Cybercrime: A New Challenge of Criminality in the Digital Age

Marius-Andrei OROȘANU[1], Mihăiță ALEXANDRU[2]
[1] "Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
andrei.orosanu@academiadepolitie.ro
[2] General Police Directorate of The Municipality of Bucharest, Romania
mihaita.alexandru@b.politiaromana.ro

Abstract

Cybercrime, encompassing a broad spectrum of illicit activities executed through digital technologies, poses a critical threat to global security, economics, and individual privacy. Key methods, such as phishing, exploit user vulnerabilities by using deceptive techniques to acquire sensitive personal and financial data. Phishing-related offenses are explicitly addressed within legal frameworks, such as those outlined in the Penal Code, where they are classified under offenses against property and public safety. This underscores the integral role of legal structures in mitigating the growing risks posed by cybercrime, particularly as technological advancements enhance the complexity of such criminal activities. Additionally, the widespread use of fake websites for phishing purposes heightens the dangers of identity theft, financial fraud, and compromised banking systems, with long-lasting implications for victims' credit scores and financial stability.

Index terms: cybercrime, phishing, website, cyberattack, financial crime

1. Introduction

Cybercrime, also known as cyber criminality, represents one of the greatest challenges of the 21st century, having a significant impact on the economy, national security, and the daily lives of citizens. With the development of digital technologies and global interconnectivity, cybercriminals have found new ways to exploit computer vulnerabilities to commit crimes, ranging from the theft of personal and financial data to attacks on critical infrastructures, encompassing any illicit activity conducted through computer systems.

Globally, these crimes are perpetrated by individual offenders, hacker groups, or even nation-states using cyber technologies to achieve specific goals. Cybercrime manifests in a wide range of illegal activities, with **phishing** being one of the most notable methods. Phishing involves deceiving victims in various ways, leading them to voluntarily provide personal information, such as authentication data for different computer systems (banking applications, online payment websites, etc.).

One of the most common phishing techniques involves creating fake web pages that mimic the official sites of banking institutions, specifically designed to mislead users into entering their personal and banking information, thereby enabling the perpetrators to achieve their fraudulent goals. Thus, phishing is closely linked to criminal acts falling within the scope of penal illegality, as defined in the special part of the New Romanian Penal Code, specifically:

- Title II. Offenses against Property. Chapter IV. Frauds Committed through Computer Systems and Electronic Payment Methods.

- Title VII. Offenses against Public Safety. Chapter VI. Offenses against the Safety and Integrity of Computer Systems and Data.

2. General considerations regarding cyber attacks

At times, an event that occurs on a computer or within a network is part of a larger sequence of actions designed to result in an unauthorized outcome. Such an event is subsequently classified as an integral component of an attack. An attack is not a singular occurrence, but rather a multi-faceted process involving numerous stages. During these stages, the attacker typically undertakes actions specifically directed at a particular target, often utilizing tools or techniques to exploit identified vulnerabilities within the system.

The overarching goal of this process is to achieve an unauthorized result, which is considered illicit or undesirable from the perspective of the system's user or administrator. This could involve unauthorized access, data theft, or disruption of services, all of which are outcomes the system is designed to prevent. Unlike routine, benign activities that occur on a system, an attack is defined by the intentional and methodical nature of the steps taken by the attacker. The calculated progression through these stages, aimed at undermining the system's integrity or security, distinguishes an attack from ordinary or legitimate sequences of operations. Each stage in the process reflects the attacker's deliberate effort to circumvent protective measures, culminating in an outcome that breaches the security or intended use of the system [1].

Based on their attributes, including the resources they use, the time and tools at their disposal, and the level of risk they are willing to assume, a profile can be established for cybercriminals. The most common profiles include the following:

- **Recreational or exploratory hacker** – This individual possesses limited technical knowledge and may operate as part of a team using tools readily available on the internet. However, they often do not fully understand or appreciate the risks involved. They tend to be patient but typically seek out opportunistic scenarios rather than orchestrating complex attacks.
- **Disgruntled employee** – Lacking technical expertise, this individual, similar to the recreational hacker, uses readily available resources from the internet. Unlike the previous type, the disgruntled employee is more willing to accept the risks associated with their actions. Motivated by dissatisfaction, they exploit the tools and vulnerabilities they have access to, often from within the organization.
- **Activist targeting an organization for political or ethnic reasons** – Generally, this type of cybercriminal does not have specialized technical skills and relies on third-party services for execution. While they may exhibit patience, certain circumstances may compel them to act hastily. Similar to the other profiles, they also use publicly available resources and are generally risk-averse in their approach.
- **Industrial operative spy** – An industrial spy in the context of cybercrime often engages in data breaches to illegally obtain sensitive information such as trade secrets, proprietary technologies, or business strategies from competing organizations. They customize their tools and resources to suit the specific objectives of their attacks. Although technically proficient, they do not fully embrace the risks involved, often carefully weighing their actions to avoid detection or failure.
- **Cybercrime group or organization** – Distinct from previous individuals, this category includes groups or organizations, which can vary significantly based on their goals, resources, and the time they invest in criminal activities. Such groups operate based on the intelligence they gather and in the absence of information, they are willing to wait

patiently. Their objectives often revolve around acquiring material gains or large sums of money. These groups develop their own resources and customize their tools to maximize efficiency and success [2].

3. Phishing

Phishing is a broad term used to describe any type of cyberattack in which an attacker impersonates a trusted source to obtain sensitive information. In traditional phishing schemes, attackers typically distribute fraudulent and malicious emails to a large number of recipients. It is common for phishing campaigns to target thousands of individuals simultaneously, aiming to deceive only a small fraction of the intended audience.

Phishing attacks prioritize quantity over precision. Despite the indiscriminate nature of these attacks, cybercriminals can still gather valuable information from their victims through easily replicable, mass-distributed emails. The primary objective of such emails is to compromise personal data or infiltrate larger networks by exploiting the most significant cybersecurity vulnerability: the human user. Rather than attempting to breach sophisticated digital defenses directly, attackers leverage phishing techniques to deceive individuals into willingly granting access to sensitive data or systems.

To increase the likelihood of success, attackers often customize phishing emails to make them appear authentic, using official logos or fake email addresses that mimic legitimate sources. Phishers typically pose as trusted entities such as hospitals, financial institutions, or employers. These messages are crafted with alarming or urgent language to pressure victims into taking actions that may include clicking on malicious links, downloading malware-infected attachments, or providing personal credentials.

Once a victim complies, the attacker can compromise their system and extract sensitive data, often without needing to use advanced technical methods or even a single line of code. Not even the most advanced firewall can prevent a user from clicking on a malicious email, and once a single computer is infected, the malware can propagate across the entire network, posing a significant threat to the organization’s security infrastructure.

3.1. Phishing via Fake Bank Websites

Accessing and providing personal information on fraudulent websites can have severe consequences for users, as follows:

- **Identity Theft**: Personal information obtained through phishing (such as national identification numbers or identity card details) can later be used to open bank accounts, apply for loans, or commit other types of fraud in the victim's name.
- **Theft of Funds**: When attackers acquire banking details, they can directly access the victim's accounts, draining them or conducting unauthorized transactions.
- **Compromise of Bank Cards**: If credit or debit card details are stolen, they can be used for illegal purchases or to withdraw cash from ATMs.
- **Credit Score Damage**: Identity theft and illegal use of banking data can result in a decline in the victim’s credit score, making it more difficult to secure loans in the future.

3.2. How Does Phishing via Fake Bank Websites Work?

The main stages of a phishing attack using fake bank websites are as follows:

- **Creation of a Fake Website**: Attackers develop a website that closely resembles the official site of a bank. It may include the bank’s logo, colors, text, and even a subtly modified URL (for example, instead of "bank.com," the URL might be "bank-security.com").

- **Distribution of the Fraudulent Link**: Victims receive links to the fake website through emails, SMS, or social media, accompanied by an urgent message requesting immediate action (e.g., "Your account has been blocked. Please log in to reactivate your account.").
- **Provision of Information**: Once the victim accesses the page and enters login credentials or banking information, the data is captured by the attackers in real-time.
- **Use of Information**: The attackers use the obtained data to access the real bank accounts, perform illegal transactions, or sell the data on the dark web.

3.3. Preventive and combative measures against bank phishing

To safeguard the security of information systems and protect personal data, authorities and public institutions with relevant responsibilities, along with service providers, non-governmental organizations, and other civil society representatives, engage in collaborative efforts and prevention programs focused on combating cybercrime. These entities, working together, promote policies, best practices, measures, procedures, and minimum security standards for information systems.

In addition, these organizations conduct public awareness campaigns to educate users about the risks of cybercrime. The Ministry of Justice, Ministry of Internal Affairs, Ministry for the Information Society, Romanian Intelligence Service, and Foreign Intelligence Service continuously maintain and update databases related to cybercrime. The National Institute of Criminology, operating under the Ministry of Justice, regularly conducts studies to identify the causes and conditions that contribute to cybercrime and create favorable environments for such offenses.

Moreover, the Ministry of Justice, Ministry of Internal Affairs, Ministry for the Information Society, Romanian Intelligence Service, and Foreign Intelligence Service offer specialized training programs for staff tasked with preventing and countering cybercrime, ensuring they are equipped with the necessary skills and knowledge to address these rapidly evolving threats.

This comprehensive approach, involving coordinated efforts across various sectors, aims to strengthen national cybersecurity and minimize the risks posed by cybercriminal activities [3].

To prevent phishing through fake websites, users must reman vigilant and follow several essential security measures:

- **Verify the URL**: It is essential for users to verify the website's URL carefully before submitting any information. Legitimate banking websites utilize secure URLs that begin with "https://" and feature accurate domain names. Even the slightest variation in the website's address should prompt immediate caution.
- **Avoid Clicking on Links in Unsolicited Emails or SMS**: Users should avoid clicking on links received in suspicious messages and instead manually navigate to the bank's official site by entering the address in the browser.
- **Use Two-Factor Authentication (2FA)**: Many banks offer two-factor authentication, which adds an extra layer of security. Even if attackers obtain the password, they would still need a code generated on a secondary device to access the account.
- **Constant Monitoring of Bank Accounts**: Users should regularly check their bank statements to detect any unauthorized transactions.
- **Install Updated Security Software**: A good antivirus program can detect phishing websites and prevent access to them [4].

To combat cybercrime globally, coordinated actions between governments, international organizations, and the private sector are necessary. Key measures include:

- **International Cooperation**: Cybercrimes know no borders, making cooperation between countries essential. Initiatives such as the Budapest Convention (the first international treaty on cybercrime) and collaboration through organizations like Europol and Interpol are crucial in combating these offenses.

- **Education and Awareness**: Both companies and individual users must be educated about cyber risks and adopt solid cybersecurity measures, such as using two-factor authentication and protecting personal data.
- **Investment in Cybersecurity**: Governments and companies must invest heavily in cybersecurity technologies and the development of specialized teams capable of quickly responding to cyberattacks.
- **Legislation and Law Enforcement**: Continuously updating cybersecurity laws and swiftly punishing cybercriminals are essential to reducing cybercrime.

On the other hand, combating cybercrime is an extremely challenging task due to several factors, including:

- **Online Anonymity**: Cybercriminals can operate anonymously or hide their real location by using VPN networks and other encryption techniques, making it difficult to identify them.
- **Technological Dynamics**: Technology evolves rapidly, and cybercriminals constantly change their attack methods, forcing authorities and companies to always be one step behind in implementing security measures [5].
- **Digital Black Market**: On the Dark Web, criminals can easily buy and sell stolen data, hacking tools, and even cyberattack services, facilitating global cybercrime.

The process of collecting data within the digital environment and converting it into legally admissible evidence is determined by the specific clues and leads present in the investigated case. These clues dictate the appropriate investigative procedures that must be followed. For instance, if the investigation begins with an email address (e.g., name@mail.com), the initial priority is typically to establish the identity of the person or entity associated with that address. This may involve tracing the ownership of the email account, determining its activity, and assessing any potential links to the case.

In contrast, if the clue involves a web address (e.g., http://namewebsite.com/webpage), the investigative approach shifts. Investigators should first view the website in question using a browser to gather initial observations. In more comprehensive investigations, specialized software may be employed to download and preserve an exact copy of the entire site for further analysis. It is critical to remember, however, that during such investigative actions, the IP address of the computer used to access or download the website could be recorded by the web server under investigation, potentially exposing the investigating party's identity or location.

Furthermore, users can often be identified and traced by examining log files stored on servers. These logs contain records of user activities and interactions, such as connecting to or disconnecting from the internet, which can provide crucial evidence regarding the timing, location, and identity of the individuals involved. By analyzing these logs, investigators can reconstruct a timeline of digital activities, potentially revealing key actions linked to the case, such as unauthorized access or fraudulent transactions. As a result, careful attention must be paid to these digital traces, as they play a pivotal role in uncovering the full scope of cybercrime [6].

4. Case Study

The following information is based on the operational activity of the General Police Directorate of the Municipality of Bucharest, Romania in combating cybercrime.

I. On December 1, 2021, individuals AB and CD, through unauthorized entry of data, created a fake webpage similar to the internet banking site of X SA bank (accessible via the URL https://login.xn--bcrr-jh5a.com/users/login, appearing in search results for "24 banking X" on Google). Their intent was to produce legal consequences, specifically obtaining credentials necessary to access the bank accounts of the clients through the internet banking service. These actions fall

under the provisions of Article 325 of the Romanian Penal Code, which criminalizes the offense of computer-related forgery.

II. On January 1, 2022, AB and CD went to the X SA bank, where they fraudulently used falsified official documents, purportedly issued by Romanian authorities, under the names "CI" and "MD" to present themselves with false identities. Their aim was to deceive the bank employees into opening bank accounts, issuing associated bank cards, and activating internet banking services. These actions fall under the provisions of Article 327 (1) of the Romanian Penal Code, which criminalizes the offense of false identity.

III. On February 1, 2022, AB and CD used two falsified official documents, purportedly issued by Romanian authorities under the names "CI" and "MD," to create user accounts on the K cryptocurrency platform. These actions fall under the provisions of Article 323 of the Romanian Penal Code, which criminalizes the offense of forgery in official documents.

IV. On March 1, 2022, AB and CD, without the consent of the account holder MN, used the login credentials they had obtained through the method described in section I to access the online banking system of X SA bank.

They then illicitly transferred 500,000 lei from MN's bank account to bank accounts under the names "C.I." and "M.D." These actions fall under the provisions of Article 250 (1) and (2) and Article 360 (1), (2), and (3) of the Romanian Penal Code, which criminalize the offenses of fraudulent financial transactions and unauthorized access to an information system.

In an increasingly connected world, the protection of information systems becomes essential. Consequently, Romanian legislation has aligned with international standards, adopting strict measures against cybercrime, which poses a significant threat to the economic and national security of states, as well as the privacy and safety of individual users. As technology advances, cybercrime becomes increasingly sophisticated, requiring global solutions and international cooperation to mitigate its impact. Education, legislation, and innovation in cybersecurity are key to effectively addressing this emerging global challenge.

The ENSA report on cybercrime activity presents the following statistics regarding phishing:

- **26.2 billion** losses in 2019 due to Business Email Compromise (BEC) attacks.
- **42.8%** of all malicious attachments were Microsoft Office documents.
- **667%** increase in phishing scams in just one month during the COVID-19 pandemic.
- **30%** of phishing emails were delivered on Mondays.
- **32.5%** of all emails used the keyword "payment" in the subject line [7].

5. Conclusion

In summary, the increasing prevalence of cybercrime, especially phishing attacks conducted through fake bank websites, underscores the necessity for effective legislative measures to address and mitigate this issue. As cybercriminals adopt more sophisticated methods, it is important for law enforcement agencies to strengthen their capabilities in managing and responding to such threats. The role of the police is significant in investigating cybercrime, enforcing existing laws, and promoting public awareness about the dangers associated with online activities.

Additionally, individuals should understand the importance of being informed and cautious when using devices that store personal information. Familiarity with safe online practices is important in reducing the risk of becoming a victim of cybercriminals. By combining appropriate legal frameworks with public education and proactive law enforcement efforts, it is possible to foster a safer online environment that minimizes the risks of cybercrime and protects personal data.

References

[1]. I.C. Mihai, L. Giurea, "Analiza profilului infractorilor cibernetici", *Criminalitatea informatică,* II, Craiova, Romania: SITECH 2016, pp. 45-52.

[2]. *Manualul Investigatorului în Criminalitatea Informatică*, Ministerul Comunicațiilor și Tehnologiei Informației [Online] Available: https://www.scribd.com/doc/268511908/Manualul-Investigatorului-Criminalitatii-informatice. Accessed: October 6, 2024.

[3]. *Legea nr. 161 din 19 aprilie 2003 cu modificările și completările ulterioare,* Romanian Parliament, Romanian Official Monitor nr. 279 din 21 aprilie 2003. [Online] Available: https://legislatie.just.ro/Public/DetaliiDocument/43323

[4]. *Phishing: A Cyber-Security Guide for Employers and Individuals,* Zywave, 2020 [Online] Available: www.sutcliffeinsurance.co.uk/wp-content/uploads/2020/03/Phishing-Attacks-Guide.pdf Accessed: October 10, 2024.

[5]. *Convenția privind Criminalitatea Informatică,* Council of Europe, 2023 [Online] Available: https://eur-lex.europa.eu/RO/legal-content/summary/convention-on-cyber crime.html. Accessed: October 10, 2024.

[6]. I.C. Mihai, I.F. Popa, B.G. Tătaru, "Procedura investigațiilor online", *Securitatea în Internet,* Craiova, România: SITECH 2008, pp. 146-149.

[7]. *Phising, raportul privind situația amenințărilor,* European Union Agency for Cybersecurity, January 2019-April 2020. [Online] Available: www.enisa.europa.eu/publications/report-files/ETL-translations/ro/etl2020-phishing-ebook-en-ro.pdf. Accessed: October 14, 2024.