JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2021 Volume 11
https://doi.org/10.47459/jssi.2021.11.41

NEW FORMS OF CRIME ON THE NET

Marlena Lorek[1], Norbert Malec[2]

[1]Rzeszów University of Technology, Poland
[2]University of Natural Sciences and Humanities in Siedlce, Poland

E-mails: [1]mlorek@prz.edu.pl, [2]norbek@poczta.fm

Received 18 February 2021; accepted 15 June 2021; published 30 June 2021

Abstract. The article indicates the threats of crime on the Internet and the specificity of criminals' activities. Moreover, the content of the work shows how dynamically crime is changing on the Internet and it may affect all users. Nevertheless, the youngest are the most vulnerable to the actions of criminals because they can easily trust a perpetrator, who wants to commit a crime against a minor. Today, we all use different websites more frequently because the current pandemic situation in the world shows that both study, play and work only takes place in the virtual world (Hofmolk 2009).Online crime is now very dynamic and dangerous due to the high number of victims that were affected this type of online crime. Each of us could fall victim to hackers more than once in the network, however, we managed to react and prevent entry into our devices and data theft. The most dangerous thing is that the perpetrators are often anonymous because finding these people is almost impossible due to their skills in this area. The police have many mechanisms to combat this phenomenon, however, in many cases it is impossible to confirm who was the perpetrator of the incident online. Identification in the network is very difficult to detect because the perpetrators do not leave behind any signs such as: fingerprints, image or voice. The aim of the article was to indicate new forms of crime on the Internet and to show the broad spectrum of activities of offenders on the Internet. It was also indicated how big is the dynamics of crime and the emergence of newer and newer forms of online activity.

Keywords: crime; police; computer crime; internet fraud; hacking; sniffing; computer sabotage; cracking; phishing

Reference to this paper should be made as follows: Lorek, M., Malec, N. 2021. New forms of crime on the NET. *Journal of Security and Sustainability Issues*, 11, 457-462. https://doi.org/10.47459/jssi.2021.11.41

JEL Classifications: K24

Additional disciplines: political sciences and administration

1. Introduction

Crimes committed online are commonplace, however, it is not known exactly how many of them are unreported, because the victims do not want to report such an incident. Many types of crimes, both economic and criminological, can be committed on the Internet, apart from committing only against life. Nowadays, in the age of Covid-19, crime has moved online and these traditional forms are transferred to virtual reality. Criminals, one could say, have found new directions of financial gain through trafficking in weapons, human beings, violence (hate), forgery, pedophilia or a number of frauds.

In the present day, a criminal act in the network affects everyone and even minors who use the network for the purpose of learning who has moved to the virtual world. Children and adolescents often receive notifications, for example, accepting links, which allows the perpetrator to enter their devices and manage them. The theft of data, contacts or photos were often used against their owners and later received threats that if they did not pay the specified amount, their image could be used, for example for pornographic content. The main formation that is at the forefront of securing crime in the network is the police, and its officers monitor the network 24 hours

a day, every day, in order to verify, for example, activities related to an attack on the servers of companies, ministries or individuals using the network (Jurgilewicz, 2020).

2. Crimes in Internet

The Police is a formation whose task is to ensure the safety of citizens. Currently, technological progress indicates that the police are increasingly confronted with fighting and activities aimed at securing property online (Lorek 2017). Online attacks are now dominant and the police are recording more and more of them. You have to take into account the fact that all computer frauds (Kucharczyk 2021) are not recorded online, because often the injured persons do not report such incidents for fear of further attacks. Currently, the police are struggling with many incidents regarding theft in the network or hacking into private user accounts or hacking into corporate, company or bank data. The assessment is dealing with the plague of false information, e-mails or notifications that redirect to false websites when clicked, where, after entering the data, criminals have access to our bank or online accounts. The worst thing is that in the era of Covid-19, everyone works and learns using Internet media, which is why it becomes an even more common threat to the youngest. More than once, one of us has been affected by such a criminal act where we have lost data or someone has stolen the data to our bank accounts. The lockdown time resulted in continued use of the Internet therefore, making many economic operations, such as purchases, made that data accessibility is facilitated for criminals. Police to operate more efficiently and to secure the network, the Office for Combating Cybercrime has been distinguished in its structure where effective action is taken to detect the perpetrators of crimes are made on the web. This unit constantly monitors modern technologies where can counteract to reduce the acts or incidents that are recorded in ICT technology. This office focuses especially on activities related to them tasks and include, among others:

1. coordinating and monitoring activities related to counteracting and combating cybercrime by all provincial and (Warsaw) police headquarters in the field of operational and reconnaissance activities, as well as cooperation with the Central Police Investigation Bureau in this regard,

2. conducting operational and reconnaissance activities belonging to the office,

3. onducting activities in the field of cooperation with government bodies such as: courts, public prosecutor's office or other state institutions, as well as with private units that operate in the field of recognition of tasks remaining within the competence of the bureau,

4. activities related to international cooperation within the scope of activities related to cooperation with the Bureau for International Police Cooperation with regard to the functioning of the office,

5. 24-hour coordination of activities aimed at minimizing activities related to the emergence of crimes on the Internet (Internet) and combating them in cooperation with Police units at the national and foreign level, as well as with authorities and entities outside the police

6. conducting consultations related to technological progress as well as initiating and conducting research with national and international entities in order to identify new solutions in the fight against cybercrime (Dudek 2020).

Nowadays, it is difficult to define one definition that would describe crime in the network, because along with technological development, newer and newer discoveries arise, but they are not homogeneous because of such progressive technological development. Violation of the law in this respect includes, inter alia, behavior inconsistent with ethical activities in the network. Sometimes some users on the web cannot determine the moment when they break this very barrier where a crime can be dealt with in the computer. Currently, in the era of such great development, access to the Internet is very common and we can commit a crime every day using websites, but we were not necessarily aware of the perpetrators of this action.

Recipients on the web, both adults and children, often due to the lack of awareness of the current forms of threats, may accidentally log into the links sent, which at first glance may indicate that, for example, we won a competition, but collecting the prize is possible by logging in and accessing to your data, it will allow you to send the prize to the address indicated, which is actually a fraud, however, the user has already indicated his address or other sensitive data. All persons operating in the network should check several times whether their

activities in the network are legal and are not punishable for committing a crime. Today, hackers can break into our e-mails, smartphones, tablets or computers, where they can easily reach our contacts where, for example, they will send inappropriate information or photos that will offend recipients, which may contribute to misunderstanding and causing inappropriate behavior towards friends (Kowalewski, Kowalewski 2017).

Computer crime is a fairly general and vague concept because it is not easy to pinpoint a single definition as this concept is very dynamic with the expansion of online activities. Criminals are looking for newer and newer gaps to create new space for committing criminal acts using networks and new media that will allow them to achieve significant financial benefits. This crime can most simply be defined as a deviation from the applicable law and the tool of the crime is a computer or other digital media (Jakubski 1996). New forms of crime allow for hacking, theft or fraud not only in relation to data contained in users' devices, but also to steal money or computer programs. The police often, after reporting a crime online, are not able to detect who was the perpetrator, because specialists in the field of crime on the Internet often act in such a way that the security forces could not detect the perpetrators (Kośiński 2015).

Types and qualifications of computer crimes:

- **cracking**- breaking the security of servers in public but also private networks in order to extort data that will later be misused by the perpetrators of this crime. Software code data is most often stolen, and such cracker actions can cause huge financial losses for companies. In addition to financial losses, important are the image-related losses related to trust in, for example, banks, insurance companies and many others that have personal data of members of the society (Kosiński 2015). Security in relation to sensitive data is most important for the entire security system of the network.
- **unauthorized obtaining of information (hacking)**- the beginning of hacking indicates the fact that the first telephone networks were established. Initially, these were break-ins into the network of the perpetrators in order to make free calls in telecommunications connections (Bogacki 2013). The new form of this criminal attack primarily bypasses https on Macs, Linux or Windows and can be used by Wi-Fi hotspot operators. Hackers can successfully crack and monitor the movements of the user's network. An attack in this form can be carried out using all available network operators, including these public Wi-Fi networks, so it is important that people using public networks are vigilant because this form of crime can most often occur here (Wang 2005).
- **Internet fraud-** this is the most common type of crime committed online. The crime against property in this case is committed with the use of data carriers with the help of digital tools where the perpetrator uses someone else's, which is voluntarily given to the perpetrator by the injured party, this may happen unconsciously because the offender may impersonate, for example, a competition and extort data about the injured person. Victims are very often misled, which has many consequences related to the interception of data (Rychlewska-Hotel 2020).
- **SMS scam**- these are simple scams consisting in extorting money from people available on various types of websites who pay for sending SMS text messages. Network users most often receive e-mail messages that make them willing to take part in an intelligence test and check their IQ. To achieve such a result, it is possible to send a paid message and receive an SMS. Users to send such a message receive instructions on how to perform it step by step and at this point they lose their funds. The perpetrator usually does not specify the price of such a message, therefore the bill for this message can be very large. Sometimes the fraud is made on the basis of the user's lack of knowledge that, for example, a message that is supposed to cost a few pennies costs even several dozen zlotys and it results from the regulations of such a lottery that one text message is generated several times for which a fee is charged from the user without his knowledge.
- **Nigerian fraud**- commonly known as the advance payment, it is committed by writing and sending letters. In the era of technological development, perpetrators send a message to e-mail for this purpose. When writing a message to the addressee, they often indicate how difficult their life and health situations are, and they ask for help and give them the money they need. Sometimes they refer to our distant family members to make their message more credible. The victim is assured that they will be reimbursed if they pay for stamp duty, for example, as well as for the inheritance lawyers. This is one of the popular forms of online fraud.

- **phishing**- the most popular type of attacks, mainly directed in e-mail or SMS. The criminals here want to provoke users to act as intended. Criminals easily reach the addressee by, for example, impersonating courier companies, offices of various types, mobile network operators as well as our friends that we have on our devices using the above messages directed at the victim, trying to extort login details: bank accounts, social accounts or systems we have logged in our electronic devices. In addition, by their actions, they can persuade the victim to log into selected websites that are already infected, and thus they can obtain confidential data. For this, they often use appropriate software that is very similar to real websites, e.g. of the bank with which we have an account. They can also use attachments that are infected and can infect our devices and thus share confidential data we have.
- **spear-phishing**- is directed towards a selected addressee and the attack is aimed at exerting a specific target that the perpetrator has chosen for the victim. These perpetrators usually pretend to be, for example, our business partners with whom we are in constant contact, therefore this situation does not arouse suspicions, therefore the messages received from them may be personalized and relate to a specific economic activity. The perpetrators previously carefully analyze our position at work, contacts with contractors in order to obtain the widest possible information that is secret and not available to competitors in a given industry (Kasperkiewicz 2019).
- **computer sabotage**- the perpetrator is not authorized to transmit IT data. If such an act of destruction, removal, damage or obstruction of the operation of such computer systems is committed, it is punishable by imprisonment from 3 months to 5 years (Siwicki 2012). The perpetrator may also counteract the functioning of systems that are very important for the country's defense, the functioning of the government administration or state institution or local government, as well as security in communication. Such actions may lead to destabilization of the state as it may disturb or prevent the automatic processing of such data (Radoniewicz 2013).
- **sniffing (computer wiretapping)**- this crime is defined as sniffing or eavesdropping (Stokłosa, Bilski, Pankowski). The term you can understand that it is an activity related to the interception of information by unwanted persons, such activities are aimed at interrogating local networks or Wi-Fi wireless networks in order to obtain as much prohibited information as possible. Sniffing is one of the forms of network criminals who use appropriate tools or computer programs to analyze the largest possible amount of data that is available on the Internet (Klaus 2021).
- **port scanning**- is used by the perpetrator when he finds a vulnerability in computers. This crime occurs by using a port scanner and sending TCP packets to computers in order to have information about open ports, operating systems and services offered by systems. Data theft and data interception can be continuous and invisible. Network users should be aware of the risks and avoid suspicious sites that may lead to data loss (Parkitny 2017).
- **smurf attack-** is a type of network flooding flooding (ICMP flooding) attack. This can be done when the injured person has a worse connection. The ICMP Echo Request forgery attack is possible only when we change the address of the attacked server. This activity in the network is broadcast to active network systems, which may result in them sending ICMP Echo Reply to a spoofed source address. This attack is most popular in small local networks.
- **spoofing**- this is spoofing an IP address and impersonating a given system in order to steal data. It is possible by installing malware or bypassing access control systems. This form of operation is realized by placing prepared data packets in the network as well as by using an incorrect protocol. Spoofing is also impersonating e.g. an e-mail and forging e-mail headers to indicate that a given address is correct, but it is crafted in order to obtain trusted data. DNS spoofing is nothing more than redirecting traffic to a different IP address by modifying the DNS server.
- **ransomware blackmail**- previously, criminals used ransomware to indicate that the computer lock was imposed by law enforcement agencies. Currently, ransomware is tasked with encrypting all personal information it can only find on electronic devices. Victims of this virus can no longer use their disks and important documents. Such extensive use of the Internet can only increase this type of crime in the form of pests attacking our devices (Dudkowski 2020).

- **frustrating obtaining information**- it is a person who does not have the authority to destroy, damage or obstruct access to IT data, or disrupts or completely prevents automatic processing, collection and transfer of data, is punishable. It can also work to the detriment of material damage to the injured party in the network. Prosecution of such a person committing this type of crime is possible at the request of the injured party (Radoniewicz 2013).

3. Conclusions

Digitization and technological development contribute to increasing crime online. Technology is now everywhere used to store personal data or other important information that can always be stolen by appropriate computer systems. The perpetrators have the appropriate equipment and knowledge that allows them to cheat and steal online because they go unpunished and catching them is very rare or completely impossible. Currently, we all work remotely and it results from a pandemic situation, which is why economic crime has increased in the network because more and more payment operations allow criminals to act more freely and obtain large financial benefits from this type of criminal act. The threat of crime on the Internet affects not only private individuals but also state institutions, governmental institutions, and large corporations, which indicates that it is currently difficult to avoid perpetrators acting against Internet users. More and more online crime training and courses should now be introduced to avoid unwanted fraud in the future. Prevention in this respect should make users aware of the high risk posed by inappropriate use of websites. We should use newer and newer forms of network and equipment security in order not to steal data by criminals.

References:

Bogaci P., *Hacking in terms of art. 267 of the CC*, (Hacking w ujęciu art. 267 KK), Warszawa 2013, https://czasopisma.beck.pl/monitor-prawniczy/spis-tresci/archiwum/c/a/1100/

Dudkowski Ł., Ransomware - what is it and how to remove it? How to protect yourself, (Ransomware – co to jest i jak go usunąć? Jak się zabezpieczyć), 2020, https://seqred.pl/ransomware-co-to-jest-jak-sie-zabezpieczyc-jak-usunac/

Dudek Z., *Crime of Police officers. A sociological study*, (Przestępczość funkcjonariuszy Policji. Studium socjologiczne), Wrocław 2020.

Hofmolk J., *Internet as a new common good* (Internet jako nowe dobro wspólne), Warsaw 2009.

Jakubski K. J, *Computer crime - an outline of the problem*, (Przestępczość komputerowa – zarys problematyki), PIP 1996.

Kasperkiewicz J., *The crime of phishing - what is it and what is the penalty for its commission? art. 287 of the Criminal Cod*, (Przestępstwo phishingu – na czym polega i jaka kara grozi za jego popełnienie? art. 287 kodeksu karnego), https://cyberlaw-by-judyta.com/2019/01/18/przestepstwo-phishingu-na-czym-polega-i-jaka-kara-grozi-za-jego-popelnienie-art-287-kodeksu-karnego/

Jurgilewicz M. et al., *The Police's role in the field of improving functioning fuel sector as an element of energy safety management in Poland,* WSEAS Transactions on Business and Economics, Volume 17, 2020, s. 657-664.

Klaus L., The most common types of hacking attacks on the Internet, (Najczęściej spotykane rodzaje ataków hakerskich w Internecie), 2021, https://nordvpn.com/pl/blog/ataki-hakerskie/

Kosiński J., *Cybercrime pradigms*, (Pradygmaty cyberprzstępczości), Warsaw 2015.

Kowalewski J., Kowalewski M., *Information threats in cyberspace, cyberterrorism*, (Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm), Warsaw 2017.

Kucharczyk K., *Difficult fight with hackers. The police are doing worse and worse*, (Trudny bój z hakerami. Policja radzi sobie coraz gorzej), Rzeczpospolita 2021, https://www.rp.pl/Telekomunikacja-i-IT/303119886-Trudny-boj-z-hakerami-Policja-radzi-sobie-coraz-gorzej.html

Lorek M., *Motivating in the Polish Police*, (Motywowanie w polskiej Policji), Rzeszów 2017.

Parkitny K., Port Scanning - Administrator Toolbox, (Skanowanie portów – przybornik administratora), 2017, https://www.support-online.pl/skanowanie-portow-przybornik-administratora/

Rychlewska-Hotel A., Criminal liability for fraud (Article 286 of the CC),(Odpowiedzialność karna za oszustwo art. 286 k.k.), Kraków 2020.

Siwicki M., Division and definition of cybercrime, (Podział i definicja cyberprzestępstw), Warszawa 2012.

Radoniewicz F., Criminal liability for the hacking offense, (Odpowiedzialność karna za przestępstwo hackingu), Warszawa 2013.

Stokłosa J., Bilski T., Pankowski T., *Data security in IT systems*, (Bezpieczeństwo danych w systemach informatycznych), Warsaw 2001.

Wang W., *Secrets of the internet, hacking and security*, (Tajemnice internetu, hackingu i bezpieczeństwa), Gliwice 2005.

Marlena LOREK, Rzeszów University of Technology, PL. Research interests: international security, policy,
ORCID ID: 0000-0002-6814-8162.

Norbert MALEC, University of Natural Sciences and Humanities in Siedlce, PL. Research interests: international security.
ORCID ID: 0000-0003-0119-2705.