HOME OFFICE AND CYBERCRIME DURING THE COVID-19 PANDEMIC

Nikolett Gyurián Nagy

Abstract

The study focuses on cybercrime in home office, which is developing at an ever-faster pace and constantly follows new trends. The purpose of the research is to explore the relationship between the transition to working from home and the increasing trend of cybercrime. The research is based on the processing of secondary results. The method of the research is a systematic literature review and the research was done using keyword pairs (cybercrime and home office; covid and home office; cybercrime and covid). The central question of which was the relationship between working from home and the increasingly frequent cybercrime. Most companies have seen an increase in cyber-attacks during Covid-19 pandemic and the most common type of attacks are phishing messages. The study confirms the increase of cybercrime due to the recent change to online communication and work. According to the results, there is a relationship between the increasing trend of cybercrime and the increasing frequency of working from home. The post-covid cyber security priorities clearly shows the companies' initiative towards security: most of them are transforming the organization to be secure, mostly through the use of security services, training, multi-step authentication or enhanced device security want to achieve. Nowadays, the companies worldwide spend more than 55 billion dollars (per year) on a secure digital transition.

Key words: cybercrime, Covid-19, home office

JEL Code: O15, H12

Introduction

Cyber-attacks know no borders and are evolving at a very fast pace. They are closely related to online fraud, and these two terms are often confused. Cybercrime could be expressed in terms such as ransomware, server access or attacks on PayPal accounts. Their targets can be governments, businesses and individuals. Complex criminal networks around the world are able to coordinate complex attacks in minutes, and the period overshadowed by Covid is no exception, when cybercrime took on new dimensions as a result of the transition to online

communication and work. During the Covid period, 46% of companies experienced a cyber threat. Google reported that it had detected 18 million malware and phishing e-mails per day related to the Covid-19 pandemic situation in one week. These scams were mostly emails sent on behalf of credible government organizations such as the WHO (Guardian, 2020). It is also important to highlight India, where online attacks have increased by 86% between March and April 2020 since the lockdown. This is an unprecedented increase, but obviously the lack of security measures also plays a part here. Incidentally, in India, the case when they tried to sell the Statue of Unity for 4 billion dollars is mentioned as one of the most scandalous incidents. Fraudsters claimed the proceeds would go towards helping the government's aspiration against Covid (Roy, Anand, 2020). Computer attacks against healthcare organizations have doubled, for example, in the Czech Republic, the hospital in Brno was attacked in such a way that the entire IT system had to be shut down and urgent surgeries had to be postponed (Cyberlaw, 2020).

1 Methodology

The research is based on a systematic literature review. The central question of the research is what the connection between home office/remote working and the increasingly common cybercrime is. I primarily searched for scientific results in the Web of Science and Scopus databases. Based on preliminary research and validation, I created three pairs of keywords: „cybercrime and home office “, „covid and home office“, and „cybercrime and covid“. I found 215 studies for the three keyword pairs, of which only 25 studies dealt with cybercrime. The other 190 studies were more about the introduction, transition and effects of remote work caused by Covid-19. In addition to WOS and Scopus, I also looked at the announcements of Interpol, FBI and statistical institutions on the subject.

2 Remote working in the Covid-19 era

The Covid-19 pandemic has changed many aspects of our lives and work. International and local governments have drawn the attention of companies to the necessary measures. As a result, many companies tried to switch to working from home. Working from home appeared in the 2000s, when developing technology made it possible to have everything available for working in the home of the employee. In the beginning, it was popular because its introduction prevented commuting and provided flexibility in the field of work. As a result of Covid-19, many companies switched to working from home, for all jobs where this was feasible. These measures redefined the traditional concept of the home office, which was only typical of

certain types of work, of an occasional nature, or in unique employee circumstances (Xiao et al., 2021). The authors of the study mentioned in the previous point assume that perhaps one of the biggest challenges for most companies was the transition to working from home, since until now the concept was known in the country, yet it was treated with distrust. However, the pandemic situation overrode this view, and it was important for all employers and employees whose job allowed it to be ordered to work from home (Poór et al., 2020).

3 Most common types of online scams

There are many old and new types of scams. We can often meet money transfer scams when we transfer a certain amount of money to the other party (Norris, Brookes, 2021). It should be mentioned, that nowadays transfer scam is on a declining trend. The main reason for this is the introduction of security controls for payment gates. In case of webshop scams, the victim receives the package, pays, but opens only after payment. The package does not contain the purchased products. Instead, in the package is brick, wrong product or others (Whittaker, Button, 2020). In case of product service scams the victim sends the product to the address provided on the internet or personally hands over the product for repair, possibly also the price of the repair, but does not get back the product (most often mobile phone or technical device). Ticket scams are mostly realized in ticket duplication. Trading with fake products is a very common type of online scams. This type of scams usually is realized in social media or in online want-ad sites. Trust based scams are rather rare form of fraud. In this case, the offenders have already made some successful transactions with the buyer and only after this become criminals. (Kollár, 2018). The phishing is one of the earliest forms of scams. In this case, scammers try to obtain information through messages in order to create false profiles from the obtained personal data. The lottery scam is another form of phishing where the damage is much more serious. In reality, there is no lottery and there is no prize waiting for the user. In case of video scams or the process of video scamming the user involves tricking into viewing an infected video, containing malware (Puram et al., 2011).

3.1 Typical cyber-attacks during the Covid-19 pandemic

Nowadays, we can already arrange in groups the attacks that come into focus during the pandemic, according to their types:

- *Remote access infrastructure* - Perhaps one of the biggest problems in telecommuting was accessing the data needed for work. In order to facilitate this, companies have developed their remote access infrastructure. However, they did not expect how large

an attack surface they would give cybercriminals. This group is the most decisive of the attacks (Khishamova, Begishev, 2022).

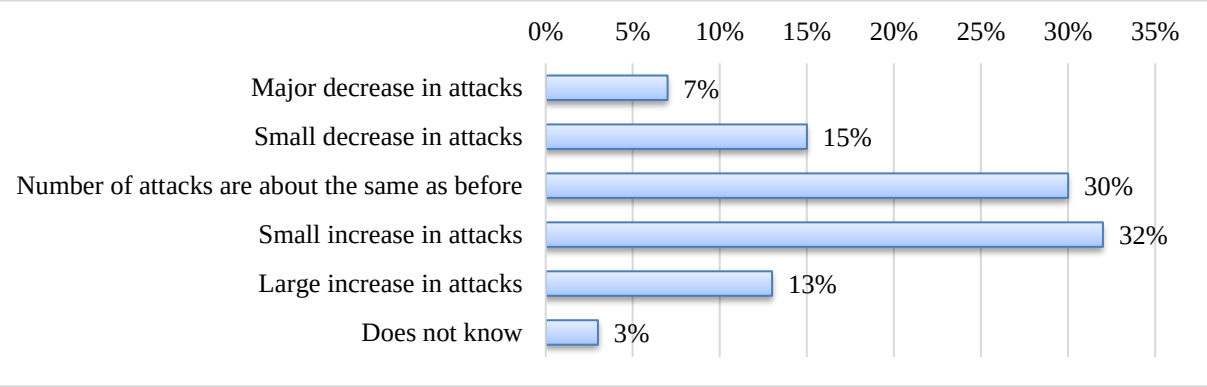
- *Traditional phishing attacks and malware* - As the online community grew, so did traditional phishing attacks and malware (Gryszczyńska, 2021).
- *Classic fraud schemes* - Another group is the adaptation of classic fraud schemes with social engineering methods (Naidoo, 2020).
- *Digital communication platform attacks* - Another group of attacks during Covid-19 is aimed at digital communication platforms. Here, I would highlight the Zoombombing phenomenon as an example, when outsiders join video conferences uninvited by deciphering ID codes and share inappropriate content (Lee, 2022).
- *Other* - Attacks in online games and pornographic materials and messages distributed on social networks form a separate group (Khishamova, Begishev, 2022).

From the point of view of management, the first four groups are considered really important and relevant.

4 Corporate experiences with cyber attacks during remote work

Based on responses from IT security professionals across the world, the COVID-19 pandemic has affected the rate of cybers-attacks but not as much as expected, with most organizations having made the switch to remote working.

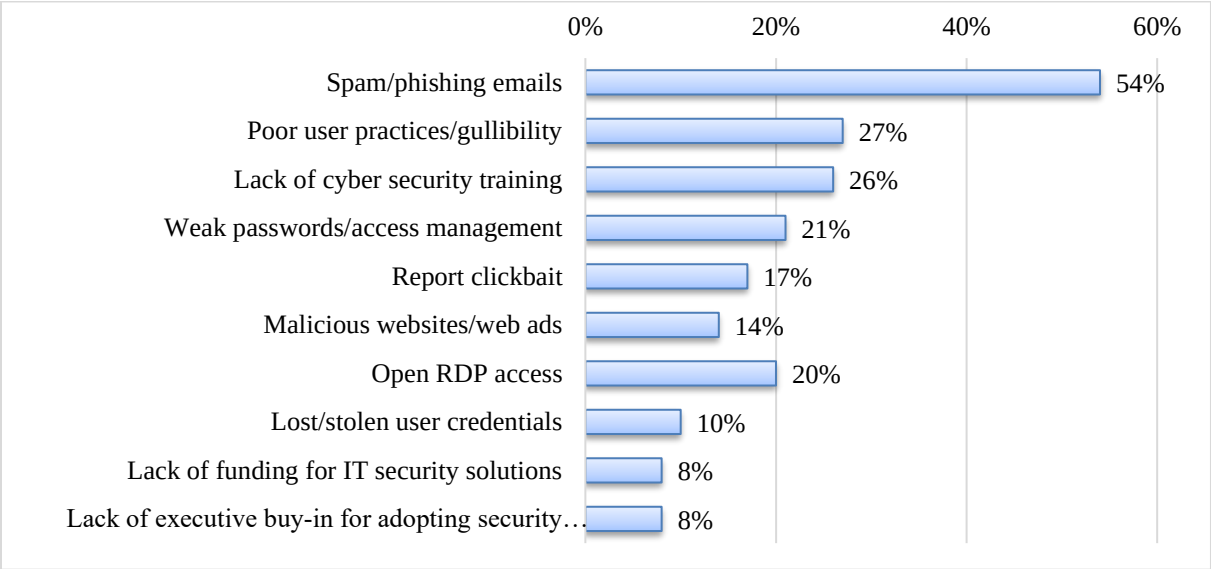
Fig. 1: Changes in cyber-attack frequency following COVID-19



Source: Statista (2022a)

Nearly two thirds of company representatives surveyed stated that the number of attacks they experienced had either remained the same as before the pandemic, or increased slightly during this time (Statista, 2022a).

Fig. 2: Most common delivery methods and cybersecurity vulnerabilities causing ransomware attacks, worldwide



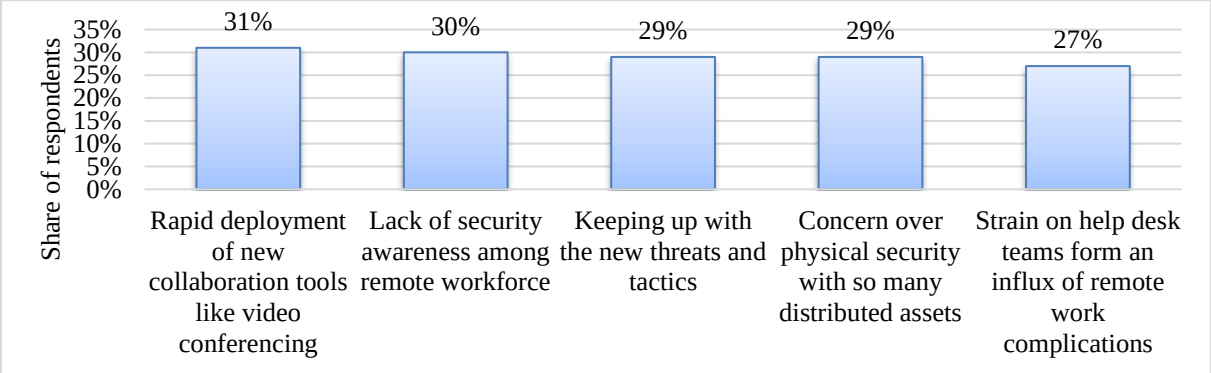
Source: Statista (2021a)

Figure 3 shows the results of a worldwide survey, which reveals the causes of ransomware attacks typical of SMEs. More than half of the respondents indicated that phishing messages are the most common cause of ransomware. However, inexperience, lack of cybersecurity training, use of weak passwords, or the use of RDP infrastructure for remote access are weaknesses (Statista, 2021a).

Since the beginning of the COVID-19 pandemic, the Asian region has experienced the highest daily VPN and RDP authentication in remote access technologies at 68%. Remote access is least used in the EU. However, all regions reported an increase in telecommuting as companies relied heavily on remote access technologies to allow them to work from home during the pandemic (Statista, 2021b).

The attackability of remote access technologies can also be influenced by various factors. For example, the device used by employees can also be an attack alternative, which is not equipped with the necessary security programs, or passwords are saved by the device. Specifically, a survey conducted on this topic in the US and the UK in 2020 revealed that 49% of respondents in the US and 39% of respondents in the UK use their company applications on personal devices such as laptops, tablets or smartphones and networks. This type of behavior makes companies more vulnerable to cyber threats (Statista, 2021c).

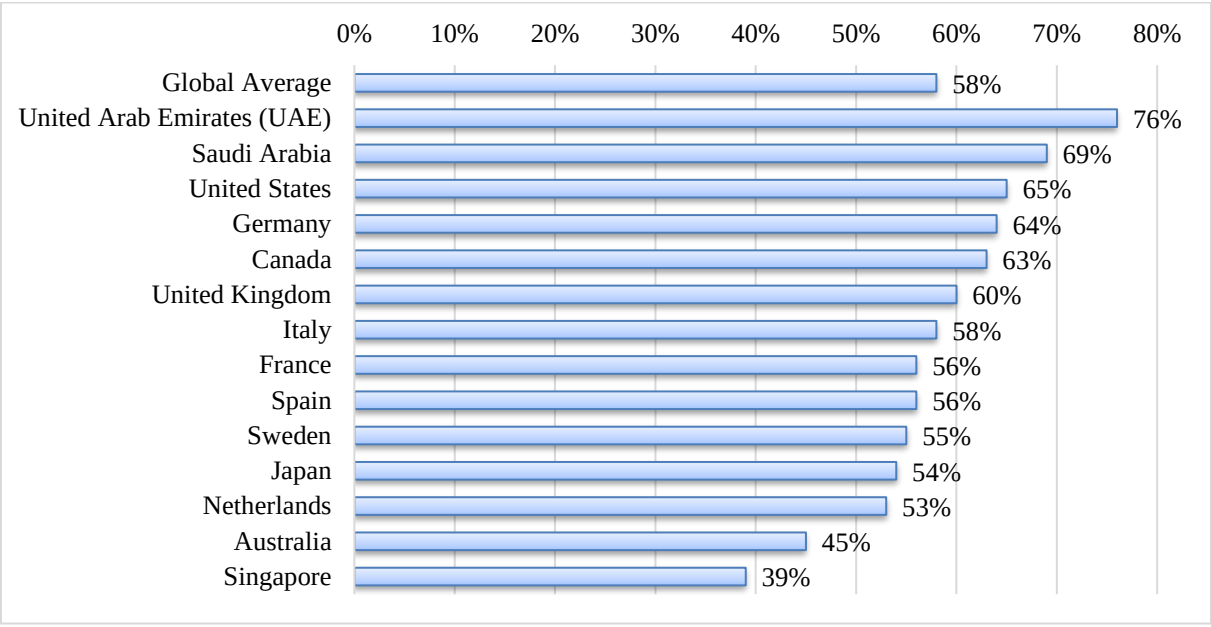
Fig. 3: Most important challenges in keeping the remote workforce secure worldwide



Source: Cybersecurity Workforce Study (2021), Statista (2021d)

The most important challenge in keeping remote workforce secure in 2021 was the rapid deployment of new collaboration tools, such as video conferencing. At the same time, one third of respondents considered the lack of security awareness among remote workforce to be a challenge in 2021 (Cybersecurity Workforce Study (2021); Statista (2021d).

Fig. 4: Percentage of CISOs saying their business has seen more targeted attacks since enabling widespread remote working worldwide

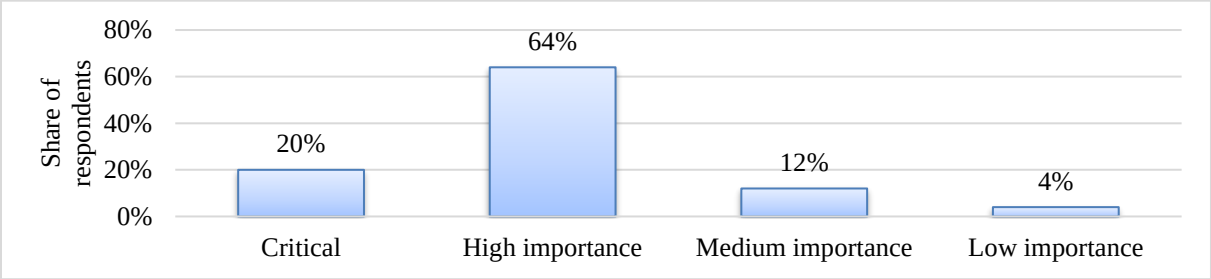


Source: Voice of the CISO Report (2021), Statista (2021e)

Chief Information Security Officers (CISOs) in the United Arab Emirates, Saudi Arabia and the United States (US) have largely seen their business experience more targeted cyber attacks since widespread remote working became possible from 2021. And the Netherlands

evaluates telecommuting more positively compared to the global average of 58% (Voice of the CISO Report (2021); Statista, 2021e).

Fig. 5: Importance of protecting users against phishing and cyber attacks



Source: Statista (2022b)

Based on a survey conducted among IT security professionals, 64% of respondents stated that protecting users against various cyber-attacks is very important when enabling remote work, while 20% considered it critical. This demand became even more widespread after the coronavirus pandemic and the subsequent closures in 2020 (Statista, 2022b).

Conclusion

It is clear, that the outbreak of COVID-19 has greatly accelerated digital transformation initiatives in companies around the world. Millions of employees have been sent to work from home. This change has also increased the need for a secure digital work environment and network infrastructure, which companies have to deal with even if they were not prepared for it. Based on the research results so far, the most important thing would be prevention, i.e. building strong cyber security. This is also extremely important because it is very difficult to track down fraudsters based on police data and enormous financial damage is caused as a result of such attacks. In 2020, a global survey of post-covid cyber security priorities was also conducted, which clearly shows the companies' initiative towards security: almost 95% are transforming the organization to be secure, mostly through the use of security services, training, multi-step authentication or enhanced device security want to achieve. This process has already started since the outbreak of the pandemic. This is also proven by the development of the amounts spent on cyber security from 2017 to 2021. A certain level of growth was already noticeable around 2017 and 2018, but the really big jump happened in 2020, when companies worldwide spent 55 billion dollars on a secure digital transition.

There are very small number of sources that examine the relationship between cybercrime and the home office. Based on the research of Gryszczyńska (2021), the "Warning List" was created

in Poland during the pandemic, which contains domain names used to fraudulently obtain data and financial resources. Although the research did not show a significant increase in the number of cybercrimes committed in Poland during the pandemic, changes were observed in the attack scenarios used by the perpetrators. Buil-Gil et al. (2020) proved the connection between cybercrime and Covid-19: cybercrime almost doubled during Covid-19. Furthermore, the relationship was confirmed in his research by Miró-Llinares (2022).

Overall, the results show that there is a strong correlation between the increasing trend of cybercrime and the increasing frequency of working from home. The reason for the success of the attacks could have been the companies' lack of preparation, which includes unprotected networks, the use of external tools or the lack of information about cyber security for employees; and the organized and diverse modern work of cybercriminals.

I identify the main limitations of the research in the relatively small number of literature sources and in the fact that it is somewhat difficult to collect data on such crimes, either due to the issue of their detection or their disclosure.

On the other hand, I see great research potential in the topic. In my opinion, a good method would be domestic primary research, followed by an international comparison if additional data is available.

Acknowledgment

I would like to express my appreciation to the Digital Consumer Protection’s research team at Széchenyi István University for the successful collaboration. I would like to extend my gratitude to the team of Vehicle Industry Research Center and Digital Development Center, who provided the place for our work and support us.

References

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., Díaz-Castano, N. (2020). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. European Societies 23(1), 47-59. https://doi.org/10.1080/14616696.2020.1804973

Cybersecurity Workforce Study. (2021). A Resilient Cybersecurity Profession Charts the Path Forward. Online: https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

Dumchikov, M., Fomenko, A., Yunin, O., Pakhomov, V., Kabenok, Y. (2022). The essence and classification of cybercrime in the field of computer information. Amazonia Investiga, 11(51), 291-299. https://doi.org/10.34069/AI/2022.51.03.29

Miró-Llinares, F. (2022). The impact of COVID-19 on cybercrime trends. Online: https://rm.coe.int/presentation-fernando-miro-llinares-the-impact-of-covid-19-on-cybercri/1680a1e42f

Norris, G., Brookes, A. (2021). Personality, emotion and individual differences in response to online fraud. *Personality and Individual Differences*.

Gryszczyńska, A. (2021). The impact of the COVID-19 pandemic on cybercrime. *Technical Sciences*. 69(4). DOI: 10.24425/bpasts.2021.137933

Guardian News and Media. (2020). Google detecting 18m malware and phishing messages per day related to covid-19. The Guardian. Online: https://www.theguardian.com/australia-news/2020/jul/ 14/google-detecting- 18m-malware-and-phishing-messages-per-day-related-to-covid-19

International cyber law: interactive toolkit. (2021). Brno University Hospital Ransomware Attack. https://cyberlaw.ccdcoe.org/wiki/Brno_University_Hospital_ransomware_ attack

Kishamova, Z., I., Begishev, I., R. (2022). Digital crime in the context of a pandemic: main trends. *Russian Journal of Criminology*. 16(2), 185-198. DOI:10.17150/2500-4255.2022.16(2).185-198

Kollár, Cs. (2010). A magyarországi online csalások fontosabb tulajdonságai. *Belügyi Szemle* 10. 56-70.

Lee, C., S. (2021). Analyzing Zoombombing as a new communication tool of cyberhate in the COVID-19 era. *Online Information Review*. 46(1), 147-163. https://doi.org/10.1108/OIR-05-2020-0203

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems.* 29(3). 306-321. https://doi.org/10.1080/0960085X.2020.1771222

Poór, J., Balogh, G., Dajnoki, K. , Karoliny, M., Kun, A. I., & Szabó, Sz. (2020). Koronavírus-válság kihívások és HR válaszok: Magyarország 2020 (A kutatás első fázisának

kiértékelése): Kutatási jelentés. Budapest: *Szent István Egyetem Gazdaságés Társadalomtudományi Kar Menedzsment és HR Kutató Központ*.

Proofpoint. (2021). Voice of the CISO Report. Online: https://www.courthousenews.com/wp-content/uploads/2021/05/pfpt-us-wp-voice-of-the-CISO-report.pdf

Puram, P., K., Kaparthi, M., Rayaprolu. A., K., H. (2011). Online scams: taking the fun out of the internet. *Indian Journal of Computer Science and Engineering (IJCSE)* 2(4). 559-565.

Roy, A., Anand, N. (2020). Scammers try selling world's tallest statue as pandemic boosts India's cyber crime. *The Thomson Reuters*. Online: https://www.reuters.com/article/us-health-coronavirus-india-fraud-idUSKBN21P0KH

Statista. (2021a). Most common delivery methods and cybersecurity vulnerabilities causing ransomware infections. Online: https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/

Statista. (2021b). Remote access technology use increase 2020. Online: https://www.statista.com/statistics/1226084/remote-access-technology-use-by-region/

Statista. (2021c). IT security habits of remotely working employees in the United States and the United Kingdom in 2020. Online: https://www.statista.com/statistics/1229274/remote-work-employee-security-habits-uk-us/

Statista. (2021d). Most important challenges in keeping the remote workforce secure worldwide in 2021. Online: https://www.statista.com/statistics/1297613/global-challenges-keeping-remote-work-secure/

Statista. (2021e). Percentage of CISOs saying their business has seen more targeted attacks since enabling widespread remote working worldwide in 2021. Online: https://www.statista.com/statistics/1259560/ciso-organization-cyberattacks-remote-work-by-country/

Statista. (2022a). Changes in cyber attack frequency following COVID-19 as of 2021. Statista research Department. Online: https://www.statista.com/statistics/1257974/changes-in-cyber-attacks-covid19/

Statista. (2022b). Remote work: importance of protecting users against phishing and cyber attacks. Online: https://www.statista.com/statistics/1258263/remote-work-protection-against-cyber-attacks/

Whittaker, J., Button, M. (2020). Understanding pet scams: A case study of advance fee and non-delivery fraud using victims' accounts. *Australian & New Zealand Journal of Criminology* 53, 497-514.

Xiao, Y., Becerik-Gerber, B., Lucas, G. and Roll, S.C. (2021). Impacts of working from home during COVID-19 pandemic on physical and mental well-being of office workstation users. *Journal of Occupational and Environmental Medicine*, 63(3),

Contact

PhDr. Nikolett Gyurián Nagy, PhD.

Széchenyi István University, Kautz Gyula Faculty of Economics, Department of Leadership and Marketing

Egyetem tér 1., 9026 Győr, Hungary

nagynikolett.sze@gmail.com