ProDefence

Cyber Security Services

"CLICK HERE, NOW THERE"

INVESTOR'S FEVER

The article aims to explore these insidious tactics in detail, provide an understanding of how these criminals operate, and outline effective measures to prevent and combat these frauds. We will provide essential advice and strategies for both current and potential victims and financial institutions to strengthen defenses against these increasingly refined cyberattacks. By raising awareness and implementing robust security practices, we can hope to better protect both our financial resources and personal information.

Alexandru Angheluș

Special thanks in support of the document

Zaborilă Florin Ionuț – Officer in the IPJ Iași

Computer Crimes Investigation Department

"**INVESTOR FEVER**" defines the behavior of people who, from simple users of technology and the Internet, become big investors through them, ignoring everything they have acquired by a certain age: intuition, selective trust, suspicion, relevant information, etc.

From the statements of the victims you can learn what they experienced during that period of their lives:

- "I invested 20,000 euros and I already have a gain of 150,000, but I can't get it out. The consultant says that draws affect the following trades in the long run."
- "After 10,000 euros invested I received 10% of the amount, but if I continue to invest after 12 months I can extract 45% of the amount from the account."
- "I lost 7500 euros with investments, and the police told me it was impaled... some fools, they don't know that's how it is in investing, you lose... You still win, because that's what the consultant told me from the beginning."
- "I started sending money and bought shares, but I don't tell anyone... that you know how people are, envious."
- "The Bank said that behind the investment there was a charlatan who tricked me, but I don't believe it! That man and I talked a lot, he told me about his family, he also had problems, he was upset that he worked long hours."

1. Introduction

Evolution of financial fraud

Fraud, in its broadest sense, refers to any intentional act of deception performed for personal gain or to cause harm to someone else. It is a concept that manifests itself in multiple forms, ranging from simple deception to complex schemes involving the manipulation of systems or processes.

When we talk about financial fraud, we refer to those acts of deception that aim to obtain illegal financial benefits. It may involve the manipulation or exploitation of financial systems, such as banks or capital markets, or it may directly involve individual victims through scams and deceptions. Financial fraud includes a wide range of illegal activities, such as identity theft, credit card fraud, Ponzi schemes, and other types of scams aimed at obtaining money, goods, or services without having a legal right to them.

Fraud committed through computer systems and electronic means of payment Criminal Code

According to the Romanian Criminal Code, these frauds are mentioned in the special part, which refers to "Crimes against property", Chapter IV, Art. 249-250-251 and is punishable by imprisonment.

Computer fraud - Art. 249 - Introduction, modification or deletion of computer data, restricting access to such data or preventing in any way the operation of a computer system, in order to obtain a material benefit for oneself or another, if damage has been caused to a person, is punishable by imprisonment from 2 to 7 years.

Fraudulent performance of financial operations - Art. 250- Performing a cash withdrawal, loading or downloading of an electronic money instrument or transfer of funds, by using, without the consent of the holder, an electronic payment instrument or identification data allowing its use, is punishable by imprisonment from 2 to 7 years.

- The performance of one of the operations referred to in paragraph 1 shall be punished with the same penalty. (1) by the unauthorised use of any identification data or by the use of fictitious identification data.

- The unauthorized transmission to another person of any identification data, in order to carry out one of the operations provided for in para. (1), is punishable by imprisonment from one to 5 years.

Acceptance of fraudulently performed financial operations – Art. 251 – Acceptance of a cash withdrawal, loading or downloading of an electronic money instrument or transfer of funds, knowing that it is carried out using a falsified electronic payment instrument or used without the consent of its holder, is punishable by imprisonment from one to 5 years.

- The acceptance of one of the operations referred to in paragraph 1 shall be punished with the same penalty. (1), knowing that it is carried out through the unauthorised use of any identification data or through the use of fictitious identification data.

In recent decades, with the advancement of technology and the massive digitalization of financial services, we have witnessed a significant transformation in the nature and complexity of financial fraud. This evolution reflects not only changes in the tools and methods used by cybercriminals, but also the continuous adaptation to new environments and user behaviors in the digital space.

In the past, financial fraud was often limited to more direct and less sophisticated tactics, such as identity theft through traditional methods or mail-order scams. However, in the age of the internet and ubiquitous connectivity, criminals have begun to exploit the online environment to develop schemes that are much more complex and difficult to detect.

Modern financial fraud is based on a variety of advanced digital techniques. From phishing and social engineering, to malware and sophisticated cyberattacks, criminals have a wide range of tools at their disposal to manipulate, deceive and steal from their victims. These methods are not only more effective, but also allow for anonymity, thus increasing the range and impact of attacks.

A peculiarity of today's financial fraud is the ability of criminals to adapt quickly to new technologies and trends. In the context of an increasingly connected world, where more and more transactions take place online, criminals have developed the ability to quickly exploit any vulnerability. This includes using social media to spread fake investment schemes, compromising the security of mobile apps for unauthorized access to bank accounts, and even exploiting emerging technologies such as cryptocurrency and blockchain to devise new types of scams.

This constantly evolving financial fraud means that both consumers and financial institutions need to be constantly vigilant and adapt to new threats. Education and awareness are vital, as are investments in cybersecurity and transaction monitoring systems. By understanding the evolution of these frauds, we can develop more effective strategies to prevent and combat them.

2. Fake Investment Fraud

Methods of deception

Fake investment fraud is a major threat in the modern financial world, affecting both individual investors and sometimes large-scale financial markets. These deception schemes are designed to appear as convincing and profitable as possible, using various methods to lure and manipulate victims.

Misleading Ads: This tactic is highly effective due to wide and easy access to the general public through online platforms and social networks. Ads can come in the form of eye-catching banners, sponsored posts, or even personalized recommendations. The use of false testimonies or the involvement of public figures, whether through unauthorized use of their images or false associations, is meant to create a sense of legitimacy and trust. This can make it difficult for investors to distinguish between genuine and false opportunities.

Fraudulent Emails and Messages: Criminals often use emails and direct messages to contact potential victims. These messages are often well-written and appear to come from legitimate financial institutions or trusted advisors. The aim is to gain victims' trust and get them to divulge personal information or invest in fake schemes.

Fake websites: Websites created to support these fake schemes are often made with a high degree of professionalism. They can include fake reviews, impressive charts, and even simulated trading systems to provide a semblance of authenticity and success. These sites can be difficult to distinguish from legitimate ones, making them dangerous for investors.

Time Pressure: Time pressure tactics play on human psychology, creating a sense of urgency that can cause victims to act quickly without having time to analyze the situation in detail. Criminals may claim that supply is limited in time or that investment opportunities are "once in a lifetime". This often leads to rash and reckless decisions on the part of victims.

Being aware of these tactics is the first step in protecting against fraud through fake investments. It is essential that investors always check the source of any investment offer and be skeptical of promises of high profits with low risk. It is also important to consult with trusted financial advisors and do thorough checks before committing to any type of investment.

Examples of fraud

Fake investment fraud represents a vast and diversified territory in the world of financial crime, each with its own distinct peculiarities and mechanisms. These schemes are often cleverly designed, with the main aim of exploiting the trust and lack of information of potential victims. Criminals orchestrating such fraud are often very knowledgeable about human psychology and financial market mechanisms, using this knowledge to mask their illicit activities.

A key element in the success of these schemes is to present them as legitimate and highly profitable investment opportunities. They are often packaged and promoted in a misleading manner, using financial industry language and graphics to appear authentic. Criminals can use various channels, from the internet and social media to traditional sales networks, to reach a wider audience.

Ponzi schemes:

- These schemes are named after Charles Ponzi, who used this method in the 1920s. The essence of a Ponzi scheme is to pay out existing investors' profits from funds brought in by new investors, instead of generating real profits.
- Ponzi schemes often start by paying high profits to attract even more investors. But as the number of new investors decreases, the funds for paying profits run out, which inevitably leads to the collapse of the scheme.
- A notorious example is Bernie Madoff's scheme, which was the largest fraud of this type in history.

Investments in Non-Existent Goods:

- These schemes involve promises to invest in projects or assets that are either completely fictitious or grossly exaggerated in their value.
- Examples may include investments in untapped gold mines, rare lands or breakthrough technologies. Criminals create compelling stories, complete with false documentation and testimonials to appear legitimate.
- Victims are lured with the prospect of big and quick gains, but in reality, those assets or projects do not exist or are completely unviable.

Fake Share Offers:

- This method involves selling shares for companies that do not exist or that are overvalued. Criminals can create fake websites and marketing materials to convince investors of the potential of the "company".
- They are often used in what's called a "pump and dump," where the value of shares is artificially inflated, after which criminals sell them quickly before they collapse.
- Victims find themselves owning shares that are virtually worthless.

Investing in Cryptocurrencies:

- With the increasing popularity of cryptocurrencies, numerous fake investment schemes based on cryptocurrencies have also developed.
- These schemes may involve new, unknown cryptocurrencies advertised as the next Bitcoin, or investment platforms that promise high profits from cryptocurrency trading.
- Many of these schemes collapse after raising a sufficient amount of funds, leaving investors with significant losses.

<u>Investments made on fake platforms:</u>

- The victim is persuaded to use a fake investment platform, which is run by criminals.
- The platform is a perfect clone of investment platforms, offering users the values of shares, amount earned, the opportunity to buy and other shares, but what the victim does not know is that all values are altered by the criminal because the platform does not communicate with investment infrastructures.
- Big earnings are achieved only as a VIP member, and this status is earned through serious investments, but in reality it is a way to convince the user to "invest" more money.

Recognizing these types of fake schemes is vital for any investor. It is crucial to conduct thorough research, consult trusted financial experts, and avoid any investment that seems too good to be true. Vigilance and education are the best weapons against these types of financial fraud.

3. Apps used and Access to Bank Accounts

Dangerous application installation tactics

Cybercriminals use a variety of sophisticated methods to trick users into installing dangerous apps that allow them access to bank accounts and other sensitive information. Understanding these tactics is crucial to being able to recognize and prevent threats to personal and financial security.

Phishing Messages and Emails:

- One of the most common methods is sending emails or messages that appear to be from financial institutions or other trusted entities. These messages may prompt users to download an app for "security updates" or to "check for recent transactions."
- Phishing messages are often very convincing and can include logos and designs that mimic those of legitimate institutions.

Misleading Ads on Online Platforms:

- Online ads can be used to promote apps that appear legitimate but are actually tools of malware. These ads can appear on respectable websites, making them appear more believable.
- Sometimes these ads can exploit browser vulnerabilities to initiate automatic downloading of the dangerous application.

Spoofing popular apps:

- Criminals can create fake versions of popular apps that, once installed, can access confidential information. These clone apps can be found in unofficial app stores or even in some cases on official platforms.
- Users can be lured to download these apps by promises of additional features or by copying some aspects of the original apps.

Exploiting compromised or fake web pages

- Criminals can use compromised or fake web pages, whose image and functionality is similar to that of legal investment platforms, misleading victims.
- Users directed to these fake platforms will live an investor's experience, they will see

Social Media Exploitation and Messaging:

- Criminals can use compromised or fake social media accounts to send download links to malign apps. Messages can come from friends or acquaintances of the victim, increasing the chances that they will trust and download the app.

QR Code and Direct Links:

- QR codes or direct links leading to app downloads can be placed in public places or on advertising materials. Once scanned or accessed, they can initiate the download of a dangerous application without the user's knowledge.

By becoming aware of the tactics used by cybercriminals to spread dangerous applications, users can take more effective precautions to protect their personal and financial data. Understanding the risks associated with downloading and installing unauthorized apps is a crucial first step in ensuring online security.

Risks associated with apps used

The risks associated with applications used by cybercriminals are diverse and can have serious consequences for both individual security and the integrity of users' financial data. These malign apps are designed to steal information, compromise devices, and facilitate unauthorized access to financial assets and personal accounts.

Identity Theft:
Dangerous apps can collect personal information such as names, addresses, dates of birth, and even social security numbers. This data can be used to commit identity theft, allowing criminals to access bank accounts, open new loans, or commit other crimes under the victim's identity.

Access to Financial Information:
Many of these apps directly target the theft of financial information, such as credit card numbers, online bank account credentials, and other financial details. Access to this information may lead to theft of funds or unauthorized transactions.

Remove/Influence Multiple Authentication (2FA/ MFA)
Intercepting or manipulating double/multiple authentication of banking applications will allow cybercriminals to continuously authenticate in banking applications, modify access data and implicitly trade directly from the application, without the victim seeing their activities.

Malware and Ransomware:
Certain apps can install malware or ransomware on the victim's device. The malware can track user activities, intercept data, or damage the system. The ransomware blocks access to data on your device, demanding a ransom to unlock it.

Compromising device security:
Installing dangerous apps can weaken your device's overall security, making it vulnerable to additional attacks. This can include opening network ports, disabling antivirus protection, or creating loopholes for other criminals to access your device.

Espionage and Monitoring:
Some apps can be used to spy on user activities, including accessing the device's camera and microphone. This can lead to serious breaches of privacy and the collection of sensitive information.

Phishing and Social Engineering:
Apps can also be used to run phishing campaigns, sending fake messages that appear to come from trusted sources to obtain sensitive information.

Reputational damage:
In cases where criminals gain access to the victim's social media accounts, they may send compromising messages or posts that may damage that person's reputation.

4. Illustration of the Fraud Scheme

The complexity of the fraud process

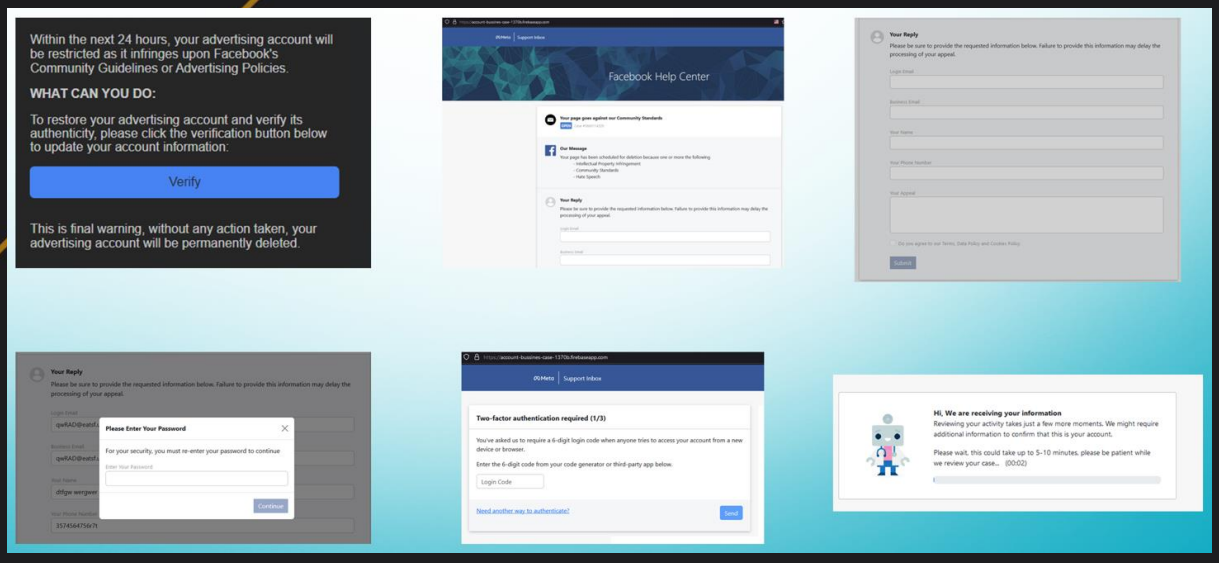
The fraud process is quite complex and has several variants of development, depending on the level of training of the user (potential victim) from a technical point of view and the power of persuasion of the offender over the person who has already reached the communication phase with him.

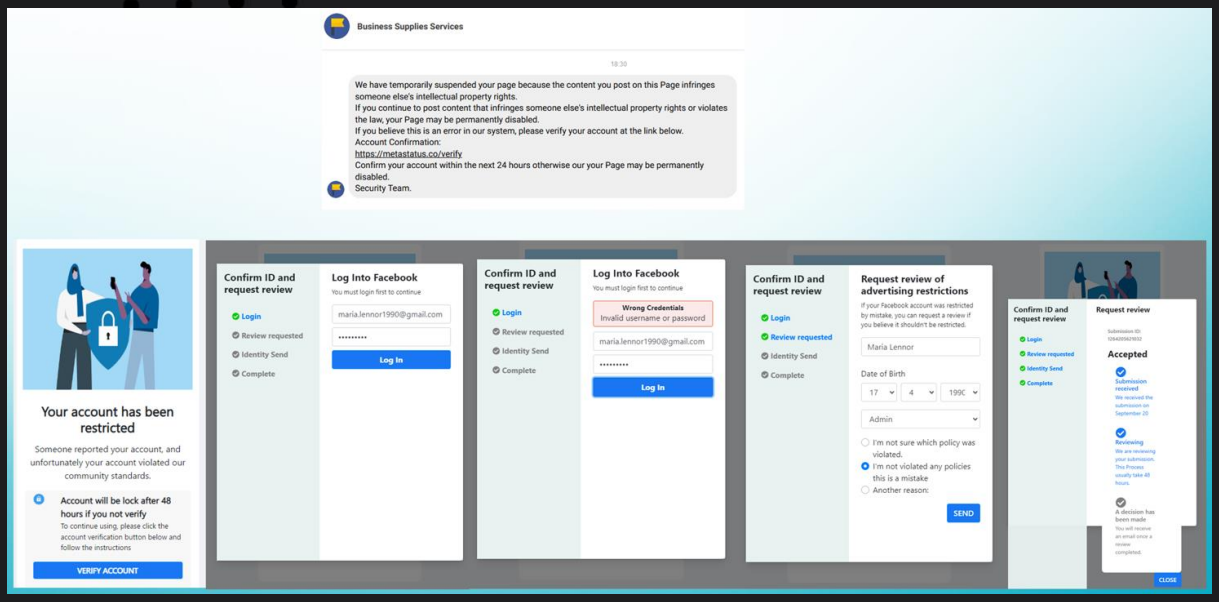
The initial attack – obtaining the necessary resources

A first important aspect in the fraud process is the contact with potential victims, which can be done in a direct way, through a targeted approach or in an indirect way by placing false information in the online environment, through messages, posts, comments and / or advertisements promoting the fraud scenario.

a. New accounts: Social media accounts or other platforms created specifically for launching information online. Low credibility in the direct approach, but impactful if added to compromised social media pages.
b. Compromised accounts: Accounts obtained by purchasing them or by other methods, such as malware or phishing.

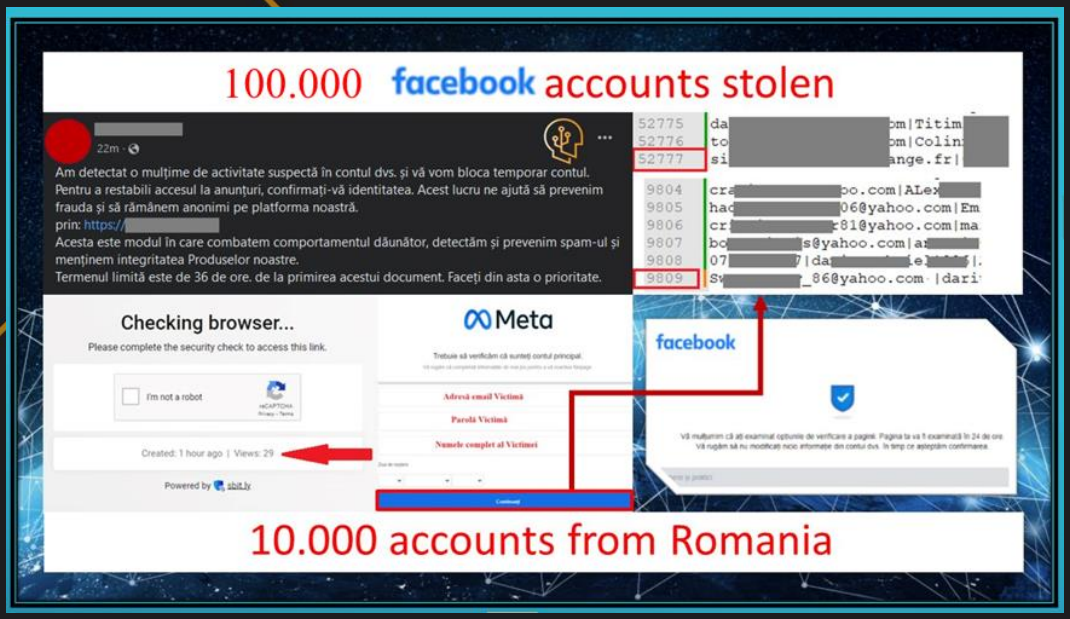
An example of a phishing cyberattack, which was carried out through messages and/or by tagging the person or page owned. These messages announced the violation of the platform's rules and asked the owners to confirm their identity, so as not to lose access.





Access and personal information added to fake pages gave attackers access to victims' accounts, with the next step being to block rightful holders from accessing compromised accounts and pages. To make their job easier, the creators of fake pages also added the ability for the victim to declare if they are a page admin.

A single campaign of this type gathered in a few days 100,000 accounts of Facebook users, and initially it was established that 10% of them belong to victims in Romania, because their sorting was done by identifying lines of text containing local domains ".ro" and the automatic classification set by attackers "| EN". Later, after more detailed analysis of the data collected by criminals, it was found that many victims did not meet the initial sorting criteria, but their first and last names are Romanian. This changed the percentage to over 45% at the expense of Romanian users, the attack clearly targeting Romanian-speaking people, regardless of their current location.

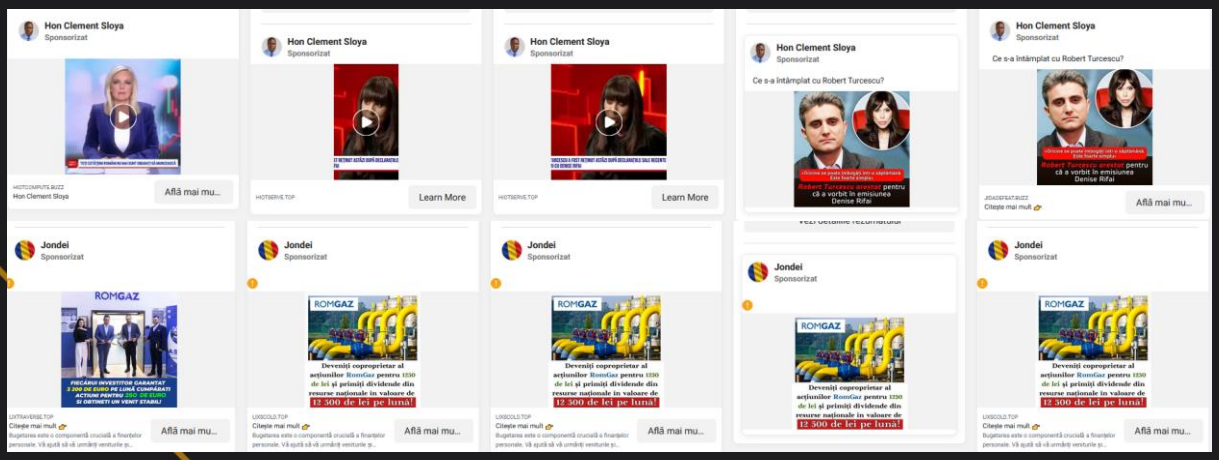


Exploiting Compromised Accounts/Pages – Targeting Victims

When it comes to the Attacker, he can have several roles in the conduct of the initial attack or only one:

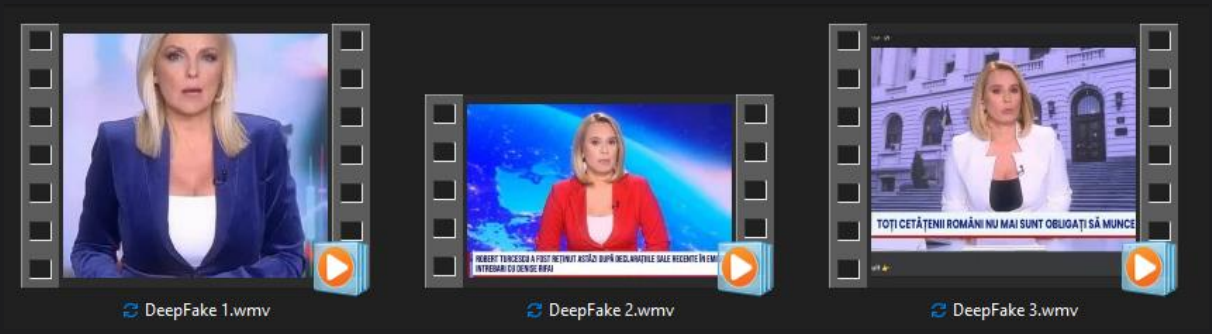
- The role of the cybercriminal who launches phishing or malware campaigns to obtain access data of social media accounts,
- The role of the offender who received/purchased access data and exploits them by launching the next stage of fraud.

The biggest interest of attackers is to compromise accounts that manage/generate ads. These accounts are used to create ads promoting financial fraud, while generating high costs for compromised and exploited accounts. Costs to be borne by holders of bank cards inserted into ad generation platforms.



The purpose of exploiting accounts is to promote fraud and implicitly direct possible victims to fake pages used in the fraud process. The stages of carrying out this process can be seen in the picture.

And with an unusually high frequency, the theft of the visual identity of influential people and the generation of fake or Deep Fake video sequences (fake videos generated by Artificial Intelligence through which a person's image and voice are cloned) are used

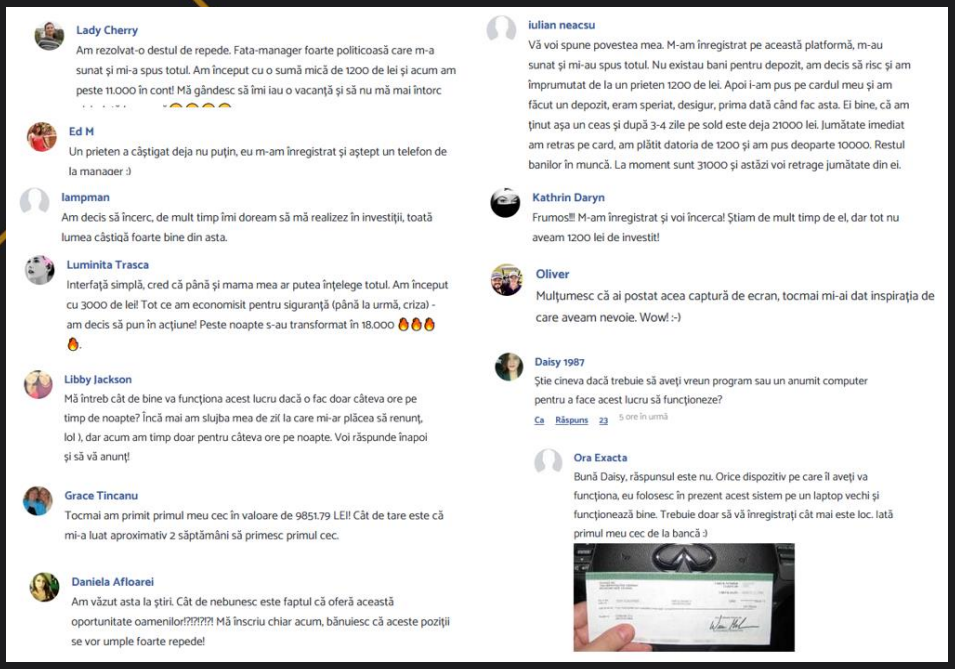


Careless or uneducated cyber-users will enter the scenarios created by attackers and play the role of the victim, as they reach this position by accepting visual manipulation. Generally, manipulation is done by sending information / warning messages and a temporary limit is mentioned, which has the role of removing the user from his comfort state, which will make him not pay attention to details.

The user arrived on the fake page is greeted by an avalanche of images and texts that support the fraud scenario, but also contain false statements of people who claim that they are already part of that business, bought the product or invested in shares, and the results are those described by the administrators of the fake pages.

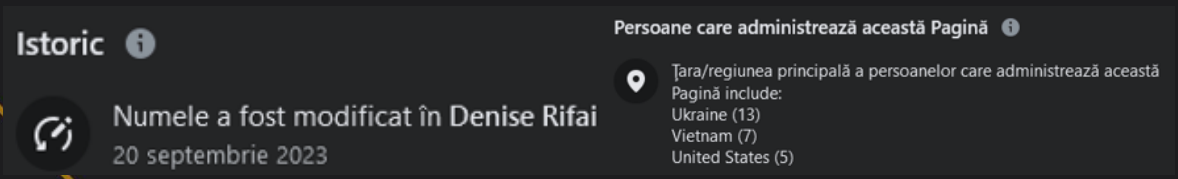
Social engineering has an important role to play.

Fake comments encompass a multitude of situations to cover a large scale of technology users eager to earn money or comments tailored to the ultimate goal of fraud/scam.

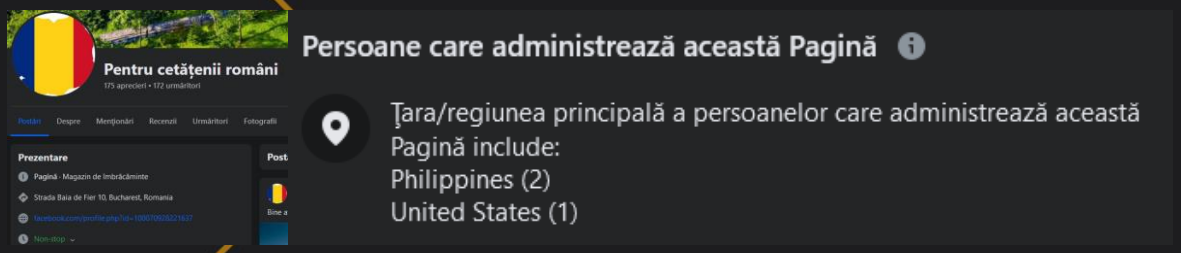


- *Technical help for those who are not good* at it, but would like to,
- *Gained a "friend"* - So it's something tested,
- *Easy to use application "that even mom could..."* – Include fools and elderly people,
- *Quitting your job for high earnings* – If that guy can, let's give it a try.
- *"I just got my first check..."* – "Guarantee" of winnings,
- *"I saw it on the news"* – It's something said on TV, so it's good...
- *"These positions will fill up quickly..."* – Fast that maybe we don't all get hold of anymore.
- *"There was no money ... I borrowed"* – Convincing those who do not have money, but could borrow.
- *"I made a deposit, I was scared, it was the first time..."* – Subtle elimination of doubts and conviction to try.
- ..... etc.

Pages generating fraudulent ads are undergoing major image and administration changes.



An example of a phishing campaign on users in Romania. During the analysis period, the account had generated 420 ads with the fraud campaign, and at a current verification, the account indicates a number of 510 generated ads, the last one running on October 26, 2023.



Current page status: Online, but with a different name...

... another country, other targets for fraud.

The interest of criminals and the purpose of those mentioned is to convince users to access fake pages and fill in a form providing contact details, so that the person responsible for the platform can get in touch with them.

Or, as the case may be, the purpose of the scam is to trick people into buying a product or service offered by the fake page!

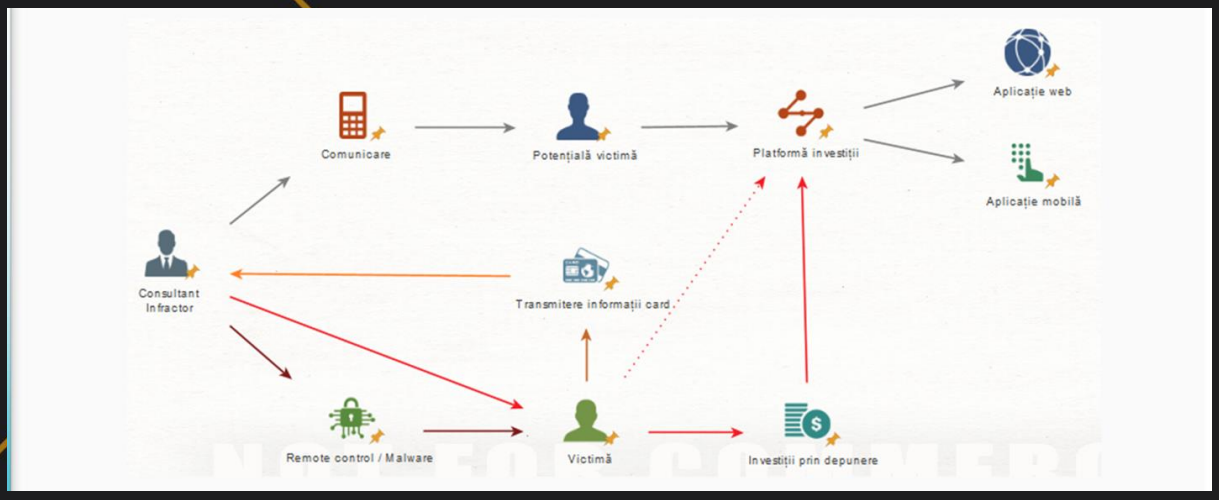
Analysis of stages of financial fraud

The contact details obtained by criminals are an important step in the fraud process, as the people who visited the fake page signed themselves up to the list of possible victims.

At this stage, the most important role is played by the Consultant, the criminal who gets in touch with the potential victim, because, through social engineering, he will do everything possible for his interlocutor to believe the whole scenario around the fraud and convince him that he is 100% a winner in this operation.

Keeping as the main topic financial fraud through investments in cryptocurrencies or shares of successful companies, it should be understood that the attacker will come into contact with users with different levels of education, technical skills and age. Investigations found that financial losses occurred through direct investment by users, sending funds to criminals, using fake apps and using remote control apps, giving criminals access to users' devices to help them set up accounts on fake platforms and even using their banking apps.

The flow of activities carried out can be understood from the image below, but at the same time one can observe the adaptability of offenders to the level of training of victims, sometimes part of the objectives to be eliminated, because they reach the money without requiring a lot of effort.



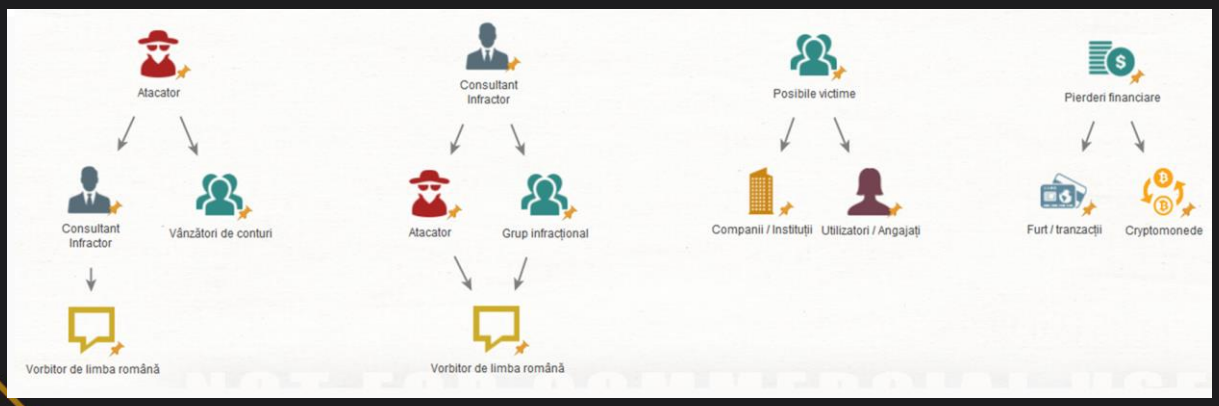
Concluding by analysing the fraud process, we have a clear picture of the roles of criminals, users and financial losses.

The initial attacker can only be the person who launches the phishing / malware campaigns, to obtain access data and sell them to criminals who will deal with fraud, can be part of the fraud team or one and the same person as the consultant who completes the fraud process.

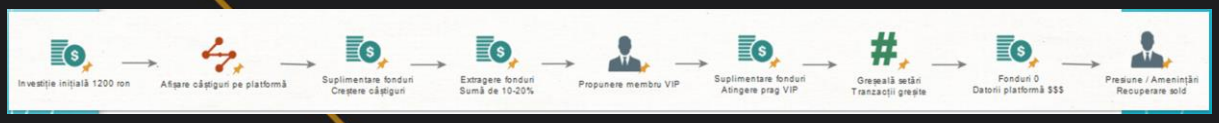
The consultant can be, as mentioned, the original attacker himself or is part of a criminal group, in which everyone has his role. According to victims' statements, the offenders are Romanian speakers, often with a specific Russian accent.

Possible victims are companies/institutions whose accounts have been compromised and exploited to create ads and users involved at each stage of the fraud scenario.

The victims of fraud (fake investments) are users eager for quick earnings, but lacking digital education, cyber education and easily manipulated people.



Large financial losses are due to the victim's manipulation in the investment process, criminals applying techniques to gain the victim's trust, but it can go as far as imposing debts to the investment platform and even threats to recover fictitious outstanding balances.



5. Prevention and Protection for Users

Warning signs of possible fraud

The warning signs of possible financial fraud are crucial to recognize and prevent falling into the traps of criminals. Each of these signs indicates potential risks and requires increased vigilance from users:

a. Offers with unusually high yields:

In the investment world, a general rule of thumb is that high returns usually come with risks to match. Any offer promising substantial profits without corresponding risk is suspect. These offers may be part of a Ponzi scheme or other types of scams.

b. Pressure to act quickly:

The tactic of creating urgency is often used to prevent potential investors from critically analyzing the offering. In these cases, criminals may argue that the opportunity is "once in a lifetime" or that immediate action is needed to benefit from the conditions offered.

c. Requests for personal or financial information:

Unexpected requests for sensitive information are a clear sign of fraud. Criminals can use this data to access bank accounts, for identity theft or other illegal activities. Any such request should be treated with great caution.

d. Lack of transparency or unclear documentation:

Legitimate investment offers are usually transparent and accompanied by clear and detailed documentation. Lack of transparency, ambiguous or unclear documentation, or reluctance to answer specific questions are signs that something is wrong.

e. Unsolicited communication:

Unsolicited emails, phone calls, or messages offering investment opportunities or requesting personal information should be treated with suspicion. These methods are often used in phishing campaigns to gain access to confidential information.

Recognizing these warning signs is a crucial step in protecting against financial fraud. It is important for users to be vigilant, ask questions, and conduct thorough research before making any financial decisions. Prevention starts with information and awareness of risks.

Prevention Tips

To avoid the pitfalls of financial fraud, it is essential to take a proactive and informed approach to managing your finances and personal information. Here are some detailed prevention tips that can help protect you:

a. Conduct thorough research:

- Source verification: Before investing, make sure that the entity and offering are legitimate. Search for information about the company and its products or services.
- Consultation of financial regulators: Check whether the entity is registered or regulated by a recognised financial authority.
- Seeking independent advice: It is always helpful to get a second opinion from an independent financial advisor who can objectively evaluate the offer.
- Seek expert advice: Ask for the opinion of a cybersecurity professional when there are suspicions about the web pages or platforms to which you have been directed.

b. Protect your personal information:

- Vigilance in communication: Be extremely cautious when asked for personal or financial data. Do not provide this information through unsafe channels or unauthorized persons.
- Data protection: Use data protection techniques, such as encryption and secure storage, to keep your information confidential. Personal.

c. Use online security practices:

- Software update: Make sure your operating system and apps are always up to date to protect against security vulnerabilities.
- Use double/multiple authentication: Enables multi-factor authentication on all major accounts to add an extra layer of security.

d. Avoid impulsive decisions:

- Analysis and reflection: Take time to evaluate each financial opportunity and weigh the pros and cons. A well-thought-out financial decision is always safer.
- Avoid pressure: Don't be pressured into making quick decisions, especially in stressful or pressured situations.

e. Monitor your financial accounts:

- Regular checks: Regularly review bank statements and transactions for any suspicious or unauthorized activity.
- Transaction alerts: Setting alerts for unusual or large transactions can be an effective way to detect fraud quickly.

By implementing these practices, you will be able to increase your level of protection against potential financial fraud. Awareness and continuing education are essential in this process, as offenders' methods can change and evolve. Always keep an eye out for the latest fraud tactics and adapt your security strategies accordingly to keep your finances safe.

6. The role of financial institutions

Security and monitoring measures

a. Advanced Fraud Detection Systems:

- These systems use sophisticated algorithms and machine learning to identify unusual or suspicious transactions, helping to detect potential fraud early.
- Behavioral analysis and risk modeling are also used to assess transaction patterns and identify unusual activity.

b. Security of technological infrastructure:

- Securing IT infrastructure involves protecting customer data and banking systems from cyberattacks using advanced encryption technologies and robust security solutions.
- Continuous updating and maintenance of IT systems is vital to stay ahead of cybercriminals' increasingly sophisticated methods.

c. Multi-factor authentication and Account Security:

- The implementation of multi-factor authentication (MFA) provides an extra layer of security, requiring more than just a username and password to access an account.
- MFA can include elements such as phone-generated codes, security questions, or fingerprints, significantly increasing the security of online accounts.

Customer education in cybersecurity

Customer education in cybersecurity is a crucial aspect in financial institutions' strategy to combat fraud. By informing and training customers, they can significantly reduce the risk of them falling victim to illegal activities online.

a. Security Awareness Programs:

- Educational Materials: Providing brochures, guides and other informational materials explaining different types of cyber fraud, such as phishing, vishing, smishing and other social engineering techniques.
- Real Examples and Case Studies: Presenting real cases of fraud can help customers better understand risks and recognize warning signs.

b. Regular Communication with Customers:

- Newsletters: Periodically sending newsletters that include security tips, warnings about new types of fraud and recommendations for online protection.
- Social Media Channels: Using social media platforms to spread awareness and reach a wider audience.

c. Online Safety Training:

- Webinars and Workshops: Organizing online educational sessions and events where cybersecurity experts provide practical advice and answer customer questions.
- Simulations and Tests: Implementing phishing simulations to teach customers how to identify suspicious emails and messages.

d. Customer Support:

- Helplines: Providing a dedicated hotline where customers can report suspicious incidents and receive immediate support.
- Personalized Consulting: Providing personalized advice and support for customers who need help managing the security of their online accounts.

e. Security Updates and Warnings:

- Security Notifications: Sending alerts via email or text messages when suspicious activity is detected on the customer's account or when new threats appear.
- Updated Information: Maintain a section on the bank's website with the latest news and advice in the field of cybersecurity.

Through these measures, financial institutions not only protect their own resources, but also contribute to creating a safer financial environment for all users. Education and continuous cooperation with customers, along with the implementation of the latest security technologies, are essential in the fight against financial fraud. This combined approach helps build trust in the financial system and effectively protect client assets from cyber threats.

Thus, the role of financial institutions is crucial not only in the efficient management of finances, but also in ensuring a safe and protected environment for financial transactions in the digital age. By working closely with regulators, other institutions and customers, they can continue to improve defences against sophisticated financial fraud.

7. Compromise Response Plan

Immediate action after fraud detection

a. Notification of financial institutions:

Contact the bank or financial institution involved immediately. Cancelling or immediately blocking any credit/debit cards and online access to accounts is crucial to prevent further losses.

b. Change your login credentials:

Change passwords and security details for all affected online accounts. This includes email accounts, social media platforms and any associated online service.

c. Reporting to competent authorities:

Report fraud to the Police, the National Directorate of Cyber Security and other relevant authorities, such as the national financial fraud supervisory authority. It can help investigate and prevent other similar cases.

d. Credit monitoring:

In the case of identity theft, it is important to monitor your credit reports for any unauthorized activity. Credit monitoring services may be considered to alert of any suspicious changes.

Recovery of losses and securing accounts

a. Preservation of evidence:

Save all discussions, documents, email addresses, phone numbers of people you interacted with. Avoid deleting installed apps or formatting devices involved in the incident.
The information can help identify how the fraud was carried out, but also the identity of the criminals.

b. Review of transactions:

Review all recent transactions for unauthorized activity. This will help determine the level of compromise.

c. Detailed documentation and reporting of the incident:

Keep a detailed record of all communications and actions taken after fraud detection. This includes any report to the police, correspondence with the bank and security changes made.

d. Consultation with a financial or legal expert:

In complex cases, it may be helpful to consult a financial or legal expert to guide you through the process of recovering losses and protecting your rights.

e. Reassessment of security measures:

Review and improve security practices to prevent similar incidents in the future. This may include investing in more advanced security solutions, reviewing security policies and raising awareness of data protection.

8. Conclusion

The importance of awareness and prevention

Awareness and prevention are essential in the fight against financial fraud. In an increasingly digitalised world, where financial transactions take place largely online, the potential for illegal activities is amplified. It is therefore crucial that both individuals and financial institutions are well informed and take proactive measures to protect themselves against these threats.

The role of awareness:

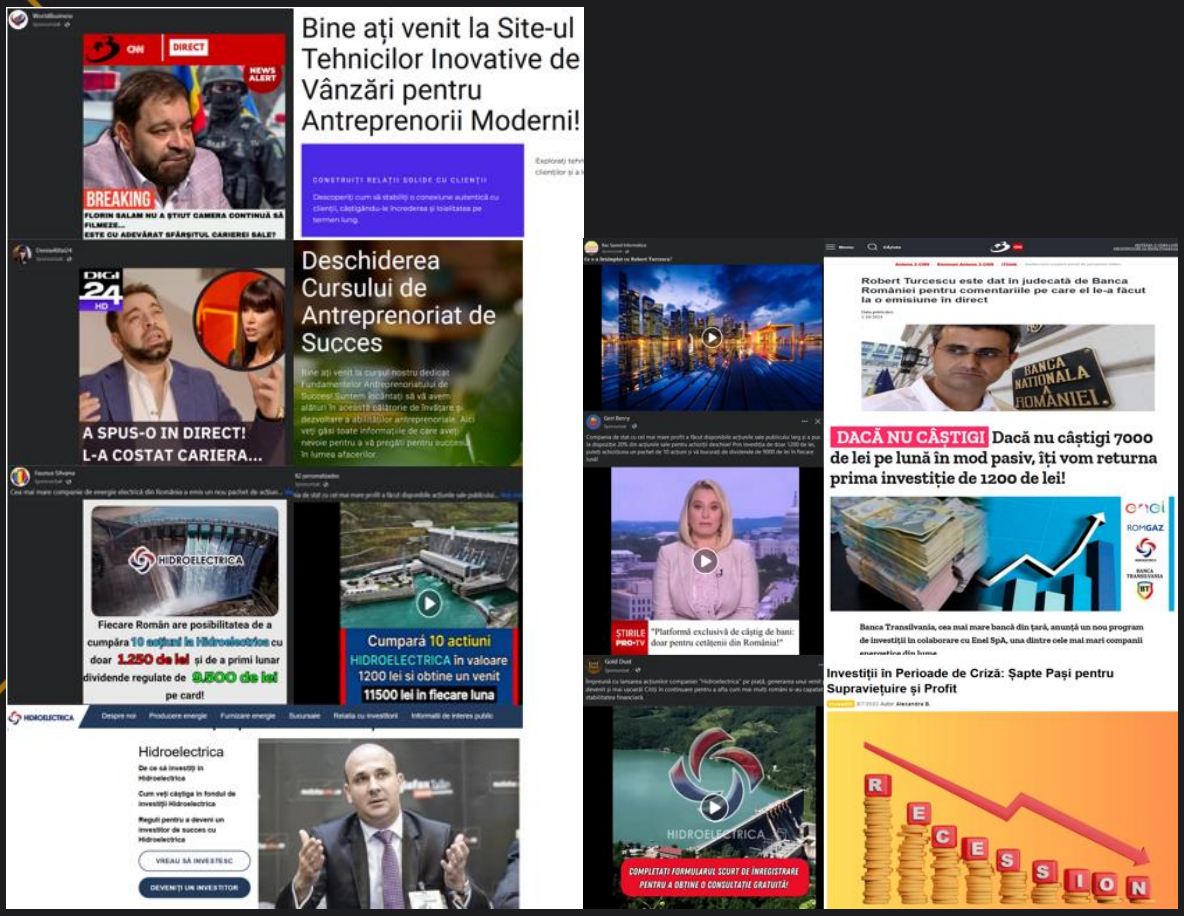
- **Education:** Being well informed about the different types of financial fraud and their warning signs can make the difference between being a victim and preventing an attack. Continuing education is vital to keep pace with the ever-changing methods of offenders.
- **Information Sharing:** Disseminating personal knowledge and experiences related to financial fraud in communities can help raise general awareness and protect others.

The importance of prevention:

- **Security measures:** Implementing robust security measures, both at a personal and institutional level, is essential to block criminals from accessing information and financial resources.
- **Continuous vigilance:** Maintaining an attitude of vigilance and regularly reviewing security practices ensures that we are always one step ahead of criminals.

Finally, preventing and combating financial fraud is a shared responsibility. Through collaboration between consumers, financial institutions and regulators, we can build a safer and more protected financial environment. Risk awareness and proactive security measures are not only a safeguard against financial loss, but also an essential step towards maintaining a safe and confident digital society.

9. Bonus: Ongoing fraud campaigns



Sources and further reading

Phishing attack – **Cyber AID**
https://www.cyberaid.eu/atacul-de-tip-phishing/

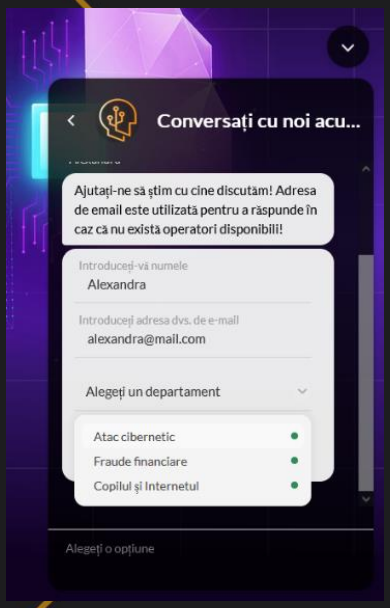
Bank Phishing – **Online Safety**
https://sigurantaonline.ro/phishing-ul-bancar/

Cybersecurity Articles – **Prodefence**
https://www.prodefence.ro/articole-securitate-cibernetica/

Online fraud detection – **DNSC**
https://www.dnsc.ro/cautare?ceCaut=frauda

Cyber Intelligence – Using Profiling – **ISACA | DNSC**
https://dnsc.ro/vezi/document/isaca-cyber-intelligence-using-profiling/

Cyber Edequation – Parents and Children – **Prodefence**
https://www.youtube.com/@AlexandruAnghelus/videos



Cyber Chat

Before sending personal data or money to a stranger, it is better to ask for the opinion of specialists. It's free and I can help you not make wrong decisions!

https://www.cyberaid.eu/ | https://sigurantadigitala.ro/

Available only in Romanian !

”You say that everything is a lie and that they are all thieves, but the same YOU give all your personal data and money to a person who told you stories by SMS or on the phone”

ProDefence

Cyber Security Services