CZU: 81`373.43:[343.53:004] DOI: https://doi.org/10.5281/zenodo.10089346

NEOLOGISMS AND CYBERCRIMES

Ina VOLOSCIUC
Lecturer
Moldova State University, Faculty of Letters
Department of English and French for Specific Purposes
0000-0001-7642-8255

Cybercrimes, deeply rooted in every modern society and have rapidly increased in number and advanced thanks to IoT devices and the Internet. The present article aims to identify neologisms known as cybercrimes and check their availability in online dictionaries.
Key-words: *Neologisms, cybercrimes, phishing, online dictionaries, Collins online dictionary*

Introduction

Personal experience has urged to focus on the topic of cybercrimes, neologisms, new word or expression in a language, or a new meaning for an existing word or expression [1], that have grasped my linguistic curiosity throughout the years, but also because of the telephone call on Viber, that I received in late 2022. Different article titles have recently appeared in the local online media, preventing the Moldovan population about widely spread cybercrime of receiving phone calls from fraudsters who pretend to be operators of issuing banks, so as to update people's banking card data and phish out personal information, the crime known as *phishing*. Fortunately for me, I did not fall victim to the hacker attack and refused to provide any personal information on the telephone. The professional, respectable and merely magic voice of the hacker changed immediately, understanding that he/she would not get any information from me. This Viber call taught me a valuable, life-philosophy lesson that did not cost me more than a minute of a telephone conversation with a stranger. As the idea, that something negative can happen to everybody but me is a traditional mistake made by most of the global digitalized humanity. This case made me think

about other possible illegalities that can take place in our lives online, with the impact offline, due to growing opportunities of e-commerce, online transactions and still developing cybersecurity.

he management of the Republic of Moldova prioritizes the extension of the digital agenda and, therefore, focuses on the development of the National Security Strategy: "The strategic vision regarding ensuring the cyber security of our country was discussed during the public consultations, carried out in the context of the elaboration of the National Security Strategy. Cybersecurity experts, representatives from civil society and government institutions, as well as academia and the private sector, spoke about immediate and long-term actions to increase our country's cyber resilience." [2]

As to the legislation in force of the Republic of Moldova, the law on cyber security was recently adopted and published in the Official Gazette on May 2, 2023. It will enter into force on January 1, 2025. "The adoption of the law on cyber security is an important step for the Republic of Moldova to improve its resilience to hybrid threats and to create institutions in accordance with the relevant EU provisions. The EU is happy to see the results of the Rapid Cyber Security Assistance Project for the Republic of Moldova", said Jānis Mažeiks, the Ambassador of the European Union to the Republic of Moldova. [3]

We can also follow the destructing effect of cybercrimes in the Internet Crime Report 2022 presented by the Federal Bureau of Investigation (FBI). The damages caused by cybercrimes exceed ten billion US dollars in 2022 that is three billion more than in 2021. The number of complaints in 2022 reached 800,944 received by the FBI's Internet Crime Complaint Center (IC3) [4] of cybercrimes and cyber-enabled frauds.

Hence, the list of internet generated crimes is growing. Therefore, in 2022 we identified sixty-five neologisms, connected to cybercrimes: *identity theft, ransomware, sextortion, spoofing and phishing, online predators, money mule, DDoS attacks, cryptojacking, money laundering, vishing, web attacks, SQL injections, cross-site scripting, password attacks, eavesdropping attacks, brute-force and dictionary network attacks, insider threats, man-in-the-middle attacks, AI-powered attacks, drive-by attacks, spear phishing attacks, whale phishing attacks, malware, trojan horses, teardrop*

attack, ping of death attack, PuP's, hacking, software piracy, espionage, password sniffers, credit/debit card fraud, email bombing, cryptocurrency scam, online investment scam, online dating scam, known as romance scam, fake lottery scam, product or drug scam, commercial scam. [5]

The present article aims at continuing the research dedicated to currently appeared cybercrimes, identify new ones, and therefore, raise public awareness to avoid becoming a victim of cybercriminals.

Boost of e-crimes

The pandemic of COVID-19 Sars Cov 2 and the lockdown have led to the boost of e-crimes. People had to spend hours online facing the consequences of the isolation so as to comply with the regulation, having limited access to any usual everyday activity, stay connected with the outside world mainly through internet. This is how the cybercriminals took advantage of the new opportunities provided by the pandemic to commit e-crimes and make more money.

And here again the statistics comes with information about the spike of *phishing*, the practice of using fraudulent emails and copies of legitimate websites to extract financial data from computer users for purposes of identity theft [6]. "New data gathered by Google and analyzed by Atlas VPN, a virtual private network (VPN) service provider, is shedding more light on the scope of this. According to the report, in January, Google registered 149k active phishing websites. In February, that number nearly doubled to 293k. In March, though, that number had increased to 522k – a 350% increase since January." [7] Freedom From Fear Magazine pointed out that 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.

Top 5 e-crimes during 2018-2022

The list of Internet facilitated crimes is growing. The recent 2022 INTERNET CRIME REPORT [8] made by Federal Bureau Of Investigation identified top 5 e-crimes during 2018-2022:

Technical support (tech support) refers to a range services companies provide to their customers for products such as software, mobile phones, printers, and other electronic, mechanical or electromechanical products. Technical support services usually provide users with help in solving some common problems rather than providing training on how to use the product. [9] Ex: I called my tech support guy, bristling with frustration. (Times, Sunday Times)

Electronic extortion - one of the forms of the crime of extortion, and it occurs when the extortion itself or its requirements are achieved by using electronic or digital tools and means, or more precisely by using information and communication technologies to implement any element of the crime. [10] Ex: Perhaps it is hyperbolic to call the process of turning overpayments into debts extortion. (The Guardian (2019)

Non-payment - a failure to pay a sum of money that you owe. / *Non-delivery* is a failure to deliver (goods, products, etc) purchased online. Ex: If your problem concerns nondelivery of or dissatisfaction with goods and you paid with a credit card, you may be able to withhold payment. [11]

Personal data breach - any event that compromises the confidentiality, integrity, or availability of personal data. [12] Ex: Legal experts said that this was a breach of data protection law by collecting personal information in an unfair or underhand manner. Times, Sunday Times (2015) [13]

Phishing - the practice of trying to trick people into giving secret financial information by sending emails that look as if they come from a bank. The details are then used to steal people's money, or to steal their identity in order to commit crimes. Ex: This suggests that the fraudster has gained crucial information about you, possibly through phishing emails. The Guardian (2021) [14]

List of e-crimes

The list of e-crimes continues:

Business email compromise (BEC) is a specific type of phishing attack, a spear phishing attack to be precise – with the objective being to trick employees into taking harmful actions, typically sending money to the at-

tacker, one of the most damaging and expensive types of phishing attacks in existence, costing businesses billions of dollars each year. [15]

According to the source [16], there are five primary types of BEC attacks:

False Invoice Scam - the phisher pretends to be a vendor requesting payment for services performed for the company and presents as one of an organization's suppliers and uses a realistic template but changes the bank account information to an account controlled by the attackers. Ex: They were accused of siphoning off cash through false invoices. Times, Sunday Times

CEO Fraud - the attacker sends an email – supposedly from the CEO – instructing the recipient to take some action as to close a business deal or send sensitive information to a partner. Ex: A joint investigation supported by Europol has led to the dismantling of a Franco-Israeli criminal network involved in large-scale CEO fraud. [17]

Account Compromise - an account with login details known by one or more unauthorized individuals, attacker takes advantage of a compromised email account within an organization to request invoice payments from customers while changing the payment details to those of the attacker. Ex: We're sharing an update on our work against malicious mobile apps available in the official Apple and Google app stores that are designed to compromise people's Facebook accounts. [18]

Attorney Impersonation - scam starts with an email that appears to be from the attorney asking the purchaser to transfer money for the property which the person is buying. However, the email is a fake and the bank details are those of an account belonging to the fraudster, not the attorney. The email appears to come from the attorney, either because the cybercriminal has hacked into the purchaser's email account or because they have "spoofed" (deceived) his/ her email address. [19]

Data Theft – e-crime that targets HR and Finance personnel and attempts to steal sensitive information about an organization's employees. This information can then be sold on the Dark Web or used in planning and executing future attacks. [20] Ex: Pharmacy services provider PharMerica has disclosed a massive data breach impacting over 5.8 million patients, exposing their medical data to hackers. [21]

However, the rest of the e-crimes are also worth-knowing:

Investment e-scam - another sub-group that induces investors to make purchases based on false information, these crimes usually offer the victims large returns with minimal risk, however increased the number od cryptocurrency investment fraud. [22]

Liquidity Mining - victims are enticed to link their cryptocurrency wallet to a fraudulent liquidity mining application. Scammers then wipe out the victims' funds without notification or permission from the victim. [23] Ex: Some of the risks associated with liquidity mining include impermanent loss, project risks and potential rug pulls. [24]

Hacked Social Media - scammers used hacked social media accounts to perpetrate a fraudulent investment opportunity using cryptocurrency, targeting existing friends of the hacked user. [25] Ex: Your Social Media Has Been Hacked And You Don't Even Know It [26]

Spoofing - the act or an instance of impersonating another person on the internet or via email [27], fraudsters pretend to be someone or something else to win a person's trust. The motivation is usually to gain access to systems, steal data, steal money, or spread malware. Here we can also mention *Government Impersonation* - scammers pretend to be calling from government agencies, to receive your personal data), *Attorney Impersonation* (mentioned above) and *Celebrity Impersonation* - impersonating a well-known celebrity or social figure, the scammers feign a friendship with the targeted victim who is eventually enticed to learn how to invest in cryptocurrency or is given the opportunity to invest by the scammer. [28] Internet users are asked to to send money for different reasons, like claiming a prize, donating to a charity, or giving help of some kind, however you need to be sure that the person asking you to support is real.

Ex: There is no reason why someone could not be held liable for impersonating a celebrity or another high profile person online. [29]

Real Estate Professionals - the scammer contacts a real estate agent, usually offering to buy a very expensive property for cash or cryptocurrency. Once engaged, the fraudster will expose their control of fictitious accounts with purported value of millions of dollars to entice them to engage in their investment scheme. [30] Ex: Real estate scams cost buyers,

sellers, property owners, renters, and real estate professionals upward of a billion dollars every year. [31]

Closing Wire Fraud - a scammer hacks the email inbox of a principal party in a real estate transaction, he/she identifies an imminent closing, creates a fake email address from what appears to be a reputable source and provides the real estate buyer with wiring instructions for closing funds, directing them into that account. Unsuspecting buyers wire their funds to the scammers instead of the closing company, money wired to nefarious accounts, especially in offshore and often unregulated banks, are incredibly difficult to recover and are often never seen again. [32] Ex: Educating yourself and your clients about the most prevalent real estate scams and learning how to protect both yourself and your clients is a crucial line of defense that will help make real estate scams like these a thing of the past. [33]

Employment - victims apply for fake positions online at an investment firm or company supposedly affiliated with investing. Instead of a job, the victims are instead offered advice investment advice. The investment is fraudulent and designed to retrieve as much money from the target as possible. [34]

Advanced fee - businesses or individuals are required to pay a fee before receiving promised stocks, services, money, or products, which ultimately are never given. The targets of the fraud receive a solicitation (by letter, fax, or e-mail) from someone posing as a business representative or government official promising that a large sum of money will be deposited into the target's bank account. To ensure this, the recipient of the letter is asked to pay a percentage of the total amount that purportedly will be wired or transferred. Advance fee fraud scams originate in a number of countries and may use internal conflicts or other circumstances specific to that country as a pretense under which funds must be transferred abroad. [35] Ex: It says that the fraudsters usually approach investors in shares, foreign exchange or contracts for difference but are also involved in advance-fee loan fraud. Times, Sunday Times (2018) [36]

To highlight the words that where included for the first time in the FBI Report, however, not because of their novelty but their frequency of

these cyber-threats. These are Botnet, Harassment/Stalking, SIM Swap, Threats of Violence.

Botnet - a network of computers infected by a program that communicates with its creator in order to send unsolicited emails, attack websites, etc [37] Ex: A botnet is a network of hijacked computers used to carry out cyberattacks. The Guardian (2022) [38]

Harassment/Stalking – also known as online harassment and cyberstalking, an extension of cyberbullying, the practice of using electronic communications to harass someone persistently and the use of the internet to contact someone or find out information about them in a way that is annoying or frightening. [39]

Behavior associated with cyberstalking are catfishing, when someone uses a fake identity in order to pursue an online relationship on social media websites like Facebook [40] and doxing, short for document tracing, obtaining personal information about a person and then publishing it online [41]

SIM Swapping - also known as *SIM splitting, simjacking*, or *SIM hijacking*, is a technique used by fraudsters to get control of your phone number. With your phone number, hackers can take advantage of two-factor authentication to gain access to your bank accounts, social media accounts, and more. [42]

Threats of Violence – an expression of an intention to inflict pain, injury, self-harm, or death not in the context of extortion [43] Ex: The use of computer systems to cause, facilitate, or threaten violence against individuals, that results in (or is likely to result in) physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstance, characteristics or vulnerabilities. [44]

Prevention Aspect

As to the prevention aspect, according to Microsoft every internet user is to be aware of one of the main rules of all times, address the official source. The multinational technology corporation suggests to use two-factor authentication, enable 2FA, even if an attacker gets your username and password, they still will not be able to gain access to your accounts and personal information; do not open emails or attachments from suspi-

cious sources, check if the link was sent by a friend; be wary of offers that are too good to be true, the only free cheese is in the mousetrap; do not overshare online you give the personal details from your social media profiles, it will make their scams seem more legitimate; talk to your kids about online safety and what they post online; secure your computers and devices by using antivirus software, firewalls, and email filters to protect your personal information.

Conclusions

The article under consideration has focused on 30 cybercrimes, crimes committed by means of computers or the internet, which are at the same time lexemes with neological status. However, it is important to highlight that most of the neological formations can be deciphered without consulting a dictionary, in our case we have addressed the Collins online dictionary, as it is one of online lexicographical corpuses that updates quickly and is free, as well as some other sources as Coucil of Europe, Freedom From Fear Magazine, Techopedia, Check Point, Europol, FBI, Meta, Britannica, Microsoft, etc.

From the amount of the analyzed glossary we can categorize the neologisms able to be understood and apprehended, mainly formed through combining, such as *Data Breach*, *Threats of Violence, Hacked Social Media, Real Estate Professionals* that deliver us information from the words already existing that can be decoded, the new product has mainly a negative connotation. However, the neologisms formed by shortening and blending certain words and creating new lexemes, therefore inhaling new beginning for *BEC, Botnet, Phishing*, the word that inspired me to focus on the issue of cybercrimes not only of linguistic curiosity but also of necessity to inform the readers about the threat of cyber-attacks and boost of cyber-crimes, that deeply rooted in every modern society and advanced due to IoTdevices and the Internet.

References:

1. Collins online dictionary. Disponibil: https://www.collinsdictionary.com/dictionary/english/neologism

2. Guvernul RM, VIZIUNEA STRATEGICĂ PRIVIND ASIGURAREA SECURITĂȚII CIBERNETICE A FOST CONSULTATĂ PUBLIC LA GUVERN. Disponibil: https://gov.md/ro/content/viziunea-strategica-privind-asigurarea-securitatii-cibernetice-fost-consultata-public-la
3. Delegația Uniunii Europene în Republica Moldova. Cu sprijinul UE, Moldova a adoptat Legea securității cibernetice. Disponibil: https://www.eeas.europa.eu/delegations/moldova/cu-sprijinul-ue-moldova-adoptat-legea-securit%C4%83%C8%9Bii-cibernetice_ro?s=223
4. FEDERAL BUREAU OF INVESTIGATION. 2022 INTERNET CRIME REPORT Disponibil: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf , p. 3
5. CONFERINȚA Integritate prin cercetare si inovare USM 10-11 noiembrie 2022, p. 83 https://cercetare.usm.md/wp-content/uploads/Volumul-II_Stiinte-umanistice.pdf
6. Collins online dictionary. Disponibil: https://www.collinsdictionary.com/dictionary/english/phishing
7. Freedom From Fear Magazine. Cyber-crime during the COVID-19 Pandemic. Disponibil: https://f3magazine.unicri.it/?p=2085#:~:text=This%20seismic%20change%20in%20how,a%20proliferation%20of%20e%2Dcrimes.&text=A%20sharp%20surge%20of%20fake,designed%20by%20criminals%5B6%5D
8. FEDERAL BUREAU OF INVESTIGATION. 2022 INTERNET CRIME REPORT. Disponibil: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
9. Techopedia. Technical Support. Disponibil: https://www.techopedia.com/definition/9675/technical-support-tech-support
10. From Virtual Threats to Real-Life Consequences: Understanding Electronic Extortion. Disponibil: https://masaar.net/en/from-virtual-threats-to-real-life-consequences-understanding-electronic-extortion/
11. Collins online dictionary. Disponibil: https://www.collinsdictionary.com/dictionary/english/nondelivery

12. Thomson Reuters Practical Law. Personal data breach. Disponibil: https://uk.practicallaw.thomsonreuters.com/w-014-8192?transitionType=Default&contextData=(sc.Default)&firstPage=true
13. Collins online dictionary. Disponibil: https://www.collinsdictionary.com/dictionary/english/breach-of-data
14. Collins online dictionary. Disponibil: https://www.collinsdictionary.com/dictionary/english/phishing
15. Check Point. How Business Email Compromise (BEC) Works. Disponibil: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-email-security/business-email-compromise-bec/#:~:text=Business%20email%20compromise%20(BEC)%20is,sending%20money%20to%20the%20attacker
16. FEDERAL BUREAU OF INVESTIGATION. 2022 INTERNET CRIME REPORT. Disponibil: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
17. Europol. Franco-Israeli gang behind EUR 38 million CEO fraud busted. Disponibil: https://www.europol.europa.eu/media-press/newsroom/news/franco-israeli-gang-behind-eur-38-million-ceo-fraud-busted
18. Meta. Protecting People From Malicious Account Compromise Apps. Disponibil: https://about.fb.com/news/2022/10/protecting-people-from-malicious-account-compromise-apps/
19. ShackletonRisk. Impersonation Fraud. Disponibil: https://www.shackletonrisk.co.za/impersonation-fraud/
20. Check Point. How Business Email Compromise (BEC) Works. Disponibil: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-email-security/business-email-compromise-bec/#:~:text=Business%20email%20compromise%20(BEC)%20is,sending%20money%20to%20the%20attacker
21. BleepingComputer. Disponibil: https://www.bleepingcomputer.com/tag/data-breach/
22. FEDERAL BUREAU OF INVESTIGATION. 2022 INTERNET CRIME REPORT, p. 30 Disponibil: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
23. FEDERAL BUREAU OF INVESTIGATION. 2022 INTERNET

CRIME REPORT, p. 12 Disponibil: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
24. What Is Liquidity Mining: How to Profit from a Decentralized Ecosystem. Disponibil: https://learn.bybit.com/investing/what-is-liquidity-mining/
25. FEDERAL BUREAU OF INVESTIGATION. 2022 INTERNET CRIME REPORT, p. 12 Disponibil: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
26. What Is My IP Address. Your Social Media Has Been Hacked And You Don't Even Know It. Disponibil: https://whatismyipaddress.com/your-social-media-has-been-hacked-and-you-dont-even-know-it
27. Collins online dictionary. Disponibil: https://www.collinsdictionary.com/dictionary/english/spoofing
28. FEDERAL BUREAU OF INVESTIGATION. 2022 INTERNET CRIME REPORT,p. 12 Disponibil: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
29. Liability for Impersonating Someone Online. Disponibil: https://www.michalsons.com/blog/liability-impersonating-someone-online/9696
30. FEDERAL BUREAU OF INVESTIGATION. 2022 INTERNET CRIME REPORT, p. 12 Disponibil: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
31. 10 Sneaky Real Estate Scams + How to Protect Your Clients (& Yourself)Disponibil: https://theclose.com/real-estate-scams/
32. 10 Sneaky Real Estate Scams + How to Protect Your Clients (& Yourself)Disponibil: https://theclose.com/real-estate-scams/
33. 10 Sneaky Real Estate Scams + How to Protect Your Clients (& Yourself)Disponibil: https://theclose.com/real-estate-scams/
34. FEDERAL BUREAU OF INVESTIGATION. 2022 INTERNET CRIME REPORT, p. 12 Disponibil: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
35. Britannica. Advance fee fraud. Disponibil: https://www.britannica.com/money/advance-fee-fraud

36. Collins online dictionary. Disponibil: https://www.collinsdictionary.com/dictionary/english/advance-fee
37. Collins online dictionary. Disponibil: https://www.collinsdictionary.com/dictionary/english/botnet
38. Microsoft. What is SIM swapping & how does the hijacking scam work? Disponibil: https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-sim-swapping
39. Collins online dictionary. Disponibil: https://www.collinsdictionary.com/dictionary/english/cyberstalking
40. Collins online dictionary. Disponibil: https://www.collinsdictionary.com/submission/12686/catfishing
41. Collins online dictionary. Disponibil: https://www.collinsdictionary.com/submission/13023/doxing
42. Microsoft. What is SIM swapping & how does the hijacking scam work? Disponibil: https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-sim-swapping
43. FEDERAL BUREAU OF INVESTIGATION. 2022 INTERNET CRIME REPORT. Disponibil: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
44. Council of Europe. What is cyberviolence? Disponibil: https://www.coe.int/en/web/cyberviolence