DOI azonosító: https://doi.org/10.53304/PS.2024.1-2.12

NAGY, ÁGNES

The criminalistics of cybercrimes committed in cyberspace[1]

"The old robber gangs have died out, but have been replaced by large international robber barons, who are not using violence, but cunning and in any case more success in capturing often very considerable amounts of value. They are organised on a large scale and operate according to a fixed programme, every detail of which is worked out with the utmost meticulousness. They have dedicated investigative and field investigative units, as well as operational members and fences. If one of them is caught, he will never betray his associates, but they will help him as much as possible."

Pál Angyal [2]

Introduction

Thanks to the advancements in modern computing and information technology, various commercial services are now more quickly and conveniently accessible, and managing financial matters has become simpler, often without the need for personal presence. The pandemic has also contributed to the shift of the population, community life, and social relationships to the internet.

In Hungary, unlawful activities carried out in the name of financial institutions through calls targeting bank clients began to appear in January 2021. It was already evident then that the perpetrators had shifted their operations from violent money-making crimes to cyberspace, where they could conceal and obscure their identities. Unfortunately, the further shift in crime towards this direction was foreseeable, along with the continuous and

[1] This study is the English version of the presentation delivered at the conference 'The Science and Practice of Law Enforcement' held in Pécs 27.06.2024.

[2] Angyal, P. (1915): Criminal-etiological significance of the culture Special edition, Studies in Criminal Law, Pécs. 20

significant increase in the number of online offenses and the resulting damages.

The Fourth Industrial Revolution is an ongoing global process, as a result of which 77.41% of the population over the age of 15 uses the internet in Hungary.[3] The presence in the digital space has an impact on the dynamic rise of crimes committed on online platforms, which is primarily due to the lack of security awareness in the use of the global internet on the victims' side.

The lack of use of electronic protection systems, the peculiarities of the online space, and human gullibility are further problems for victimisation. The criminological characteristic of crimes committed in cyberspace is that criminals can exploit human factors to carry out their criminal activities by manipulative means.

With one click, fraudsters can reach thousands or tens of thousands of victims in the online space, so there is a strong need for the society's education on internet safety, and for more effective prevention solutions to effectively reduce the number of victims.

The new dimension, that is, the digital existence, poses new challenges for the whole of humanity, including, of course, law enforcement authorities. These challenges require new solutions and responses by which effective results can be achieved.

In both the national and international literature, several authors have defined cybercrime as a generic term, distinguishing two main categories within this: one is a group of criminal activities committed exclusively by using information systems. Typically, the object of these crimes is the information system, thus they are also referred to as purely IT or cybercrimes.

The second group is made up of traditional crimes committed using information systems, such as fraud, extortion, money laundering, harassment,

[3] Data published by the National Media and Infocommunications Authority on 2th May 2023. Source: https://nmhh.hu/cikk/238466/Internetes_kozonsegmeresi_adatok_2023_I_negyedev
(Internet usage among residents aged over 15 (EDME-Gemius 15+ inland – 2023. I. quarter) Accessed: 22.07. 2024

or even drug trafficking. In the case of these offences, the information system is used as a means of committing the offence.[4]

The present study deals specifically with the second category of cases, within which I will mainly focus on fraud and information system fraud

I aim to give you a brief insight in this case into the methods of perpetration, and how they are changing.

I am going to describe the procedural steps taken during the investigation and their results, as well as the successes and the difficulties that emerged.

In the subject to be covered, the focus will not be on theoretical issues and concepts, as knowledge of these is assumed, and I will build on this to present the area to be covered. I will not therefore analyse and reflect on what has already been published in the literature, but I am going to present the practical possibilities.

I am going to refrain from presenting the full, all-encompassing criminal procedure, and will only present the activity that takes place in the context of fraud.

In the study, I present some problems, which I hope to get solved in the near future.

Modus Operandi

a)

The perpetrators often prefer social engineering[5] attacks, such as phishing, instead of applying technical solutions.

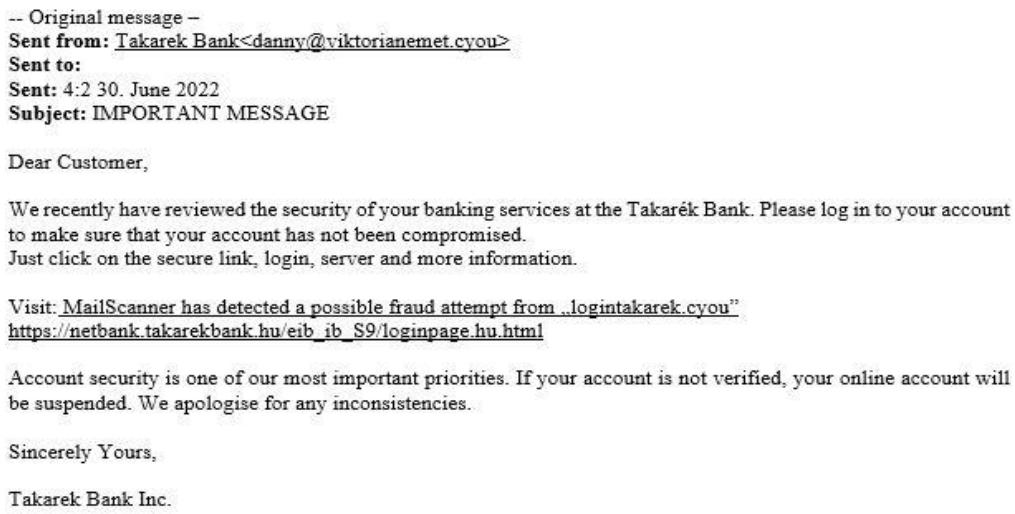
Phishing is a popular method of obtaining sensitive data such as passwords, and credit card numbers, and is often used to deliver malicious software to devices on behalf of well-known banks, financial institutions, or financial service providers. In addition, e-mail messages have recently

[4] Mezei K.(2019/4-5.): Challenges of cybercrime regulation in the criminal law, Public Prosecutors' Paper, Budapest. 22

[5] psychological manipulation, influencing

been increasingly sent on behalf of public authorities (even the police). The users are asked to log in to their accounts electronically or to provide their credit card details for data reconciliation.

The letter usually includes a link to help the victim get to the given website; however, it does not point to the real website of the bank or financial institution, but to a fake website that looks eerily similar. (Picture 1.)



-- Original message –
Sent from: Takarek Bank<danny@viktorianemet.cyou>
Sent to:
Sent: 4:2 30. June 2022
Subject: IMPORTANT MESSAGE

Dear Customer,

We recently have reviewed the security of your banking services at the Takarék Bank. Please log in to your account to make sure that your account has not been compromised.
Just click on the secure link, login, server and more information.

Visit: MailScanner has detected a possible fraud attempt from „logintakarek.cyou"
https://netbank.takarekbank.hu/eib_ib_S9/loginpage.hu.html

Account security is one of our most important priorities. If your account is not verified, your online account will be suspended. We apologise for any inconsistencies.

Sincerely Yours,

Takarek Bank Inc.

Figure 1
Phishing

b)
This can also be done by the so-called *pharming* phishing method, where the perpetrators also use fake websites to obtain the data, but by means of malicious or spy software, they redirect the user from the original site to another fake website. When the unsuspecting victim logs in on these websites, the phishers immediately get their username and password, and then by using the obtained data they access the user's bank account and then

often transfer the amounts of money from the affected bank account to other accounts within a short period of time.[6]

c)
Sending SMS messages is a simpler and faster communication channel, where the perpetrator, misusing the name of a service provider or authority, contacts the victim by pretending there was an expired service or debt. To facilitate payment, they send a link leading to a fake (phishing) website, aiming to obtain personal and banking information for fraudulent purposes. (*Smishing*).

Here's a refined version of your sentence for better flow:

These fake SMS messages often include claims like 'your package has arrived but cannot be delivered,' 'your subscription needs renewal,' or 'your bank account will be blocked. The messages are usually written in poor Hungarian and contain a link that directs to a fake, phishing website.

d)
Another method is the so-called v*ishing* scam, where IP-based telecommunication devices are used, and the perpetrators persuade the victim to provide personal or financial information, transfer money to them, or share bank card details for data reconciliation, claiming that the card has been blocked and needs to be reactivated.[7]

In almost every case, the perpetrator pretends to be a bank representative or bank security specialist, with the aim of obtaining information by using VOIP (internet-based) calls.

They can select any phone number (even ones with real subscriber data), allowing the real caller to remain hidden.

In this act, the perpetrator contacts the victims by misusing the name of the financial institution, aiming to obtain personal and banking information

[6] Kitti M. (2019/4-5.): Challenges of cybercrime regulation in the criminal law, Public Prosecutors' Paper, Budapest. 32
[7] Ibid. 32

for fraudulent purposes. This also includes cases where no data is shared, however, the perpetrator creates a false impression in the victims, leading them to transfer money voluntarily to a bank account being a part of a fabricated story. This account is controlled by the perpetrator indirectly or directly.

It is very common for the perpetrator, posing as a representative of a financial institution, to persuade the victims to install the AnyDesk program, thus unknowingly granting remote access to their computers or phones. Once the victims log into their bank accounts and provide the necessary information, the perpetrators take control of the accounts.

Another common tactic used by perpetrators, after initiating a call in the name of the bank, is to convince their victims that a suspicious transaction has been made from their accounts or that they have been attacked. They are then persuaded to transfer their money to a new account, which could either belong to the fraudsters (opened by a straw man) or, in a more advanced way, to another victim's account (donor account). Unfortunately, in many cases, the victim doesn't even realize that they are transferring money to a different financial institution instead of their bank.

e)
In crimes related to online marketplaces, the perpetrator contacted the victim under the pretence of making a purchase, then sent a link to a fake (phishing) website to the victim's email, misusing the name of the online marketplace or the shipping company. The aim was to obtain personal and banking information for fraudulent purposes (so-called Foxpost scams).

f)
Investment fraud through fictitious websites is becoming increasingly common, where perpetrators exploit the victim's gullibility and greed to obtain significant sums of money, often promising investments in Bitcoin.

g)

The so-called Nigerian fraud[8], where the perpetrator asks for the transfer of a certain amount of money on the grounds of need, has also not disappeared (this includes the classic "asking for help" scams, "romance" scams, and scams where money is cheated from the victim with the promise of a reward or inheritance). In Nigerian scams, the perpetrators use some forms of misleading communication, typically by email, to persuade the victim to transfer money. The fake letters and requests usually ask for help: to recover refugee property or unlawfully taken inheritance, to obtain money that is temporarily unavailable for some reason, etc. Social media sites and online dating portals have been used to spread a version of the Nigerian scams, where the perpetrator builds a romantic relationship with the prospective victim before asking for money with a touching story. They intend to underpin the deceptive story with fake social media profiles, and fictitious documents that appear to be real.[9]

h)
In the past, targeted phishing was very common, where a network of perpetrators targeted a specific company. The emails sent were created in such a way that their unique features do not arouse suspicion. The perpetrators often posed as the heads of the targeted company and sent emails to the persons in charge of the finances, asking them to carry out an urgent transaction. These were the so-called CEO frauds, but nowadays the number of these cases has declined and the new methods described above have come to the fore.

[8] The "Nigerian-style" scam is one of the oldest forms of deception, which became widespread in the late 19th century and is also referred to as the Nigerian letters or 419 scam. Initially it spread by traditional mail or fax, but the development of telecommunication devices, and the spread of the Internet and e-mail have made the online space the main platform for this type of fraud. Hungarian National Bank Financial Navigator 20. July 2023. Source: https://www.mnb.hu/fogyasztovedelem/digitalis-biztonsag/az-adathalasz-csalasok-legjellemzobb-tipusai/nigeriai-csalas Accessed: 23.07. 2024

[9] Hungarian National Bank Financial Navigator 20. July 2023. Source: https://www.mnb.hu/fogyasztovedelem/digitalis-biztonsag/az-adathalasz-csalasok-legjellemzobb-tipusai/nigeriai-csalas Accessed: 23.07. 2024

i)
Marketplace fraud is still one of the most common methods of perpetration today. The offenders post fake advertisements on various online marketplaces, often for non-existent products, and then persuade interested buyers to transfer the requested amount in advance. After the successful transaction, the victim is strung along for several days with promises that the purchased item will be delivered by mail within a few days. However, this does not happen, and after a certain amount of time, the perpetrators break off all contact with the buyer.

j)
In invoice-switching fraud (*Business Email Compromise*), perpetrators attempt to obtain large sums of money from various organizations by using deceptive emails. The attackers often impersonate a leader or business partner of an organization, sending instructions to pay an invoice, and requesting the transaction to be made to an account they control. To increase the effectiveness of the method, the perpetrators often assess the internal structure and procedures of the targeted organization to send the most credible message possible to the victim.

k)
Ransomware attacks still occur today. These are malicious programs that encrypt data stored on infected systems making access to them impossible. The perpetrators demand a ransom for decrypting the data, typically requesting payment in hard-to-trace cryptocurrencies. Such attacks can lead to significant data loss and operational disruptions, especially if the victim does not have proper data backups. However, paying the ransom does not always guarantee the recovery of the files, making ransomware a serious threat to both individuals and organizations.

l)

In an online survey scam, perpetrators post fake surveys or questionnaires on various platforms (social media, website ads) to obtain confidential information such as banking details or passwords. The scammers often promise rewards, gifts, or cash prizes to motivate people to provide their personal and financial data. The information collected can then be used to commit further fraud or sold on illegal online markets, which is a common occurrence.

m)
The Wangiri call is a type of fraud where perpetrators make a brief call to a potential victim from a foreign or unknown number with the intent of prompting the recipient to call back. The return call is directed to a premium-rate service line with high per-minute charges, resulting in significant costs for the victim, who is often unaware of the call's expense. The fraudsters profit from the phone charges generated. Additionally, when victims attempt to call back, it may appear that the call was unsuccessful, leading to the line not being properly disconnected, causing further financial losses.

The investigation

All the cases of the above-mentioned methods of perpetration were revealed during the investigation, and the testimonies of victims, bank employees who were interrogated as witnesses, and the statements of suspects have shed light on the perpetrators' methods.

The crimes presented showed that today's criminalist (Fenyvesi) needs a very different way of thinking than 10 years ago and that with the changing crime structure, some investigative tactics need to change.

From 2nd March 2020, the Immediate Payment System (Azonnali Fizetési Rendszer – AFR) has been introduced in Hungary, which is mandatory for all financial institutions according to the regulation of the Hungarian National Bank, under which a transfer made in the frame of a banking

transaction is completed within five seconds, 24 hours a day, and 7 days a week.

The most important task of the law enforcement authorities in case of the offences described in this study is to take immediate rapid response measures during the investigations, while keeping in mind the urgency and timeliness, and to act as quickly and efficiently as possible following the information provided by the victim or the bank.

Once the person concerned informs the authority that he/she has become a victim of an "online fraud" and provides the necessary information for the investigating body, the first and most important procedural step that has to be taken to separate the victim and to compensate the damages, is to seize and recover the amount of money obtained criminally, as soon as possible, and to prevent further criminal acts (e.g., money laundering).

This also requires very close cooperation between the financial sector and law enforcement authorities, so that the decision on the coercive measures concerning property, taken by the investigating authority can be implemented by the affected bank in question without delay and any further transactions can be suspended. The primary objective is to keep the funds in question within the domestic banking system.

Of course, financial institutions also need to communicate and cooperate, as in many cases transactions involving the amounts concerned, can be interrupted and the amounts recovered can be returned to the victim.

During the criminal procedure, seven fundamental criminological questions must be clarified to fully establish the facts of the case. Without addressing these questions, prosecuting authorities cannot confirm that they have an accurate understanding of the relevant facts, the historical past, and the facts to be prosecuted.[10]

The most important aspect is the application of the "first strike" (erster Angriff)[11] formulated in criminology, which is implemented by initiating a

[10] Fenyvesi, Cs. – Herke Cs. – Tremmel, F.(2022): Eds.: Criminalistics Publisher Ludovika, Budapest. 44
[11] Ibid. 45

seizure and conducting immediate data collection and background research.

In these procedures, the analysis of previous actions, the prompt acquisition and evaluation of bank account numbers, phone numbers, straw men, and other data is essential, as experience has shown that crimes are committed in an organized and serial manner, making their complete detection a difficult task.

During the investigation, the proper evaluation of digital traces, the introduction of covert tools, the application of correct interrogation tactics, and the implementation of coercive measures concerning assets are of great importance.

The characteristics of the committed crimes are that the previously mentioned emails did not come from a bank's email address, the subject line is inaccurate, there are spelling and grammatical errors/poor in Hungarian, and they direct the recipient to a fake website.

If the deception occurs over the phone, the call usually comes at an inconvenient time (at work), and the victim is misled by the "helpful employee" and the use of "technical terms," often resulting in the installation of the AnyDesk program or the transfer of necessary information. The phone calls are long, and they do not hang up even if waiting is required – this ensures that the victim cannot call their bank. They exploit the victim's lack of experience, who rarely logs into online banking, is unfamiliar with it, and has limited computer knowledge.

The knowledge of the methods presented also creates difficulties in the investigation and in reducing the number of crimes, as the perpetrator's helpfulness and use of technical terms often convince the victims. They then say they will "connect the appropriate colleague" or the call centre, where similar tactics are used, but at this point, the data is already being extracted, as if for a security check, and during the long conversations, the victim is not allowed to hang up. The perpetrator who completes the crime is also helpful, reassuring the victim that everything is fine with their account, that it is now secure, and claiming to be the "real bank employee," even directing the victim to the police immediately.

Assets subject to seizure or freezing are increasingly found in foreign accounts, Revolut accounts, or cryptocurrency, making asset recovery a lengthier process in such cases.

Summary

One of the most important goals is the comprehensive development and strengthening of society's resilience to cybercrimes. To achieve this, knowledge and tools must be provided that help people understand the importance of cybersecurity and establish appropriate protections. In addition, users must recognize cyber threats and receive effective management methods at all levels of society. Therefore, it is necessary to widely develop citizens' awareness of safe internet use and their ability to respond to such threats.

The police aim to engage society as a whole, achieve nationwide reach, and prevent all offenses occurring in the online space. Every age group and target audience must be reached, regardless of geographical conditions.

Digital awareness and education are key to addressing cybersecurity challenges. Whether it's members of institutions and organizations or individuals, they must be continuously informed about the latest threats and best practices.

In 2022, a comprehensive nationwide project called "CyberSHIELD" (KiberPAJZS) was launched to raise awareness about online user consciousness and the importance of basic digital security knowledge. One of the founding members of the project was the National Police Headquarters. The Project supports the achievement of its goals through coordinated, consistent efforts with unified branding elements, by sharing existing experiences, utilizing them internationally, and through process development.

In today's active cyberwarfare, investigative authorities require continuous (both open and covert) digital data collection and up-to-date comprehensive databases. Using this data, crime detection is carried out by specialized units with the most powerful computers and programs available.

Criminologists must also participate in fast, efficient, and continuous (priority) training and practice. It will not be enough to rely solely on a specially trained team of experts; individual investigators must also learn the key knowledge related to hardware, software, the internet, data storage devices, and PC accessories. In our view, this will be the greatest challenge for criminologists worldwide in the coming years and decades.

Beyond all this, criminology increasingly requires highly skilled so-called ethical hackers—those who conduct digital intrusions to help map, detect, and identify digital criminals, servers, and systems. At the same time, they are capable of disrupting and disabling the operational scope of these threats.[12]

[12] Fenyvesi, Cs. (2024): The system of criminalistics. Jura 2024/1. 116