HOW DID CYBERCRIMINALS 'SURVIVE' DURING THE PANDEMIC?

Georgios Germanos*[1], Nikolaos Georgiou[2]

Abstract

During the covid-19 pandemic, citizens, companies and organizations were obliged to adapt to new daily routine, where the Internet held a predominant role. Remote working and learning, online shopping, entertainment and social media usage have created a bigger "pool" of potential victims of cybercrime. This forced cybercriminals to ameliorate the modus operandi they were using, or invent new, to achieve their purposes, according to their motivations. More specifically, the number of typical cybercrimes, such as cyber attacks (e.g. man-in-the-middle, ransomware, etc.), frauds and online sexual exploitation / abuse of children, has increased, but, in parallel, law enforcement authorities and relevant organizations worldwide have come across new business models: online markets on the dark web were fake vaccines or medical examination certificates were sold, industrial espionage and a huge amount of fake news / misinformation with further effects on social stability and trust in public authorities. To tackle the above challenges, new prevention and investigation policies were required to be put into force from the side of the governments and the law enforcement authorities.

Keywords: cybercrime, cyber attack, dark web, misinformation, fake news, covid - 19 pandemic

[1] Georgios Germanos, Ph.D. Candidate, Cybersecurity, Department of Informatics and Telecommunications, University of Peloponnese, Greece & Cybercrime Investigator, Cyber Crime Division, Hellenic Police, *Corresponding Author, email: germanos@uop.gr, ORCID ID: 0000-0001-7682-4573
[2] Nikolaos Georgiou, Cybercrime Investigator, Cyber Crime Division, Hellenic Police, email: n.georgiou@cybercrimeunit.gr, ORCID ID: 0000-0001-8708-2739

Introduction

The covid-19 pandemic created significant challenges in the lives of people. One of the major changes was the transfer of most of human activities to the home, and many of them to the computer screen and the cyberspace. Walking with friends has been replaced by socializing on social media, going to the cinema by watching a movie on the computer or smart TV, while for most people work has become teleworking and education has become distance learning.

A characteristic example of the increasing usage of Internet are the statistics related to Greece. With each passing year, the relationship of Greeks with technology shows a continuous increase in all important indicators: internet access, online time, devices, participation in social media, e-commerce, use of mobile devices. The year of the pandemic (2020) accelerated this trend at a steady pace. More specifically, according to the research in a representative nationwide sample of 10,000 people 13-74 years old:

- Internet use reached 96% of Greeks 13-74 years old. It is found in almost 90% at the ages of 55-64, while it has exceeded 70% at the ages of 65-74.
- 91% of children aged 5 to 12 use the internet and at the age of 10-12 almost all children are online (97%).
- When someone starts using the Internet, it soon becomes a daily use, which is why from 96% of users 92% state that they are online every day.
- Also, when someone enters the online world, he discovers its benefits and facilities, which is why nine out of ten Greek women (90%) had their own smartphone, so that they can enter the internet at any time and from any place. 87% of the Greek public now uses the internet via mobile phone and 81% daily.
- Eight out of ten (78%) had at least one profile on social networks.
- Almost seven out of ten (68%) -mainly between the ages of 18 and 54- have made at least one online purchase in the first half of 2020[3].

As the pandemic disrupted work habits and family life, cybercriminals were having a blast. They took the opportunity to exploit a completely new working environment, but also the ambient fear, doubts and uncertainties to abuse users and compromise companies. More to this, the adhesion of individuals to their screens has provided a larger attack surface for cybercriminals. The digital

[3] *Focus Bari: Pandemic speeds up Internet penetration to 96% (in Greek)*, available at https://www.naftemporiki.gr/story/1726612/focus-bari-i-pandimia-epitaxune-ti-dieisdusi-tou-internet-sto-96

switchover had already started before the pandemic, with the rise of e-commerce or the cloud. Nevertheless, teleworking or hybrid work, shared between home and office, allowed cybercriminals to target workers more easily, more frequently online.

Criminals benefited from the pandemic, as, according to Europol (Europol, 2020d), they quickly seized the opportunity to take advantage of the crisis by adapting their modes of operation or engaging in new criminal activities. Factors contributing to the increase in crime include:

- High demand for some products, protective equipment and pharmaceuticals;
- Reduced mobility and the flow of human users in the EU as well;
- Citizens are staying at home and increasingly teleworking, relying on digital solutions;
- Restrictions on public life will make some criminal activities less visible and displace them at home or online settings;
- Increased stress and fear that may create vulnerability to exploitation;
- Reduced supply of certain illegal goods in the EU.

In this work, we examine how cybercriminals ameliorated the modus operandi they were using, and which new they invented, to achieve their purposes, according to their motivations. The most characteristic criminal behaviors were related to cyber attacks, frauds, online sexual exploitation / abuse of children, online selling of fake / fraudulent products or services, as well as misinformation, which are the subjects of the sections and sub-sections of the rest of the work. We also discuss the responses to the new challenges by law enforcement authorities and governments.

It should be noted that, due to the fact that the covid-19 situation emerged too fast, the scientific research and the publications on the cybercrime trends are very limited.

I. Cyber attacks

The latest data show that cyber attacks in Europe are doubling as hackers seem to have taken advantage of the pandemic that brought people closer to computers. The number of serious cyber-attacks against critical targets in Europe in 2020 has risen, as the pandemic has pushed people's lives into the home and online.

According to data from the EU Agency for Cyber Security (ENISA), in 2020 there were 304 significant, malicious attacks against "critical targets", i.e. more than doubled from the 146 recorded in 2019. The agency also recorded a 47% increase in attacks on hospitals and health centers over the

same period, at a time when the role of these services, due to a pandemic, was particularly critical. The figures show the growing impact of cyber-attacks for-profit worldwide, which are causing chaos in key areas of public life (ENISA, 2021).

The pandemic meant that many services had to be provided over the Internet and this happened in a hurry, so security was not the first thought. At the same time, people stayed indoors and had time to explore vulnerabilities in systems and critical infrastructure.

A survey by the British company Sophos also showed a doubling of the amount given in 2019 after such attacks. Costs include insurance, business losses, liquidation and any ransom payments (SOPHOS,2021).

In September 2020, amid the pandemic, the first death was reported due to a cyber attack on the University Hospital of Düsseldorf, Germany. The cyber-attack caused great disturbance, such as postponements of surgeries, scheduled medical examinations or chemotherapy. Cybercriminals ransacked 30 hospital servers with malicious ransomware, destroying computers and data files and forcing staff to evacuate emergency patients[4].

According to FBI statistics, since March 2020 in America there has been a 400% increase in reports of cyber attacks[5]. The World Health Organization and the US Department of Health and Human Services have been the most popular targets for hackers seeking to "learn" about the covid-19 investigation. In fact, the attacks were carried out mainly through the use of malicious emails about the coronavirus, in order to deceive people to click on dangerous links[6].

The Czech Republic reported a cyber attack on Brno University Hospital, which forced the hospital to shut down its entire computer network, postpone emergency surgeries and re-transfer patients with acute problems to another nearby hospital[7].

Europol reported that the number of cyberattacks against organizations and individuals was significant and is expected to increase (Europol, 2021). The criminals have used the COVID-19 scam to launch pandemic-themed social engineering attacks to distribute various malware packages.

[4] *The Düsseldorf Cyber Incident*, available at https://ifsh.de/en/news-detail/the-duesseldorf-cyber-incident
[5] *FBI sees a 400% increase in reports of cyberattacks since the start of the pandemic*, available at https://www.insurancebusinessmag.com/us/news/cyber/fbi-sees-a-400-increase-in-reports-of-cyberattacks-since-the-start-of-the-pandemic-231939.aspx
[6] *Elite hackers target WHO as coronavirus cyberattacks spike*,available at https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive-idUSKBN21A3BN
[7] *Hackers Target Healthcare Industry During COVID-19 Pandemic*, available at https://www.aon.com/cyber-solutions/thinking/hackers-target-healthcare-industry-during-covid-19-pandemic/

Cybercriminals also tried to take advantage of the growing number of businesses that have enabled remote connection to their organizations' systems for remote work (work from home).

There are some statistic figures regarding cyber attacks in Poland (Gryszczyńska, 2021), United Kingdom (Buil-Gil et. al, 2021) and Germany[8].

II. Exploitation of children

A study published by the United Nations Office on Drugs and Crime (UNODC) reveals the devastating effects of covid-19 on victims and survivors of human trafficking and highlights the increased targeting and exploitation of children (UNODC, 2021). According to the study, traffickers took advantage of the global crisis to their advantage by exploiting unemployed people and the increased time adults and children spent online. The study found that children were increasingly targeted by traffickers who were using social media and other online platforms to reach new victims and respond to increased demand for child abuse / exploitation material.

During the lockdown due to covid, children's lives moved from the real world into an online virtual one. Video calls with family and friends, interaction through social media, online gaming, remote education were most of their activities. "Sex offenders have found in this development a tempting opportunity to access a broader group of potential victims", Europol reported (Europol, 2020b). The report shined a light on the increased sharing of child sexual exploitation material (CSAM) online, since offenders were unable to travel for sexual purposes.

Moreover, there has been an increase in detection and reporting of CSAM on the surface web during lockdown, which indicates "the level of re-victimization of children through the distribution of image sand videos depicting them". The activity of the offenders on the dark web was also remarkable, reflecting the ongoing organized business model that has evolved and the level of threat that it poses to children. (Coman et. al, 2021).

III. Counterfeit products

The "fight" against the pandemic has been significantly affected by the ever-increasing number of illegal products. At a time when the word "counterfeit" refers to items such as money and fashion items, the global pharmaceutical industry has been significantly affected by ever-increasing illegalities.

[8] *Cybercrime a booming business - thanks to COVID*, available at https://www.dw.com/en/cybercrime-a-booming-business-thanks-to-covid/a-57499072

Europol reported that the sale of counterfeit health and product hygiene certificates, as well as personal protective equipment and counterfeit medicines, rose sharply since the crisis erupted. Counterfeiters would take advantage of shortages in the supply of certain goods and tried to supply the market with counterfeit alternatives both through the internet and through traditional trade. From 3 to 10 March 2020, more than 34,000 counterfeit surgical masks were confiscated by law enforcement authorities worldwide as part of Operation PANGEA[9].

In a major operation, Interpol thwarted major criminal networks worldwide by dismantling more than 100,000 illegal online pharmacies[10]. At the same time, more than 300 people were arrested and $20 million worth of counterfeit products were confiscated. The main target was a test kit for Covid-19, while fake vaccines from China and South Africa were discovered, containing saline and mineral water (Interpol, 2020b).

Despite these Europol and Interpol achievements, the "battle" against the pandemic is being undermined by a rapidly growing trade in counterfeit products (masks, gloves, tests, vaccination certificates and other items that contribute to the spread of the virus) sold online (Geldenhuys, 2021).

i. Vaccines

The drug trade (over $ 1 trillion a year) is becoming an attractive target for all sorts of outlaws, who often conduct anonymous online transactions.

There are many reasons why the trade in fake vaccines is growing, including high demand - which has outpaced supply during the pandemic. The cost of developing vaccines nationally has made them difficult to access, especially for the poorest countries. This has ultimately led to unequal access to vaccines worldwide, with most of them controlled by the most powerful countries.

Meanwhile, the relative ease of producing a fake vaccine, which could possibly only be detected when it does not protect someone from the virus, means that the barrier to this "market" entry may be relatively low.

ii. Certificates

[9] *Rise of fake 'corona cures' revealed in global counterfeit medicine operation*, available at https://www.europol.europa.eu/newsroom/news/rise-of-fake-%E2%80%98corona-cures%E2%80%99-revealed-in-global-counterfeit-medicine-operation

[10] *Thousands of fake online pharmacies shut down in INTERPOL operation*, available at https://www.interpol.int/News-and-Events/News/2021/Thousands-of-fake-online-pharmacies-shut-down-in-INTERPOL-operation.

"If you need vaccination certificates, send us a message and we will deliver authentic documents with active QR codes." This was the message from the administrators of a group on Telegram application, with more than 87,000 followers, in an attempt by digital counterfeiters to catch a clientele among vaccinators around the world.

Aggressive marketing and misinformation with the spread of unscientific theories are their common ingredients, in various group discussions, while their administrators usually accompany their nicknames with the title of "doctor". A fake vaccination certificate would cost around $250. Administrators of the groups claimed that they have "their own people" (they are talking about health workers) in each country, who can enter the details of the sham vaccine in the corresponding database in order to fool the system[11].

In addition to images of forged documents, the same groups would also post photos of so-called "satisfied customers", who allegedly collaborated with the counterfeiters (Checkpoint, 2021).

In the US, a 31-year-old woman was arrested in New York for allegedly selling 250 counterfeit vaccination cards via Instagram[12]. Her accomplice was a clinic worker who had registered 10 sham vaccines in the New York database. At the same time, Memphis customs authorities announced the seizure of another batch of counterfeit vaccination cards, which had been shipped from China to New Orleans.

Analysts of a cyber security company, who regularly check the dark web for malware products and services, found some changes in the products or services that were offered illegally and were in line with the advent of covid-19.

Initially, when there was an international shortage of protective equipment, ads for masks appeared, while the first posts for the sale of fake vaccination certificates emerged in March 2021. Even then these groups were not so popular.

However, what surprised analysts was that the sellers suddenly shifted their activity from the dark web to more common applications and especially to Telegram. The dark web is a closed ecosystem and someone who is looking to buy weapons, passports, maybe even drugs, usually ends

[11] *A passport to freedom? Fake COVID-19 test results and vaccination certificates offered on Darknet and hacking forums*,available at https://blog.checkpoint.com/2021/03/22/a-passport-to-freedom-fake-covid-19-test-results-and-vaccination-certificates-offered-on-darknet-and-hacking-forums/

[12] *Instagram User […] Charged With Selling Fake Vaccine Cards*, available at https://www.nytimes.com/2021/08/31/nyregion/fake-vaccine-cards-woman-charged.html

up there. For the fake vaccination certificates, however, their prospective clientele was larger and off-the-internet (Checkpoint, 2021).

IV. Frauds

The rapid increase in the penetration of online services, due to the coronavirus pandemic, has also led to an escalation of digital fraud efforts worldwide (Interpol, 2020a).

i. Scams

Europol reported that fraudsters quickly adapted the known fraud schemes to take advantage of the victims' anxieties and fears during the crisis. These included various types of telephone scams, supply scams and disinfection scams. A Europol-supported operation focused on transferring € 6.6 million from company to company in Singapore to gel the purchase of alcohol and FFP3 / 2 masks. The products were not received[13]. The causes of online COVID-19 scams vary and an analysis of them has been published by Chawki (2021).

ii. Phishing

"Phishing" is a well-known scam via e-mail, SMS or even messaging. In this message the scammer is presented as a reliable source, to deceive the recipients, to reveal sensitive information or to download malware. Phishing is often used with more diverse procedures, such as e.g. a user follows a link from an advertisement or an email and arrives at a page where they are asked to enter personal information and bank card details. Once they have this information, attackers can use it to steal money from a victim's account.

From March 2020 - when the first restrictive measures for coronavirus protection came into force - until July 2021, Kaspersky identified more than 1 million user attempts to visit phishing websites. Additionally, phishing ads for fake QR codes and vaccination certificates for restaurants and public events have become popular[14]. Protection from "phishing" can be quiet challenging, but there are measures which can be applied by ordinary internet users (Tran, 2020).

iii. Investment fraud

[13] *Corona crimes: suspect behind €6 million face masks and hand sanitisers scam arrested thanks to international police cooperation,* available at https://www.europol.europa.eu/newsroom/news/corona-crimes-suspect-behind-%E2%82%AC6-million-face-masks-and-hand-sanitisers-scam-arrested-thanks-to-international-police-cooperation

[14] *Over 5,000 COVID-related phishing websites luring people: Report*, available at https://www.moneylife.in/article/over-5000-covid-related-phishing-websites-luring-people-report/64871.html

Investment-related messages did also appear online, promising extremely high returns, which can include lucrative investment opportunities such as stocks, bonds, cryptocurrencies, gemstones, offshore real estate investments and real estate[15].

iv. Sim Swapping

The "Sim Swapping" model was also detected many times. The perpetrators in several cases gain illegal access to the victims' computers and steal their usernames and passwords on online banking platforms. Then, using this information, they issue authorizations, through e-government services, ostensibly on their behalf. After issuing all the necessary documents, the perpetrators use "straw men" to issue new SIM cards on behalf of the victims.

In this way they manage to bypass the security procedures of e-banking (sending SMS or Viber text to customers with a unique code for each transaction) and remove large sums of money from the victims[16].

V. Fake news – Misinformation

According to a study, published by the European Centre for Disease Prevention and Control (ECDC, 2021) on the conditions for spreading false news about vaccinations, vaccines approved by the European Medicines Agency (EMA) for use in the European Union are known to be safe and effective in preventing infectious diseases. However, there is misinformation that incorrectly associates them with health damage or other side effects. The phenomenon has grown in recent years. Vaccine misinformation is not a new phenomenon, but it has become more apparent due to the rise of social media and, more recently, the emergence of the covid-19 pandemic.

The pandemic has provided a breeding ground for misinformation on the Internet, showing how quickly new stories can emerge. Their focus on the fact that vaccination is dangerous: they reduce confidence in vaccines and lead to reluctance to take them.

The study recorded online misinformation about the vaccine in all six countries studied (Estonia, Spain, Germany, France, the Netherlands, Romania). Its authors estimate that the real extent of the problem is much greater than is perceived.

[15] *Covid has meant a cash bonanza for scammers. These people are fighting back against the fraudsters*, available at https://www.washingtonpost.com/business/2021/10/01/investor-fraud-nasaa-enforcemenet-report/
[16] *SIM swapping – a mobile phone scam*, available at https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/sim-swapping-%E2%80%93-mobile-phone-scam

It is very important - they emphasize - that the exposure to misinformation is not accidental: algorithms used by platforms such as Facebook, Twitter and YouTube, create "filter bubbles" or "sound booths" and people who have shown interest in specific issues, are even more exposed to similar elements.

Social networking platforms differ in the speed with which content is created, the reach of users, the forms and sharing options, and - consequently - their impact.

The intensity of the misinformation does not necessarily mean a greater impact.

Another parameter in misinformation is the presence of "influencers". These individuals have the ability to inspire behaviors in others. In the event that influencers dictate misinformation through their accounts, the likelihood of its spread increases (Europol, 2020c).

VI. Conclusions

From the data presented in detail, it is clear that the criminals were not intimidated by the evolution of the pandemic, but preferred to adapt the methods of their criminal action to the new situation. In other words, they took advantage of the increased presence of people in the digital world, which meant an increased number of potential victims. There were, therefore, attacks on information systems, cyber frauds, crimes of child sexual exploitation, as well as offerings of various types of counterfeit products (masks, vaccines, vaccination certificates or illness certificates). An increase in the phenomenon of misinformation was also observed, since it was easy to spread non-existent news and vague theories through the Internet.

Dealing with the phenomena requires a coordinated response by the Law Enforcement Authorities, on the one hand in the direction of investigation of criminal activities (with the involvement of the judicial authorities) (Bou Sleiman et. al, 2021), and on the other hand in the direction of prevention, through public awareness[17]. Obviously, there are best practices and recommendations [like those provided in (UNODC, 2020)], and these are the ones that should be applied - especially in the case of cybercrime, where there are no physical borders between States and cross-border cooperation is absolutely necessary.

[17] *Staying safe during covid-19: what you need to know*, available at https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know

References

Bou Sleiman, M., & Gerdemann, S. (2021). Covid-19: a catalyst for cybercrime?. *International Cybersecurity Law Review*, *2*(1), 37-45.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, *23*(sup1), S47-S59.

Chawki, M. (2021). Cybercrime in the Context of COVID-19. In *Intelligent Computing* (pp. 986-1002). Springer, Cham.

Checkpoint (2021). *Amid vaccine mandates, fake vaccine certificates become a full blown industry*, https://blog.checkpoint.com/2021/09/14/amid-vaccine-mandates-fake-vaccine-certificates-become-a-full-blown-industry/

Coman, I., & Mihai, I. C. (2021). The Impact of COVID-19. Cybercrime and Cyberthreats. *European Law Enforcement Research Bulletin*, (SCE 5), 61-67.

EU Agency for Cyber Security (ENISA) (2021). *ENISA Threat Landscape 2021*, available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

European Centre for Disease Prevention and Control (ECDC) (2021). *Countering online vaccine misinformation in the EU/EEA*, available at https://www.ecdc.europa.eu/sites/default/files/documents/Countering-online-vaccine-misinformation-in-the-EU-EEA.pdf

Europol (2021). *Internet Organised Crime Threat Assessment (IOCTA) 2021*, Publications Office of the European Union, Luxembourg.

Europol (2020) a. *Beyond the pandemic – how COVID-19 will shape the serious and organized crime landscape in the EU*, accessible at https://www.europol.europa.eu/publications-documents/beyond-pandemic-how-covid-19-will-shape-serious-and-organised-crime-landscape-in-eu

Europol (2020) b. *How COVID-19-related crime infected Europe during 2020*, accessible at https://www.europol.europa.eu/publications-documents/how-covid-19-related-crime-infected-europe-during-2020

Europol (2020) c. *Catching the virus: cybercrime, disinformation and the COVID-19 pandemic*, accessible athttps://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic

Europol (2020) d. *Pandemic profiteering - how criminals exploit the COVID-19 crisis*, available at https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

Geldenhuys, K. (2021). Exploiting the pharmaceutical market during COVID-19. *Servamus Community-based Safety and Security Magazine*, *114*(1), 24-28.

Gryszczyńska, A. (2021). The impact of the COVID-19 pandemic on cybercrime. *Bulletin of the Polish Academy of Sciences. Technical Sciences*, *69*(4).

Interpol (2020) a. *Global Landscape on Covid-19 Cyberthreat*, accessible at https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats

Interpol (2020) b. *Cybercrime: Covid-19 impact*, available at https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

SOPHOS (2021). *The Future of Cybersecurity in Asia Pacific and Japan*, https://www.sophos.com/en-us/medialibrary/PDFs/Whitepaper/sophos-future-of-cybersecurity-apj-wp.pdf.

Tran, C. (2020). Recommendations for ordinary users from mitigating phishing and cybercrime risks during COVID-19 pandemic. *arXiv preprint arXiv:2006.11929*.

UNODC (2021). *The effects of the COVID-19 pandemic on trafficking in persons and responses to the challenges*, available at https://www.unodc.org/documents/human-trafficking/2021/The_effects_of_the_COVID-19_pandemic_on_trafficking_in_persons.pdf

UNODC (2020). *CYBERCRIME AND COVID19: Risks and Responses*, available at https://www.unodc.org/documents/Advocacy-Section/UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf

Website articles / Web pages *(last access 21/11/2021)*

A passport to freedom? Fake COVID-19 test results and vaccination certificates offered on Darknet and hacking forums, available at https://blog.checkpoint.com/2021/03/22/a-passport-to-freedom-fake-covid-19-test-results-and-vaccination-certificates-offered-on-darknet-and-hacking-forums/

Corona crimes: suspect behind €6 million face masks and hand sanitisers scam arrested thanks to international police cooperation, available at https://www.europol.europa.eu/newsroom/news/corona-crimes-suspect-behind-%E2%82%AC6-million-face-masks-and-hand-sanitisers-scam-arrested-thanks-to-international-police-cooperation

Covid has meant a cash bonanza for scammers. These people are fighting back against the fraudsters, available at https://www.washingtonpost.com/business/2021/10/01/investor-fraud-nasaa-enforcemenet-report/

Cybercrime a booming business - thanks to COVID, available at https://www.dw.com/en/cybercrime-a-booming-business-thanks-to-covid/a-57499072

Elite hackers target WHO as coronavirus cyberattacks spike, available at https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive-idUSKBN21A3BN

FBI sees a 400% increase in reports of cyberattacks since the start of the pandemic, available at https://www.insurancebusinessmag.com/us/news/cyber/fbi-sees-a-400-increase-in-reports-of-cyberattacks-since-the-start-of-the-pandemic-231939.aspx

Focus Bari: Pandemic speeds up Internet penetration to 96% (in Greek), available at https://www.naftemporiki.gr/story/1726612/focus-bari-i-pandimia-epitaxune-ti-dieisdusi-tou-internet-sto-96

Hackers Target Healthcare Industry During COVID-19 Pandemic, available at https://www.aon.com/cyber-solutions/thinking/hackers-target-healthcare-industry-during-covid-19-pandemic/

Instagram User […] Charged With Selling Fake Vaccine Cards, available at https://www.nytimes.com/2021/08/31/nyregion/fake-vaccine-cards-woman-charged.html

Over 5,000 COVID-related phishing websites luring people: Report, available at https://www.moneylife.in/article/over-5000-covid-related-phishing-websites-luring-people-report/64871.html

Rise of fake 'corona cures' revealed in global counterfeit medicine operation, available at https://www.europol.europa.eu/newsroom/news/rise-of-fake-%E2%80%98corona-cures%E2%80%99-revealed-in-global-counterfeit-medicine-operation

SIM swapping – a mobile phone scam, available at https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/sim-swapping-%E2%80%93-mobile-phone-scam

Staying safe during covid-19: what you need to know, available at https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know

The Düsseldorf Cyber Incident, available at https://ifsh.de/en/news-detail/the-duesseldorf-cyber-incident

Thousands of fake online pharmacies shut down in INTERPOL operation, available at https://www.interpol.int/News-and-Events/News/2021/Thousands-of-fake-online-pharmacies-shut-down-in-INTERPOL-operation.