This journal provides immediate open access to its content under the [Creative Commons BY 4.0 license](#). Authors who publish with this journal retain all copyrights and agree to the terms of the above-mentioned CC BY 4.0 license.

DOI: 10.2478/seeur-2020-0005

TECHNOLOGY: COVID-19 AND THE 'NEW-NORMAL' LIFESTYLE VS. SECURITY CHALLENGES

Assoc. Prof. Adrian Besimi, Faculty of Contemporary Sciences and Technologies, South East European University, North Macedonia

a.besimi@seeu.edu.mk

Assoc. Prof. Visar Shehu, Faculty of Contemporary Sciences and Technologies, South East European University, North Macedonia

v.shehu@seeu.edu.mk

ABSTRACT

In the last period, especially during the COVID-19 pandemics, individuals as well as institutions globally and in North Macedonia particularly, have failed to correctly respond to the new challenges related to cyber security, online attacks, and fake news. Being that in a state of isolation and quarantine most governmental institutions have heavily relied on online tools to communicate among each other and with the public, it is quite evident that they have not been well prepared to adopt new technologies. This paper aims to bridge together the needs for technology during the COVID-19 pandemics versus the security challenges that many forget to mention. The primary focus of this paper is to elaborate on the security challenges associated with technology with several examples from incidents around the world and from North Macedonia. As such, it represents a perspective paper with focus on current and emerging advances on IT security for running the “new normal” world.

Key words: covid-19, technology, hybrid-attacks, network security.

INTRODUCTION

The “new normal” as we refer to in this paper, is actually the new way of running daily operations, including but not limited to: teaching, learning, doing business, paying, buying groceries, etc., all with the latest technology available to us. Of course, “new” in this paper is implied by the current COVID-19 pandemics, and not by the development of the society. In fact, the society adopted the latest technology, faster, only because of the pandemic situation, or simply because of the necessity.

As of March 2020, most of the countries in the world applied security measures to stop the spread of the new COVID-19 virus. This reflected everyone and every single type of business, simply because social distancing as a measure blocked many businesses to run their operations normally. The lockdown on one hand helped slow the rapid spread of the virus, but on the other hand, it heavily affected many of the known business industries. These industries ranged from the travel industry, hospitality, restaurants (with exception of delivery services), oil industry, education, sporting & entertainment, etc.

According to Fernandes (2020), the most hit industry with about 90% loss in activities is the global travel industry, which includes airlines, cruises, hotels, casinos and renting apartments. Their operations cannot be moved online or by using technology (except for casinos in some parts), since they rely on people visiting the actual location or using the real service that cannot be virtualized. In the same article, Fernandes (2020) emphasizes that local businesses may survive even though the lockdown period cannot be compensated by “eating extra dinners after lockdown” or “cutting your hair a few more times”.

Consumer behavior has changed. The research conducted by Accenture (April 2020) proves consumers are very focused on their most basic needs at present, which includes personal and family health, food, medicine, and financial security. All other needs, such as hobbies have been left for another time (i.e. are less important).

The same report emphasizes the growth in e-commerce sales, stating that, “The trend toward digital commerce is expected to continue post-outbreak with consumers reporting that the proportion of instances they shop online will increase from 32% to 37% after the outbreak, illustrating the clear need for a substantial increased investment in this channel.” Accenture (April 2020). This clearly shows that there are sectors of industry that benefited from the pandemics, in this case the e-commerce industry across the globe.

Working from home is becoming the new trend. In the report by Accenture, that summarizes the data from the survey “Accenture COVID-19 Consumer Research”, conducted between April 2 and 6, with 1,118 respondents working from home, it is said, “30% of people plan to increase the amount of work from home in the future”, indicating that the future will be different for workers that can do most of the work from the computer. This will be the “new normal”.

In this paper, by elaborating the need of technology as an enabler of the “new normal”, we will focus on the cyber threats both from the world known cases and specifically from North Macedonia where most of the observations have been done. This way we will provide facts about the correlation between the security and the current “new normal lifestyle”. We argue that the technology as enabler, not necessarily made things easier for everyone during the pandemics, since attacks caused business discontinuity in some cases and financial implications for users in other cases.

Navid Ali and others (Navid Ali et al 2020), in their paper, name the ten deadly cyber security threats amid the COVID-19 pandemic, some of which have been dealt with in our paper. They argue that the most vulnerable are the healthcare industry, the financial industry, and government organizations. They also state that today (during emergencies) it is very easy for hackers, attackers, and scammers to take advantage of others, specifically “in times when people are frightened, desperate, and most vulnerable”. This paper goes on to prove that with the increase in the number of users working online, attackers will work on taking advantage of the situation created.

According to a report by the Federal Trade Commission (Witt, 2020), from January 1 until April 15, 2020, “the FTC has gotten 18,235 reports related to COVID-19, and people reported losing \$13.44 million dollars to fraud”. This clearly strengthens the position that cyber-attacks during pandemics are causing financial implications as evidenced by FTC.

TECHNOLOGY IS THE ENABLER OF THE “NEW NORMAL”

There are many positive cases on how technology enabled running the operations on a given business. Some of these approaches were already known and available before the pandemics, and some saw this opportunity as a new potential for their digital products.

E-COMMERCE SALES

Sales of goods and services (mostly goods) have continued to grow. According to the press release by Amazon.com Inc (Amazon.com, Inc., 2020), their net sales increased 40% to \$88.9 billion in the second quarter (Q2), with increased net sales of 41% compared with the second quarter of 2019. Nevertheless, the COVID-19 situation brought extra expenses, which according to Jeff Bezos, account for around \$4 billion. It is an important fact that Amazon continues to grow regardless the COVID-19 impact. The same case applies to the Alibaba Group sales, where their reported revenues for the second quarter amount to \$21.762 billion, an increase of 34% on the year-over-year basis (Alibaba Group Holding Limited, 2020).

Local e-commerce platforms are emerging all around the world. Countries that had the lowest year-to-year increase in e-commerce adoption by companies and/or citizens are now facing increases. This statement is also supported by the latest report of the World Trade Organization - WTO (2020), which says, “an increased use of e-commerce in certain areas as well as e-commerce-enabling services and technologies, generally highlighting the importance of electronic commerce has been ascertained”.

DIGITAL CONTENT

There has been a spike in the usage of digital contents during the lockdown. A report by New York Times, based on the data from daily traffic on major entertainment websites in the United States, clearly shows the spike after the lockdown, as seen in Figure 1. In this figure, the spike of usage for the major platforms starts immediately after the first day of the lockdown imposed by many US States, such as California on March 19th, followed by other states. The need to consume digital content increased with the lockdown.

Figure 1 - Average of daily traffic for major entertainment websites in US (Courtesy of NY Times)

Another fact that supports the statement that there has been an increase in digital content consumption is the Netflix case (S&P Global Inc., 2020), with more than doubled of their subscriber base in the first half of this year compared with 2019, with 26 million this time around versus 12 million last year. Other online digital content providers (TikTok, Instagram), online media (Twitch), online games and others have seen an increase in the number of their users..

COMMUNICATION, COLLABORATION AND COORDINATION

Communication is always important. Meetings, seminars, discussions, especially lecturing during pandemics in remote locations have been facilitated by many available technologies, such as: Zoom, Google Meet & Classroom, Teams and Office 365, WebEx, and others. According to a report by App Annie (Lexi, 2020), that has analyzed app downloads for major streaming service providers, "Business apps topped 62 million downloads across iOS and Google Play during the week of March 14-21, 2020 worldwide — its biggest week ever. This was up 45% from the week prior — the highest growth among any category across the app stores combined that week — and up 90% from the weekly average of Business app downloads in 2019." This worldwide increase or spike has brought many headaches to the providers of these services. Since most of them are big players in the industry, their business continuity has not been influenced that much by the spike itself.

SECURITY CHALLENGES

The facts mentioned in the above section of the article, truly support our general idea that technology is an enabler of various processes and businesses, specifically during pandemics such as the COVID-19.

Nevertheless, it is not always as good as it sounds. Various groups of “interests” see this crisis and pandemics and the use of technology only for conducting business as an opportunity to cash-in. Some may refer to these groups as “activists”, “hackers”, “terrorists”, “criminals”, etc. For purposes of this paper, we will call them “hackers”. Cyber-attacks mentioned in this section of the paper include real examples of implications in daily operations of businesses and individuals, ultimately costing in terms of money lost and/or spent to improve security.

A joint advisory from the United Kingdom’s National Cyber Security Centre (NCSC) and the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), published on April 8 2020 (NCSC, DHS and CISA, 2020), provides information with examples on what they call “COVID-19 exploitation” some of which are mentioned later in the paper.

PHISHING

Phishing, according to the Oxford English Dictionary is defined as “The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.” - <https://www.lexico.com/en/definition/phishing>

Phishing is also known as social engineering at its best. The idea behind phishing is simply managing people by scamming them, or simply through a net to catch a fish, any fish. A simple email pretending to be someone else, mass-sent to all employees may result in few victims (“fish”). Their account can be compromised and thus an access to confidential data can be obtained.

Phishing can be done by SMS, plain e-mail, or phone. During Covid-19 pandemics, these attacks have increased all over the world.

Figure 2 shows an SMS phishing attempt, impersonating UK Government sent to citizens implying that they need to collect 458 GBP as a “promise to battle COVID 19”. This attempt

inside has a URL that does not correspond to the UK Government official address and it is clearly an attempt to collect data from citizens by leveraging the current pandemics.

Figure 2 - UK Government themed SMS phishing. Photo courtesy of NCSC, DHS and CISA (2020)

When the victim taps the impersonated URL on the message, their personal data is being collected and misused later in the real governmental website.

Another example from North Macedonia, as reported in MKD-NCCIR (2020), an E-mail phishing attempt by impersonating Ministry of Internal Affairs, was launched during July to some citizens in North Macedonia with an attached malware that stated in the content something in the form of “Please download the invitation to the police department for a potential crime”. The attachment (a PDF with ISO extension) was in fact a malware known as: MSIL/Kryptik.DJ (see more at <https://fortiguard.com/encyclopedia/virus/6870008>) which acts as a Trojan and can allow “establishing remote access connections, capturing keyboard input, collecting system information, downloading/uploading files, dropping other malware into the infected system, performing denial-of-service (DoS) attacks, and running/terminating processes”.

Recently there have been detected a series of scamming and/or spoofing pages on social media, specifically Facebook to collect user data and/or build user database. A recent one in North Macedonia was launched by impersonating “NLB Banka” (Figure 3). This case is a typical spoofed page where the attacker is launching a campaign in order to get more users to “like” and follow the page, pretending to be a relevant bank from North Macedonia, and promising users donation in money. As seen from Figure 3, more than 6000 people from North Macedonia got involved in this spoofed Facebook page, including a few of our friends.

The benefit of the scammer/spoofers in this case is that, he/she can freely sell this page at the highest bidder with the followers included in the page. The prices for these transactions may range roughly from 100-5000 Euros.

Figure 3 - Scamming attempt by spoofing major banks name in North Macedonia to increase user base and “sell” the Facebook Page

HACKING AND CRACKING

Hacking and cracking are more sophisticated than the phishing attacks. **Hacking** Twitter was amongst the biggest hacks in 2020. Twitter cases (Figure 4) of Elon Musk, Apple, Jeff Bezos, Bill Gates, resulted in collecting Bitcoins of value around \$100K for the Hackers.

Figure 4 - Tweets from hacked accounts of Bill Gates and Elon Musk

In an update released by Twitter (August 2020) related to this incident, the root cause of this incident was a phishing attack. Perpetrators were able to obtain passwords of system tools used by Twitter engineers and use that information to hack into the system and further compromise accounts of celebrities.

Cracking passwords by using brute-force techniques is commonly used amongst hackers. Brute-force tries hundreds of thousands and millions of combinations of potential passwords (using a dictionary) to find the right one. This way they can get access to the server and or data and compromise the integrity of web pages. There are variations of such attacks known as dictionary attacks that are led by the assumption that the user is using a password from a dictionary.

A major problem exists with the behavior of end users, and the diversity of passwords used by a single user in multiple platforms he has access to. According to Cranor (2016) and FTC, the average American has around 130 online accounts. More than half of the users rarely or never change their passwords and they reuse the same passwords in different systems. This means that if one system is compromised (e.g., a database breach of unencrypted passwords), then all other accounts of the same user are breached as well. Such breaches are more common than one would think. Based on the online service (Have I Been Pwned:

DDOS ATTACKS

Attacks on infrastructure and/or servers is one of the most serious attacks that can affect many people and business continuity during pandemics. If infrastructure and servers are down during pandemics, there is no alternative.

According to Wikipedia, “a denial-of-service (DoS) attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet”. The idea behind DoS is to simply make it impossible for the “target” to serve other clients except for you. Distributed Denial of Service (DDoS) leverages several hundred, thousand and even million of hosts to attack a single target. To simplify it, DDoS in real life means: you get 10,000 questions from people that you need to answer all of them at a given time, and immediately you get 10,000 more questions, which practically means it is impossible to answer them all and you “crash”!

During the day of elections in North Macedonia, there were two major DDoS attacks. One was related to the hack of time.mk, which also had another DDoS attack. Time.MK DDOS Attack was generated from more than 20 million IP addresses, according to the founder of Time.MK, Trajkovski, Igor (June 2020), shown in Figure 6. This attack made it impossible for the website to serve visitors, due to the enormous list of hosts attacking the time.mk server.

Figure 6 - Time.mk founder tweet on the 20 million IP addresses used to attack the website. Photo courtesy of @mkrobot

One of the most problematic attacks on the day of elections in North Macedonia (July 15, 2020) was the attack on the main website of the State Election Commission that was serving the

preliminary results on the day of elections (<https://rezultati.sec.mk/>). This website, which serves as official source of information during elections, was compromised and political parties started pointing fingers on the results. In fact, it was an orchestrated DDoS attack on the website to deny any service to the visitors of the website. The Ministry of Internal affairs, the Sector for Computer Crime and Digital Forensics have started an investigation into this matter (see announcement at <https://mvr.gov.mk/vest/12482>).

HYBRID CYBER ATTACKS

Often, systems are attacked using hybrid approaches. Attackers will search for the Achilles heel of the system and target those vulnerabilities. The case of Twitter hack as well as Time.mk hack can be classified into this category. While the attack on Twitter resembles a standard phishing attack, it also has elements of attackers obtaining access to internal network tools, which are normally protected by firewalls. Details of how attackers obtained access to these tools have not been disclosed by Twitter yet. In this case, a combination of two cyber attacks has been done, which is also known as hybrid cyber-attacks.

In the case of time.mk, attackers were able to obtain the password of the system, by targeting secondary websites that are indexed by time.mk. According to the founder of the site Trajkovski, Igor (June 2020), the DDoS attack was mainly a decoy to disrupt the site and attackers obtained access to the system through a weak password. In addition, in this case, more details have not been disclosed as the case is still under investigation.

PRIVACY

A final concern is the case of trusting companies with our data. In the age of COVID-19, there was an emergence of new tools that were widely used by millions of people, enterprises, and governmental institutions. One such example is the well-known video conferencing tool Zoom, which was exposed to use hidden data mining approaches, data sharing and other insecure practices (Wakefield, 2020). Similar or even more serious threats have been detected with Chinese owned companies that would share gathered detailed information from end users and send them to the Chinese Government. One of the most problematic cases discussed recently is the one with the social network TikTok, as reported by Doffman (2020). The case with TikTok has caused many countries to completely ban the application.

CONCLUSION

For the time being and based only on the literature review and the examples provided in this paper, we can clearly say that everyone is vulnerable to potential attacks that can go above cyberspace and in some cases in some form of hybrid threats.

Hakak and others (Hakak et al 2020), in their paper of analyzing cyber incidents, conclude that the crucial problem during the COVID-19 period, when using the technology as an enabler, is the actual “shift of the cyber security landscape from an enterprise to a home environment”. This means that people are not experts of security and their home environment is not planned and organized to handle various attacks, whereas inside an organization, a lot of security measures, both from the technical and organizational/policy wise point of view, are in place and there are teams handling these issues.

The importance of IT Security literacy is crucial and needs to be revisited by major organizations around the world, specifically by governments soon. In time of pandemics, such as the COVID-19 pandemics, when we heavily rely on technology and infrastructure to carry on our daily activities, any security breach may be difficult to handle since there is no option B.

Institutions must follow stricter password policies, enforcing password complexity and frequent renewal. In addition, there is no excuse not to use two factor authentications, which will allow for a secondary confirmation of the users’ identity via a personalized device: token generators, mobile phones, SMS confirmations, etc. Employees must be trained to recognize fishing attacks. This might not be entirely possible, as we have seen that even major companies or even IT experts are often successfully targeted by such attacks. However, training will allow users to recognize obvious attacks and protect themselves. A simple ‘never share your password with anyone’ must be a rule for every governmental employee.

Another major concern is the IT staffing of governmental institutions in North Macedonia. There is a huge gap between salaries in the IT sector in the public domain compared to the private domain. This is especially true in the field of IT security and digital forensics. As such, governmental institutions that rely on their own resources and low paid governmental employees will always be vulnerable to attacks. One solution would be to delegate such duties to private specialized contractors, albeit this solution would present a large financial burden.

REFERENCES

- Bizumic, B. (2015). Ethnocentrism. In R. A. Segal & K. von Stuckrad (Eds.), *Vocabulary for the study of religion* (Vol. 1, pp. 533–539). Leiden, the Netherlands: Brill Academic Publishers.
- Coulmas, F (1992) *Language and Economy*, Oxford: Blackwell.
- "ISA - International Sociological Association: Books of the Century". International Sociological Association. 1998. Retrieved 2012-07-25.
- Bourdieu, Pierre (1984). *Distinction*. Routledge. pp. 5 & 41. ISBN 0-674-21277-0.
- Fernandes, Nuno (2020). *Economic Effects of Coronavirus Outbreak (COVID-19) on the World Economy*. University of Navarra, IESE Business School; European Corporate Governance Institute (ECGI). Published: March 22, 2020
- Accenture (2020). *How COVID-19 will permanently change consumer behavior. Fast-changing consumer behaviors influence the future of the CPG industry*. Published April 2020.
- World Trade Organization (2020). *E-commerce, trade, and the covid-19 pandemic*. Published: May 2020. Source:
https://www.wto.org/english/tratop_e/covid19_e/ecommerce_report_e.pdf
- Koeze, Ella and Popper, Nathaniel (2020). *The Virus Changed the Way We Internet*. New York Times. Published: April 7, 2020. Source:
<https://www.nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html>
- Sydow, Lexi (2020). *Video Conferencing Apps Surge from Coronavirus Impact*. AppAnnie. Source: <https://www.appannie.com/en/insights/market-data/video-conferencing-apps-surge-coronavirus/>
- NCSC, DHS and CISA (2020). *Advisory: COVID-19 exploited by malicious cyber actors*. United Kingdom's National Cyber Security Centre (NCSC) and the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Published: April 8th, 2020.
- Twitter. *An update on our security incident*. (August 2020). Retrieved August 12, 2020, from https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html
- Trajkovskski, Igor (June 2020). *Twitter Status on Time.mk hack*. Source:
<https://twitter.com/mkrobot/status/1283751915629748226>
- MKD-NCCIR (2020). *Фишинг кампања која таргетира македонски адреси за е-пошта со лажно претставување на испраќачот како "Полиција на Република Македонија"* - Agency for electronic communications - National Centre for Computer Incident Response. Published: July 31, 2020. Source:
<https://mkd-cirt.mk/2020/07/31/fishing-kampanja-koja-targetira-makedonski-adresi-za-e-poshta-so-lazhno-pretstavuvanje-na-isprakjachot-kako-policija-na-republika-makedonija-kontakts-moi-gov-mk/>
- Cranor, Lorrie (2016). *Time to rethink mandatory password changes, FTC*. Source:
<https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes>
- Wakefield, Jan (2020). *Zoom boss apologizes for security issues and promises fixes*, BBC. Published: April 2020, Source: <https://www.bbc.com/news/technology-52133349>

- Doffman, Zak (2020). Warning—Apple Suddenly Catches TikTok Secretly Spying On Millions Of iPhone Users. Forbes. Published: June 26, 2020. Source:
<https://www.forbes.com/sites/zakdoffman/2020/06/26/warning-apple-suddenly-catches-tiktok-secretly-spying-on-millions-of-iphone-users/#1daa387c34ef>
- Amazon.com, Inc. (2020, July 30). Amazon.com Announces Second Quarter Results. Retrieved from Amazon.com, Inc. Source:
<https://press.aboutamazon.com/news-releases/news-release-details/amazoncom-announces-second-quarter-results>
- Alibaba Group Holding Limited. (2020, August 20). Alibaba Group Announces June Quarter 2020 Results. Retrieved from Alibaba Group. Source:
https://www.alibabagroup.com/en/news/press_pdf/p200820.pdf
- S&P Global Inc. (2020, July 16). Netflix, Inc. NasdaqGS:NFLX FQ2 2020 Earnings Call Transcripts. Retrieved from Netflix, Inc. Source:
https://s22.q4cdn.com/959853165/files/doc_financials/2020/q2/Netflix,-Inc.,-Q2-2020-Earnings-Call,-Jul-16,-2020.pdf
- Witt, P. (2020). COVID-19 scam reports, by the numbers. Division of Consumer Response & Operations. Federal Trade Commission. Retrieved from:
<https://www.consumer.ftc.gov/blog/2020/04/covid-19-scam-reports-numbers>
- S. Hakak, W. Z. Khan, M. Imran, K. R. Choo and M. Shoaib, "Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies," in IEEE Access, vol. 8, pp. 124134-124144, 2020, doi: 10.1109/ACCESS.2020.3006172.
- Khan, Navid Ali; Brohi, Sarfraz Nawaz; Zaman, Noor (2020): Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. TechRxiv. Preprint.
<https://doi.org/10.36227/techrxiv.12278792.v1>