frame which consists of methods and processes to achieve an aim [15]; as for the teaching and learning, it is defined as the preparation phase of the development process in which this process results with a new theory or system. Design-based research is a flexible method that is based on a cooperative study of researchers and participants and also aims to improve the quality of educational applications with real-world practices [16]. In order to develop an online learning system researcher should follow the design and development processes. Since the most important result of design-based research methodology is the production of a new learning system or educational application [17] in this study design-based methodology was preferred to be used.

Rapid prototyping instructional design method includes the development of a working model of instructional product with analyzing, designing, developing, and evaluating instructional innovation. The aforementioned prototype does not constitute the final product, but it describes and visualizes the final product conceptually as being a simple but working model of it [18].

[19], who indicate that rapid prototyping is a more suitable instructional design method to overcome the complexity of instructional processes in terms of human resources, sorted out the steps of the method as follows:

1. Defining learning objectives by doing need assessment and content analysis
2. Constructing the prototype
3. Utilizing the prototype
4. Installing and maintaining the system

[19] emphasize that well understanding of the needs, content, and goals are the results of the parallel processes of designing, researching, utilizing, and installing. [20] points out that rapid prototyping is used particularly for enhancing the course level instruction rather than producing a complete instructional program. Therefore, in this study, the steps of the rapid prototyping instructional design method were followed.

3. FINDINGS

The process of using the rapid prototyping instructional design method in developing an online learning system about information security and each of the steps of implementation were explained as follows:

3.1. Defining needs and objectives:

Subjects that will be taught to end users are determined after the information security literature [21, 22, 23] was examined. Topics were defined as follows:

- Using licensed software
- Safe internet usage
- Safe e-mail usage
- Safe password policy
- Security software
- Personal information sharing

Aforementioned topics were divided into subjects. For each subjects learning objectives are defined. Thereby, the following objectives are aimed for end users to achieve after finishing all the subjects in the learning environment:

- To be able to explain the benefits of using licensed software,
- To be able to express the dangers that individuals using unlicensed software may encounter,
- To be able to explain the risks involved in unwanted / junk emails
- To be able to give an example of a phishing email
- To be able to explain the benefits of using multiple email addresses
- To be able to explain using the carbon copy (cc) function in the email
- To be able to explain the temporary internet files,
- To be able to list the benefits of deleting web browsing history
- To be able to express what SSL certificate is,
- To be able to explain the importance of SSL certificate
- To be able to explain the benefits of using a firewall,
- To be able to explain the risks of sharing contact information on the internet,
- To be able to explain the risks of sharing personal information on the internet,
- To be able to give examples of strong passwords,
- To be able to explain things that should not be done while creating a password,
- To be able to explain corporate e-mail usage principles,
- To be able to explain how to protect against malicious software,

3.2. Constructing the prototype – design:

At this stage, the prototype design of the online learning environment was realized in accordance with the needs and learning objectives.

- When reaching the web site, it is the web page, which consists of all the topics to be learned, shown to the end user first. These topics are delineated with related thumbnails (See. Fig. 1).

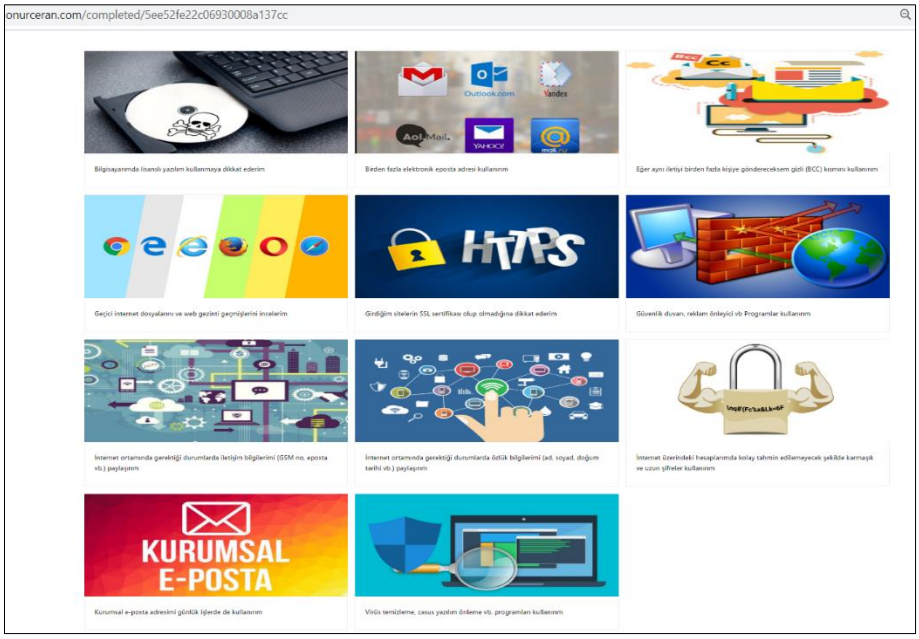

Figure 1. Homepage of the Online Learning System.

- End user has the flexibility of starting and continuing to whichever subject he wants.
- The content of the subjects determined is gathered together through open sources and added to related pages. Text, image, and video media are used for representing contents. One example of learning content is shown in Fig. 2.

Figure 2. An Example of the Learning Content.

3.3. Utilizing the prototype – research:

Expert opinions were received for defining conformity of web design of the online learning system from 3 experts who have PhD. degree in computer education and instructional technologies. For the expert opinion, a web design scale produced in the context of the master thesis titled "Çankaya İlçesi Milli Eğitim Müdürlüğü'ne Bağlı İlköğretim Okullarına ait Web Sitelerinin Grafik Tasarım Açısından İncelenmesi ve Örnek Web Sitesi Tasarımı Hazırlanması" [24], was used. All permissions were obtained to be used in this study from the author. Suggestions that were agreed on by two of the three experts are listed in table 1 and these suggestions were applied to the prototype.

Table 1. Changes Applied to the Prototype According to the Expert Opinions.

Applied changes
A logo was designed and applied to the online learning environment.
Important parts of the texts included in the training content were highlighted by using different colors and bold fonts.
The text content was justified.
A homepage screen was added to welcome the end user.
Low-resolution photos were replaced with high-resolution ones, all reduced to the same size.
The purpose of the development of an online learning environment and introductory information were added.
The contact information of the researcher was added to the homepage.
Links that could be accessed from each training topic page were added to the "site map" page.
The last update date of the online learning environment was added.
The information that the educational content was compiled from open sources was added to the learning environment homepage.
"Useful links" were added to the learning environment.
The introductory title for the learning environment has been updated.
The statement stating that any data belonging to end users will not be shared with third parties has been added on the homepage of the learning environment.

Expert opinions were received for defining conformity of content of the online learning system from 3 experts 2 of whom have PhD. degree in management information systems and one of whom is PhD. candidate and working as law enforcement on cybercrime. Suggestions that were made by three experts are listed on Table 2 and changes were applied to the prototype in pursuance of these suggestions.

Table 2. Changes in the Content According to the Expert Opinions.

Applied changes
Content regarding data loss has been expanded.
SSL Certificate explanation has been simplified.
An anti-adware topic has been added.

3.4. Installing and maintaining the system:

In line with the expert opinions received, changes were made to the online learning environment which was published on the domain name www.onurceran.com and the system was finalized. According to that;

- While the end users were redirected to the page where all the topics were shown when they first reached to the online learning system in the first version of the site, now they are redirected to the homepage, in the final one.
- In the first prototype, heading of the explorer was written in lower-case and it is the same as the domain name "onurceran.com". However, in the final one it is updated as "BİLGİ GÜVENLİĞİ FARKINDALIK EĞİTİMİ" and written in capital letters.
- There was not any logo to identify and symbolize the learning environment in the first prototype. After receiving the expert opinions, a logo was designed (Fig. 3) and applied to the final design of the learning environment.

Figure 3. Logo Used in the Learning Environment.

- There was no information about the researcher in the first prototype. In accordance with the expert opinions, personal and contact information were added to the final prototype. In addition to that, the last update date of the learning environment was added as illustrated in Fig. 4.

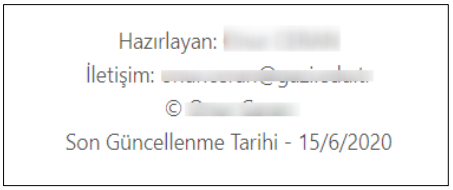

Figure 4. Personal, Contact and Update Information.

- The web page which consist of topics in the first prototype were labeled as a "site map" in the final one. As shown in Fig. 5, in line with the expert opinion received, the visuals belonging to the topics were resized to the same dimensions to provide unity and redesigned as icons describing the subject. The phrase "tamamlandı (completed)" designed for each completed topic on the first prototype has been preserved in the final one.

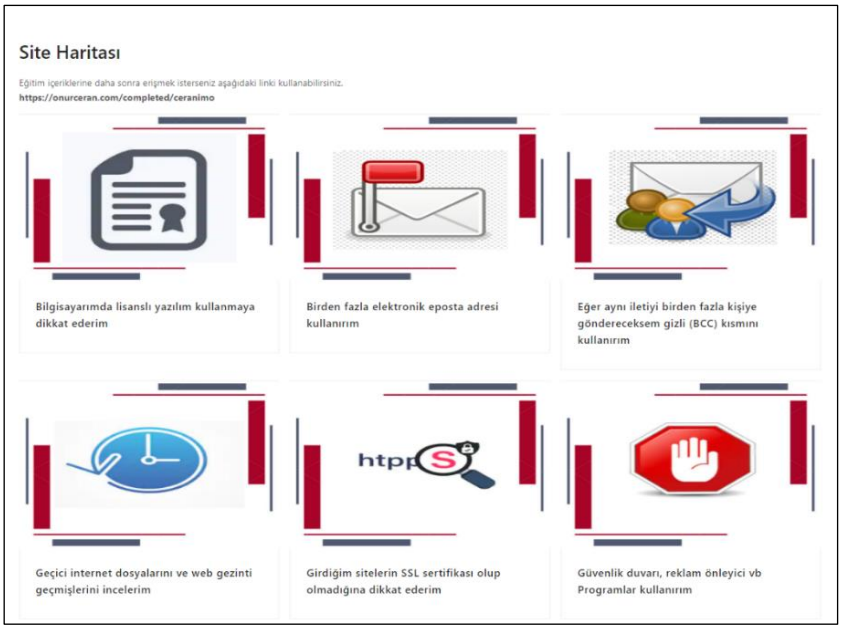

Figure 5. Site Map.

3.5. The Learning Path

All the subjects are designed to follow the same learning path. It starts with the definitions, description of the technology used or enables the applications to be used and how it works. It is followed by the importance of the mentioned technology or the attitude. This regards with both the advantages of preventive measures and risks or probable harms in case of the lack of the desired attitudes. At the end the user launches video content related with the desired behavior about the subject. Fig. 6 illustrates an example of learning environment for subject of "SSL Certificate" as described. The learning environment consists of eleven subjects to be learnt as follows

1. Usage of Multiple E-mail Account
2. Usage of Licensed Software
3. Firewall and Ad blocker Software
4. Anti-virus and Anti-Spyware Software
5. Temporary Internet Files and History Records

6. Password Policy
7. SSL Certificate
8. Secure E-mail
9. Official E-mail
10. Personally Identifiable Contact Information
11. Personally Identifiable Identity Information

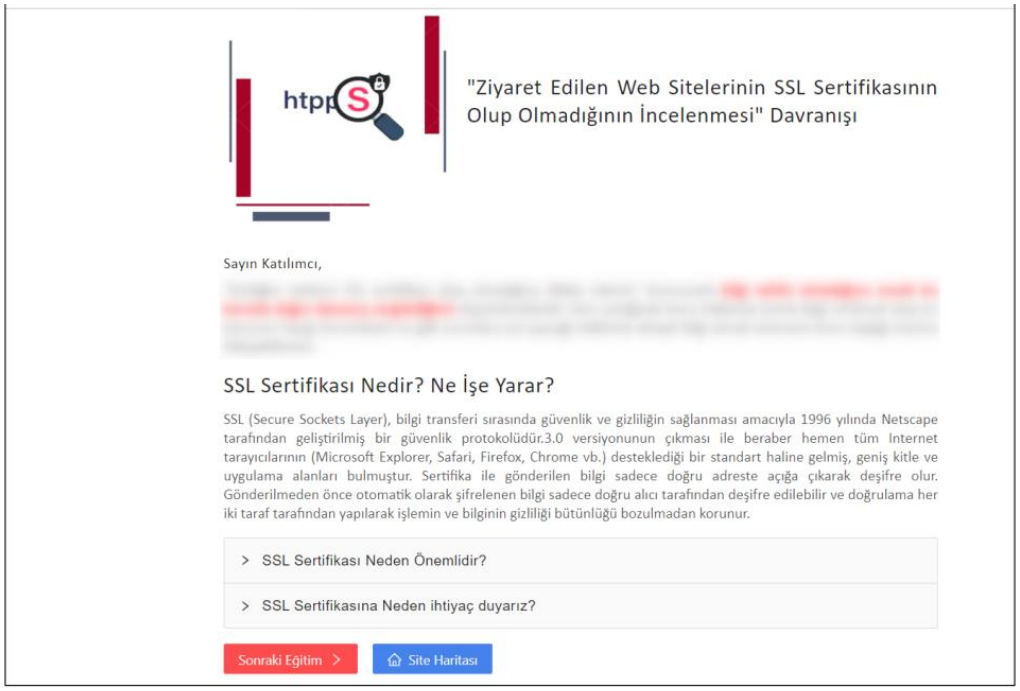

Figure 6. Content for Subject of SSL Certificate.

4. CONCLUSION

Despite the great effort and budget spent in the creation of scientific researches and the products revealed, it is observed that the threats to information security do not decrease and at the same time they are insufficient in preventing threats that end users or corporate systems are exposed to. In this regard, the importance of educating people, the weakest link in the security chain, has emerged. In this context, from a 10-year-old child playing online games on his/her parents' smartphones to an 80-year-old individual who pays his/her electricity bill using online services, it is obvious that everyone should be aware of the importance of information security and be able to take certain measures to protect themselves from these threats. [25] reported that Britain, America, Canada, Australia, Estonia, Japan, France, Finland, the Netherlands, and Russia are trying to adapt their information and information security strategies and they are in an effort to raise or create awareness. Information Security Association [26] stated that in the last 30 years, the information security awareness of relevant institutions and organizations was carried out within the scope of activities related to the promotion and use of systems, tools and technologies; They emphasized that this situation is insufficient to change behaviors about the subject.

Considering the size of the target audience to be trained, it was concluded that the most suitable environment for information security education is online learning environments. On the common denominator of accessing data regardless of time and place, access to quality-enhanced education and materials with reduced costs and increased cost-effectiveness, and the ability to use a large number of educational materials by a large number of learners at the same time are considered as advantages of

online learning environments [27]. However, there are studies in the literature that show that web technologies can provide unlimited connections for unlimited content, that the learner cannot find the information he/she is looking for in this high amount of non-linear content, moreover, he cannot determine which piece of information he needs and thus causes problems related to the usability of the system [28, 29]. For this reason, a prototype website was prepared for information security education and the learning environment topics were examined and limited to the studies in the literature.

REFERENCES

[1] Simon, K. We Are Social. 2019, p. 221. Retrieved from https://wearesocial.com/global-digital-report-2019.

[2] Sarre, R., Lau, L.Y., & Chang, L.Y.C. Responding to cybercrime: Current trends 2018. Taylor & Francis.

[3] Filkins, B. IT Security spending trends 2016. SANS.

[4] Susan, M., Keen, E. Gartner forecasts worldwide information security spending to exceed $124 billion in 2019 2018. https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019.

[5] Matt, G. Internet crime report. Annual, (202) 324-3691, *Internet Crime Complaint Center*, 2018, p. 28, Retrieved from https://pdf.ic3.gov/2018_IC3Report.pdf.

[6] Michael, L. Assessing the trends, scale and nature of economic cybercrimes: Overview and issues 2017. *Crime, Law and Social Change, 67*(1): 3–20.

[7] Giles, H. & Dekker, M. Smartphones: Information security risks, opportunities and recommendations for users 2010. ENISA.

[8] Woongryul, J., Kim, Jeeyeon, Y, Lee, Dongho, W. A practical analysis of smartphone security 2011. *Symposium on Human Interface*, Springer, pp. 311–20.

[9] Amankwa, E., Loock, M., & Kritzinger, E. A conceptual analysis of information security education, information security training and information security awareness definitions 2014. *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, IEEE, pp. 248–52. DOI.org (Crossref). doi:10.1109/ICITST.2014.7038814.

[10] Rowe, D., Marry, C., Lunt, M., & Ekstorm, J.J. The Role of Cyber-Security in information technology education 2011. *Proceedings of the 2011 Conference on Information Technology Education - SIGITE '11*, ACM Press, p. 113, DOI.org (Crossref), doi:10.1145/2047594.2047628.

[11] Tejaswini, H. & Rao, H, R. Protection motivation and deterrence: a framework for security policy compliance in organisations 2009. *European Journal of Information Systems*, *18*(2): 106–25. DOI.org (Crossref), DOI:10.1057/ejis.2009.6.

[12] Eminağaoğlu, M. & Gökşen, Y. Bilgi güvenliği nedir, ne değildir? Türkiye'de bilgi güvenliği sorunları ve çözüm önerileri 2009. [Information Security; What Is And What Is Not, Information Security Problems In Turkey And Some Related Solutions] *Dokuz Eylül University, Journal of Institute of Social Sciences*, *11*(4).

[13] Sasha, B. & Squire, S. Design-based research: putting a stake in the ground 2004. *Journal of the Learning Sciences*, 13,(1): 1–14. DOI.org (Crossref), doi:10.1207/s15327809jls1301_1.

[14] Ocak, M.A. Öğretim tasarımı modelleri 2015. Instructional Design Models, Instructional Design Theorems, Models and Applications, Anı Press, pp. 32–257.

[15] TLA. Turkish language association, 2020. Retrieved from https://sozluk.gov.tr/?kelime=tasar%C4%B1m.

[16] Feng, W. & Hannafin, M.J. Design-based research and technology-enhanced learning environments 2005. *Educational Technology Research and Development*, *53*(4): 5-23. Springer.

[17] Kuzu, A., Çankaya, S., & Mısırlı, Z. A. Design-based research and its implementation in the design and development of learning environments 2011. *Anadolu Journal of Educational Sciences International*, 1(1): 19-35.

[18] Stokes, J.T. & Richey, R.C. Rapid prototyping methodology in action: a developmental study 2000. *Educational Technology Research and Development*, *48*(2): 63-80

[19] Tripp, S.D. & Bichelmeyer, B. Rapid prototyping: an alternative instructional design strategy 1990. *Educational Technology Research and Development*, *38*(1): 34-44, Springer.

[20] Şimşek, A. "Öğretim Tasarımı ve Modelleri. Instructional design and models, instructional technology foundations: theories, research, trends. Pegem Akademi, pp. 99–116, 2013.

[21] McCormac, A., Zwaans, T., Parsons, K., Dragana, C., Butavicius, M., & Pattinson, M. Individual differences and information security awareness 2017. *Computers in Human Behavior*, vol. 69, pp. 151–56.

[22] Parsons, K., Dragana, C., Pattinson, M., Agata, M., & Tara, Z. The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, vol. 66, pp. 40–51.

[23] Öğütçü, G. *E-dönüşüm sürecinde kişisel bilişim güvenliği davranışı ve farkındalığı analizi*. [Analysis of Personal Information Security Behavior And Awareness in E-Transformation Process] Başkent Üniversity, 2010.

[24] Korkut, O. Çankaya İlçesi Milli Eğitim Müdürlüğü'ne bağlı ilköğretim okullarına ait web sitelerinin grafik tasarım açısından incelenmesi ve örnek web sitesi tasarımı hazırlanması. [The examination of the websites of the primary schools depending on Çankaya County Directorate of Education from the aspect of graphic design principles and preparation of example website design] Gazi University, Ankara, 2012.
[25] Franke, U. & Joel, B. Cyber Situational Awareness–a systematic review of the literature 2014. *Computers & Security*, vol. 46, pp. 18–31.
[26] Bostan, A. & Şengül, G. *Siber Güvenlik Farkındalığı Oluşturma*. [Development of Cyber Security Awareness] Grafiker Yayınları, 2018, Retrieved from https://www.sasad.org.tr/uploaded/Siber-Guvenlik-ve-Savunma-Farkindalik-ve-Caydiricilik.pdf.
[27] Panigrahi, R., Praveen, R.S., & Dheeraj, S. Online learning: adoption, continuance, and learning outcome-a review of literature." *International Journal of Information Management*, vol. 43, Dec. 2018, pp. 1–14. DOI.org (Crossref), DOI:10.1016/j.ijinfomgt.2018.05.005.
[28] Micarelli, A. & Filippo, S. A case-based system for adaptive hypermedia navigation. *European workshop on advances in case-based reasoning*, Springer, 1996, pp. 266–79.
[29] Otter, M. & Hilary, J. Lost in hyperspace: metrics and mental models. *Interacting with Computers*, vol. 13, no. 1, Oxford University Press Oxford, UK, 2000, pp. 1–40.