Cyber Fraud Schemes: Modus Operandi, Tools and Techniques, and the Role of European Legislation as a Defense Strategy

Papathanasiou Anastasios, Liontos George, Liagkou Vasiliki, Glavas Euripides

Open Science Index, Computer and Information Engineering Vol:18, No:4, 2024 publications.waset.org/10013594.pdf

***Abstract*—**The purpose of this paper is to describe the growing problem of various cyber fraud schemes that exist on the internet and are currently among the most prevalent. The main focus of this paper is to provide a detailed description of the modus operandi, tools, and techniques utilized in four basic typologies of cyber frauds: Business Email Compromise (BEC) attacks, investment fraud, romance scams, and online sales fraud. The paper aims to shed light on the methods employed by cybercriminals in perpetrating these types of fraud, as well as the strategies they use to deceive and victimize individuals and businesses on the internet. Furthermore, this study outlines defense strategies intended to tackle the issue head-on, with a particular emphasis on the crucial role played by European legislation. European legislation has proactively adapted to the evolving landscape of cyber fraud, striving to enhance cybersecurity awareness, bolster user education, and implement advanced technical controls to mitigate associated risks. The paper evaluates the advantages and innovations brought about by the European legislation while also acknowledging potential flaws that cybercriminals might exploit. As a result, recommendations for refining the legislation are offered in this study in order to better address this pressing issue.

***Keywords*—**Business email compromise, cybercrime, European legislation, investment fraud, Network and Information Security, online sales fraud, romance scams.

I. Introduction

In the ever-expanding realm of the internet, cyber fraud schemes have emerged as a significant and pressing concern. This paper aims to explore the proliferation of various cyber fraud schemes and shed light on the modus operandi, tools, and techniques employed by cybercriminals. The focus centers on four primary typologies of cyber frauds: BEC attacks, investment fraud, romance scams and online sales fraud. By understanding the methods used by cybercriminals, this study seeks to raise awareness and provide crucial insights for safeguarding individuals and businesses against these deceptive practices. There are four main cyber fraud topologies:

1. *Business Email Compromise (BEC) Attacks*: These sophisticated schemes involve impersonation of trusted entities, typically targeting businesses and their employees. The attackers manipulate communication channels to deceive victims into transferring funds or sensitive information unwittingly.
2. *Investment Fraud:* Cybercriminals exploit the allure of lucrative investment opportunities to deceive individuals into parting with their hard-earned money. The schemes may present fraudulent investment schemes or manipulate existing market conditions to extract funds from unsuspecting victims.
3. *Romance Scams:* Operating on emotional manipulation, romance scams involve creating fake personas to establish online romantic relationships with the sole intent of exploiting victims financially.
4. *Online Sales Fraud:* Cybercriminals set up fraudulent online marketplaces, auctions, or classified ads to swindle unsuspecting buyers, offering counterfeit products or simply absconding with payments without delivering the promised goods.

To effectively deceive and victimize their targets, cybercriminals rely on various techniques, such as social engineering, phishing, malware distribution and data breaches. These tactics exploit human vulnerabilities and technological weaknesses, amplifying the impact of cyber fraud schemes.

Having in mind the above main cyber fraud topologies, the primary objectives of this paper are:

1. *Analyzing Four Key Typologies of Cyber Fraud:* The paper focuses on investigating four fundamental typologies of cyber frauds, namely BEC attacks, investment fraud, romance scams, and online sales fraud.
2. *Unveiling Cybercriminal Methods and Strategies:* One of the central goals of the paper is to shed light on the tactics employed by cybercriminals to perpetrate their fraudulent activities.
3. *Proposing Defense Strategies*: To combat the rising threat of cyber fraud, the paper presents defense strategies. These strategies are intended to equip individuals and businesses with proactive measures to safeguard against cyber fraud.
4. *Evaluating the Role of European Legislation:* A key objective is to assess the impact of European legislation in the fight against cyber fraud. The paper explores how the legislation has evolved to tackle the challenges posed by evolving cyber fraud schemes, emphasizing the role of legal measures, cybersecurity awareness initiatives, and user education.
5. *Identifying Advantages and Innovations*: The paper aims to highlight the advantages and innovations introduced by European legislation to combat cyber fraud.
6. *Addressing Potential Flaws and Recommending*

Anastasios Papathanasiou is with University of Ioannina, Greece (e-mail: anastasios.papathanasiou@gmail.com).

Improvements: The paper critically examines the European legislation to identify any potential flaws that cybercriminals might exploit. In doing so, it provides recommendations for refining the legislation to better counteract cyber fraud and enhance overall cybersecurity efforts.

In summary, the objectives of this scientific work encompass comprehensive exploration, analysis, and proposal of defense strategies to tackle cyber fraud with a specific focus on the role of European legislation in safeguarding individuals and enterprises.

II. Research Methodology

This paper utilized a systematic methodology to investigate the growing problem of cyber fraud schemes and the role of European legislation in addressing them. The systematic approach ensured a rigorous and organized research process, allowing for comprehensive exploration and analysis of the subject matter. The search for the theoretical part of this research was conducted using keywords such as "online frauds", "European Legislation", "NIS 1", "cybercrime", "BEC schemes" etc. Following a pilot search, we employed an inclusion/exclusion procedure where articles irrelevant to our study were excluded, while those relevant to our research were included and analyzed. Furthermore, additional searches using the referenced works of relevant articles were also conducted (snowball effect).

III. Cyber Fraud Schemes/Topologies

Presently, the internet is witnessing significant financial damage caused by four primary cyber fraud schemes/ topologies, enumerated and analyzed below:

A. Business Email Compromise

In BEC fraud attacks, cybercriminals use social engineering and data attacks to acquire earnings. They intercept electronic correspondence of businesses and modify invoices by changing the seller's bank account number in an existing or new business relationship. This tricks businesses into transferring funds to the fraudsters' account, believing it to be a legitimate payment to their partner. The fraudsters often create a new email address resembling the seller's to deceive the buyer.

Phishing is another method employed by the fraudsters, where they use the seller's account to send deceptive emails. One version/category of BEC fraud is CEO fraud, wherein the criminals impersonate the company's CEO through phishing emails. By hacking the company's email system, they send emails appearing to be from the CEO, using a similar email address. Their intention is to urgently persuade the victim to transfer money to a bank account controlled by the fraudster, leaving little time for assessment and creating doubt.

In BEC/CEO fraud attacks, the approach differs from traditional phishing. Here, the fraudsters target specific victims and environments. They gather information from publicly available sources to create highly convincing deception tactics. Initially, the fraudsters obtain email passwords to gain access to email accounts. By doing so, they intercept the email exchanges between companies and redirect them to their own email addresses. This allows them to monitor and analyze the communication between business units. With the help of filters, the fraudsters quickly identify the buyers and sellers involved in the transactions. BEC/CEO fraud attacks can take various forms depending on the target. While emails are the primary method, some cases involve messaging and phone calls. However, the underlying principle remains consistent – to deceive the victim into transferring money to the fraudster's account, either by believing they are paying a genuine invoice or acting on behalf of their CEO [1].

Once the preparation phase is complete, the fraudsters gain access to emails containing invoices and begin sending their own fraudulent invoices or altered payment details to the business entity. They typically explain in an email that their account number has changed, providing a reason for the switch. When the organization makes a payment, the business representative believes they are sending money to a legitimate partner's account. However, the funds end up in the fraudster's account. After receiving the funds, the fraudster may transfer the assets to accounts in other countries or withdraw the proceeds in cash from ATMs [2].

Tools:

- Hacking tools – Software from clear and dark web
- E-mail services/providers
- Phone calls
- Messaging services
- Instant money transfer services

Techniques:

- Social engineering techniques
- Impersonation

B. Online Sales Fraud

Online sales fraud is a diverse category with various methods of execution and many cases involve advance payments between the fraudster and the victim. In one common scenario, the fraudster sells a product and receives payment in advance without delivering the goods to the buyer (non-delivery fraud). Conversely, some fraudsters pose as buyers, convincing sellers to use special payment services or pay for shipping. They then send a fake shipping link (fake shipping fraud).

Another version of this fraud involves setting up fake online shops to deceive unsuspecting customers. In these cases, the fraudsters lure victims into making purchases from non-existent or illegitimate websites.

The first step in this scheme primarily contains searching for potential victims on online sales platforms, and then collecting information through posted ads or by posting ads, or through creating a fraudulent online shop. The fraudsters communicate both on and off the sales platforms.

The attack phase of online sales fraud can take various approaches. When the fraudster poses as the buyer, they persuade the victim to use a special payment or shipping service, claiming it is a faster, more convenient, or cheaper option. The victim is then provided with a link to a fake payment or shipping website. The fraudster tricks the victim into providing their payment card details or authorizing transactions via a banking app or electronic ID, bypassing two-factor authentication [3].

Once the fraudster has the payment card details, they may transfer money to companies like FinTech, tokenize the card for purchases, or withdraw cash from ATMs. If they gain access to the victim's internet bank, they can make transfers to online or foreign bank accounts. In some cases, the fraudster sends the victim a link to a fake payment site (e.g., PayPal) to falsely show a payment has been made, leading the victim to send the goods without receiving payment.

In other instances, the fraudster deceives individuals by posting fraudulent sales ads. Victims who wish to buy the product are asked to pay in advance before the goods are sent. However, the victims either receive nothing, or the goods turn out to be fake, of poor quality, or damaged.

Tools:

- Online sales platforms
- Messaging services
- Fake websites, domain hosting
- Email services/providers
- Instant money transfer services
- Banks, electronic ID, banking tools for remote login
- Ads

Techniques:

- Social engineering techniques
- Impersonation

C. Romance Scam

In romance scams, the initial objective of the fraudster is to establish a deep sense of trust with the victim. This is achieved through prolonged and consistent communication, often spanning several months. During this time, the victim may develop strong feelings for the fraudster, who typically presents themselves as an attractive and high-ranking individual, such as a soldier, doctor, oil rig worker etc.

Once the fraudster believes that the victim's trust has been sufficiently gained, they begin to solicit money and request transfers to foreign bank accounts. In some cases, the fraudster employs a different tactic, asking the victim to purchase vouchers with digital codes and then share these codes via text message. This allows the fraudster to redeem the vouchers at a location far from the victim's area, making it harder to trace the scam. Overall, romance scams exploit emotions and trust, leading victims to fall for the fraudulent persona and unwittingly part with their money or sensitive information.

In romance scams, the victim typically encounters the fraudster on a dating app or social media platform. The fraudster adeptly assumes the persona of a doctor or soldier, someone perceived as trustworthy with noble intentions. They often claim to be far away from their home and family, adding an element of vulnerability to their narrative.

As communication progresses, trust is cultivated, sometimes spanning an extended period. The fraudster employs various means, including phone calls and occasional video chats, though the latter may conveniently exhibit poor quality due to a "bad connection," keeping their true identity concealed. To deepen the illusion of authenticity, the fraudster shares photographs, fostering a sense of intimacy, interest, and trust.

In the attack phase of a romance scam, the fraudster deploys various deceptive tactics to manipulate the victim's trust and emotions. One common approach involves concocting an extraordinary situation, where the fraudster claims to be in dire need of financial assistance due to being far away from home and unable to access their own funds. To entice the victim further, the fraudster often makes enticing promises, assuring the victim that they will receive even greater returns as a 'thank you' for helping. This emotional appeal prompts the victim to initiate money transfers, believing they are offering genuine aid. The scam may unfold in multiple steps, with the victim initially convinced to transfer one sum of money. Subsequently, the fraudster fabricates further unexpected events, compelling the victim to believe that additional transfers are necessary to resolve the perceived crises. This cycle may persist until the victim's financial capacity is exhausted, prompting them to halt further transactions. Tragically, some victims may even resort to taking loans or mortgaging their homes in a desperate attempt to continue "helping" the fraudster, unaware that they are falling deeper into the intricate web of deception. In summary, the attack phase preys on the victim's compassion and willingness to assist someone in need, resulting in severe financial repercussions while the fraudster continues to exploit and manipulate their emotions.

In another version of the romance scam's attack phase, the fraudster employs a clever ploy involving a package or luggage supposedly containing valuable items like money or gold. The fraudster claims to be in a remote location or undergoing an overseas deployment, thereby lacking a current address to receive the package. To elicit the victim's assistance, the fraudster requests that the victim cover the costs of import duties, shipping, and insurance for the package. They assure the victim that they can hold onto the package until the fraudster can personally retrieve it. To facilitate the money transfer, the fraudster provides the victim with instructions on where to send the funds, along with specific account information. Once the victim complies and sends the money, the fraudster may resort to various excuses to request additional funds, providing different account numbers for each transaction. These deceptive tactics continue to manipulate the victim, who may believe they are genuinely aiding the fraudster and safeguarding their valuables. Unfortunately, the cycle persists as the victim remains convinced of the fraudster's sincerity, leading to repeated money transfers and mounting financial losses [4], [5].

Tools:

- Channels/platforms for communication and reaching victims: Dating apps/platforms
- Messaging services
- Bank transfers, Western Union, MoneyGram
- Phone calls
- Video calls
- Photographs often found though stock images available online
- Fake websites for shipping fees

Techniques:

- Social engineering

D. Investment Fraud

This type of fraud is characterized by online fraudsters offering various forms of easy earnings, encouraging potential victims to invest in various forms of assets (virtual currencies, products, gold, funds, etc.) with promises of unrealistically high returns. They make unrealistic claims of high returns, but in reality, it is a deceptive scheme to exploit and defraud unsuspecting individuals [6].

In this type of fraud, the fraudsters set up fake websites to create an illusion of legitimacy and lure victims into registering and expressing interest in investment opportunities. These fraudulent websites are instrumental in the social manipulation scheme. The victims often discover these websites through search engines, social media ads, or email solicitations, making these channels tools that enable the scam. Once a victim registers on the fake website, indicating their interest, the fraudsters initiate contact, often posing as financial advisors during phone calls. To conceal their real identity and location, they may use Voice over Internet Protocol (VoIP) calls. In some cases, the fraudsters make initial contact via phone without any prior registration. During the phone calls, the fraudsters skillfully employ social engineering techniques to gain the victim's trust and convince them to invest. They exploit the victim's desire for easy earnings and play upon the allure of unrealistically high returns promised through the investment opportunity. By combining the deceptive website setup, strategic use of communication channels, and effective social engineering tactics, the fraudsters successfully manipulate victims into investing their money, leading to significant financial losses for the unsuspecting individuals. It is crucial for individuals to remain cautious and verify the legitimacy of any investment opportunities encountered online to avoid falling victim to this form of fraud.

In a common scenario of this fraud scheme, the fraudster targets victims with limited computer knowledge and suggests installing remote access software under the guise of assistance. The free version of this software is commonly used to hide the fraudster's IP address during control of the victim's computer. Once the software is installed, the fraudster gains unrestricted access to the victim's computer and guides them to enter payment details for cryptocurrency purchases. If the victim uses online banking, the fraudster tricks them into revealing login credentials, including two-factor authentication details if present. Initially, the investment appears to be directed to a reputable exchange, with funds seemingly under the victim's control. However, in a later stage, the fraudster creates a malicious exchange account and transfers the victim's funds, taking full control. The victim, seeing apparent growth in their "investment," often invests more money. Only later, when attempting to retrieve their money, do they realize they have been scammed. After the victim discovers the deception, the fraudsters may further manipulate them by offering assistance in recovering the lost funds, resulting in additional gains for the scammers.

In summary, this scam preys on victims' lack of computer knowledge, gaining control of their computers through remote access software, and manipulating them into investing money that ultimately ends up in the hands of the fraudsters [7], [8].

Tools:

- Remote access software
- Fake websites – domain hosting
- Ads
- Crypto wallets
- Currency exchange
- Channels/platforms for reaching victims: search engines, social media platforms
- VoIP calls and spoofed phone numbers

Techniques:

- Social engineering

IV. Legal Tools for Investigation and Combating Cyber Fraud Cases/Crimes

In the ever-evolving landscape of digital technology, the rise of cyber fraud cases and crimes has become a pressing concern for individuals, businesses, and governments alike. To effectively combat these sophisticated and elusive threats, the law enforcement and legal communities have been continually developing and refining a diverse array of legal tools. These legal tools for investigation and combating cyber fraud cases/ crimes encompass an array of legislative measures, international cooperation agreements, and advanced forensic techniques. More analytically:

A. Freezing and Confiscating the Assets and Profits of Illicit Activities

Efficient cross-border collaboration is crucial in combating transnational cyber fraud crimes and seizing the tools and profits of illicit activities. Freezing and confiscating the assets involved are powerful measures in tackling such offenses. The existing legal framework in the European Union for mutual recognition of freezing and confiscation orders is outlined in Regulation (EU) 2018/1805, approved by the European Parliament on 14th November 2018. This regulation enables effective cooperation among member states to combat cyber fraud and ensure that criminals cannot benefit from their ill-gotten gains across international borders. Furthermore, in the realm of crime investigation, particularly cases involving financial impact such as cyber fraud and property damage, Law Enforcement Agencies (LEAs) commonly employ a fundamental investigative practice based on the American doctrine "follow the money." This strategy entails uncovering the trail of financial transactions and data to trace illicit activities. Achieving this objective may involve lifting bank or financial secrecy and delving into financial records and transactions. To expedite and streamline the process, LEAs can obtain a written express order from the investigating prosecutor without the need for court intervention or approval from a judicial council. This allows for a more agile and efficient investigation, granting the necessary authority to examine financial data and trace money flows in cases of suspected crimes, bolstering the efforts to combat cyber fraud and other financially-driven offenses [9].

B. Disclosing Information about Malicious Users in EU

Gaining access to electronic evidence for investigations presents a complex and time-consuming challenge, especially due to varying legislations across European Union member states and the physical location of data storage. However, when investigating cases involving electronic evidence like email addresses or internet protocol (IP) addresses within an EU country, data can be collected and transferred from one member state to another by adhering to the guidelines of Directive 2014/41/EU, known as the European Investigation Order (EIO). This directive is the most comprehensive regulation for facilitating cooperation between EU member states, ensuring efficient and swift access to electronic evidence. The investigation process can be further expedited with the introduction of the common European framework for accessing electronic evidence, particularly the E-evidence Regulation. This framework enables law enforcement and judicial authorities to more easily and quickly obtain the electronic evidence they require, streamlining the investigative procedures even further [10].

C. Join Investigation Teams in EU

Another alternative EU investigation tool is the Joint Investigation Teams (JITs). The JITs serve as an advanced tool for international cooperation in criminal matters within the European Union. A JIT is established through a legal agreement between competent authorities of two or more EU member states, aimed at conducting joint criminal investigations. The legal framework for forming JITs between member states is outlined in Article 13 of the 2000 EU Convention on Mutual Assistance in Criminal Matters (2000 EU MLA Convention) and the 2002 Council framework decision on JITs.

Another option for tackling cybercrime is the Joint Cybercrime Action Taskforce (J-CAT) model. J-CAT operates under the European Cybercrime Centre (EC3) of Europol and functions as a group focused on combating cybercrime through collaborative efforts and expertise from multiple member states [11].

D.Disclosing Information about Perpetrators of Cyber Frauds, outside EU

In cyber fraud cases where electronic evidence is located in a third country outside the European Union, EU judicial authorities must follow a formal procedure to request legal assistance from foreign authorities. This process involves submitting requests for mutual legal assistance through instruments like Mutual Legal Assistance Treaty (MLAT), International Letter of Request (ILOR), Letters Rogatory, or Letters of Request, commonly known as "judicial assistance". When a state requests assistance in obtaining evidence located in another state to aid in criminal investigations or proceedings, it is referred to as the "requesting state," while the state from which the assistance is sought is the "requested state." It is important to note that mutual legal assistance is specifically designed for gathering evidence, not intelligence or other types of information. This formal process ensures cooperation and legal validity in cross-border investigations, allowing EU judicial authorities to access crucial evidence located in third countries [12].

V. Suggestions/Proposals to Prevent Cyber Fraud

Ensuring comprehensive protection against cybercrime, including online fraud, demands the implementation of a diverse array of technical and non-technical measures within an organization. These measures encompass everything from personal education to advanced algorithms rooted in machine learning. In this paper, we have curated a list of what we believe to be the most pivotal measures, which are outlined below:

A. Implementation of Necessary Technical and Organizational Security Measures, in Compliance with International Standards

Companies can enhance their resilience against cyber fraudsters by adopting best practices and cybersecurity strategies, as well as all necessary technical and organizational information security measures in compliance with the international standard for Information Security Management Systems (ISMS) in new edition ISO/IEC 27001:2022 [13].

B. Fraud Detection Software

Fraud detection software can be used by banks and financial institutions in order to detect and prevent fraud. For instance, when an individual tries to open bank accounts using stolen identity information, when a user makes unusually cash payments related to its regular business activities plus when unusual IP addresses are observed making transactions to bank's customers. Moreover, when there is a sudden change in transaction limits as well as when the beneficiary’s name is mismatched/misspelled [14].

C.Protection of Against Phishing through Targeted Education and Awareness

By implementing a cybersecurity awareness program and campaign, an organization informs and educates employees about cyber threats they might face. Organizations can start cybersecurity awareness training, including a policy brief, trainings and regular staff meetings sharing information and concerns [15].

D.Prevent Fraud in Enterprises and Digital Banking Using Artificial Intelligence and Machine Learning

Nowadays, traditional methods developed against traditional frauds have become quite inadequate. AI, by using ML algorithms, has efficiently replaced traditional methods of detecting fraudulent transactions. The reasons are twofold:

a) ensure faster and more effective identification of suspicious financial transactions among million users,
b) cost reduction for financial institutions.

AI and ML enable banks' anti-fraud teams to quickly and immediately identify anomalous transactions that fall outside of an individual’s normal behavior, including sudden large deposits or credits to another account. Therefore, AI and ML prevent fraud while minimizing and eliminating the cyber-attacks threatening the banking sector, including password attacks (account takeover), faking identities (identity fraud), digital automated payments (bot attacks), illegally acquired money transferred on behalf of someone else (mule accounts), malicious activities accomplished through interaction (social engineering) and authorized payments (push payments) where fraudsters use techniques to trick the victim to deposit money into their account [16].

VI. The Role of European Legislation in Combating Cybercrime

Recognizing the urgency of the matter, European legislation has embarked on a journey to enhance cybersecurity awareness and protect individuals and businesses from cyber fraud schemes. By continuously adapting to evolving technologies, European legislation has sought to stay one step ahead of cybercriminals. The description of the legal framework used by EU over the years is described analytically below:

- *NIS 1:* The NIS Directive, formally known as the Directive on security of network and information systems (NIS Directive), plays a pivotal role in bolstering cybersecurity across the European Union (EU). Introduced as the NIS1 Directive (EU 2016/1148) in 2016, it stands as the first comprehensive legislation on cybersecurity to be adopted EU-wide. To ensure uniformity and consistency, each EU member state has integrated the directive into its national legislation. Among the primary obligations arising from the NIS1 directive for every member state are as follows:

1. Participation in Cooperation Group and CSIRT Network: Each member state must be actively represented in both the Cooperation Group and the CSIRT (Computer Security Incident Response Team) network. These collaborative entities foster information exchange, coordination, and joint efforts to combat cyber threats collectively.
2. Development of National Strategy: In adherence to the NIS1 directive, every member state must establish a comprehensive national strategy concerning the security of network and information systems. This strategy should delineate strategic objectives and include appropriate policy and regulatory measures aimed at achieving and maintaining a high level of cybersecurity.
3. Designation of National Competent Authorities: Each member state must appoint one or more national competent authorities, referred to as 'competent authorities,' to oversee the security of network and information systems. These authorities must cover, at a minimum, the sectors outlined in Annex II and the services mentioned in Annex III of the directive.
4. Establishment of CSIRTs: The NIS1 directive mandates each member state to designate one or more CSIRTs, which must comply with the requirements outlined in point (1) of Annex I. These CSIRTs are responsible for risk assessment and handling incidents in accordance with a well-defined process. The designated CSIRTs should cover the sectors mentioned in Annex II and the services referred to in Annex III.
5. Implementation of Penalties: Member states are required to define and enforce penalties for violations of national provisions established based on the NIS Directive. These penalties should be effective, proportionate, and dissuasive, ensuring a strong deterrent against non-compliance.
6. Identification of Essential Service Operators: By November 2018, member states must identify the operators of essential services operating within their territories. This identification aids in understanding the critical sectors that require heightened protection against cyber threats.
7. Submission of Summary Reports: Starting from August 2018, and subsequently on an annual basis, member states must provide a summary report on the notifications received to the Cooperation Group. The report should encompass details such as the number of notifications, the nature of the incidents reported, and the measures taken as per Articles 10, 14, and 16 of the NIS Directive.

The NIS1 directive serves as a landmark initiative in enhancing cybersecurity measures across the European Union. Its comprehensive and coordinated approach ensures that all member states are well-equipped to face the evolving challenges posed by cyber threats. By enforcing the directive's provisions, the EU strives to safeguard its critical infrastructure and digital ecosystem, promoting a secure and resilient cyber environment for its citizens, businesses, and institutions alike [17].

- *NIS 2:* In December 2021, the European Commission took a significant step in bolstering cybersecurity across the European Union by adopting a proposal for the revised Directive on Security and Information Systems - the NIS2 Directive. This proposal aims to rectify the shortcomings of its predecessor, the NIS1 Directive, by introducing several key elements that reinforce the EU's cybersecurity landscape. The main features of the NIS2 Directive include:

1. Broadening Scope and Size Cap: The NIS2 Directive seeks to encompass additional sectors critical to the economy and society. Notably, it introduces a size cap, meaning that all medium and large companies operating within the selected sectors will be included in the regulatory framework.
2. Unified Classification of Entities: The distinction between operators of essential services and digital service providers, as present in the NIS1 Directive, is eliminated in the NIS2 proposal. Instead, entities will be categorized based on their importance, divided into essential and important categories, subjecting them to different supervisory regimes as deemed necessary.
3. Strengthening Security Requirements: The NIS2 proposal mandates companies to adopt a risk management approach, emphasizing the implementation of a minimum list of basic security elements. This step ensures a higher level of cybersecurity readiness across various organizations. Additionally, the proposal outlines more specific provisions regarding the incident reporting process, the content of reports, and timelines for reporting.
4. Securing Supply Chains and Supplier Relationships: Recognizing the importance of secure supply chains, the NIS2 Directive requires individual companies to address cybersecurity risks within their supply chains and supplier

Open Science Index, Computer and Information Engineering Vol:18, No:4, 2024 publications.waset.org/10013594.pdf

relationships. On a broader scale, the proposal strengthens supply chain cybersecurity for key information and communication technologies at the European level. To achieve this, Member States, in collaboration with the European Commission and the European Union Agency for Cybersecurity (ENISA), will conduct coordinated risk assessments of critical supply chains.

5. Stricter Supervisory Measures and Harmonized Sanctions: The NIS2 Directive introduces more rigorous supervisory measures for national authorities and imposes stricter enforcement requirements. Furthermore, it aims to harmonize sanctions regimes across EU Member States, ensuring consistency in cybersecurity penalties and enhancing overall cybersecurity accountability.
6. Empowering the Cooperation Group: The NIS2 proposal seeks to enhance the role of the Cooperation Group in shaping strategic policy decisions concerning emerging technologies and new trends in cybersecurity. The proposal promotes information sharing and cooperation among Member State authorities, including improved operational collaboration for effective cyber crisis management.
7. Coordinated Vulnerability Disclosure Framework: The NIS2 Directive establishes a basic framework for coordinated vulnerability disclosure, wherein responsible key actors are designated to report newly discovered vulnerabilities across the EU. Additionally, an EU registry will be established and operated by the European Union Agency for Cybersecurity (ENISA) to facilitate vulnerability disclosure.

The NIS2 Directive represents a significant leap forward in enhancing the EU's cybersecurity preparedness. By addressing the deficiencies observed in the NIS1 Directive and introducing a comprehensive set of measures, the EU aims to create a more secure and resilient digital landscape, safeguarding critical infrastructures, businesses, and citizens from evolving cyber threats [18].

- *2022/2555 Directive:* In December 2022, the European Commission took a significant step in enhancing cybersecurity across the European Union by adopting a proposal for the revised Directive on Security and Information Systems - the 2022/2555 Directive. This new Directive sets more rigorous standards in cybersecurity for both enterprises and the public sector, holding executives of companies and enterprises accountable in case of noncompliance. The 2022/2555 Directive encompasses several key elements aimed at fortifying the EU's cyber resilience. The main features of the 2022/2555 Directive include:

1. National Cybersecurity Strategies and Designation of Authorities: Member States are mandated to adopt national cybersecurity strategies to outline comprehensive approaches to safeguarding their digital environments. Additionally, 2022/2555 Directive obligate member states to create authorities dedicated to fields like cyber crisis management and computer incident response teams (CSIRTs) [19].
2. Cybersecurity Measures for Critical Sectors: The 2022/2555 Directive introduces cybersecurity risk-management measures and reporting obligations for entities operating in critical sectors. This includes sectors dealing with energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructures, ICT service management, public administration, space, postal and courier services, waste management, manufacture-production, and distribution of chemicals, production-processing, and distribution of food, manufacturing, digital providers, research, and entities identified as critical under Directive (EU) 2022/2557. By imposing specific cybersecurity standards on these sectors, the EU aims to protect vital services and infrastructure from cyber threats.
3. Cybersecurity Information Sharing: The 2022/2555 Directive establishes rules and obligations on cybersecurity information sharing. This encourages the exchange of relevant cybersecurity information among entities and stakeholders, fostering a collaborative and proactive approach to cybersecurity.
4. Supervisory and Enforcement Obligations: The new Directive imposes supervisory and enforcement obligations on Member States to ensure compliance with the cybersecurity standards set forth in the directive. This includes monitoring and overseeing the implementation of national cybersecurity strategies, reporting mechanisms, and the establishment of competent authorities and CSIRTs.
5. European Cyber Crisis Liaison Organization Network (EU-CyCLONe): The 2022/2555 Directive establishes the EU-CyCLONe to facilitate the coordinated management of large-scale cybersecurity incidents and crises at the operational level. This organization also serves as a platform for the regular exchange of relevant cybersecurity information among Member States, Union institutions, bodies, offices, and agencies, fostering a collective response to cyber threats.
6. Imposing Administrative Fines: The directive outlines the general conditions for imposing administrative fines on essential and important entities. This measure ensures that entities operating in critical sectors adhere to cybersecurity standards, with financial penalties serving as a deterrent against noncompliance.

Overall, the 2022/2555 Directive marks a significant advancement in the EU's efforts to enhance cybersecurity resilience. By setting higher standards, promoting information sharing, and holding entities accountable for cybersecurity measures, the EU aims to create a safer and more secure digital environment for its citizens, businesses, and critical infrastructure [20].

- *Advantages and Innovations of European Legislation:* The European legislation takes a comprehensive approach to cybersecurity, aiming not only to enforce legal requirements but also to cultivate a culture of proactive risk mitigation. One of the key aspects of this approach is prioritizing user education, which plays a pivotal role in equipping both businesses and individuals with the knowledge and skills necessary to identify and counter cyber threats effectively.

By emphasizing user education, the European legislation acknowledges that cybersecurity is a collective responsibility. It recognizes that individuals and organizations must work together to safeguard digital environments against ever-evolving cyber threats. Proactive risk mitigation involves not only implementing technical safeguards but also empowering users with the understanding of potential risks and best practices to avoid falling victim to cyber-attacks.

The legislation's focus on user education has several crucial benefits. Firstly, it enhances overall cybersecurity awareness among the general population. When people are informed about common cyber threats, phishing scams, and social engineering tactics, they are less likely to become unwitting victims. Empowering users with cybersecurity knowledge creates a more resilient digital society.

Secondly, businesses and organizations benefit significantly from user education. Cybersecurity incidents often occur due to human error or lack of awareness. By educating employees and users about cybersecurity best practices, companies can reduce the likelihood of data breaches and other security incidents. This not only protects sensitive information but also preserves the organization's reputation and financial well-being.

Moreover, user education fosters a proactive approach to cybersecurity. Rather than solely relying on reactive measures to deal with cyber incidents after they occur, informed users are more likely to take preventive actions and report suspicious activities promptly. This proactive stance can thwart potential attacks or minimize their impact, saving valuable time, resources, and costs.

To implement effective user education, the European legislation may encourage partnerships between governments, private sector entities, and educational institutions. Collaborative efforts can help develop comprehensive cybersecurity training programs that reach a broader audience, including schools, universities, businesses, and non-profit organizations.

In conclusion, the European legislation's emphasis on user education demonstrates a forward-thinking and inclusive approach to cybersecurity. By fostering a culture of cybersecurity awareness and proactive risk mitigation, the EU aims to create a safer and more resilient digital ecosystem for its citizens and businesses. Educating users empowers them to become active participants in safeguarding their online presence and contributes to the overall cybersecurity posture of the region. This holistic approach recognizes the interdependence between individuals and organizations in the fight against cyber threats and lays the groundwork for a more secure and interconnected future.

- *Potential Vulnerabilities and Recommended Improvements:* The European legislation on cybercrime has come a long way in addressing the growing challenges posed by digital threats. However, like any complex legal framework, it is not without its potential flaws and areas that could benefit from improvement. In this analysis, we will explore some of these potential flaws and propose suggestions to enhance the effectiveness of European cybercrime legislation.

1. *Lack of Harmonization:* One significant challenge in the European Union is the lack of harmonization among member states' cybercrime laws. While various directives and regulations exist, there are still inconsistencies in how countries interpret and apply these laws. This can create confusion for businesses and individuals operating across borders and may hinder seamless cooperation in cybercrime investigations.

– *Suggestion:* To improve harmonization, the European Union should continue its efforts to streamline cybercrime laws across member states. This could involve more robust cooperation between national law enforcement agencies and the establishment of a central authority responsible for coordinating cross-border cybercrime investigations.

2. *Jurisdictional Challenges:* With cybercrime often transcending national boundaries, determining jurisdiction can be a significant challenge. Criminals can exploit loopholes and jurisdictional gaps to evade prosecution, making it difficult to hold them accountable.

– *Suggestion:* The EU should work towards creating clearer guidelines on jurisdiction for cybercrimes that span multiple countries. Additionally, enhancing international cooperation and extradition treaties can help ensure cybercriminals are not immune to prosecution.

3. *Fast-paced Technological Advancements:* The rapid evolution of technology poses a constant challenge for legislation to keep up. New cyber threats emerge regularly, and traditional legal frameworks may struggle to adapt quickly enough to address these emerging challenges adequately.

– *Suggestion:* The EU should implement mechanisms to facilitate ongoing reviews and updates of cybercrime legislation to keep pace with technological advancements. Establishing a dedicated body to monitor cybersecurity trends and propose necessary legal adjustments could help ensure the legislation remains relevant and effective.

4. *Data Protection and Privacy Concerns:* While robust cybercrime legislation is essential, it must also strike a balance with data protection and privacy concerns. Some provisions may inadvertently encroach on individuals' rights to privacy and data security.

– *Suggestion:* European legislation should be crafted with a strong emphasis on safeguarding individuals' privacy rights. Implementing robust data protection measures and ensuring proper oversight and accountability in the collection and use of personal data will help strike the right balance between cybersecurity and privacy.

5. *Insufficient Collaboration with the Private Sector:* The private sector plays a crucial role in combating cybercrime, as businesses are often the primary targets of attacks. However, there may be inadequate collaboration between the public and private sectors, hindering the exchange of threat intelligence and best practices.

– *Suggestion:* Encouraging stronger public-private partnerships is vital for effective cybercrime prevention. The EU can incentivize information sharing between law enforcement and private companies and establish frameworks for coordinated incident response and threat intelligence sharing.

6. *Cybercrime Training and Awareness:* Despite having robust legislation, the overall effectiveness of cybersecurity measures can be limited if end-users lack awareness and training on cyber threats. Cybercriminals often exploit human vulnerabilities through social engineering and phishing attacks.

– *Suggestion:* The EU should invest in public awareness campaigns and cybersecurity training initiatives targeted at businesses, schools, and individuals. By educating the public about common cyber threats and best practices for online safety, the EU can create a more resilient cyber-aware society.

7. *Lack of Standardization in Reporting:* There may be inconsistencies in reporting cyber incidents across member states, which can hinder comprehensive data analysis and response efforts.

– *Suggestion:* The EU should establish standardized reporting requirements for cyber incidents to facilitate data sharing and analysis. This will enable better understanding of cybercrime trends and facilitate more effective policy responses.

In conclusion, while the European legislation on cybercrime has made significant progress in addressing digital threats, there are still potential flaws that need to be addressed. By focusing on harmonization, jurisdictional challenges, adapting to technological advancements, privacy concerns, collaboration with the private sector, cybercrime training and awareness, and standardization in reporting, the EU can strengthen its cybercrime legislation and better protect its citizens and businesses from the ever-evolving cyber threats in the digital age. Continuous efforts to improve the legislative framework will be crucial in ensuring a safer and more secure cyber environment for the European Union.

VII. Conclusions

As cyber fraud schemes continue to evolve and pose significant risks to individuals and businesses worldwide, this paper emphasizes the critical importance of understanding these schemes' intricacies. By exploring the modus operandi, tools, and techniques used by cybercriminals, and acknowledging the role of European legislation, this study seeks to foster a safer digital landscape and empower all stakeholders to combat cyber fraud effectively. Proactive measures, improved legislation, and heightened cybersecurity awareness collectively form the foundation for a resilient defense against cyber threats.

In the first part of this work, a comprehensive analysis of various cyber fraud schemes such as BEC attacks, investment fraud, romance scams, and online sales fraud was provided. Through a detailed analysis of cybercriminal strategies, it shed light on their deceptive tactics, aiding in the recognition and prevention of potential threats. Essential defense strategies were also analyzed, like cybersecurity awareness training and advanced technical controls, empowering individuals and businesses to protect against cyber fraud effectively.

In the second part of this work, we demonstrated how the European legislation tries to cope with the ever-growing threats in the digital landscape. EU legislation has paved the way for cross-border cooperation, harmonization of cybersecurity laws, and the establishment of robust measures to protect citizens, businesses, and critical infrastructure. The legislation's emphasis on user education, public-private partnerships, and data protection demonstrates a proactive approach to creating a safer cyber environment.

However, it is not without its flaws. The lack of harmonization among member states' cybercrime laws, jurisdictional challenges, and the rapid pace of technological advancements present challenges that must be addressed. Additionally, striking a balance between cybersecurity and privacy concerns is vital to safeguarding individuals' rights. By acknowledging and rectifying these flaws, the European legislation can further strengthen its effectiveness, foster greater collaboration, and continuously adapt to evolving cyber threats, ensuring a safer and more secure digital future for the European Union.

Acknowledgments

We acknowledge support of this work from the project “Immersive Virtual, Augmented and Mixed Reality Center of Epirus” (MIS 5047221) which is implemented under the Action “Reinforcement of the Research and Innovation Infrastructure”, funded by the Operational Programme “Competitiveness, Entrepreneurship and Innovation” (NSRF 2014-2020) and co-financed by Greece and the European Union (European Regional Development Fund).

References

[1] Europol, "Internet Organized Crime Assessment (IOCTA)", 2023, Retrieved August 2, 2023, from https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN.pdf

[2] Al-Musib, Norah, Al-Serhani, Faeiz, Humayun, Mamoona, Jhanjhi, Noor. "Business email compromise (BEC) attacks." Materials Today: Proceedings, vol. 81, 2021, pp. 647. doi: 10.1016/j.matpr.2021.03.647.

[3] Arumugam, Nalini, Mohamad, Faizah, Shanthi, Alice, Dharinee, Sai. "A Study on Online Shopping Scams." International Journal of Social Science Research, vol. 10, 2021, pp. 22. doi: 10.5296/ijssr.v10i1.19290.

[4] Nomleni, Kristin. "Analysis of The Romance Scam Phenomenon in Interpersonal Communication Love Scammers and Victims."Volume 12, 2023, pp. 202-221. doi: 10.35508/jikom.v12i2.9179.

[5] Nomleni, Kristin. (2023). Analysis of The Romance Scam Phenomenon in Interpersonal Communication Love Scammers and Victims. 12. 202-221. 10.35508/jikom.v12i2.9179.

[6] Eurojust. "Eurojust Guidelines on How to Prosecute Investment Fraud.", July 2021, Retrieved August 1, 2023, from https://www.eurojust.europa.eu/sites/default/files/assets/eurojust_guidelines_how_to_prosecute_fraud_07_2021.pdf

[7] Marguerite Deliema and others. "Profiling Victims of Investment Fraud: Mindsets and Risky Behaviors." Journal of Consumer Research, vol. 46, issue 5, February 2020, pp. 904–914.

[8] Fadhil, Hassan. "Social engineering attacks techniques." International Journal of Management Science and Engineering Management, 2023, vol. 3, pp.18-20.

[9] Brandão, Nuno. "The right of defence under Regulation (EU) 2018/1805 on the mutual recognition of freezing orders and confiscation orders." New Journal of European Criminal Law, vol. 13, 2022, pp. 203228442210843. doi: 10.1177/20322844221084334.

[10] Olber, Paweł. "The European Investigation Order as a mechanism for international cooperation in criminal cases to combat cybercrime."

Przegląd Policyjny, vol. 137, 2019, pp. 174-187. doi: 10.5604/01.3001.0014.2406.

[11] Geraci, Rosa. "Beyond mutual recognition: the rules of joint investigation teams." Optime, vol. 13, 2022, pp. 29-40. doi: 10.55312/op.v13i2.378.

[12] James, Joshua I & Gladyshev, Pavel. (2016). A survey of mutual legal assistance involving digital evidence. Digital Investigation. 18. 10.1016/j.diin.2016.06.004.

[13] Cruz, Mario & Laguna, Jessica & Huillcen, Herwin & Vargas, Edgar & Valdivia, Flor. (2021). Implementation of an Information Security Management System Based on the ISO/IEC 27001: 2013 Standard for the Information Technology Division. 10.1007/978-3-030-63665-4_21.

[14] Sarma, Dhiman & Hossain, Sohrab & Alam, Wahidul. (2020). Bank Fraud Detection using Community Detection Algorithm. 10.1109/ICIRCA48905.2020.9182954.

[15] Aldawood, Hussain, Skinner, Geoff. "Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review." doi: 10.1109/TALE.2018.8615162.

[16] Srokosz, Michal, Bobyk, Andrzej, Ksiezopolski, Bogdan, Wydra, Michał. "Machine-Learning-Based Scoring System for Antifraud CISIRTs in Banking Environment." Electronics, vol. 12, 2023, pp. 251. doi: 10.3390/electronics12010251

[17] Carvalho, J.a.V.; Carvalho, S.; Rocha, A. European Strategy and Legislation for Cybersecurity: Implications for Portugal. Cluster 1060 Computing 2020, 23, 1845–1854. https://doi.org/10.1007/s10586-020-03052-y

[18] European Parliament, Cybersecurity in the EU: Overview of challenges and state of play, 2021, Retrieved August 3, 2023, from https://www.europarl.europa.eu/RegData/etudes/BRIE/20 107021/689333/EPRS_BRI(2021)689333_EN.pdf

[19] NIS 2: A new directive to strengthen cybersecurity measures in the EU, Retrieved August 14, 2023, from https://strike.sh/blog/NIS2-Directive-Cybersecurity

[20] Parliament, E. Directive (EU) 2022/2555 of the European Parliament and of the Council of 21 March 2022 laying down measures 1074for a high common level of cybersecurity across the Union. Official Journal of the European Union 2022, pp. 1–87

Open Science Index, Computer and Information Engineering Vol:18, No:4, 2024 publications.waset.org/10013594.pdf