The European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2020.10.03.117

ICEST 2020

International Conference on Economic and Social Trends for Sustainability of Modern Society

CYBER LITERACY AS ONE OF THE MAIN DISCIPLINE NECESSARY IN MODERN TIME

I. A. Magomedov (a)*, H. A. Murzaev (b), A. L. Zolkin (c)
*Corresponding author

(a) Chechen State University, 32 Sheripov Street, Grozny, Russia, ismwork@mail.ru
(b) Chechen State University, 32 Sheripov Street, Grozny, Russia
(c) Volga State University of Water Transport (Samara branch), 62-64 Molodogvardeyskaya Street, Samara, Russia, alzolkin@list.ru

Abstract

The work illustrates the need of the cyber literacy in modern time as a discipline thought in the higher education institutions and in the secondary school as well. Due to the unawareness of treats from cyber-attacks user's privacy can be infiltrated and thus the personal information or date can be stolen or erased. In this paper, the problem of cyber literacy is considered and studied, as lately the number of attacks increased. Examples of massive cyber-attacks that have occurred due to insufficient cyber literacy are considered. The following cyber-attacks are also briefly explained: phishing emails, Drive-by download, Homograph Attack. These cyber-attacks represent the most common treats that occur in the present days. Based on the research conducted, solutions to the problem of cyber literacy have been derived. Also, the cyber-attacks of two periods of 2018 and 2019 are considered and compared with the usage of EU countries, which are Nederland, German, UK, Ireland and Denmark.

Keywords: Cyber literacy, discipline, cyber-attack, phishing emails, drive-by download, homograph attack.

1. Introduction

There is no doubt that lately there has been a revolution in information communication and computation technology, and yet the technological progress is continuing and nowhere near of stopping (Konsbruck, 2001). This event can be compared equally with the revolution that took place around the mid-18th century (Madhushree et al., 2019). Therefore, the dramatic change influences not only technological side, but have influences on our daily life, work, educational institutions, society and etc.

The technological progress unlocks vast opportunities and yet might have in the hands of unskilled user opposed consequences to the first mentioned statement. We live in the 21th century and the generation can be safely described as generation of information technology or in other words the generation of the Internet. Integration of the Internet in our daily life went with the development of the information technology (Mentsiev et al., 2019). And with the development of the Internet, many opportunities have opened up for all kinds of scammers who take advantage of the unawareness of people, or rather their illiteracy. And in order to lessen the damage from all kinds of "hackers", it is crucial to increase the level of cyber literacy of the population. And the introduction of cyber literacy, as a discipline, in modern educational institutions can significantly contribute to this (Mentsiev & Chebieva, 2019; Pritam et al., 2011). For a better effect the secondary schools also can be considered with the higher education institutions (Burkaltseva et al., 2019; Loki et al., 2014). This article describes the reasons why cyber literacy is necessary as a discipline in modern educational institutions.

2. Problem Statement

The Influence of Information communication and computation technology is increasing day by day and it is influencing all the segments of our life, with a visible advantage and some hidden drawbacks. Therefore, it is important to study the issue thoroughly and teaching it in educational institutions will have a positive effect on it.

3. Research Questions

The importance of the introduction of cyber literacy discipline in educational institutions will be covered in the article. Unawareness of the users, of the treats from the Internet, and its effect to the personal and workplace environment. The treats that are most common in the Internet and their influence and damage to the user.

4. Purpose of the Study

The aim of the study is to demonstrate the importance of knowledge and its further improvement in cyber literacy of the population by introducing a discipline in the educational institutions.

5. Research Methods

Vulnerability of a modern network user will be discussed in this paragraph. It is well known that technologies improve every year and new updates fixes old mistakes. Even with the new improvements the hackers find a new way of braking the defence and end up stealing information (whether its personal information, bank accounts or some other) (Alexei, 2020; Michael & Jennifer, 2013). Therefore, some of the main treats, that are most common in the present will be discussed.

Fake applications

The studies show that the level of cyber literacy is much higher than, for example, 10 years ago. However, the fact is that hackers also know about this, and therefore their approaches are becoming more sophisticated. If earlier, scammers could only steal money from a phone account (using calls and SMS), now with the occurrence of online banking (apps), the scope is widened. There are many options to do this. For instance, one of these options is fake applications. Most often, fakes pretend to be popular instant messengers, applications for cryptocurrencies, music, or even a real game (Manuel, 1996). Therefore, it is important to monitor, what is happening on the screen of the device, that are used (whether it is a smartphone, tablet, PC, etc.).

Drive-by download

Drive-by download is a fairly new type of cyberattack: now a user don’t need to download anything, due to this technology a user can become infected simply by visiting a website. This mainly happens with those who do not update their applications, such as browsers. Hackers use bugs in the old version of the application to quietly run their code (Aikaterinaki, 2009; Kaushik & Nabanita, 2016).

Therefore, users need to understand that using official applications is much safer than using websites, since developers immediately put a number of checks into them. But, the more potential victims come from a mobile device, the more temptation for a hacker to attack them, despite all the difficulties.

Sometimes scammers hire a whole team of coders, designers, layout designers, managers in order to copy the application in a quality manner. And sometimes, user really need to have a good level of cyber literacy to distinguish a fake from a real application.

A variety of cyberattacks and their progression

It should be noted that most of the cyber-attacks are not specifically targeted at anyone, these are ordinary trojans or phishing emails that very often surf the net. The victims of such attacks, as a rule, are those who have not taken care of their safety or their cyber literacy. For example, a network user receives an e-mail with attractive content: messages about fake winnings, about the sale of a product, etc. Most people ignore such letters; however, the proportion of illiterate (in cyber-attacks) people is also not small. The trusting user opens the letter, follows the link or opens the file attached to the letter, after which nothing happens. More precisely, the user thinks so, although infection occurred at that very moment. "Infected" thinks that some kind of mistake has occurred, closes the letter and forgets about it. After some time, the user notices that the amount of money has disappeared on the bank card or, in general, has been completely erased. And there are many such examples (Blazhevich et al., 2019; Reichman, 2013).

Homograph attack

Also, fraudsters can, using various sites or applications, force network users to pass verification of a social page. After which, again, nothing will happen, at least the infected person will think so. The fact is that scammers completely copy the appearance of the login page of a site or application, while posting the

https://doi.org/10.15405/epsbs.2020.10.03.117
Corresponding Author: I. A. Magomedov
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

whole thing with a fake URL. There are even various programs designed specifically to generate fake URLs (Jacks et al., 2011).

This scam is called a Homograph Attack. Now most browsers themselves determine the possible danger, but this does not always help, and therefore the Homograph Attack should not be discounted.

This example clearly shows that the issue of cyber literacy among the population, today, is more important than ever and one can save from these treats by knowing them. Therefore, it is important to teach the safety.

6. Findings

According to data from the 2019 Global Economic Forum Global Risk Report, data fraud as well as cyber-attacks are the fourth and fifth global risks that every organization faces. By their significance, these risks are equated with environmental problems.

ACR is the official annual report on cybercrime. The report for 2019 contains information that hacker attacks in the world occur almost every 14 seconds. InfoWatch specialists conducted a study in which it turned out that in 2019 over 14 billion confidential records had leaked to the network. A report also provided by InfoWatch says that compared to 2018, in 2019, the increase in the number of leaks worldwide increased by 10%. However, in Russia the percentage of leakage is much higher, approximately 40% .

DLA Piper also provided its report, which cited the statistics of GDRP (the general regulation of the protection of personal data of the EU), which refers to the number of notifications of cyber-attacks (Table 1).

If compare 2019 and 2020, one can establish that the growth in the percentage of notifications of cyber-attacks was 12.6%. However, experts predict an inevitable increase in these indicators in the coming years.

But it is interesting that the total number of registered cybercrimes is only 10-12% of the actual number of cybercrimes. Understanding why this is not so difficult with the registration of cybercrimes. The fact is that the majority of affected citizens and organizations that have undergone a cyber-attack (in most cases this is extortion on the network) are afraid to seek professional help, as they are afraid of the possible publication of stolen information.

The above analysis once again confirms that the problem of cyber literacy of the population, today, is more relevant than ever.

Table 01. Number of cyber-attacks notifications. With the chosen two periods: 2018-2019 (from May to January and 2019-2020 (from January to January)

Countries	2018-2019	2019-2020
Netherlands	15400	25247
Germany	12600	25036
UK	10600	11581
Ireland	3800	6716
Denmark	3100	6706

7. Conclusion

To conclude, it can be said that despite all the efforts of information technology companies to ensure the information security of the population, the issue of cyber literacy does not lose its relevance and the need to increase it is growing every day.

Today, information technology is implemented in almost all areas of human life. Under such conditions, the damage caused by hackers is very large if even a simple toaster can be attacked. However, with a good level of cyber literacy, all damage can be minimized.

Cyber literacy, today, as a discipline, is necessary in modern educational institutions.

References

Aikaterinaki, N. (2009). Drive-by download attacks: Effects and detection methods. *IT Security Conference for the Next Generation.* https://pdfs.semanticscholar.org/be51/-669c3489c3d75f7421d077989bbf35e9dd7f.pdf

Alexei, C. (2020). Data Leaks 2019: statistics, cybersecurity trends and measures to reduce the risks of hacking. https://vc.ru/services/103616-utechki-dannyh-2019-statistika-tendencii-kiberbezopasnosti-i-mery-po-snizheniyu-riskov-vzloma

Blazhevich, O. G., Burkaltseva, D. D., Shalneva, V. V., Smirnova, E. A. … & Gadayeva, K. R. (2019). Municipalities: opportunities to improve financial security. *Revista Inclusiones, 6,* 120-133.

Burkaltseva, D. D., Blazhevich, O. G., Gabrielyan, O. A., Savchenko, L. V., … & Abubakarov, M.A. (2019). Development of the financial security of the state: neutralization of threats. *Revista Inclusiones, 6,* 294-312.

Jacks, T., Palvia, P., Schilhavy, R., & Wang, L. (2011). A Framework for the Impact of IT on Organizational Performance. *Business Process Management Journal*, *17*(5), 846-870.

Kaushik, B., & Nabanita, D. (2016). Impact of Information Technology on the TeachingLearning Process. *International Research Journal of Interdisciplinary & Multidisciplinary Studies (IRJIMS)*, *2*(11), 131-138.

Konsbruck, R. L. (2001). Impacts of Information Technology on Society in the new Century. *Route de Chavannes*. https://www.zurich.ibm.com/pdf/news/Konsbruck.pdf

Loki, M., Walter, O., Ngati, F. ,& Nyakweba, B. (2014). Effects of information technology in learning institutions. *International Journal of Economics, Commerce and Management*, *2*(10), 1-15.

Madhushree, L. M., Revathi, R., & Aithal, P. S. (2019). A Review on Impact of Information Communication & Computation Technology (ICCT) on Selected Primary, Secondary, and Tertiary Industrial Sectors. *Munich Personal RePEc Archive.* https://pdfs.semanticscholar.org/6d1e/efffcf75109813bc12c62b879e7afaff9295.pdf?_ga=2.173379744.2094127337.1587642477-269733478.1572028875

Manuel, C. (1996). The Rise of the Network Society (2nd Edition). *The Information Age Economy, Society and Culture, 1.*

Mentsiev, A. U., Almurzaeva, P. H., Ashakhanova, M. Z., Anzorova, A. I., & Dauletukaeva, K. D. (2019). The impact of digital technology on the study of languages and the development of digital education. *Journal of Physics: Conference Series, 1399,* 1-6.

Mentsiev, A. U., & Chebieva, H.S. (2019). Modern Internet Security Threats and Countermeasures. (overview). *Engineering Herald of the Don*, *3*(54), 16.

Michael, B., & Jennifer, R. (2013). *How to Build it, How to Keep it, and Why it Matters.* Alpina Publisher.

Pritam, S. N., Vineeta, N., & Akhilesh, C. P. (2011). Impact of Information Technology on Learning, Teaching and Human Resource Management in Educational Sector. *International Journal of Computer Science and Telecommunications*, *2*(4), 66-72.

Reichman, I. (2013). *The practice of media measurement.* Alpina Publisher.