Online Journal of Communication and Media Technologies, 2023, **13**(4), e202358
e-ISSN: 1986-3497

OPEN ACCESS

Research Article

The impact of educational training on improving the vigilance of public officials against cyber-attacks

Astrit Hulaj [1]
0000-0002-4059-2034

Artan Dreshaj [2*]
0000-0003-0204-8502

[1] Faculty of Computer Science and Engineering, University for Business and Technology, Pristina, KOSOVO
[2] Faculty of Contemporary Sciences and Technologies, South East European University, Skopje, NORTH MACEDONIA
[*] Corresponding author: artan.dreshaj@gmail.com

Citation: Hulaj, A., & Dreshaj, A. (2023). The impact of educational training on improving the vigilance of public officials against cyber-attacks. *Online Journal of Communication and Media Technologies, 13*(4), e202358. https://doi.org/10.30935/ojcmt/13784

ARTICLE INFO

Received: 4 Mar 2023

Accepted: 24 Aug 2023

ABSTRACT

Cybersecurity today is a phenomenon of global and multidimensional proportions. Protecting against cyber-attacks is a challenge for governments and the private sector. Increasing the security and protection of data and critical infrastructure against cyber-attacks is one of the essential factors of an institution that manages confidential data. The authors first present the findings from the research conducted regarding the skills that public officials have on various risks from cyber-attacks. The authors then present the results from testing the skills of public officials through the simulation of two cyber-attacks and the method applied by one public institution in Kosovo (as case study for this research is used Ministry of Internal Affairs - MIA) to raise the awareness of its officials about the various risks of cyber-attacks. Also, this paper focuses on analyzing the results before and after increasing the skills of MIA officials against cyber-attacks, as well as giving concrete recommendations from the results and analyses made. The presented results show that the applied method for raising the awareness of public officials on the risks of cyber-attacks has given impressive results. The obtained results are supported by statistics obtained from the conducted tests.

Keywords: cyber-attacks, cyber security, phishing, education, awareness, CERT

INTRODUCTION

Information technology today has an impact key in many fields (Hulaj & Shehu, 2018), such as education, government, industry, medicine, the military, etc. Information technology has played an important role in educational institutions, especially after the COVID-19 pandemic (Awajan, 2023; Nasongkhla & Shieh, 2023). Today many economic, commercial, cultural, social, and governmental activities (Li & Liu, 2021) and interactions between various countries are used based on information technology (Hulaj et al., 2022). Changes are so fast that it is not easy for technology users or governments to stay on trend with technology developments. Moreover, we live in the IoT and AI era (Hulaj et al., 2023), where technology is a significant factor in modern learning (Alanezi, 2022), communication, etc. Technological developments are so fast that no country can be immune to such technological progress, including the countries of the Western Balkans. Also, rapid progress is observed in Kosovo in information technology, especially in state institutions (government institutions). Government institutions of Kosovo have so far managed to provide most of the services for citizens, businesses, and other categories online. Through online services for citizens and businesses in Kosovo, the government of Kosovo offers effective and fast services, access to services from any point and distance, promotion of economic and social development, etc.

Providing online services and accessing the Internet presents a significant risk and exposure to cyber-attacks (Yusif & Hafeez-Baig, 2021). According to Internet World Stats (2021), the global Internet penetration rate of the population presented as a percentage is about 65.6%, with more than 5,168,780,607 internet users. Accessing the Internet and providing services to citizens and businesses online presents the risk of exposing sensitive data to cyber-attacks. Therefore, protecting this data from cyber-attacks is a challenging issue. The main challenge for all users connected to the Internet is how to provide fast and efficient services and how to provide it while protecting their data from cyber-attacks. The trend of cyber-attacks is constantly increasing and has shown an increase after the Russia-Ukraine war. Attackers exploit the weaknesses that eventually exist in the various hardware, software, and communication layers to carry out cyber-attacks. To achieve penetration, hackers use different methodologies, techniques, and procedures to achieve their objectives of access to critical state systems. In 2020, many attacks challenged the governments of various countries with a level of sophistication of cyber-attacks through the chain cyber-attack through SolarWinds software. Then the attacks happened on colonial pipeline in 2021 through ransomware-type attacks (Watney, 2022). In the period 15-16 July 2022, hackers attacked government systems in Albania through massive attacks that had the purpose of erasing systems, access to confidential data, using data for state purposes, etc. With such attacks, Kosovo is constantly challenged, especially with phishing attacks. At the same time, when challenged with cyber-attacks on the government systems in Albania, hackers also attacked Kosovo's state systems. However, thanks to prior investments in network infrastructure and security, it was possible to prevent such attacks, and the penetration of hackers into government systems was impossible. Hackers managed to break into some applications that provided services to citizens, but they had not managed to penetrate critical systems and sensitive state data.

Today, there are several risks, each more significant than the other. Among the main dangers exposed to which Internet users (whether individuals or institutions) are various cyber-attacks such as malware attacks, phishing attacks, man-in-the-middle attacks, SQL injection attacks, denial-of-service attacks, etc. **Malware attack** is one of the most frequent types of cyber-attacks. Malware is malicious software that can install on the victim's device without the victim's consent and performs actions without the knowledge of the victim's system. **Phishing attack** is a type of attack that hackers use to steal user data, including login credentials and credit card numbers. The logic used in the phishing attack is to disguise the sender as a trusted source, convincing the victim to open an email, instant message, etc. With action attempts to deceive the receiver into clicking a malicious link, which can lead to the installation of malware and theft of user credentials, gaining access to sensitive data. **Man-in-the-middle** attacks are when an unintended actor positions himself in a conversation between a user and the web application. **SQL injection attack** is a common attack vector that uses malicious SQL code to manipulate the database to gain access to sensitive information. **Denial-of-service attacks** are denial-of-service (DoS) attacks. The logic used by denial-of-service attacks is generating uncontrolled traffic, which blocks a machine or network, making it inaccessible to the intended users.

To protect against cyber-attacks, the governments of different countries seek and use various alternatives and apply specific preventive measures. However, these alternatives and used measures do not guarantee that such attacks will not occur. However, some steps are necessary to prevent or reduce the effects of such attacks. One of the essential steps to prevent cyber security threats and cyber-attacks is the awareness of users who use information and communication technology (ICT) devices and services. This research paper will focus on presenting the current cyber security situation, risks, and actions by the Ministry of Internal Affairs (MIA) to educate its officials to increase their vigilance to improve cyber-attacks. As this research shows, the education of officials plays an essential factor in protecting data and critical infrastructure against attacks.

RELATED WORK

In this section, we will review some related works to this field of research published by other authors. Global Cyber Security Capacity Center undertook a second review of the maturity of cyber security capacity in Kosovo in 2019 (Bund & Esteve-Gonzalez, 2020). The objective of this review was to enable Kosovo to understand its cybersecurity capacity to prioritize government investments in cybersecurity capacity and to help measure progress in implementing the recommendations from the first review made in 2015. As described in the content of this report, evaluation cooperation with the Ministry of Economic Development did not include MIA as one of the primary institutions in the Government of Kosovo responsible for cyber security policy making and implementation. This report does not include in its composition the plan of execution of activities based on the National Cyber Security Strategy of Kosovo (KNCS). Therefore, this was the cause why the report does not describe the correct situation and activities taken by the Government of Kosovo to enhance cyber security.

Duić et al. (2017) introduce the concepts and principles of cyber threats that affect security in an international context. In this paper, the authors present the challenges different countries face in cyber-attacks and their impact on international relations. However, the authors in this paper do not show any practical steps that include educating technology users against cyber-attacks. Jang-Jaccard and Nepal (2014) show the risks that can come from the execution of malware to carry out cyber-attacks. The authors then show an overview of software, hardware, and network vulnerabilities. They present existing defense techniques and vulnerabilities that existing methods have to prevent such attacks. Finally, based on their research, the authors propose a method for protection against cyber-attacks.

Cherdantseva and Smart (2020) present an analysis of the cyber situation in general in Australia. Then, they show an analysis of the risks and training centers about cyber security. They also present the problems that universities have in retaining qualified academic staff regarding cyber security. Finally, in this research, the authors show the strategy developed by the Australian federal government for protection against cyber-attacks. Based on this research, the authors recommend the need for education, training, and awareness of users (Alharbi & Tassaddiq, 2021). AlSobeh et al. (2023) discuss cyber security issues for teenagers in Jordan. They address the effects and impact that the last cyber-attacks in Jordan have had on teenagers in Jordan. Based on the research conducted on adolescents and the data collected, the authors offer recommendations to start with educational programs for teenagers throughout Jordan to increase cybersecurity awareness. The authors point out that through education, teenagers can be better equipped with the knowledge to protect themselves and their society from the risks of possible cyber-attacks.

Watney (2022) addresses cyber security threats and cyber-attacks against state and non-state critical infrastructure. The authors provide an analysis of the increase in cyber-attacks against critical infrastructure and state systems, with particular emphasis on the focus of the research on cyber-attacks carried out by hackers through ransomware-type attacks. Also, they focus on the challenges that state governments have today to protect themselves from cyber-attacks and recommend that countries should have well-prepared staff and experts to protect against cyber-attacks against government systems and critical state infrastructure.

Unlike the research conducted by other authors, we have used another strategy and methodology to increase the level of education of MIA officials on the risks that may come from cyber-attacks. Initially, we gathered information about officials' skills in cyber-attacks. Then we tested their skills in the field of cyber-attacks by simulating a cyber-attack, and after the implementation of the simulation of the cyber-attack and the collection of results by the cyber-attack completed training for all MIA officials to increase their skills in the field of cyber-attacks. Finally, has been simulated a second cyber-attack to see how much the awareness of MIA officials improved against cyber-attacks. Below are presented the strategy used, the methodology, and the results achieved.

PROBLEM FORMULATION AND RESEARCH METHODOLOGY

Problem Formulation

In recent years the increase of electronic services has increased the number of cyber-attacks on government infrastructure. In 2018, in the time, when the government of Kosovo decided on a 100% tax for products produced in Serbia and Bosnia and Herzegovina, the information systems of the Government of Kosovo identified hundreds of cyber-attacks with IP addresses originating from the countries of the Western Balkans. The target of these cyber-attacks was the e-mails of officials in the Ministry of Foreign Affairs. Cyber-attacks on government systems continued in 2019, where during 2019 were attacked several government websites, and the IP addresses of the attackers were from several countries and different continents. In 2020, there was a cyber-attack on the information system at the Ministry of Finance, where the objective was to generate property taxes. The cyber-attack had taken place from within the state infrastructure. Also, cyber-attacks of various natures have continued in 2021 and 2022, where there has been a tendency to steal the passwords of government officials through phishing attacks.

A threat to government information systems is the lack of awareness of public administration officials about cyber threats. The lack of skills of government officials to manage passwords and privileges in the Ministry of Finance in the information system of the treasury has resulted in a loss of about two million euros. Also, there is an increase in cyber-attacks in the private sector, especially in the banking sector, but the problem is the non-reporting of incidents by the private sector. Therefore, these events have influenced MIA to undertake awareness-raising actions for its officials and create professional IT staff for cyber-attacks.

Research Methodology

The hypotheses presented in this research are to find the causes that lead to cyber-attacks and to propose solutions that reduce the risks of cyber-attacks on government infrastructure. In this research, the methodology used is quantitative and qualitative. This research first collected data on the capabilities of government officials for cyber-attacks. Data collection in this research make through a questionnaire that contains seven basic questions about cyber-attacks and to be taken actions if the government official suspects a cyber-attack. The design of the questionnaire by the Community Emergency Response Team (CERT) management was carried out and included closed questions. The purpose of CERT was to collect data about the capabilities of officials against cyber-attacks so that they could come up with proposals and analyses about the state of the existing capabilities of officials. The reason for selecting closed questions in the questionnaire was to provide the officials with an easy-to-complete and short questionnaire. The purpose of this questionnaire was to data collection regarding the skills of government officials for cyber-attacks and their actions in these situations. This questionnaire classified officials into three categories. The first category included all professional officials. The second category included personnel in leadership positions, while the third category included IT officials (here included officials of all IT categories).

Data collection questions on officials' cyber-attack skills

In this research, was prepared a multi-level questionnaire to improve the quality of the questionnaire. The questionnaire contained seven closed-ended questions to gather data intended by CERT about officials' skills of cyber-attack risks and their actions in such cases. The questionnaire is to be simple for all categories of officials, including MIA officials at the central and local levels, regardless of their position at the ministry. The completion of the questionnaire had an approximately equal extent in the entire territory of Kosovo (including officials at the registration centers at the local level and officials at the ministry), with a difference of 2% more by officials at the central level than officials at the local registration centers. The prepared questionnaire has included the following questions.

Q1. Select one of the categories (IT, manager, professional).

Q2. Do you use PCs and official email (yes, no)?

Q3. What is your level of IT skills (very good, good, poor)?

Q4. Have you received any suspicious emails? (yes, no)?

Q5. If you received a suspicious email, how did you act (where you are required to provide credentials, open any documents attached to the email, etc.): opened it, clicked the link, deleted it, or have you consulted with officials of IT?

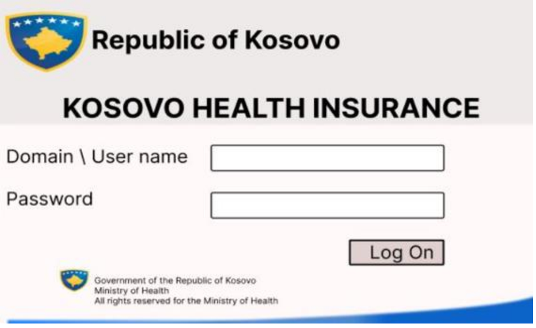
Q6. Have you been the victim of a cyber-attack, where are stolen your credentials for email, Facebook, Instagram, etc. (yes, no)?

Q7. If you have been the victim of a cyber-attack, what is your first action?

The results for each of the questions will present in the results section.

Simulation of cyber attacks

After collecting data on the skills of government officials in their response to cyber-attacks, CERT officials tested the skills of government officials through a simulation cyber-attack. In this case, note that CERT officials regularly send emails to government officials to inform them about phishing emails and the dangers that can



Republic of Kosovo

KOSOVO HEALTH INSURANCE

Domain \ User name

Password

Log On

Government of the Republic of Kosovo
Ministry of Health
All rights reserved for the Ministry of Health

Figure 1. View of the application for the authentication of officials (Source: Authors)

come from these attacks. A few days before cyber-attack simulation, CERT officials sent an informational email to all officials asking them to be careful about phishing attacks and report any suspicious emails to CERT.

Simulating the first cyber attacks

Following the informational email, CERT officials began preparations for the cyber-attack simulation. The cyber-attack simulation was prepared in complete secrecy by CERT team. CERT team analyzed several options for conducting the cyber simulation. After some analysis, CERT team decided that the cyber-attack simulation corresponded to the expectations had officials at that time. At that time, the government expected that determine the implementation of the law on health insurance for all state officers. Therefore, CERT team decided to link the cyber-attack to this law. The simulated cyber-attack was of the phishing type. For this case, CERT team prepared a web application that we hosted on an internal government network server, whereas the link to access to web application we sent to the officials via email. To make the sent email reliable, we sent the phishing email from an external domain. The phishing email required government officials to authenticate with the official account, through the official email and password, to proceed with other health insurance registration steps. Officials had three days to register. **Figure 1** shows the view of the official authentication application for the first cyber-attack.

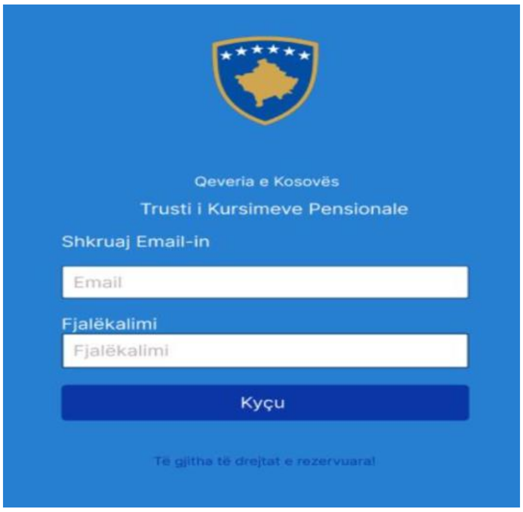
The purpose of this simulation of cyber-attacks was to test the skills of the government officials of how much they are aware of the risks that cyber-attacks bring to them. The data we aimed to collect through this phishing cyber-attack simulation were:

- The number of officials who report the problem to CERT team.
- The number of officials who will be victims of this cyber-attack.
- The number of government officials that ignore this cyber-attack and take no action.

The results and analysis section will show the data collected through the first cyber-attack simulation.

The method applied to improve awareness of cyber-attacks

After analyzing the results obtained from the simulation of the first cyber-attack, the results of which were not good, CERT team proposed to provide educational training for all officials to increase the awareness of officials to cyber-attacks and the risks that can come from them. But as a start, it was proposed to provide training for the officials of the ministry. Note that the education of officials is essential not only against cyber-attacks but also in many other areas. On-the-job staff education is effective in many fields as buildings (Matondang & Sitompul, 2021), cyber security, schools (Khamcharoen et al., 2022), cyberspace (Hu & Gong, 2022), various businesses, etc. Cybersecurity education has two elements: first, people need to be made aware of the need to take precautions, and then teachers need to provide the skills they need to take the necessary precautions (Venter et al., 2019). CERT team prepared the training for all MIA officials called cyber education. "Cyber education" training covered several topics: how to manage the use of accounts and passwords, how to be aware of online downloads, how to be careful when accessing public areas on Wi-Fi networks, how to understand phishing emails, how to be careful when using data storage devices (USB, micro SD, etc.), how to protect yourself from malware, especially ransomware, how to take care of the security of personal and official data, etc. The training about cyber security for MIA officials was holed at the government training center and provided in groups of 25-30 officials. This training included all the officials of MIA.



Qeveria e Kosovës

Trusti i Kursimeve Pensionale

Të gjitha të drejtat e rezervuara!

Figure 2. View of the application for the authentication of officials in the second cyber-attack (Source: Authors)

Simulation of second cyber-attacks

To understand the results of the training and self-education of officials against cyber-attacks, CERT team began preparations for the simulation of a second cyber-attack, so the second cyber-attack simulation, CERT team, decided to be similar to the first cyber-attack, so the phishing. The focus of such a cyber-attack was to test the improvement of the officials' skills, against cyber-attacks of this nature, after their training. So, the simulation of the second cyber-attack suited the pandemic situation with COVID-19 in Kosovo. Respectively, the second cyber-attack was related to the return of funds withdrawn by 10% from the pension savings fund. The amount in value of 10% of the pension trust was withdrawn by each citizen of Kosovo from their accounts during January-June 2021, based on the government Kosovo law on economic recovery no. 07/L-016, dated 4 December 2020, where through the approval of this law, the Government of the Republic of Kosovo enabled all citizens of Kosovo who had a pension trust possibility of the withdrawing 10% of the amount of their pension trust. Also, based on this law, the Government of Kosovo will reimburse this amount withdrawn in the following years. Therefore, the second cyber-attack simulation was supposed to be related to this field of action. The simulation of the second cyber-attack, in essence as the simulation of the first cyber-attack, was prepared by CERT team in complete secrecy.

After approval from the highest hierarchy of the ministry and preparation of the cyber-attack, CERT team sends emails to 1223 MIA officials (number of officials who were in MIA on the date of sending the email). Through email, have been informed officials about the return of their pension trust in the amount of 10% by the Government of Kosovo, which they had withdrawn some months ago. Officials were also required to verify the implementation of the return of their funds by authentication with their official usernames and password. The email was sent to MIA officials by CERT from a private email address and an external domain which domain purchased by the ministry only for this simulation. The description of the email to be as convincing as possible for the officials was the Kosovo Pension Trust. However, if officials would go to the email and click on the email received or the mouse was put over the email received, all can be seen that the phishing email was external and had nothing to do with the official email. **Figure 2** presents the view of the application for the authentication of officials in the second cyber-attack simulation.

RESULTS AND DISCUSSIONS

Results on Officials' Skills of Cyber Attacks

In this section, we will present the results regarding the skills declared by officials about cyber-attacks. We obtained the results through a questionnaire sent to 1345 officials for completion. The questions included in this research for data collection are presented in the sector of research methodology, respectively, in the sub-sector of research questions. The data collected for each research question we will show below. **Figure 3** shows the number of officials that have completed our study divided by different categories.

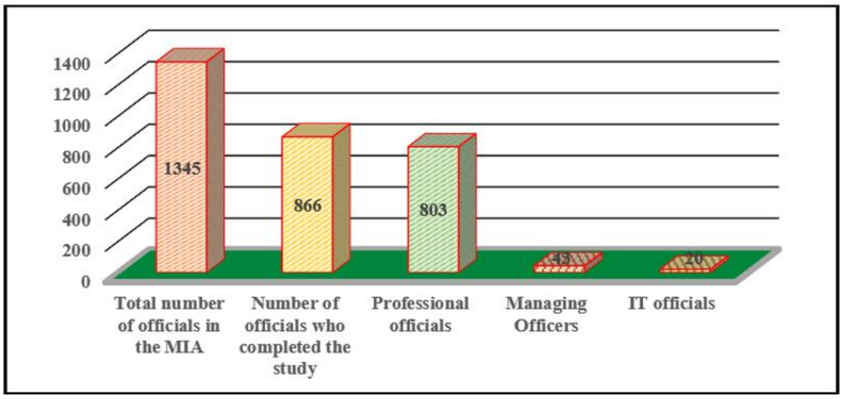


Figure 3. Research results based on question Q1 (Source: Authors)

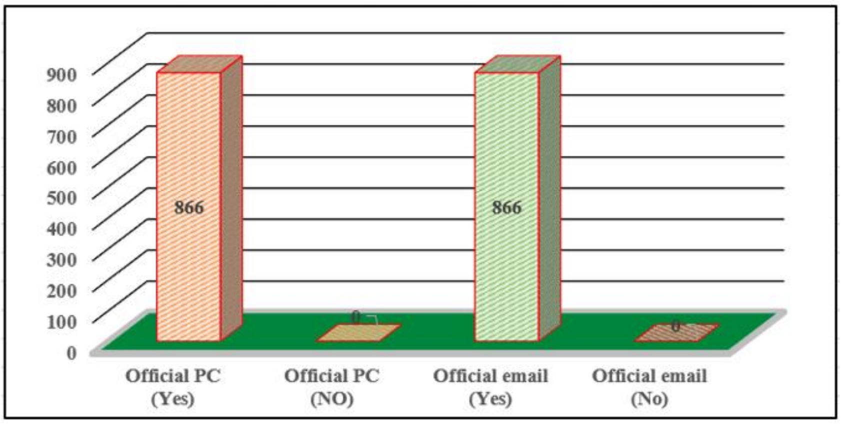


Figure 4. Research results based on question Q2 (Source: Authors)

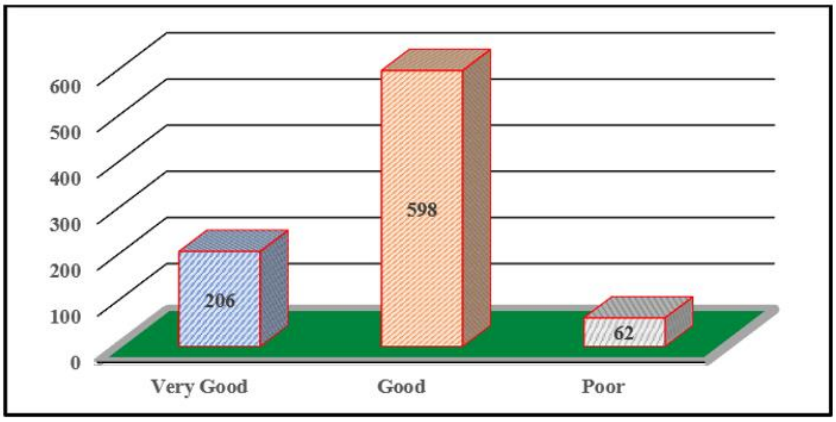


Figure 5. Research results based on question Q3 (Source: Authors)

Figure 4 shows the results around the declaration of officials if they have a PC and official email. Through question Q2 in the research questionnaire, we aimed to collect data on MIA officials involved in this research if they have a PC or official email because officials can have an official email configured on their phones but do not have a PC. This question shows all the officials who participated in the research had a computer and an official email (**Figure 4**).

Figure 5 shows the results of the declaration of officials on the skills they have in the IT field. Through question Q3 in the research questionnaire, we gathered information regarding the official's skills in IT. Out of 866 respondents, 206 responded that they have good skills, 598 responded to officials that they have good skills, and only 62 said they have poor skills regarding IT (**Figure 5**).

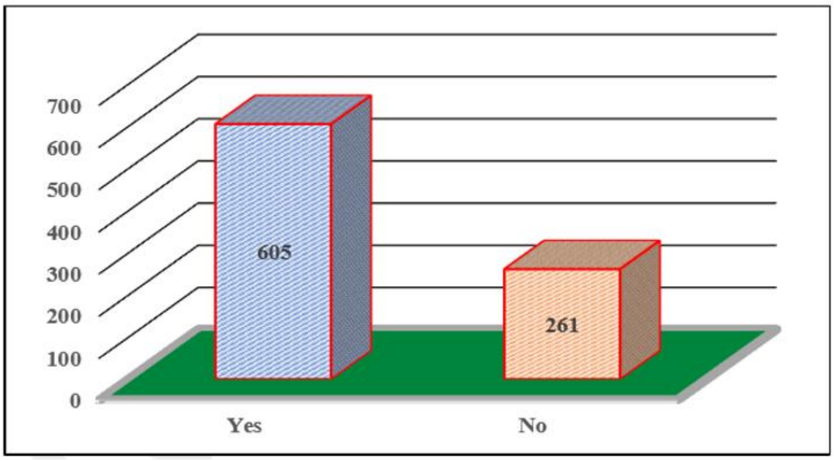


Figure 6. Research results based on question Q4 (Source: Authors)

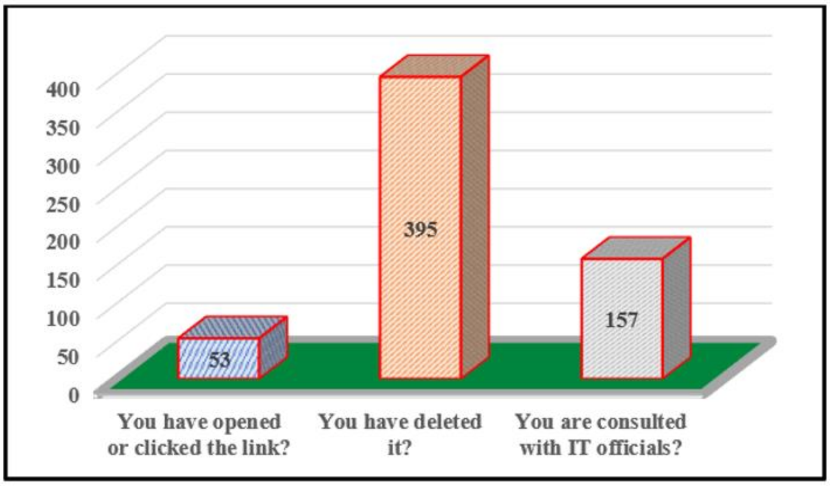


Figure 7. Research results based on question Q5 (Source: Authors)

Through question Q4 in the research questionnaire, we aimed to collect data if officials had any suspicions about any emails they had received. Of the respondents, 605 officials responded that they received phishing emails, and 261 officials responded to have not received such phishing emails. Figure 6 shows the results of this research question.

Then, through question Q5, we aimed to collect data on the actions taken by MIA officials who declared that they had received suspicious emails. Of the 605 who responded that they received suspicious emails, 53 said that they opened the attached document or clicked on the link, 395 said to have deleted it, and 157 responded that they consulted with IT officials about receiving suspicious emails. Figure 7 shows the results for research question Q5.

Through question Q6, we gathered information regarding whether MIA officials have been a victim of a cyber-attack. Out of 866 respondents, 156 responded that they had been victims of a cyber-attack, and 710 officials responded that they had not been victims of any cyber-attack. Figure 8 shows the results of research question Q6.

While through Q7, in the research questionnaire, we aimed to collect data on which was their first action if they have been victims of a cyber-attack. Out of the 156 respondents, who said that they were the victim of a cyber-attack, 3 of them reported that they had fulfilled the requirements requested by the attackers, 4 of them declared that call to the police, and 179 said that they had reported the case to CERT. Figure 9 shows the results of research question Q7.

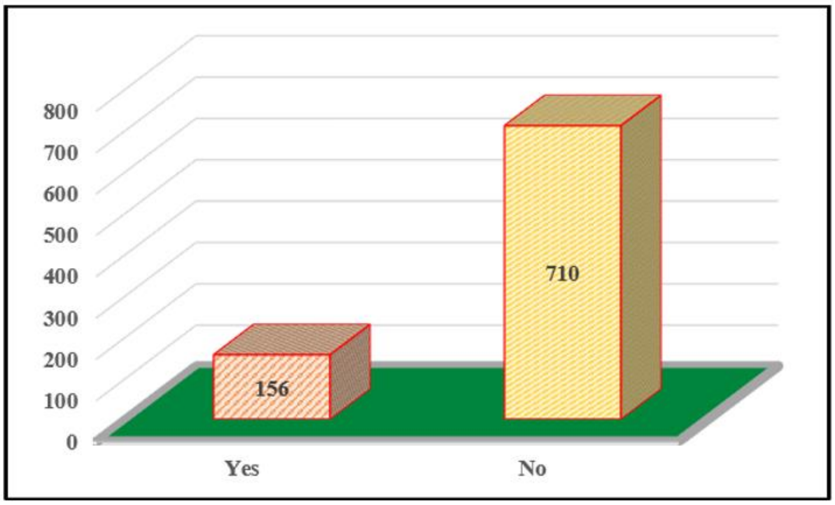


Figure 8. Research results based on question Q6 (Source: Authors)

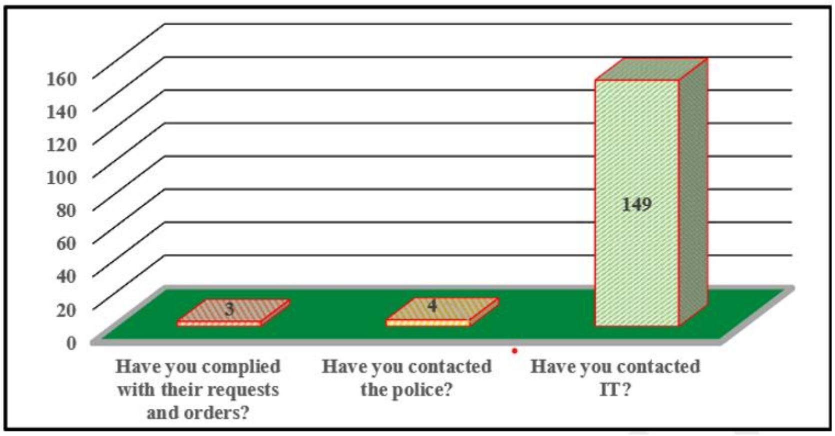


Figure 9. Research results based on question Q7 (Source: Authors)

Table 1. Some information that we have saved in our database after the officials are log in

No	Username	Password	Date & time of authentication	Computer name
1	It is not presented	Null	21/02/2022 11:08	MIA009
2	It is not presented	Null	21/02/2022 11:11	MIABB003
3	It is not presented	Null	21/02/2022 11:11	MIABL008
4	It is not presented	Null	21/02/2022 11:13	MIALB050
5	It is not presented	Null	21/02/2022 11:13	MIABA100
6	It is not presented	Null	21/02/2022 11:14	MIACC105
7	It is not presented	Null	21/02/2022 11:14	MIA006

Results of Testing the Skills of Officials Against Cyber Attacks

Following data collection on the skills the officials have declared they have regarding cyber-attacks and warnings about the dangers that may come from cyber-attacks, CERT team has prepared a cyber-attack simulation. To implement such an attack, CERT team initially received the necessary approvals within MIA. The methodology and method of preparing described the first cyber-attack simulation in detail in the sub-sector simulation of the first cyber-attack. After completing and sending the phishing-type email to the officials, the officials started registering immediately.

Table 1 shows some information stored in the database after the authentication of officials through the application presented in **Figure 1**. In this case, within the database was stored the username (we have not shown it in **Table 1**), date and time of authentication, password, and name of the computer. To avoid any possible misuse of officials' passwords, the password field, although completed by officials, we have stored null in the database.

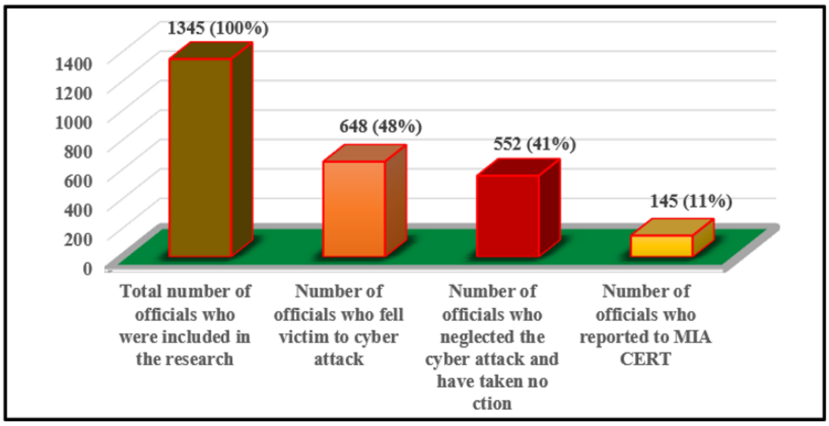


Figure 10. Data was collected from the first cyber-attack simulation (Source: Authors)

Figure 10 shows the results obtained from the simulation of the first cyber-attack. After collecting the data, we compared the data collected from this cyber-attack simulation with the data collected from the declaration of the officials on their skills of the risks they have for the first cyber-attacks presented in **Figure 3** to **Figure 9**.

From the results presented in **Figure 10**, we can see that the number of officials who were victims of this attack was very high. As we can see, 48% of officials were victims of the phishing type attack, 41% of officials had taken no action regarding the phishing email they had received, and only 11% of officials suspected it was a fraud and informed CERT team. Therefore, based on the results achieved, we can be concluded that the number of officials who were aware of the dangers of cyber-attacks was small. This situation contradicted the results the officials gathered when they asked if they were aware of the risks that may come to you from cyber-attacks (**Figure 4**). In that question, only 62 officials declare that has little skills, 598 good, and 206 very well. This situation was an alarm for the ministry leaders, who immediately began to think of solutions that would raise the awareness of MIA officials about the risks posed by cyber-attacks.

Based on results obtained from the simulation of the first cyber-attack, MIA CERT proposed and prepared education training for all MIA officials. The purpose of education training was to increase their awareness of various cyber-attacks. Details presented and methods applied to the education training prepared for MIA officials in the sub-sector of the technics used to improve security in MIA. After completing the education training on cyber-attacks and the risks that may come from them, is approved to start simulating the second cyber-attack from the highest level of management. Details about the creation, implementation, and simulation we have presented in the subsection simulation of the second cyber-attack. When finished preparing the simulation of the second cyber-attack, CERT of MIA sent the email to all MIA officials, which included the link for authentication of MIA officials. After sending the phishing email to MIA officials, some officials immediately started to report the event via email to CERT and called MIA officials CERT by phone. They tell CERT officials over the hotline that they received an email saying that returned 10% of the value was withdrawn from the pension trust a few months ago by the pension trust. They said they were suspicious about this email received and asked for advice on how to deal with the received email. But without giving much information about this email, officials who called CERT officials were advised to act on the recommendation discussed during the training. The reasoning of MIA officials CERT was that at the moment, they are not in their office, and after returning to their office, they will deal with the analysis of the email, and as soon as we analyze it, we will inform you. The email sent to the officials was active for three days. **Figure 11** show the results achieved by data collection through the simulation of the second cyber-attack.

From the results in **Figure 11**, we see that only 118 officials from 1223 officials, or 10% of the officials, were victims of the simulated cyber-attack. By comparing the results in **Figure 10** with those in **Figure 11**, we see that the number of officials who detected that this email could be fraudulent was considerable in simulating the second cyber-attack. **Figure 12** shows the data collection (comparison of results) between two cyber-attack simulations.

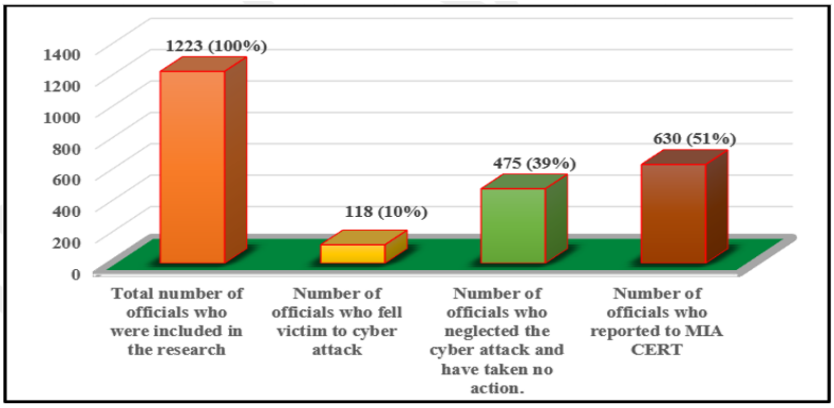


Figure 11. Data collected from the second cyber-attack simulation (Source: Authors)

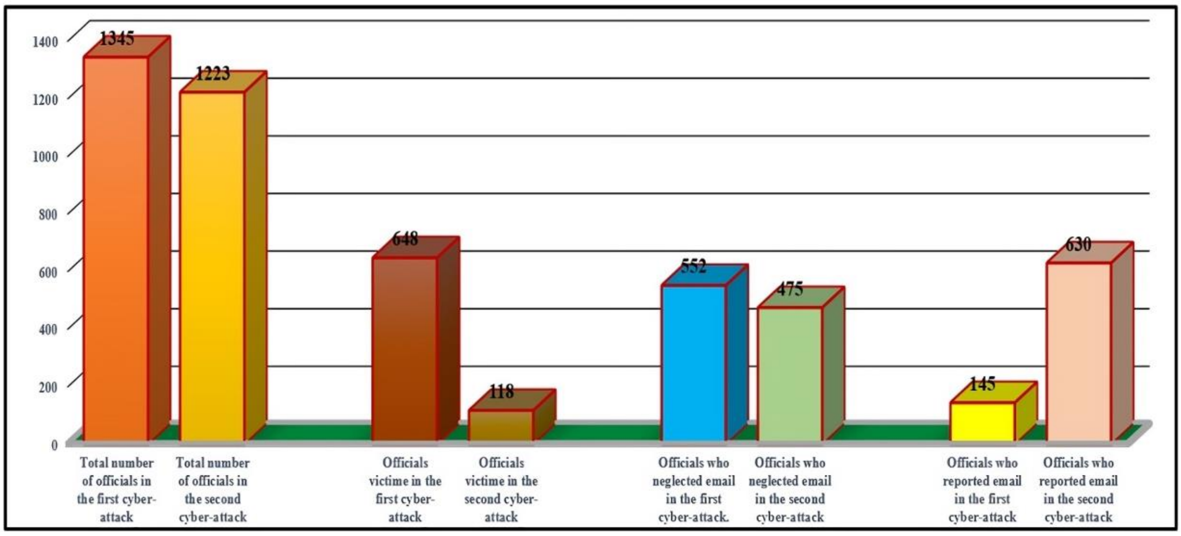


Figure 12. Comparison of results between simulation of the first cyber-attack & the second cyber-attack (Source: Authors)

If we compare the results before the educational training and after the training, we can conclude that we have an improvement in the officials' vigilance against phishing cyber-attacks. Respectively, the results from this comparison are impressive, even though they leave room to continue with their testing and education so that the officials are continuously informed about the possible risks. Therefore, based on the results presented in **Figure 12**, we can conclude that the training of MIA officials regarding the dangers of cyber-attacks has been successful and has influenced the improvement of officials' vigilance against potential threats from cyber-attacks.

CONCLUSIONS AND RECOMMENDATIONS

The findings of this research suggest that the awareness and education of officials about potential cyber-attacks have an impressive influence on reducing the risks of cyber-attacks. The results of this research show that regardless of investments in the new security networks project if the awareness and skills of the officials about cyber security are not at the right level, the protection from phishing cyber-attacks may not be successful. It suggests that educating and making officials aware of the potential risks of cyber-attacks can deliver more impressive results than investments in network infrastructure. Moreover, from the analysis and evaluation of the results of this research, we conclude that the best and most effective way to protect the network infrastructure and data within institutions is to increase the awareness and skills of officials about the risks that may come from cyber-attacks. This conclusion on the research conducted and the findings presented in this research is based. The findings show that through the education of officials against cyber-attacks, the number of officials who were victims of a cyber-attack was several times smaller after measures applied their education than before their education.

Based on the research findings, we present some recommendations that we think should be considered in the future:

- It is necessary to increase the awareness of public officials about how to use information technology resources and the risk that may come from cyber-attacks and uncontrolled use of e-mail or other devices.
- Additional awareness raising and trainings for public officials which are victims of cyber-attacks.
- Organization of cyber-attack simulations more frequently to increase the awareness of public officials about the dangers that may come from cyber-attacks.

In the end, we conclude that to have the best possible security of data and infrastructure in general, one of the key elements is to continue identifying vulnerabilities, training officials, and testing them through various cyber simulations. Moreover, this study provides a basis for future research on this topic, where researchers can further explore the ratio between officials' awareness of cyber security and the effectiveness of defense against cyber-attacks.

Author contributions: AH: conducted research, collected data, compiled scenarios, & realized simulations of cyber-attacks & **AD:** wrote paper & analyzed & interpreted results. Both authors approved the final version of the article.

Funding: This article was funded by the Ministry of Education, Science, Technology, and Innovation.

Acknowledgements: The authors would like to thank the Ministry of Internal Affairs.

Ethics declaration: The authors declared that the use of data for this research and publication of this research has been approved by the Ministry of Internal Affairs of name here. Informed consents were obtained from the participants.

Declaration of interest: The authors declare no competing interest.

Data availability: Data generated or analyzed during this study are available from the authors on request.

REFERENCES

Alanezi, A. M. (2022). An efficient framework for intelligent learning based on artificial intelligence and IoT. *International Journal of Emerging Technologies in Learning, 17*(7), 112-124. https://doi.org/10.3991/ijet.v17i07.27851

Alharbi, T., & Tassaddiq, T. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing, 5*(2), 23. https://doi.org/10.3390/bdcc5020023

AlSobeh, A. M. R., AlAzzam, I., Shatnawi, A. M. J., & Khasawneh, I. (2023). Cybersecurity awareness factors among adolescents in Jordan: Mediation effect of cyber scale and personal factors. *Online Journal of Communication and Media Technologies, 13*(2), e202312. https://doi.org/10.30935/ojcmt/12942

Awajan, N. W. (2023). The effect of implementing technology in formative assessments to ensure student learning in higher education English literature courses after COVID-19. *Online Journal of Communication and Media Technologies, 13*(2), e202320. https://doi.org/10.30935/ojcmt/13049

Bund, J., & Esteve-Gonzalez, P. (2020). Cybersecurity capacity review–Republic of Kosovo. *SSRN Electronic Journal, 3658214*. https://doi.org/10.2139/ssrn.3658214

Cherdantseva, Y., & Smart, P. (2020). Applied cyber security for applied software engineering undergraduate program. *Journal of the Colloquium for Information Systems Security Education, 8*(1), 7.

Duić, I., Cvrtila, V., & Ivanjko, T. (2017). International cyber security challenges. In *Proceedings of the 40th International Convention on Information and Communication Technology, Electronics, and Microelectronics* (pp. 1309-1313). https://doi.org/10.23919/MIPRO.2017.7973625

Hu, Z., & Gong, X. (2022). The practice of a new maker teaching model in vocational and technical education. *International Journal of Emerging Technologies in Learning, 17*(9), 241-256. https://doi.org/10.3991/ijet.v17i09.30935

Hulaj, A., & Shehu, A. (2018). An efficient algorithm to energy savings for application to the wireless multimedia sensor networks. In L. Barolli, F. Xhafa, N. Javaid, E. Spaho, & V. Kolici (Eds.), *Proceedings of the 6th International Conference on Emerging Internet, Data & Web Technologies* (pp. 349-358). Springer. https://doi.org/10.1007/978-3-319-75928-9_31

Hulaj, A., Bytyçi, E., & Kadriu, V. (2022). An efficient tasks scheduling algorithm for drone operations in the indoor environment. *International Journal of Online & Biomedical Engineering, 18*(11), 42-57. https://doi.org/10.3991/ijoe.v18i11.29977

Hulaj, A., Likaj, R., & Bajrami, X. (2023). Internet of things application for green border surveillance, based on edge detection techniques. *International Journal of Intelligent Systems and Applications in Engineering, 11*(2), 702-709. https://ijisae.org/index.php/IJISAE/article/view/2792

Internet World Stats. (2021). *World internet-users statistics and 2021 world population stats*. https://www.internetworldstats.com/stats.htm

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973-993. https://doi.org/10.1016/j.jcss.2014.02.005

Khamcharoen, N., Kantathanawat, T., & Sukkamart, A. (2022). Developing student creative problem-solving skills (CPSS) using online digital storytelling: A training course development method*. International Journal of Emerging Technologies in Learning, 17*(11), 17-34. https://doi.org/10.3991/ijet.v17i11.29931

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. *Energy Reports, 7*, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

Matondang, Z., & Sitompul, H. (2021). Evaluation of building education program field practices, *International Journal of Education in Mathematics, Science and Technology, 9*(4), 684-696. https://doi.org/10.46328/ijemst.2045

Nasongkhla, J., & Shieh, C.-J. (2023). Using the technology acceptance model to discuss factors in university employees' behavior and intention to apply social media. *Online Journal of Communication and Media Technologies, 13*(2), e202317. https://doi.org/10.30935/ojcmt/13019

Venter, M. I., Blignaut, J. R., Renaud, K., & Venter, A. M. (2019). Cyber security education is as essential as the three R's. *Heliyon, 5*(12), e02855. https://doi.org/10.1016/j.heliyon.2019.e02855

Watney, M. (2022). Cybersecurity threats to and cyberattacks on critical infrastructure: Legal perspective. *Proceedings of the European Conference on Cyber Warfare and Security, 21*(1), 319-327. https://doi.org/10.34190/eccws.21.1.196

Yusif, S., & Hafeez-Baig, A. (2021). Cybersecurity policy compliance in higher education: A theoretical framework. *Journal of Applied Security Research, 18*(2), 267-288. https://doi.org/10.1080/19361610.2021.1989271