https://fr.wikipedia.org/wiki/Office_central_pour_la_répression_du_trafic_illicite_des_stupéfiants.

3. Office anti-stupéfiants (OFAST). URL: https://lannuaire.service-public.fr/gouvernement/administration-centrale-ou-ministere_184308.

4. La Brigade des Stupéfiants de la Police Nationale “Stups”. URL: https://www.policenationale.net/brigade-stupefiants/.

5. Trafic de stupéfiant: crime ou délit? URL: https://www.jurifiable.com/conseil-juridique/droit-penal/trafic-destupefiants#:~:text=Le%20trafic%20de%20stup%C3%A9fiants%20d%C3%A9signe%20le%20commerce%20ill%C3%A9gal%20de%20substances%20psychotropes.,On%20parle%20aussi.

Колесник А., здобувач ступеня вищої освіти
Національної академії внутрішніх справ
Консультант з мови: *Ченківська Н.*

CYBERCRIME DURING THE COVID-19 PANDEMIC

The pandemic of COVID-19 and the imposed lockdown, has led to more people to be confined at home with many more hours to spend online each day and increasingly relying on the Internet to access services, they normally obtain offline.

The dangers of cyber-crime have been there for many years, but the increase in the percentage of the population connected to the Internet and the time spent online, combined with the sense of confinement and the anxiety and fear generated from the lockdown, have provided more opportunities for cybercriminals to take advantage of the situation and make more money or create disruption. It is important to note that some more vulnerable segments of the population, such as children need to spend more time online for services such as schooling. This seismic change in how we live our lives and use the Internet has prompted a proliferation of e-crimes.

Countries all across the globe are reporting an increase in cybercrime during the pandemic. For instance, in Italy, the Polizia Postale, which is the law enforcement branch in charge of the cybercrimes, reported several kinds of scams and frauds that came in the form of ads, emails, fake websites, but also through phone calls and messages. Cybercriminals are capitalizing on the anxieties and fears triggered by the pandemic, using malware, such as viruses, worms, trojan horses, ransomware and spyware, to invade, damage, steal or cancel personal data on personal computers. Stolen data can then be used for different malicious purposes, including accessing bank accounts and blackmailing the victims in exchange of ransoms. A "Corona anti-virus" software has also been flagged to the Italian law enforcement authorities. The application, BlackNet Rat, promises to protect the user's device from coronavirus, but instead, it breaches the computer's security and takes control of the computer, effectively enabling

the criminal to remotely control it. An INTERPOL assessment of the impact of COVID-19 on cybercrime has shown a significant target shift from individuals and small businesses to major corporations, governments and critical infrastructure.

With organizations and businesses rapidly deploying remote systems and networks to support staff working from home, criminals are also taking advantage of increased security vulnerabilities to steal data, generate profits and cause disruption.

In one month period (January to April) some 907,000 spam messages, 737 incidents related to malware and 48,000 malicious URLs – all related to COVID-19 – were detected by one of INTERPOL's private sector partners [3].

Malware, or malicious software, infiltrates and gains control over a computer system or a mobile device to steal valuable information or damage data. There are many types of malware, and they can complement each other when performing an attack.

Online Scams and Phishing – Threat actors have revised their usual online scams and phishing schemes. By deploying COVID-19 themed phishing emails, often impersonating government and health authorities, cybercriminals entice victims into providing their personal data and downloading malicious content.Around two-thirds of member countries which responded to the global cybercrime survey reported a significant use of COVID-19 themes for phishing and online fraud since the outbreak.

Disruptive Malware (Ransomware and DDoS) – Cybercriminals are increasingly using disruptive malware against critical infrastructure and healthcare institutions, due to the potential for high impact and financial benefit.In the first two weeks of April 2020, there was a spike in ransomware attacks by multiple threat groups which had been relatively dormant for the past few months.Law enforcement investigations show the majority of attackers estimated quite accurately the maximum amount of ransom they could demand from targeted organizations.

Data Harvesting Malware – The deployment of data harvesting malware such as Remote Access Trojan, info stealers, spyware and banking Trojans by cybercriminals is on the rise. Using COVID-19 related information as a lure, threat actors infiltrate systems to compromise networks, steal data, divert money and build botnets.

Malicious Domains – Taking advantage of the increased demand for medical supplies and information on COVID-19, there has been a significant increase of cybercriminals registering domain names containing keywords, such as "coronavirus" or "COVID". These fraudulent websites underpin a wide variety of malicious activities including C2 servers, malware deployment and phishing.From February to March 2020, a 569 per cent growth in malicious registrations, including malware and phishing and a 788 per cent growth in high-risk registrations were detected and reported to INTERPOL by a private sector partner.

Misinformation – An increasing amount of misinformation and fake news is spreading rapidly among the public. Unverified information, inadequately understood threats, and conspiracy theories have contributed to anxiety in communities and in some cases facilitated the execution of cyberattacks.Nearly 30 per cent of countries which responded to the global cybercrime survey confirmed the circulation of false information related to COVID-19. Within a one-month period, one country reported 290 postings with the majority containing concealed malware. There are also reports of misinformation being linked to the illegal trade of fraudulent medical commodities.Other cases of misinformation involved scams via mobile text-messages containing 'too good to be true' offers such as free food, special benefits, or large discounts in supermarkets.

Ransomware – Hospitals, medical centres and public institutions are being targeted by cybercriminals for ransomware attacks – since they are overwhelmed with the health crisis and cannot afford to be locked out of their systems, the criminals believe they are likely to pay the ransom. The ransomware can enter their systems through emails containing infected links or attachments, compromised employee credentials, or by exploiting a vulnerability in the system.

The COVID-19 pandemic renders individuals and society extremely vulnerable in all respects. During this crisis, we all rely more than ever on computer systems, mobile devices and the Internet to work, communicate, shop, share and receive information and otherwise mitigate the impact of social distancing. There is evidence that malicious actors are exploiting these vulnerabilities to their own advantage.

What should companies do to protect their data and their reputation?

Have strong security protocols - for organizations to not only have strong security protocols, but a strategic crisis communications plan in the event of a breach. Urgency, pace and timing makes all of the difference. Ensure that your communications are consistent, control the message as best as possible and tell the whole truth, not part of the story.

Show empathy and accountability – in responding to a breach, companies must also show a level of empathy, he said. There are victims in cybersecurity breaches, and companies must recognize their customers' or clients' information has been stolen and could possibly be made public. You have to take that with the utmost of importance. There has to be some sort of promise to make it right, to take accountability. Disclose (the breach) sooner rather than later. If you don't, someone else will, and it won't be on your terms.

Avoid creating new standards – when asked what is the biggest mistake that companies can make, it's breaking their own protocols and setting new and different communication standards as they go. There are a lot of one-off questions that come in and there is always that urge to respond. When you breach that protocol, you set a new expectation that you're going to create a one-off communication for every question, and that's just unmanageable.

Make it a team effort - another common mistake is relying on IT to manage the entire response. A lot of clients assume that IT's got it. They probably have a process. They probably have a protocol. They probably took care of all these things. And when you break down the different aspects of a cyber response, which ranges from insurance, to legal, to communications, to HR, to other aspects of it, you realize it's a team sport. There's no way a single IT department, or person or group within IT would be able to deal with all those pieces. That's why preparation at that level is so key [4].

The Council of Europe – like many other organisations – has decided to apply extraordinary measures to limit the spread of the virus and reduce risks to staff and experts. Activities on cybercrime involving physical meetings or international travel as well have been postponed. However, we cannot afford to have our efforts on cybercrime come to a standstill. The staff of the Secretariat of the Cybercrime Convention Committee in Strasbourg and of the Cybercrime Programme Office (C-PROC) in Bucharest continue to work remotely and through video-conferencing to support partners and to advance in our common efforts against cybercrime.

Criminal justice authorities need to engage in full cooperation to detect, investigate, attribute and prosecute the above offences and bring to justice those that exploit the COVID-19 pandemic for their own criminal purposes [5].

The Cybersecurity and Infrastructure Security Agency (CISA) warns individuals to remain vigilant for scams related to Coronavirus Disease 2019 (COVID-19). Cyber actors may send emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes. Exercise caution in handling any email with a COVID-19-related subject line, attachment, or hyperlink, and be wary of social media pleas, texts, or calls related to COVID-19 [6].

Список використаних джерел

1. Cybercrime. URL: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime.

2. COVID-19 cyberthreats. URL: https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats.

3. INTERPOL report shows alarming rate of cyberattacks during COVID-19. URL: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.

4. Cybersecurity in the time of COVID-19. URL: https://www.national.ca/en/perspectives/detail/cybersecurity-in-the-time-of-covid-19/.

5. News Cybercrime and COVID-19. URL: https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19.

6. Defending Against COVID-19 Cyber Scams. URL: https://us-cert.cisa.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams.