Journal of ICT in Education (JICTIE)
ISSN 2289-7844 / Vol. 8 / Issue 2 / 2021 / 60-70

Personal Data Protection Awareness through the Use of YouTube among the Youths in UUM

Mohamad Fadli Zolkipli[1], Diviya Shini Rajamanickam[2*]

[1]*School of Computing, University Utara Malaysia, Kedah, Malaysia; m.fadli.zolkipli@uum.edu.my*
[2]*School of Computing, University Utara Malaysia, Kedah, Malaysia; diviya_shini_raja@soc.uum.edu.my*

** Corresponding author*

To cite this article (APA): Zolkipli, M. F. & Rajamanickam, D. S. (2021). Personal data protection awareness through the use of YouTube among the youths in UUM. *Journal of ICT in Education, 8*(2), 60-70. https://doi.org/10.37134/jictie.vol8.2.6.2021

To link to this article: https://doi.org/10.37134/jictie.vol8.2.6.2021

Abstract

This paper is to discuss the awareness among the youth in UUM related to personal data protection. The cases of personal data protection increased day by day among the youths. Several awareness programs were done. The purpose of this study was to raise awareness of the importance of protecting personal data among the youth in Universiti Utara Malaysia. The method used to do awareness programs by using YouTube and online surveys. Awareness program using YouTube is highly recommended. The finding reveals that it can use this type of media to conduct awareness programs.

Keywords: awareness, current trend, malware, personal data, ransomware.

INTRODUCTION

Technology is evolving in lockstep with the currents of modernity. As a result, as mushrooms grow after rain, many applications are being developed. This application is not only used in the education sector, but also in tourism, services, and other fields. The slogan "everything is at your fingertips" perfectly reflects the way of life in today's society. The development of online applications has been added to some extent by the availability of smartphones and borderless internet access services. Theft of identity remains a current concern which ultimately impacts anybody who uses the Internet (Ball, Ramim & Levy, 2015).

However, the extent to which users is aware that they are sharing personal data to third parties by filling in the details required to sign in to an application. According to (Rafique, 2017), identity robbery reports are still commonly reported, but users continue to reveal more and more personal information online, particularly through e-learning systems (ELS) and social networking sites. In Malaysia, The Ministry of Personal Data Protection Malaysia is a Ministry of Communications and Multimedia (MCMC) agency whose role will be to promote awareness of the law and to provide guidance and general advice as well as main responsibility for regulating individual personal data processing.

Received Date: 13 July 2021; Accepted Date: 27 July 2021; Published Date: 31 July 2021

Social Networking Sites (SNSs) allow users to build personal profiles where much of their personal data, such as the identity card number, alias or true name, personal interests, images, and birthplace, are revealed. The usage among youth and students of SNSs has grown day by day for contact, interaction, and meetings amongst them (Ball, Ramim & Levy, 2015). The purpose of this study was to raise awareness of the importance of protecting personal data among the youth in Universiti Utara Malaysia (UUM). Malaysia received a score of ten out of ten for a measure of high risk of infection from malware use across countries. Malaysia is 9th among the 10 countries that have been measured in malware attacks (Fareen, Sivaraj, Mohammad & Ramanchandran, 2017). University students, especially UUM are also no exception in facing this problem. They have become more vulnerable to significant data security violations, because of their heavy dependency on their computers and the Internet.

This paper reports on the finding of the awareness about personal data protection among the youth via YouTube video. Following the distribution of the awareness video, several respondents were asked to respond to questions about the video, and data was collected in order to determine the extent to which students are concerned about the importance of protecting personal data. This paper is divided into seven sections. Section I contains an introduction to protection of personal information. Moreover, Section II discuss about personal data protection. Some measures of the current trend and the most recent statistic or news on personal data protection are expressed in Section III. Section IV examines the ways to prevent personal data theft via YouTube video. Section V explains the implementation, and Section VI expressed the outcome of the alertness program. Finally, the discussion and conclusion is depicted in Section VII.

LITERATURE REVIEW

Personal Data Protection

Personal data refers to any type of information that can be used to identify an individual, natural person. Personal data protection refers to a collection of strategies and processes that can be used to violate the rights, availability, as well as the integrity of your personal information (Saatci & Gunal, 2019). Personal data protection is also known as personal data security or personal information privacy and a guideline for how sensitive and important data should be collected and handled (Baskaran, Yussof, Rahim & Bakar, 2020). Personal data protection ensures that personal data is only accessible to those who have been authorized and keeps criminals from using data maliciously and assists organizations in meeting regulatory requirements (Romansky & Noninska, 2019). Personal data is classified into two types (Baskaran, Yussof, Rahim & Bakar, 2020):

a) Personal Data

Personal data includes a person's name and surname, postal address, identification card number, mobile number, email address, gender, date of birth, tracking data (for instance, the location data function on a mobile phone), an Internet Protocol (IP) address, pictures, video clips, data held by a hospital or doctor, which could be a symbol that uniquely classifies a person, and so on.

b) Sensitive Personal Data

Sensitive personal data, for instance, criminal records, physical and mental health, political views, religious or other similar beliefs, any other information deemed by the Minister.

- a company registration number.
- an email address such as info@company.com.
- anonymised data.

Current Trend of Attack on Personal Data

a) Ransomware

A ransomware attack is a malicious code that infects a user system or device; it will lock and encrypt the user data and device until they pay it to the attacker (Richardson & North, 2017). Ransomware is also one of the current trends that attack the user's personal data. A new emergence of the ransomware attack is that they aggressively attack users by extorting the victim's money, user personal data is being published. This kind of attack is getting aggressive as the number usage of technology through the internet is increasing day by day (Cristea, 2019). For example, Cristea reported that, during the covid19 pandemic. The authorities will likely send to the people related to the information about awareness during covid19 hits through email. Therefore, users tend to open emails to access the information by the authorities. But this type of method became a favourite to the hackers, as they can use this chance to send emails that they attached together with the malicious code to attack user confidential data (Cristea, 2019).

b) Malware

Malware is also called an intruding code. Malware is also one of the current trends which hackers use to attack users' personal data. The malware was originally used to be one of the experiments to find the vulnerabilities of the machine (Richardson & North, 2017). However today, malware has become a threat, where hackers steal user personal data like their house location, financial account. Either individuals, a big company like the government, or a business corporate system are also some of the targets of the malware attack. The malware attacks can be said to work like Ransomware, they attack the user machine by sending the malicious code through email and they take control of the user's machine. For example, Trojan is also one of the malware. In the Jang Jaccard article, it is reported that 60 percent of the malware attacks were Trojan in 2009 and in 2011 it increased to 73 percent (Jang-Jaccard & Nepal, 2014).

c) Phishing

Fishing the user's credential data is the term used for phishing (Gupta, Tewari, Jain& Agarwal, 2012). The latest statistics of personal data getting attacked by phishing reported by Rajasekharajah are around 32 percent. Phishing attacks use a method of persuasion to make the victims believe in them by sending

Received Date: 13 July 2021; Accepted Date: 27 July 2021; Published Date: 31 July 2021

an email or text to the victims. The attackers will try to make connections with the victims until they start to believe. The purpose is to make the victims easily give them personal data like username, password, or even card details (Rajasekharaiah, 2020). This kind of method could be really dangerous to the people who have less awareness about personal data protection especially among the elderly.

d) Sabotages from external

It is common to hear that attacks are from an outsider, but for a big organization like the government. A threat from inside should also be taken into account. Alharbi said it could be some sort of revenge on that organization by their own employees. It might be because of feeling unappreciated by the employer, therefore, the employees take revenge by helping out the hackers from inside the organization (Alharbi, 2020). Other than revenge, careless workers could be one of the reasons. They make a mistake by accidentally sending out to the wrong people an email that contains sensitive data. This kind of attitude should be taken seriously by the organization, if the same things frequently happen it is like the organization that freely opens its door to the hackers. Cristea (2019) reported in her article that 51 percent of organizations get sabotaged by their own employees in 2018.

Awareness Program Using Youtube

Personal data protection is becoming increasingly important because personal data can be misused and restrict the freedom of the owner of that personal data. In light of the concept of human rights, that is, the rights that human have solely because they are humans, based on their human dignity. One of the fundamental human rights is the right of everyone not to be subjected to arbitrary or unlawful attacks on his personal life or personal property, including his communication relationship, by a state official conducting an investigation and/or investigation into a criminal offense. Because of the alarming increase in the number of cases of personal data misuse and the negative effect on victims, the authors created an awareness video, which they are crediting and uploading to YouTube for educational purposes. Creating videos for YouTube will lead to more youths and influencers knowing and talking about personal data protection. The awareness program using YouTube will help the youths or other people to protect them from the threat. The steps to protect the personal data from being attacked by a hacker are shown below:

a) Put stronger passwords on your devices

Put stronger passwords on the devices because mobile phones, laptops, as well as tablets are easily stolen or lost. This is risky behaviour because it's not difficult for identity thieves to gain access to more of your accounts if they figure out one password (Skendzie, Kovacic & Tijan, 2018). Passwords that are long and random are the most secure. Strong passwords are essential for online security, as you've likely noticed. Consider using a passcode management system to make managing your passwords easier. Passwords are essential for avoiding hackers from retrieving the information. Based on the current National Institute of Standards and Technology's (NIST) 2017 login information regulatory framework, people might consider (Sim, Chua & Tahir, 2019):

- Getting rid of the wacky, complex mix of upper case letters, symbols, and numbers. Instead, choose something more accessible that has at least eight characters and a maximum length of 64 characters.
- Do not practice the similar passcode more than once.
- The passcode must include at least one lowercase letter, one uppercase letter, one number, and four symbols but not the characters &% #@.
- Put a password that easily remembers and do not leave a password hint out in the open for hackers to see.
- If you forget your password, you can reset it. However, change it once a year for a general refresh.

b) Configure two-factor authentication for financial and email accounts.

Two-factor authentication, also known as multi-factor authentication, is a facility that enhances extra security measures to the ordinary passcode technique of digital verification. Generally, individuals fill a user id and passcode in the absence of two-factor authentication (Celik, Alkan, & Alkan, 2020). With two-factor authentication, it is required to insert an extra authentication technique, for instance a Personal Identification Code, alternative passcode, or even your fingerprint. Persons utilizing multi-factor authentication should be required to select more than two additional user authentication after entering their user id and passcode (Skendzie, Kovacic & Tijan, 2018). As per NIST, Text message service will not be used for two-factor authentication because malicious software is for use to attack smartphone connections and compromise data.

c) Do not use public Wi-Fi

When linking to public Wi-Fi (VPN), use a Virtual Private Network (VPN). When you use a VPN, the device's circulation is encrypted between the device and the VPN server (Gandhi, Sucahyo, Ruldeviyani, 2018). This makes gaining access to sensitive data on the device even more problematic for a cybercriminal. When security is critical, utilize your cell network instead of a VPN.

d) Update your software regularly

Professionals advise keeping all application software and operating systems up to date on a regular basis. Patches should be installed whenever they become available. When programs are not patched and updated on a regular basis, your network becomes vulnerable (Tiganoaia, Cernian & Niculescu, 2017). Microsoft now has a product called Baseline Security Analyzer that can test to make sure that all programs are patched and up to date on a regular basis. This is a relatively simple and low-cost method of fortifying your network and preventing attacks from occurring (Gandhi, Sucahyo, Ruldeviyani, 2018). Update the software like antivirus software, operating system, and any other software normally used.

Received Date: 13 July 2021; Accepted Date: 27 July 2021; Published Date: 31 July 2021

e) Be cautious when opening email attachments or clicking on links.

Be wary of phishing. Phishers try to trick you into clicking on a link that will lead to a security breach. Phishers prey on employees in the expectation that they might click on malicious links that consist of viruses and malware (Tiganoaia, Cernian & Niculescu, 2017). As a result, it's important to be extremely careful of links and email attachments from senders you don't identify. Hackers could infiltrate your company's computer network with a single click. Here's an example of a rule to remember: Never provide personal or business data in reply to an email, pop-up webpage, or any other form of communication that you did not initiate. Identity theft is a risk of phishing (Gandhi, Sucahyo, Ruldeviyani, 2018). It is also the method used by the majority of ransomware attacks. The organization could aid by implementing email authentication technology that detects and blocks suspicious emails. Individuals are typically alerted that their email has been routed to a confinement directory, where they can be checked to see if it is justifiable (Tiganoaia, Cernian & Niculescu, 2017). To protect the personal information, individuals need to put some basic security measures in place to prevent them in the event that the individual information is compromised.

f) Do not give out confidential data over the cell phone, email, or text.

If a person receives a call, email, or text asking for private data from a vendor, charitable organization, security apparatus, or long-lost cousin, it is most likely a phishing scam — no matter how genuine it appears. Don't reveal any of your personal information (Skendzie, Kovacic & Tijan, 2018). If you believe the request is genuine, look up the organization's contact information and call to follow up.

g) Disable lock-screen notification

Trying to turn off lock-screen app notifications on mobile phones is an easy technique to conceal confidential details that may appear on the lock screen. To retain messages and social media notifications protected from prying eyes, disable app notifications (Sim, Chua, & Tahir, 2019). To turn off app notifications on iOS, navigate to Settings > Notifications and select an app. You can also disable app previews for all apps by going to Settings > Notifications > Show Previews and selecting "When Unlocked" or "Never." Go to Settings > Lock screen and security > Notifications on Android (Skendzie, Kovacic & Tijan, 2018). Set text previews to only show the name of the person texting you, or disable previews entirely on your lock screen. On iOS, go to Settings > Notifications > Messages > Alerts. On Android, go to Messaging > Settings > Preview Messages.

h) Data backup

Regular data backup seems to be an important element in individual internet privacy that is often overlooked. The top IT and security supervisors adhere to the 3-2-1 backup principle (Tiganoaia, Cernian & Niculescu, 2017). Primarily, preserve three duplicates of data on two various forms of media (local and external hard drives) and one copy off-site (cloud storage) (Gandhi, Sucahyo, & Ruldeviyani, 2018). If an individual turns out to be a ransomware or malware perpetrator, the one method to recover the data is to remove the computer systems and regain from a recent backup.

IMPLEMENTATION

A video about personal data protection was created and uploaded it on YouTube. Online survey is method of data collection, while YouTube is just a mechanism that we used in this study to reach the uses on awareness issues. From that we do data collection by doing online survey. The students of School of Computing (SOC) faculty were selected in this study. This survey was conducted for one week.

RESULT FORM THE AWARENESS PROGRAM

Results from the awareness program were obtained through the YouTube and survey using the google form. The total number of participants in this survey is 35 people. The participants are of the youth age between 18 and 30.

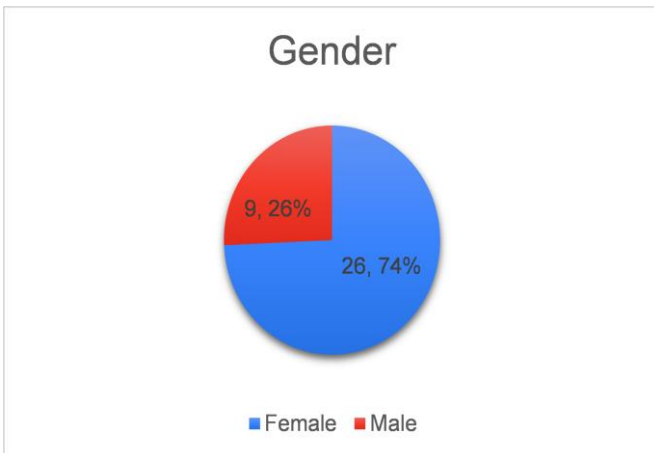

Figure 1: The total number of gender who has participated in this awareness program survey.

26 (74%) are female and the rest is male, which is 9 participants (26%). Figure 2 shows the range of age that can be categorized as youth.

Received Date: 13 July 2021; Accepted Date: 27 July 2021; Published Date: 31 July 2021

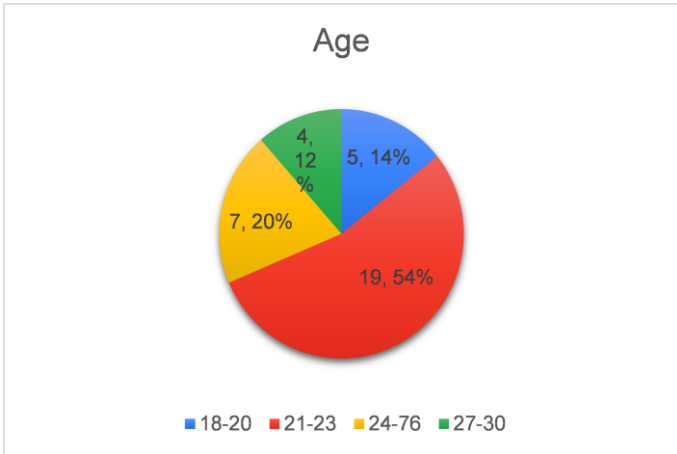

Figure 2: The age of participant

Among the range, age between 21 until 23 is the highest which is 19 (54%); the second-highest age who participated in this survey is the age between 24 until 27 which is 7 (20%). The rest are aged between 18 until 20 which are 5 (14%) and ages between 27 until 30 which are 4 (12%). Figure 3 shows a question that asks whether they know what personal data is.

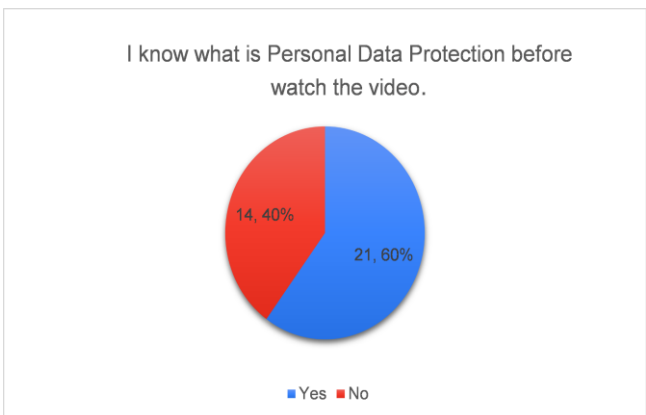

Figure 3: Participant knowledge about personal data protection before watching the video

In Figure 3, it shows that among the 35 participants. 21(60%) participants have voted yes, they know about personal data protection before watching the awareness video. The rest, 14 (40%) voted no, which meant they were not aware of personal data protection.

In Figure 4, participants have been asked before they sign up for an account whether they have been asked to agree to any policy. Among the 35 participants, 34(97%) of them have voted yes and the rest voted no which is 1 (3%). While Figure 5 shows that out of 35 participants, only 10(29%) participants who have read the policy before click yes to sign up for the account. The rest 17(48%) participants vote sometimes and 8(23%) participants vote no. This can be concluded that even though they are

aware of their personal data protection, still the number of participants who have read the agreement policy is less.

Figure 4 and 5 are related to the policy before signing up to any account.

Figure 4: Read the agreement policy before signing up to any account

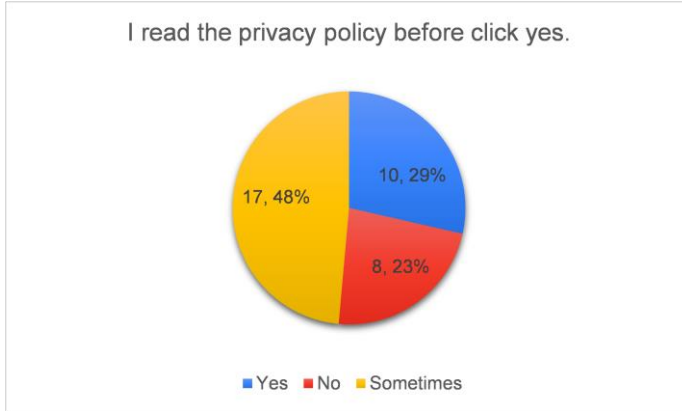

Figure 5: Read policy

This can be proven in Figure 6. Where participants have been asked whether they have used public Wi-Fi before. 29 (83%) out of 35 participants have voted yes. The rest have voted no which are 6(17%). This shows that, even though they know about personal data protection, they still have less awareness that using public Wi-Fi can actually bring harm to them

Received Date: 13 July 2021; Accepted Date: 27 July 2021; Published Date: 31 July 2021

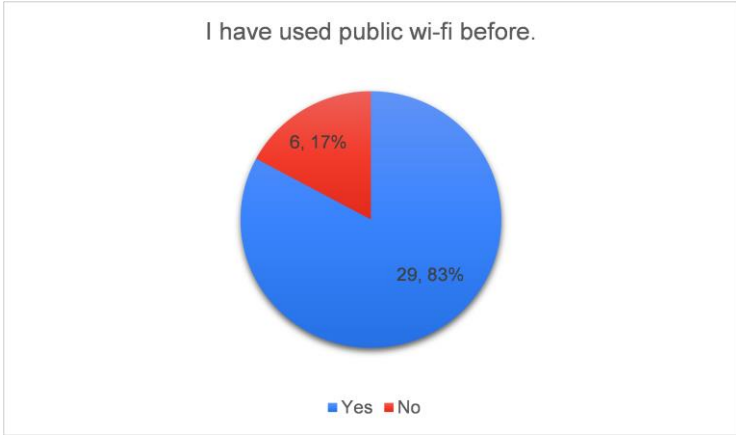

Figure 6: Used public Wi-Fi

Figure 7 shows the numbers of feedback from the participants of this survey. Participants have been asked about their feedback after watching the awareness video. 22(62.86%) strongly agree that they think the awareness video does provide enough knowledge to them related to personal data protection. 12 (34.28%) voted 'Agree' and 1(2.86%) voted 'Neutral'. Next, participants have been asked whether they gain more knowledge about personal data protection through the video. 28(80%) have voted 'Strongly agree', 5 (14.28%) agree that they gain more knowledge. While 1(2.86%) voted for 'Neutral' and 1(2.86%) of the participants voted 'Disagree'. Lastly, 26(74.28%) participants strongly agree that they understand more about personal data protection after watching the awareness video. 6(22.86%) participants voted for 'Agree' and 1(2.96%) voted they felt neutral.

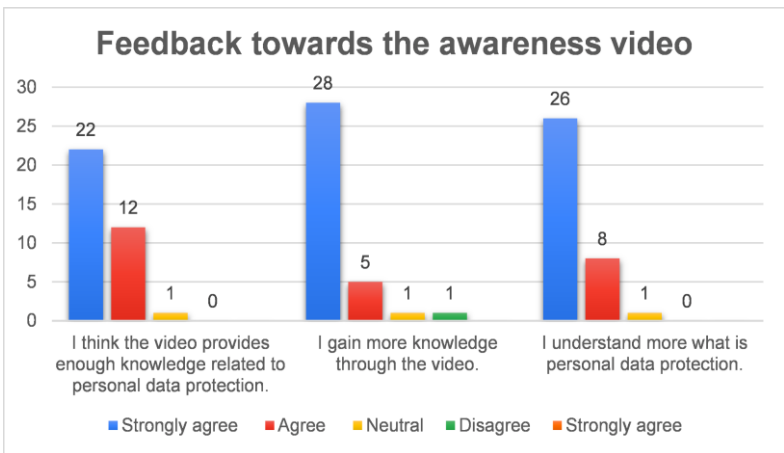

Figure 7: Participant feedback

DISCUSSION AND CONCLUSION

Through the awareness program and the survey involving 35 participants. More than 50% of the participants do know about what is personal data protection. But they still lack awareness about their personal data protection. This can be proven when only 10 participants have voted yes that they have read any policy before signing up to any account while 29 participants have used public Wi-Fi. This paper has discussed the steps to prevent your personal data from being attacked by hackers. Therefore, it is hoped that this paper will help the youth or other people to protect them from the threat. In addition, it is hoped that this paper will help future researchers to do research on the related topic.

ACKNOWLEDGMENT

The authors would like to thank all School of Computing members who were involved in this study. This study was conducted for the purpose of the System and Network Security Research Project. This work was supported by University Utara Malaysia.

REFERENCES

Alharbi, F. S. (2020). Dealing with data breaches amidst changes in technology. *International Journal of Computer Science and Security*, *14*(3), 108-114.

Ball, A. L., Ramim, M. M., & Levy, Y. (2015). Examining users' personal information sharing awareness, habits, and practices in social networking sites and e-learning systems. *Online Journal of Applied Knowledge Management*, *3*(1), 180-207.

Baskaran, H., Yussof, S., Rahim, F. A., & Bakar, A. A. (2020). Blockchain and the Personal Data Protection Act 2010 (PDPA) in Malaysia. In *2020 8th International Conference on Information Technology and Multimedia (ICIMU)* (pp. 189-193). IEEE. https://doi.org/10.1109/ICIMU49871.2020.9243493

Çelik, M., Alkan, M., & Alkan, A. O. (2020). Protection of Personal Data Transmitted via Web Service Against Software Developers. In *2020 International Conference on Information Security and Cryptology (ISCTURKEY)* (pp. 88-92). IEEE. https://doi.org/10.1109/ISCTURKEY51113.2020.9308009

Cristea, L. M. (2020). Current security threats in the national and international context. *Journal of Accounting and Management Information Systems*, *19*(2), 351-378.

Gandhi, A., Sucahyo, Y. G., & Ruldeviyani, Y. (2018). Investigating the protection of customers' personal data in the ridesharing applications: A desk research in indonesia. In *2018 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)* (pp. 118-121). IEEE. https://doi.org/10.1109/ECTICon.2018.8619912

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, *28*(12), 3629-3654. https://doi.org/10.1007/s00521-016-2275-y

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

Rafique, G. M. (2017). Personal information sharing behavior of university students via online social networks. *Library Philosophy and Practice* (e-journal).

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10-21.

Romansky, R., & Noninska, I. (2019). Cyber Space Features–Security and Data Protection Requirements. In *2019 International Conference on Information Technologies (InfoTech)* (pp. 1-4). IEEE. https://doi.org/10.1109/InfoTech.2019.8860880

Saatci, C., & Gunal, E. S. (2019). Preserving privacy in personal data processing. In *2019 1st International Informatics and Software Engineering Conference (UBMYK)* (pp. 1-4). IEEE. https://doi.org/10.1109/UBMYK48245.2019.8965432

Sim, W. L., Chua, H. N., & Tahir, M. (2019). Blockchain for identity management: The implications to personal data protection. In *2019 IEEE Conference on Application, Information and Network Security (AINS)* (pp. 30-35). IEEE. https://doi.org/10.1109/AINS47559.2019.8968708

Tiganoaia, B., Cernian, A., & Niculescu, A. (2017). The use of social platforms and personal data protection—An exploratory study. In *2017 16th RoEduNet Conference: Networking in Education and Research (RoEduNet)* (pp. 1-5). IEEE. https://doi.org/10.1109/ROEDUNET.2017.8123754