



## Security of Data and Web Applications during COVID-19

Natalija Vugdeliya<sup>1</sup>   
Nikola Nedeljković<sup>2</sup>   
Nenad Kojić<sup>3</sup> 

Received: November 20, 2021  
Accepted: November 29, 2021  
Published: April 12, 2022

### Keywords:

Cyber-attack;  
Cyber security education;  
Word Two;  
Vulnerability of system;  
Ransomware



Creative Commons Non Commercial CC BY-NC: This article is distributed under the terms of the Creative Commons Attribution-Non-Commercial 4.0 License (<https://creativecommons.org/licenses/by-nc/4.0/>) which permits non-commercial use, reproduction and distribution of the work without further permission.

**Abstract:** Numerous companies in Serbia have come under attack, including large companies, state-owned companies and institutions. Various security vulnerabilities have been identified, which clearly indicates insufficient education of employees in the field of information systems security, as well as insufficiently developed awareness of the consequences of misuse of unprotected information and vulnerability of systems and applications. This paper lists some security measures, which may prevent unauthorized access to the system and misuse of personal or sensitive data. The paper also lists some examples of attacks using ransomware, which have led to massive data losses. These attacks were carried out via email, which is one of the most common types of malware attack and brings us to the question of whether it is necessary to introduce additional education on the topic of cyber security through the school system.

## 1. INTRODUCTION

Since the beginning of the COVID-19 virus pandemic, there has been talked of a large number of instances of unauthorized access to applications and servers, the destruction of servers by DDOS attacks, as well as the abuse of data privacy. Cyber Attack Trends Report states that in the first half of 2021. “global cyber attacks increased by 29%, as hackers continue to exploit the COVID-19 pandemic and shift to remote work.” During a pandemic, a large number of jobs are done via the Internet, various online platforms or server services are used and thus become the target of cyber-attacks. The increase in the number of attacks on web applications since the end of 2019 is especially noticeable. Some subjects enter the cyber world unprepared unaware of many security vulnerabilities. According to Brooks (2021), “The year 2020 broke all records when it came to data lost in breaches and sheer numbers of cyber-attacks on companies, government and individuals.” There is a clear need to raise awareness about security risks and the consequences of a possible cyber-attack because as hardware and software protection systems become better and more comprehensive, new and more complex types of attacks are emerging. In Cyber Security Awareness, Knowledge and Behavior: A Comparative Study (2020) authors after analyzing the situation, notice the need for a quick reaction because “as rates of data usage and internet consumption continue to increase, cyber awareness turned to be increasingly urgent”. It is possible to introduce various software and hardware protections, but even the most secure systems become vulnerable due to human errors and oversight. The authors found “the increased anxiety caused by the pandemic heightened the likelihood of cyber-attacks succeeding corresponding with an increase in the number and range of cyber-attacks” in Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic (2021). In addition to the increase in the number of attacks, the level of impact on organizations and individuals in the event of a security breach is also increas-

<sup>1</sup> Academy of Technical and Art Applied Studies Belgrade (ATUSS) – Department ICT College for vocational studies, Zdravka Čelara 16, Belgrade, Serbia

<sup>2</sup> HTEC Group, Bulevar Milutina Milankovica 11b, Belgrade

<sup>3</sup> Academy of Technical and Art Applied Studies Belgrade (ATUSS) – Department ICT College for vocational studies, Zdravka Čelara 16, Belgrade, Serbia

ing. According to ACSC Annual Cyber Threat Report 2020–21 “an increase in the average severity and impact of reported cyber security incidents, with nearly half categorised as ‘substantial.’”

## 2. EXAMPLES OF INFORMATION SYSTEM VULNERABILITY

### 2.1. Example of data coverage

One instance of exposing important information was discovered and reported to the authorities by a non-governmental organization during its research on data privacy protection during the epidemic. Namely, the researchers from the non-governmental organization for the promotion of human rights and internet freedoms Šer Foundation, noticed that the username and password for access to the COVID-19 information system were publicly available on the website of a certain health institution, which could lead to serious misuse of particularly sensitive personal and health data. The COVID-19 information system includes data on the cured, deceased, tested and persons who have been sentenced to self-isolation. By publicly announcing these logging parameters, anyone had access to the system itself, more precisely, any person who saw the username and password could freely access all parts of the system, which were allowed to health institutions, institutes, laboratories, and the like.

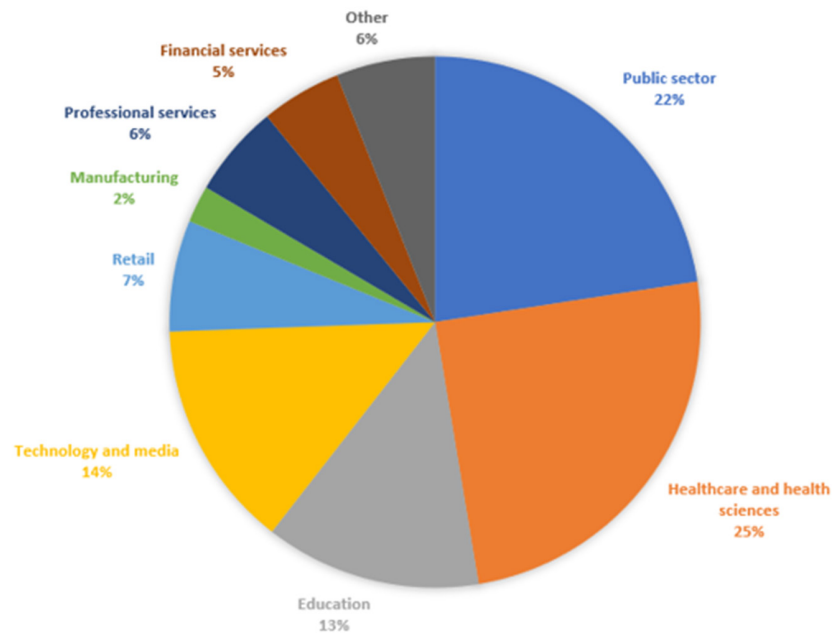
After the omission was discovered, the logging parameters were deleted, but the question still arises as to what would have happened if someone had maliciously accessed the system before, or even better, what if someone did. It was possible to see personal, health data, clinical trials, treatment information... Due to the sensitivity of the data, we can see how bad it was that the health institution made it public, not realizing the possible negative consequences, which could have been catastrophic. Let's just imagine that someone took all the patient's data and later sold it to a pharmaceutical company. All persons who were in any connection with COVID would receive advertisements for drugs on Google for years for their disease. Not to mention personal contact information, which could be misused for various purposes.

Healthcare institutions have an obligation to appoint a person in charge of data protection, but due to the limited number of staff, it may happen that an insufficiently trained and underqualified person is appointed to this position. It is still not known how the omission came about, but we can conclude that the information and security education of our citizens, and above all workers in state institutions, is at a fairly low level.

Later, a system of access was established using a qualified electronic certificate, which was most likely to be used from the very beginning. Some of the ways in which it was also possible to protect access to the system to some extent is access via VPN, which would be accessible only from laboratories and institutes and without which it would not be possible to access the application, let alone the login page, and use other people's login information. Another way to access it would be to provide a list of allowed IP addresses so that all clinics and institutes get access through their IP address and the login data itself. This can be a less secure way of protection and the problem can come if a person who has login information and is not entitled to that information, can access it from the clinic itself.

Irwin L. stated in Data breaches and cyber attacks quarterly review Q3 2021 that the healthcare and health sciences sector accounted for the most security incidents in Q3, which can be seen in Figure 1.

### Which sectors suffered the most security incidents?



**Figure 1.** Security incidents in sectors for Q3 2021.

Source: Data breaches and cyber attacks quarterly review: Q3, 2021

### 2.2. An example of weakening security

Another example is when companies, by introducing some restrictions, unknowingly make it easier for attackers. One of the ways applications restrict us is by limiting the length of the password. For years, there has been controversy about the best possible password in case of an attempted brute-force attack. Although a large number of companies have already taken some of the protection measures themselves: the impossibility of constantly trying to log in, waiting for about 10 seconds between logging in, waiting for a few minutes up to several hours after a certain number of unsuccessful logins, there are, however, many companies that have set conditions which make it easier for the attacker to access system in question. For example, companies are requesting a password to be between 8 and 20 characters in length and to consist only of letters and numbers. We come across a character type limit, which reduces the number of possible different password combinations, as well as the limit on the maximum length of the password, which is very undesirable from the internet security point of view. Most likely, after encrypting the password, if encryption occurs at all, the number of characters reaches a maximum predetermined in the database itself. This allows the attacker to guess which system is in question, and perhaps, in the worst case, the data encryption system itself. According to ACSC Annual Cyber Threat Report 2020–21 attackers “rapid exploitation of security vulnerabilities”.

### 2.3. Examples of ransomware attacks

Apart from security flaws, it is known that a malware attack can pose a serious security threat and that in addition to various inconveniences, it can also lead to serious problems and financial losses. Help Net Security stated that “malware increased by 358% overall and ransomware increased by 435% as compared with 2019.” Various institutions in Serbia also had problems with ransomware. On April 6, 2021, the mayor of Kruševac announced that the servers of the City Administration had been attacked. Such an attack locks all data that exists in the municipality,

through statements, accounts, as well as private data. An additional problem is when the backup data is stored on the same servers and devices as the originals so that any attempt to recover the data from the backup is impossible.

There were many ways to prevent it, from courses and training of workers on cyber security, in order not to open virus-infected files on business computers, to blocking the receipt of e-mail addresses outside a certain list of allowed domains. Thus, no person with an address from applications for creating temporary email addresses, which are also available for free on the Internet, could send unwanted content, until all addresses that are not in the same domain are blocked. Of course, the list of allowed domains is very limited, so it is always good to make a compromise between different solutions. Also, one of the good solutions is to install antivirus software that would scan and sign all sent messages, as well as received ones. It should be noted that it is important not to keep backups on the same devices as the originals, but on some external devices without Internet access.

A similar attack happened in Novi Sad when the system of JKP “Informatika” was attacked. As in the example in Kruševac, the work of all services was slowed down or blocked. In both cases, the attack was carried out with the help of mail, which is one of the most common malware attacks, in addition to adding files to the sites that users of the company visit. It is interesting to note that the attack took place while Novi Sad hosted a conference on technological innovation for the smart cities of the future.

In the attack itself, the goal is never to destroy the data but only the encryption so that they can charge for the decryption. All files are encrypted, and each computer says it is locked. One of the possibilities after a ransomware attack is to pay the requested amount, but the payment itself does not guarantee the return of all data. It is estimated that an average of 50:50 of returned and unrecovered data after payment of the requested amount is in a malware attack.

Similar attacks occur all over the world and are even more common than in our country. It is interesting to see that similar attacks and omissions occur in the most developed countries, and to know that they are also working on old, not updated versions of operating systems, programs... Many companies and institutions in the world have been attacked by ransomware. According to ACSC Annual Cyber Threat Report 2020–21 “Ransomware has grown in profile and impact, and poses one of the most significant threats to Australian organisations.” An additional problem is that attackers are developing new and more successful attack techniques, so even more important is quality and continuous education in the field of cyber security. Cyber Attack Trends Report states that in the first half of 2021. “Ransomware attacks surged 93% in the last 6 months, fueled by innovation in an attack technique called Triple Extortion.”

## **2.4. Examples of fraud**

Ordinary citizens are also targeted. Some of the more famous scams are of the type of inherited money abroad, relatives you have not heard of who would send you money, as well as the most famous scam of the Nigerian prince, after whom all scams of this type got their name, in which the person (attacker) presents himself as Nigerian prince asks you for a small sum of money to leave the country with some wealth: money, gold or diamonds, which you would later share. In all emails of this type, it is important to pay attention to the sender’s address, which in most cases can be a serious red flag from the very beginning that something is wrong. In addition, a

large number of messages come from foreign countries, which most often use Google Translator to send you text, which means that there are a large number of spelling mistakes, and some very strange, older, less-used words in the presentation itself. If you decide to contact that person, remember that sharing personal information is your responsibility and that it is usually impossible to find the culprit for a crime against your information, credit card, or passport.

## 2.5. Phishing is often used to attack citizens.

A large number of such messages arrive to most people daily, and usually end up in a spam folder with their providers, but one message has recently attracted a great deal of attention. It is an email, in which the person introduced himself as the Post of Serbia and asked for the amount, because some package arrived from abroad, which can be seen in Figure 2. People who do not use online shopping or do not receive packages from abroad do not know what the system is like if a package arrives that needs to pay customs, so they can immediately fill in their data and thus give the attacker everything he needs. Special attention should be paid to the sender's email, which is *Postars @ \* @ posta.rs*, which can confuse even more experienced users. Also, the URL of the page it sends you to is *tracking-posta-rs.com*, which acts as a legal domain and can be seen in Figure 3. Also, the amount itself is very intelligently done, because it is not a rounded number, but 36.24 RSD. On these occasions, it is best to contact the representative office of the institution that is thought to have sent the email. In these cases, state institutions usually leave a picture of a copy of the payment slip, so if that part is missing, it can indicate that it may be an attempt at fraud.

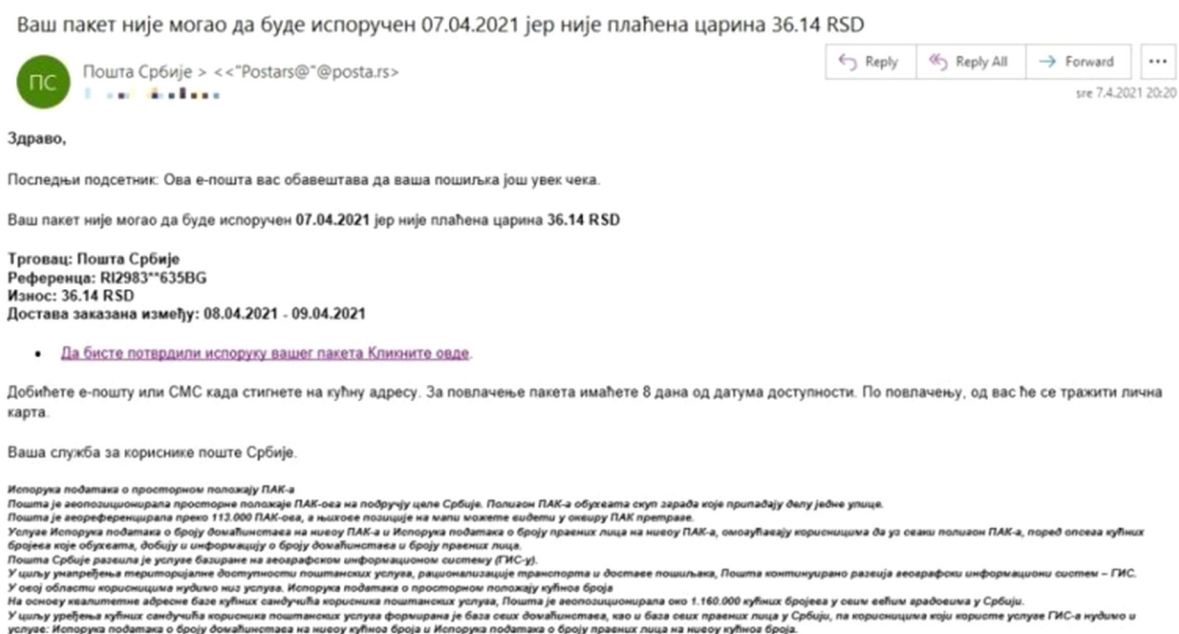
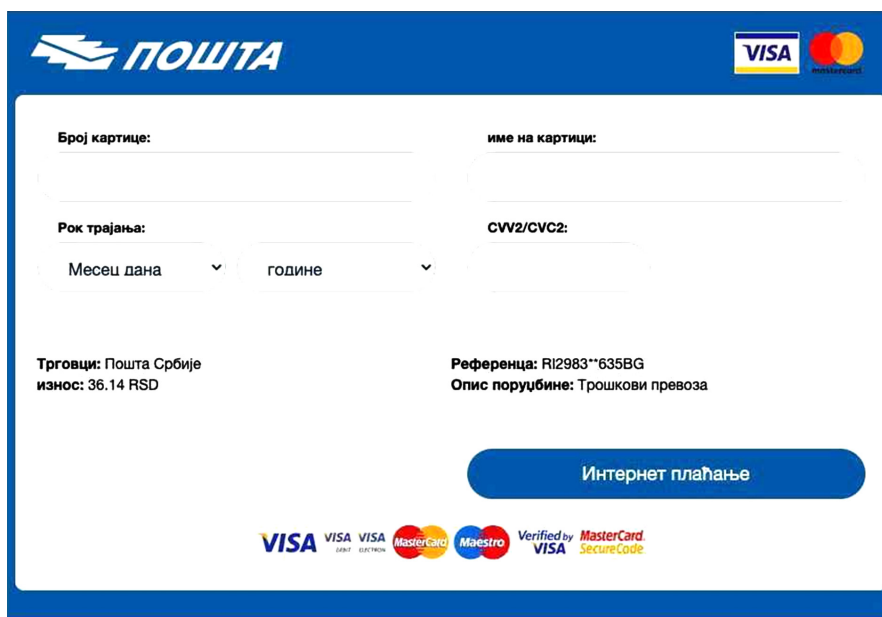


Figure 2. An example of mail fraud

At the time of the pandemic, another phishing mail also attracted attention. From the address *invitations@mup.gov.rs*, emails arrived about the alleged procedure that the Ministry of the Interior is conducting against the recipient. In fact, it is a Trojan that is attached to the message as an .iso file.





The image shows a screenshot of a payment form for 'ПОШТА' (Post). The form is titled 'ПОШТА' and features logos for VISA and MasterCard. It contains the following fields and information:

- Број картице:** (Card number) - empty field
- име на картици:** (Card name) - empty field
- Рок трајања:** (Expiration date) - dropdown menu with 'Месец дана' (Month) and 'године' (Year) options
- CVV2/CVC2:** - empty field
- Трговци:** Пошта Србије (Merchant: Post of Serbia)
- износ:** 36.14 RSD (Amount)
- Референца:** R12983\*\*635BG (Reference)
- Опис поруџбине:** Трошкови превоза (Description: Shipping costs)
- Интернет плаћање** (Internet payment) button
- Logos for VISA, MasterCard, and Maestro at the bottom.

**Figure 3.** An example of a fake payment order

Protection against a large number of attacks is in prevention. In order for citizens to understand the potential dangers of cyber attacks and be able to protect themselves, it is necessary to encourage citizens to constantly self-education. For this purpose, educational materials should be designed that is understandable and interesting, which is a serious and difficult task. Authors of Riskio: A Serious Game for Cyber Security Awareness and Education (2020) stated “Serious games have emerged as a new approach that can complement instruction-led or computer-based security training by providing a fun environment where players learn and practice cyber security concepts through the game”.

### 3. FUTURE RESEARCH DIRECTIONS

Knowing that the system connected to the network is not completely secure, it is necessary to pay attention to methods that make it difficult for attackers to access so that the attack is unprofitable for them. In order for the attackers to be maximally prevented, it is necessary to work on continuous cyber security education for all citizens. The authors intend to analyze current cyber-attacks and point out the need to include knowledge about security risks and ways of protection in basic knowledge during schooling.

### 4. CONCLUSION

Cyber-attack and security endangering examples listed above clearly show it is necessary to work on generally raising cyber awareness. For the majority of the reported cases, human oversights or errors were determined to be a cause of dangerous weak spots, which leads to the conclusion further education is especially needed for those working in companies whose system is susceptible to cyber-attacks and can often be a target of such attacks, which is, in fact, every company using a public network. Suggested steps for overcoming these issues would be creating mass education platforms, easily accessible and with clearly explained key points and topics that should be focused on. Furthermore, online courses and educations for employees are highly recommended. It should be prioritized that those in charge of IT system security are duly qualified and make sure everything is being done in accordance with company security policies.

Finally, as not only companies but also every person with internet access is exposed to various kinds of attacks, there is a need for a higher level of education regarding cyber security topics to be included in elementary and middle school programs as well.

## REFERENCES

- ACSC Annual Cyber Threat Report 2020–21, (2021) Australian Cyber Security Centre, with contributions from the Defence Intelligence Organisation (DIO), Australian Criminal Intelligence Commission (ACIC), Australian Security Intelligence Organisation (ASIO), The Department of Home Affairs and industry partners. <https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21>
- Brooks, C., Alarming Cybersecurity Stats: What You Need To Know For 2021, 02. 03. 2021. <https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-----what-you-need-to-know-for-2021/?sh=2c1e329b58d3>
- Cyber Attack Trends – 2021 Mid Year Report – Check Point Research <https://pages.checkpoint.com/cyber-attack-2021-trends.html>
- Hart, S., Margheri, A., Paci, F. & Sassone, V. (2020), Riskio: A Serious Game for Cyber Security Awareness and Education, *Computers & Security*, Volume 95, <https://doi.org/10.1016/j.cose.2020.101827>. <https://www.sciencedirect.com/science/article/pii/S0167404820301012>
- Help Net Security - Malware increased by 358% in 2020, 17. 02. 2021 <https://www.helpnetsecurity.com/2021/02/17/malware-2020/>
- Irwin, L. (2021). Data breaches and cyber attacks quarterly review: Q3 2021 <https://www.itgovernance.co.uk/blog/data-breaches-and-cyber-attacks-quarterly-review-q3-2021>
- Lallie, H., S., Shepherd, L., A., Nurse, J., R., C., Erola, A., Epiphaniou, G., Maple, C. & Bellkens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic, *Computers & Security*, Volume 105, 2021, <https://doi.org/10.1016/j.cose.2021.102248>. <https://www.sciencedirect.com/science/article/pii/S0167404821000729>
- Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F. & Basim, H., N. (2020) Cyber Security Awareness, Knowledge and Behavior: A Comparative Study, *Journal of Computer Information Systems*, DOI: 10.1080/08874417.2020.1712269

