International Journal of Research in E-learning
Vol. 7 (2), 2021, pp. 1–18

https://doi.org/10.31261/IJREL.2021.7.2.05

Agnieszka Kubacka
Carpathian State College in Krosno
https://www.orcid.org/0000-0002-5137-5668

Daniel Biały
Carpathian State College in Krosno
https://www.orcid.org/0000-0001-5698-9768

Radosław Gołąb
Carpathian State College in Krosno
https://www.orcid.org/0000-0002-2166-7416

Perception of Information Security in the Process of Distance Learning During the COVID-19 Pandemic on the Example of University Teachers' Experiences

Abstract

The COVID-19 pandemic has greatly affected every area of our lives. One of them was education, which had to undergo a huge transformation in a very short time. Overnight, the computer replaced the blackboard and became the only tool of communication between a student and a teacher. Teachers had to completely change the tools used in the teaching process and enter a completely new and, for many of them completely unknown, working environment. Online learning has replaced traditional teaching. A computer with Internet access has become a basic work tool for people who have so far used it mainly for recreational purposes. Teachers were thrown in at the deep end, for most of themit was the first time they had encountered platforms for remote communication.

As the workspace has changed, learners and teachers have begun to move much more frequently into the world of the Internet, which harbors many dangers of which quite a few people were previously unaware. For this reason, the authors decided to investigate the problem of information security in e-learning. This paper attempts to collect the experiences and assess the awareness of university teachers about information security threats while teaching during the COVID-19 pandemic. The research results presented in this paper showed that the level of awareness of the risks, that may affect academic teachers in the distance learning process, is very low. Additionally, no appropriate procedures for safe distance learning have been developed. The communication security area was practically completely overlooked during the COVID-19 educational revolution.

Keywords: distance learning, Covid-19 pandemic, distance learning security, information safety, Internet threats

The COVID-19 pandemic has greatly affected the way of work in many areas of life, including education. According to "2020 Cost of a Data Breach Report" by Ponemon Institute for IBM, 54% of organizations required remote work during this period. In the case of education, it can be assumed that during periods of full closure, it took place exclusively in a remote form, which in many cases was dictated by decisions of local or national authorities. This meant that university teachers had to change not only their working methods, but also their basic tools. The reality of lecture theatres was completely transferred to the virtual world. Distance learning became, in the vast majority of cases, the only way to continue the learning process. The computer with Internet access replaced the worn-out blackboard and for many academic teachers it was a real revolution – entering a completely new, previously unknown working environment. An environment full of dangers, including threats related to the security of communication. This paper is an attempt to find an answer as to whether the aforementioned threats have been noticed and whether any measures have been taken to eliminate them or minimise their effects.

1. Information stored on the e-learning platform and its security

The need to work remotely means that information systems no longer perform only support functions of work, but are an integral, very important part of it. Consequently, the information processed in them is an asset that must be protected. E-learning platforms are systems that store information of a different nature. These are teaching materials, exam tests that are for students who are qualified to read them. Threats to online courses include distribution of materials without the authors' knowledge, unauthorized modification of posted content, and further distribution as original materials (Scerbakov et al., 2019).

Another type of information is data on individual achievements. In addition, it is also personal information such as first name, last name, album number, PESEL, year and major of study and login information (Wozniak-Zapór, 2016). Yet another type of threat relates to the security of stored information and privacy. It can be, for example, the possibility of substitution of submitted works, confirmation of the real identity, independence of works performed by students (Jakieła, & Wójcik, 2018).

As you can see from the examples cited, this is information that should not be shared with unauthorized people, and its disclosure can cause a lot of damage. Information protection is also required by law, including the General Data Protection Regulation, the Classified Information Protection Act, the Copyright and Related Rights Act, and finally the ISO 27000 "family of standards". Guaranteeing data security is the responsibility of both the system administrator and the users. It is the latter who are the weakest link in the security system.

1.1 What is information security

Information systems security is the protection against unauthorized access to information or modification of information. Protection should cover storage, processing and transmission. Information security consists of 3 elements (the so-called information triad):

- confidentiality, which means that the information is accessible only to those authorised to receive it;
- integrity, which means that any unauthorised modification of the information is not allowed;
- availability, which means that the information can be accessed under any circumstances that are allowed by the information security policy (Liderman, 2017). Maintaining the confidentiality, integrity and availability of information contribute to information security (PN ISO 27002).

1.2 Information security threats

A user working remotely, and in fact every user of the Internet network encounters many threats on a daily basis, which may have different sources of origin and cause different effects, but regardless of this, each of them may shake one of the listed pillars of security, and thus lead to the collapse of the entire system (Stawowski, 1998). Unpreparedness and misinformation of users, their unawareness of cyber threats, as well as failure to use existing security measures make systems vulnerable to attacks, and the data stored in them ceases to be safe. (Liderman, 2012).

Threats that are encountered most often are: phishing, ransomware, malware. They are characterized by a high level of complexity and intentionality on the part of the attackers (Pipkin, 2002).

Phishing is an online identity theft in which an attacker uses fake emails and fake websites to get naïve customers to reveal sensitive information such as bank account information, website login details and similar sensitive information. Generally, phishing is a relatively new online crime. The ease of cloning a legitimate bank website to convince unsuspecting users makes phishing difficult to detect and restrict. (Amiri & Akanbi, 2015; McGahagan et al., 2021).

Ransomware is a form of malware that locks files or a user's device and then demands an anonymous online payment to restore access. Hackers create this type of software to extort money through blackmail. The way ransomware works makes it extremely harmful. Other types of malware destroy or steal data, but do not close the path to recovery. With ransomware, on the other hand, if the attacked person does not have a backup of the data to recover it, he/she has to pay the ransom. Sometimes the company pays the ransom and the hacker does not hand over the decryption key anyway (Beaman et al., 2021; Wiener, 2019; Yuste, & Pastrana, 2021).

Malware, a short form for malicious software, describes any type of program/ application that is designed to damage or steal data. This type of software includes all kinds of viruses, trojans, spyware or ransomware, adware, etc. The definition of malware, should not be considered solely as one type of software. It is a group of different programs with different functions that have one specific purpose. Malware is usually created by groups of black-hat hackers or programmers whose goal is to make money. Adware, on the other hand, is unwanted software used to display advertisements on your screen, most often in a web browser window. Earning can involve either reselling the software to other users, companies, agencies or trading it on the Dark Web. Profiteering may also consist in constructing the kind of software that enforces, e.g., payments by blocking the user and access to his/her data or by tracking transmitted data, e.g., card numbers and access data to payment systems (Beaman et al., 2021; Formosa et al., 2021; Ring et al., 2021; Skoudis, & Zeltser, 2004).

Phishing and hacking attacks using stolen data account for 51% of all successful data breach attacks, according to data released by Verizon in its Data Breach Investigations Report (2020). It should also be noted that, according to the report, the percentage of incidents involving ransomware threats has increased significantly – from 48% in 2019 to 80% in 2020. Successful attacks usually involve the installation of tracking software, theft of application data, theft of stored data, and an attempt to scan a computer network.

This influenced the authors to carry out a study on the awareness of threats the academic teachers of Carpathian Lesser Poland universities are exposed to on the Internet.

2. Analysis of test results

Seventy academics participated in the survey, conducted during the 2020/2021 academic year, during which distance learning was the only form of teaching for 7 months. Among the respondents, 44 were less than 50 years old, while 26 were older. 25 respondents taught in the engineering or technical sciences, 31 in the humanities or health sciences, and 14 in the agricultural or social sciences. Of those surveyed, 15 declared that they teach subjects thematically related to Computer Science (e.g., Information Technology or classes in Computer Science). Among the information security knowledge areas examined were:

– safe use of equipment,
– use of passwords,
– knowledge of information security threats,
– knowledge of security procedures

2. 1 Methods and tools of communication between academic teachers and students

The field of education, in comparison to other analyzed industries, is distinguished by a relatively low level of malware infections through e-mail boxes. It can be concluded that a peculiar anomaly may result from the use of unmonitored, i.e. private, e-mail boxes in this area. The conducted research seems to confirm this thesis because 41% of the respondents indicated that while conducting remote classes they happened to use a private email box for communication with pupils or students (Figure 1).

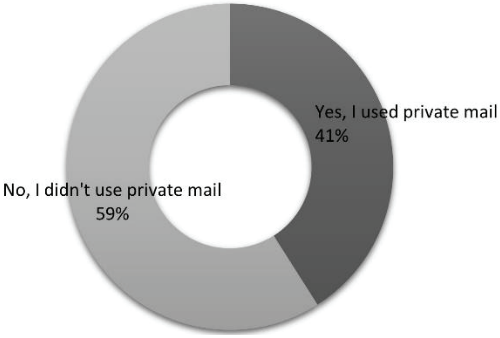


Figure 1. Using a private email inbox to communicate with students during distance learning.
Source: Own work

Additionally, most respondents, 84%, indicated that they use private computer equipment for distance learning. Only 16% use company-owned, purpose-built equipment (Figure 2).

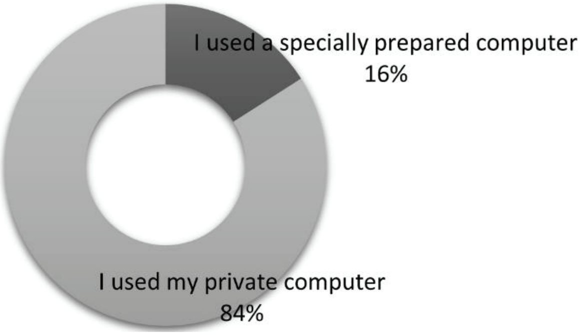


Figure 2. The type of equipment used during distance learning.
Source: Own work

Putting these two elements together, it should be pointed out that the boundary between private and business contexts is very blurred. This can lead to a situation where disclosure of access data or loss of control over a private email inbox and private computer will have serious consequences also in the business area related to distance learning.

Additionally, 23% of the respondents admitted that they happened to open an email attachment posted by a student which they had doubts about. Considering that most of the attacks happen through email attachments, this is a major information security threat. It also indicates the possibility of carrying out an effective attack, and the implementation of such an attack on even just one of the employees may have significant consequences for the entire unit. Situations like this should not happen at all, and certainly not with this intensity.

The above results may suggest that the level of awareness of the risks associated with remote working and distance learning among academic staff is very low. With stolen data accounting for 51% of all successful data breach attacks and ransomware accounting for 80% of all incidents, it seems reasonable to examine the level of awareness of these threats.

2.2 Password usage and backups

An important element that protects our data includes passwords. It is known that creating and remembering many different passwords is a huge problem. Poor password practices often lead to information security incidents. The threats here are both weak passwords and using the same password for multiple accounts or applications (Bentkowski, 2021).

The survey results showed that more than 25% of respondents indicated that they happened to use the same access password to both applications and e-learning services (company e-mail box, Zoom, MS Teams, USOS, e-learning platform, etc.) and applications and services used privately (e-mail box, access to the bank, social networking sites, auction sites, etc.). This leads to the situation where, for one in four people, revealing the access password to applications or services used privately can allow attackers to take full control in a business area. This can have serious consequences not only for the individual but also for the institution. A hijacked email box can be a source of further malware distribution or can be used for a social engineering attack.

Two-factor verification (2FA) is now becoming a standard in common applications such as social networking sites, not to mention applications or banking systems. The use of such solutions significantly reduces the risk of a successful attack, but only 33% of the respondents declared that they use them on network services that require logging in (Figure 3).

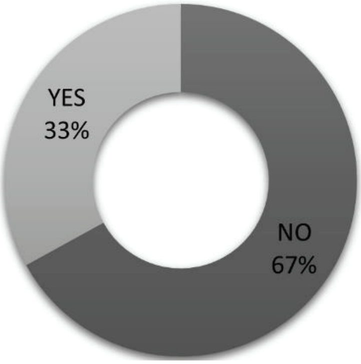


Figure 3. Use of 2FA verification.
Source: Own work

When using a single user authentication mechanism, which is most often a password, the elements such as the complexity of the password, how often it is changed, and how it is stored are crucial.

The survey suggested several passwords of varying complexity and as many as 87% identified the highest complexity passwords as the most secure. The question of the frequency of changing passwords is much worse, because in this case as many as 71% of the respondents indicated that they change their access passwords to applications used for distance learning less than once a year. In this group as many as 39% are people who declare that they do not change their access password at all (Figure 4).

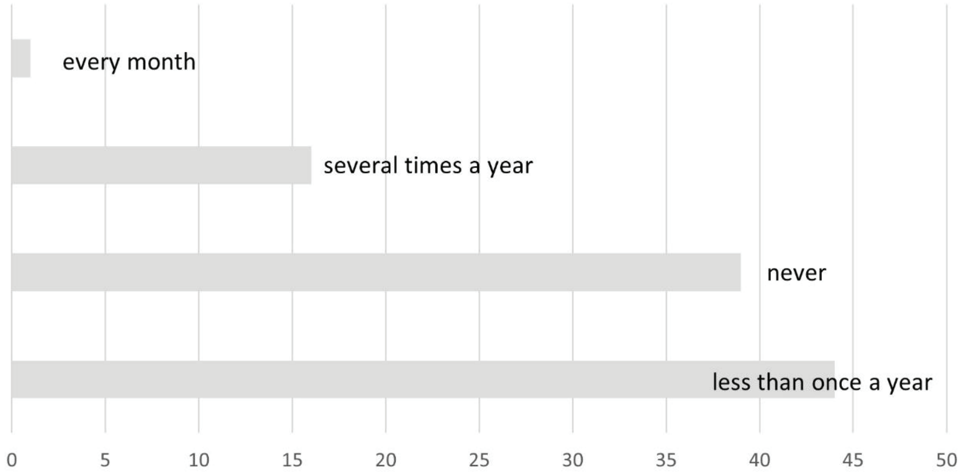


Figure 4. Frequency of access password changes to services and applications that support distance learning.
Source: Own work

The way in which access passwords are stored also has a significant impact on the level of user data security. Most respondents, 43%, declare that they remember their access passwords. The remainder save passwords in a traditional notebook (33%), an electronic notebook or smartphone (12%), and a password manager (12%) (Figure 5).

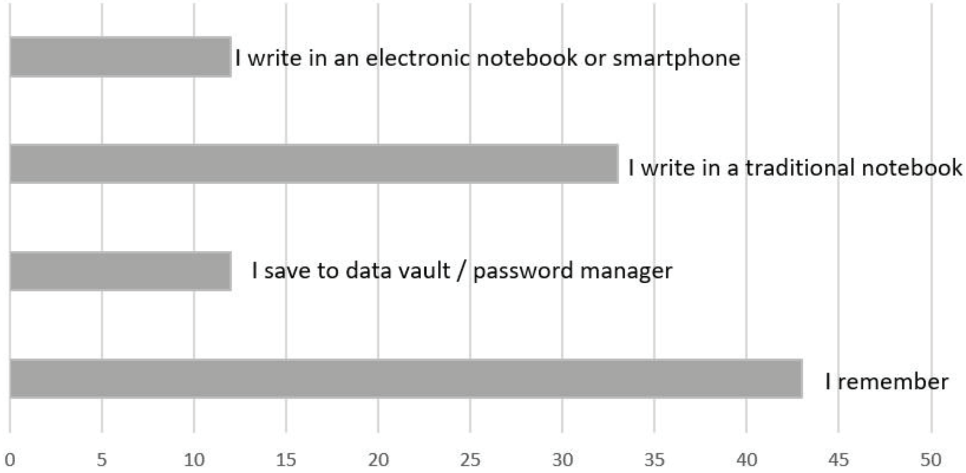


Figure 5. Ways to store passwords.
Source: Own work

Another important issue when processing data in an organization is how to protect it from unauthorized access and destruction or loss. As shown above, most lecturers use private computers during distance learning, but as shown in Figure 6, only 24% use encoding mechanisms to secure data processed on laptops or storage media such as portable drives.

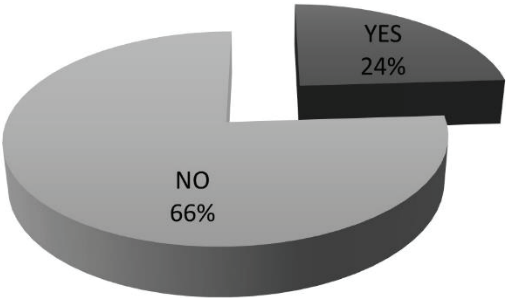


Figure 6. Use of encoding mechanisms.
Source: Own work

The area of data protection against data loss due to theft of a computer or a failure preventing the restoration of processed data also looks bad. Among the respondents as many as 47% indicated that they back up their processed data once a year or less frequently, with 1/3 declaring that they do not make such a copy at all. The frequency of backups is shown in the graph in Figure 7.

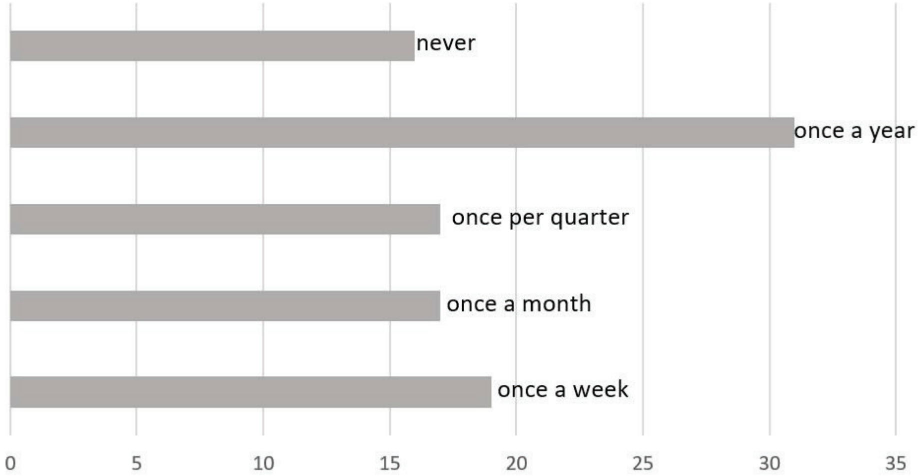


Figure 7. Backup.
Source: Own work

2. 3 Survey on knowledge of information security risks

Respondents were asked about the meaning of terms related to the threats we currently face. In the surveyed group as many as 52% of respondents admitted that they do not know the meaning of the term ransomware, 45% do not know what malware is, and 39% do not know what phishing is (Figure 8).

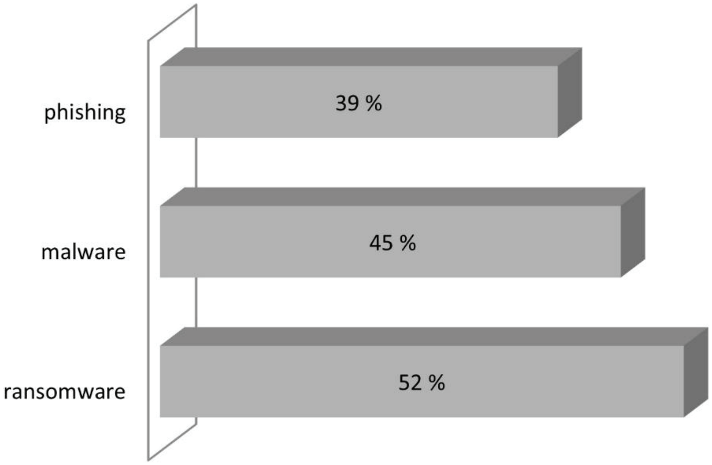


Figure 8. Percentage of respondents who do not know the meaning of the terms phishing, malware and ransomware.
Source: Own work

Figure 9 shows the percentage of people who say they have never encountered the above-mentioned threats.

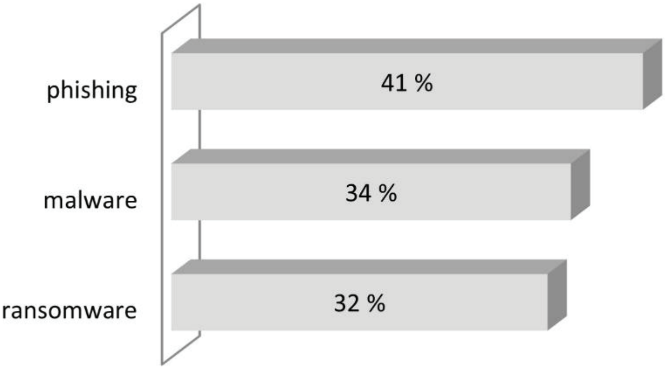
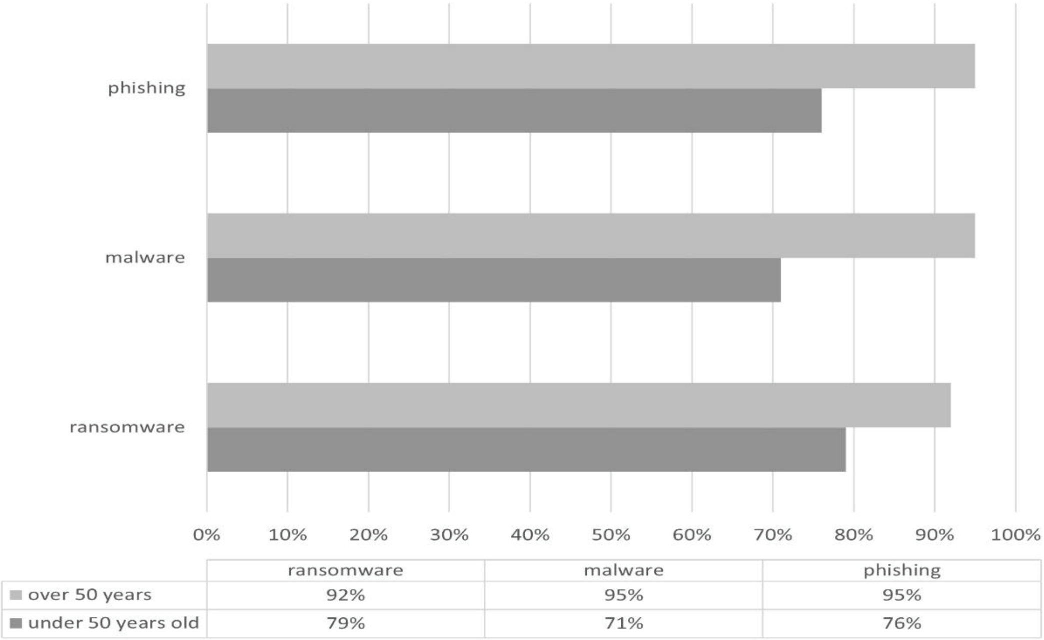


Figure 9. Percentage of respondents who have never encountered the terms phishing, malware and ransomware.
Source: Own work

Considering prevalence of these threats in the form of recorded incidents and successful attacks, it is highly unlikely that such a large percentage of respondents have never encountered them. Between September 9 and 16, 2021 alone, Internet users reported 12 different attacks belonging to the discussed threats (Giza, 2021). The presented results may suggest that the surveyed people, despite being confronted with the threats, did not take note of it - they were not able to notice and identify it.

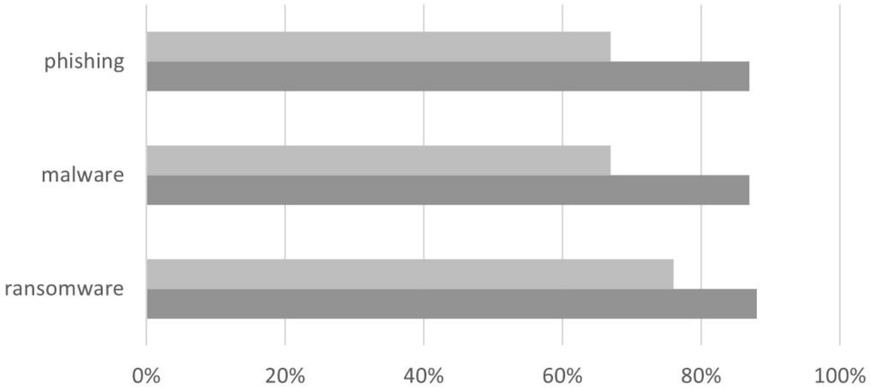
When it comes to the awareness of the threats associated with distance learning, a noticeable difference emerges among different age groups. As many as 92% of respondents aged 50 and older said they were unfamiliar with the term ransomware or had never encountered the threat. In the under 50 group, this percentage was 79%. The disproportion is even greater for malware and phishing threats, as shown in Figure 10.



	ransomware	malware	phishing
■ over 50 years	92%	95%	95%
■ under 50 years old	79%	71%	76%

Figure 10. Percentage of respondents who have never encountered the terms phishing, malware and ransomware or are not familiar with these terms by age group.
Source: Own work

A similar disproportion can be observed when comparing the collected research results in terms of the subject matter of the classes. Teachers teaching non-technical subjects are much more likely to declare that they do not know the terms describing the most popular threats or claim that they have never come across them. The described relationship is presented in the graph in Figure 11.



	ransomware	malware	phishing
■ non-technical	76%	67%	67%
■ technical	88%	87%	87%

Figure 11. Percentage of respondents who have never encountered the terms phishing, malware, and ransomware or are unfamiliar with these terms by type of subjects pursued.
Source: Own work

Low awareness of threats among users of any system is a major threat to its security. According to Kaspersky, more than 80% of all security breaches are caused by human's mistake. The risk of such a mistake can be minimized by using appropriate solutions on the hardware side, software side or implemented procedures on how data is processed during distance learning. Cisco is one of many that have additional security features that can be applied to cloud-based electronic boxes. Considering the fact that 84% of the surveyed use private computers to conduct classes remotely, and 41% declared that they happen to use private e-mail boxes to communicate with students, any actions taken by administrators responsible for maintaining security will not translate into a significant improvement in its level. As such, much of the environment used in the distance learning process remains beyond the control of security administrators.

2. 4 Knowledge of security procedures

Implementing and strictly enforcing procedures or instructions for secure remote working e. g. password policy is one element used to reduce the risk of exposure to cyber-attack (NCSC, 2021). In the surveyed group, 64% of the academic staff indicated that a consistent policy or instruction for remote instruction is implemented in the unit for which they deliver remote instruction. This means that more than 1/3 of the respondents are conduct remote work based on their security knowledge, experience and level of awareness (Figure 12).

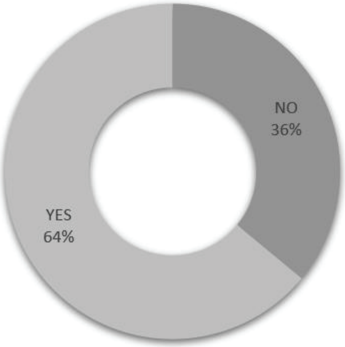


Figure 12. Implementing a remote classroom policy or instruction.
Source: Own work

Additionally, 66% of respondents declared that they do not know the procedure to be followed in the case of a security breach of data processed in remote work, and another 16% indicated that they know that such a procedure does not exist. This means that only 18% of the surveyed academics are knowledgeable about how to report a security incident in the process of their remote work (Figure 13).

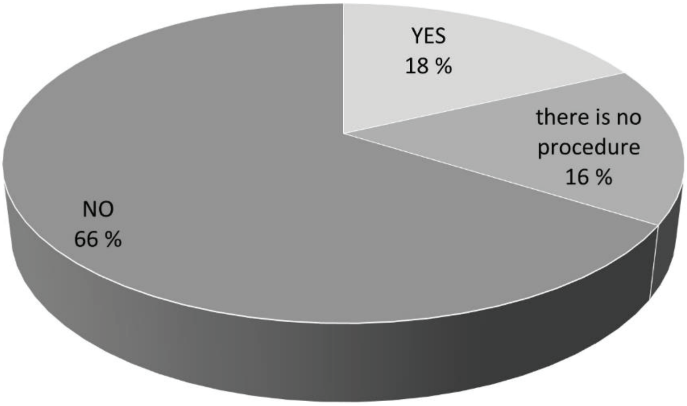


Figure 13. Knowledge of the procedure for dealing with security breaches of data processed while working remotely.
Source: Own work

Lack of awareness of threats and appropriate procedures implemented in the organization, in itself, is a serious breach in the communication and data security system, but the key seems to be the behavior of system users. Even the unconscious and unforced application of good practices in daily work can significantly reduce the risk of a serious data security breach.

Discussion

The success of e-learning requires facing all the challenges related to the implementation of distance learning technical solutions, especially the challenges related to maintaining information security.

Undermining security pillars such as the availability, integrity and confidentiality of data processed in remote education systems exposes e-learning environments to the dangers of cyber attacks. A very important element increasing the level of security is maintaining the highest possible awareness of threats among their users, as well as implementing methods to counteract these threats. The research shows that improving the security of remote education systems can be achieved by introducing technical and organizational solutions that force users to increase their awareness of cyber threats (Beaman et al., 2021). Raising awareness will allow students to benefit from effective learning in a safe environment, and universities, as solution providers, will be sure that all data processed in the system is resistant to cyber attacks.

Conclusions

Summarizing the data presented above, it should be noted that the level of awareness about ICT security threats among academic teachers conducting distance learning classes and the practices used during this type of work are significantly below current standards. To a large extent, this situation can be attributed to the very sudden change in the form of teaching caused by the emergence of the COVID-19 pandemic and to decisions made by the authorities at local and national levels. This can be evidenced by the fact that universities have failed to secure dedicated computer equipment for lecturers to use while teaching at a distance.

Additionally, institutions or organizations providing distance learning do not have procedures for conducting such classes or the implemented procedures are only symbolic, and their existence does not influence the improvement of the broadly understood information and communication security. The study revealed a complete lack of supervision by the university concerning the safety of conducting the distance learning process.

If distance learning is going to be such a widely used tool in the educational process, it is necessary to undertake actions in the field of security in many areas with a particular focus on raising the awareness of academic teachers in the field of security threats, violations, incident reporting and implementation of procedures and good practices related to working on the Internet.

Remote work with students, in terms of ICT security, does not differ strongly from the way of working in other industries, so in most cases there is no need to create a completely new procedural or technical solutions, but the implementation and adaptation of already used practices.

References

Amiri, I.S., & Akanbi, O.A. (2015). A Machine-Learning Approach to Phishing Detection and Defense, Waltham, Elsevier, ISBN 9780128029466.

Beaman C., Barkworth A., Akande T., Hakak S., & Khan M., (2021), Ransomware: Recent advances, analysis, challenges and future research directions, Computers & Security, 111, ISSN 0167-4048, DOI: 10.1016/j.cose.2021.102490.

Bentkowski, M. (2021). Generowanie łatwych do zapamietania haseł z wykorzystaniem łańcuchów Markowa (Generating easy-to-remember passwords using Markov strings), retrieved from https://sekurak.pl/generowanie-latwych-do-zapamietania-hasel-z-wykorzystaniem-lancuchow-markowa/ (accessed 15.08.2021).

Formosa, P., Wilson, M., & Richards, D., (2021), A principlist framework for cybersecurity ethics, Computers & Security, 109, ISSN 0167-4048, DOI: 10.1016/j.cose.2021.102382.

Giza M. (2021). Przegląd ataków na polskich internautów (6–19.09.2021 r.) [Overview of attacks on Polish internet users], Retrieved from https://sekurak.pl/przeglad-atakow-na-polskich-internautow-6-19-09-2021-r/ (accessed 21.09.2021).

Information technology – Security techniques – Information security management systems – Overview and vocabulary PN-EN ISO/IEC 27000:2018.

Jakieła J., & Wójcik J., (2018). Przegląd problemów bezpieczeństwa informacji oraz prywatności w akademickim nauczaniu na odległość. [Review of information security and privacy issues in academic distance learning], Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach [In Polish], 355: 31-44, ISSN 2083-8611.

Kaspersky Security Awareness (2021). Training programs to help you build a cybersafe organization. Retrived from https://www.kaspersky.com/enterprise-security/security-awareness (accessed 9.09.2021).

Liderman, K. (2008). Analiza ryzyka i ochrona informacji w systemach komputerowych (Riskanalysis and information protection in computer systems), Warszawa, PWN, ISBN 9788301153700.

Liderman, K. (2017). Bezpieczeństwo informacyjne (Information security), Warszawa, PWN, ISBN 9788301175009.

McGahagan, J., Bhansali, D. Pinto-Coelho, C. & Cukier, M. (2021), Discovering features for detecting malicious websites: An empirical study, Computers & Security, 109, DOI: 10.1016/j.cose.2021.102374.

Ponemon Institute Report (2020). Cost of a Data Breach Report 2020 IBM, Retrieved from https://www.ibm.com/security/data-breach (accessed17.09.2021).

Ring, M., Schlör, D., Wunderlich, S., Landes, D. & Hotho, A. (2021). Malware detection on Windows Audit Logs using LSTMs. *Computers & Security*. 109. DOI: 102389. 10.1016/j.cose.2021.102389.

Scerbakov, A., Scerbakov, N. & Kappe, F. (2019). Security Vulnerabilities in Modern LMS, DOI: 10.33965/el2019_201909C038.

Skoudis, E., & Zeltser, L. (2004). Malware: Fighting Malicious Code, Pearson Education, Saddle River. ISBN 9780131014053

The National Cyber Security Centre (2021). Reducing your exposure to cyber-attack, Retrieved from https://www.ncsc.gov.uk/ (accessed 17.09.2021).

Verizon Report (2020). Data Breach Investigations Report 2020, Retrieved from https://www.verizon.com/business/resources/reports/dbir/ (accessed 9.09.2021)

Wiener, G. (2019). Cyberterrorism and Ransomware Attacks, New York, Greenhaven Publishing. ISBN 9781534503403

Woźniak-Zapór, M. (2016). Zarządzanie bezpieczeństwem informacji – metody przeciwdziałania zagrożeniom bezpieczeństwa informacji na platformie e-learningowej [Information security management – methods of counter acting information security threats on the e-learning platform], *Bezpieczeństwo. Teoria i praktyka* [In Polish], 4: 87-97, ISSN2451-0718.

Yuste, J. & Pastrana, S. (2021). Avaddon ransomware: an in-depth analysis and decryption of infected systems. *Computers & Security,* 109, DOI:10.1016/j.cose.2021.102388

Agnieszka Kubacka, Daniel Biały, Radosław Gołąb

Postrzeganie bezpieczeństwa informacji w procesie kształcenia na odległość podczas pandemii COVID-19 na przykładzie doświadczeń nauczycieli akademickich

Streszczenie

Pandemia COVID-19 w znacznym stopniu wpłynęła na każdy obszar naszego życia. Jednym z nich była edukacja, która w bardzo krótkim czasie musiała przejść ogromną transformację. Z dnia na dzień komputer zastąpił tablicę i stał się jedynym narzędziem komunikacji między uczniem a nauczycielem. Nauczyciele musieli całkowicie zmienić narzędzia wykorzystywane w procesie nauczania i wejść w zupełnie nowe, dla wielu z nich zupełnie nieznane środowisko pracy. Nauka online zastąpiła tradycyjne nauczanie. Komputer z dostępem do Internetu stał się podstawowym narzędziem pracy dla osób, które dotychczas wykorzystywały go głównie w celach rekreacyjnych. Nauczyciele zostali rzuceni na głęboką wodę, po raz pierwszy zetknęli się z platformami do zdalnej komunikacji. Wraz ze zmianą przestrzeni roboczej uczniowie i nauczyciele zaczęli coraz częściej przenosić się w świat Internetu, który kryje w sobie wiele niebezpieczeństw, z których wiele osób wcześniej nie było świadomych. Z tego powodu autorzy postanowili przyjrzeć się problemowi bezpieczeństwa informacji podczas e-learningu. Wyniki badań zaprezentowane w niniejszej pracy sugerują, że poziom świadomości zagrożeń, jakie mogą spotkać nauczyciele akademiccy w procesie zdalnego nauczania, jest bardzo niski. Dodatkowo nie istnieją odpowiednie procedury dotyczące bezpiecznej pracy w sieci. Problem bezpieczeństwa komunikacji został praktycznie całkowicie pominięty w czasie rewolucji w procesie nauczania jaka wydarzyła się w czasie COVID-19. W niniejszym artykule podjęto próbę zebrania doświadczeń i oceny świadomości nauczycieli akademickich na temat zagrożeń bezpieczeństwa informacji podczas nauczania podczas pandemii COVID-19.

Słowa kluczowe: uczenie się na odległość, pandemia Covid-19, bezpieczeństwo uczenia się na odległość, bezpieczeństwo informacji, zagrożenia internetowe

Агнешка Кубацка, Даниэль Бялы, Радослав Голомб

Восприятие информационной безопасности в процессе дистанционного обучения во время пандемии COVID-19 на примере опыта преподавателей вузов

Аннотация

Пандемия COVID-19 сильно повлияла на все сферы нашей жизни. Одним из них было образование, которое за очень короткое время должно было претерпеть огромные преобразования. В одночасье компьютер заменил доску и стал единственным средством общения между учеником и учителем. Учителям пришлось полностью изменить инструменты, используемые в процессе обучения, и войти в совершенно новую, для многих из них совершенно неизвестную рабочую среду. Онлайн-обучение пришло на смену традиционному обучению. Компьютер с доступом в Интернет стал основным рабочим инструментом для людей, которые до сих пор использовали его в основном в развлекательных целях. Учителя были брошены в крайность, они впервые столкнулись с платформами для удаленного общения. Поскольку рабочее пространство изменилось, учащиеся и учителя стали гораздо чаще переходить в мир Интернета, который таит в себе множество опасностей, о которых многие люди раньше не подозревали. По этой причине авторы решили разобраться в проблеме информационной безопасности во время электронного обучения. Результаты исследования, представленные в этой статье, показывают, что уровень осведомленности об угрозах, с которыми могут столкнуться академические учителя в процессе дистанционного обучения, очень низок. Кроме того, нет надлежащих процедур для безопасной работы в сети. Проблема безопасности связи была практически полностью обойдена во время революции в обучении, произошедшей во время COVID-19. В этой статье делается попытка собрать опыт и оценить осведомленность академических учителей о рисках информационной безопасности во время обучения во время пандемии COVID-19.

Ключевые слова: дистанционное обучение, пандемия Covid-19, безопасность дистанционного обучения, информационная безопасность, интернет-угрозы

Agnieszka Kubacka, Daniel Biały, Radosław Gołąb

Percepción de la seguridad de la información en el proceso de educación a distancia durante la pandemia COVID-19 sobre el ejemplo de las experiencias de los docentes universitarios

Resumen

La pandemia de COVID-19 ha tenido un gran impacto en todas las áreas de nuestras vidas. Uno de ellos fue la educación, que tuvo que sufrir una gran transformación en muy poco tiempo. De la noche a la mañana, la computadora reemplazó a la pizarra y se convirtió en la única herramienta de comunicación entre el alumno y el maestro. Los profesores tuvieron que cambiar por completo las herramientas utilizadas en el proceso de enseñanza y entrar en un entorno laboral completamente nuevo y completamente desconocido para muchos de ellos. El aprendizaje en línea ha reemplazado a la enseñanza tradicional. Un ordenador con acceso a Internet se ha convertido en la herramienta básica de trabajo de las personas que lo han utilizado anteriormente principalmente con fines recreativos. Los profesores fueron arrojados al abismo, se encontraron por primera vez con plataformas de comunicación remota. A medida que cambiaba el espacio de trabajo, los estudiantes y profesores comenzaron a moverse cada vez más hacia el mundo de Internet, que encierra muchos peligros, muchos de los cuales antes desconocían. Por este motivo, los autores decidieron analizar el problema de la seguridad de la información durante el e-learning. Los resultados de la investigación presentados en este artículo sugieren que el nivel de conciencia de las amenazas que pueden encontrar los profesores académicos en el proceso de aprendizaje a distancia es muy bajo. Además, no existen procedimientos específicos para el funcionamiento seguro de la red. El problema de la seguridad de las comunicaciones se pasó por alto prácticamente por completo durante la revolución de la enseñanza que se produjo durante el COVID-19. Este artículo intenta recopilar experiencias y evaluar la conciencia de los profesores académicos sobre las amenazas a la seguridad de la información mientras enseñan durante la pandemia de COVID-19.

Palabras clave: aprendizaje a distancia, pandemia de Covid-19, seguridad en el aprendizaje a distancia, seguridad de la información, amenazas de Internet