

## Financial Fraud in the Era of Digital Transformation

### الاحتيال المالي في ظل التحول الرقمي

Farah Aicha

University of Algiers 1, Faculty of Law

a.fareh@univ-alger.dz

Date of submission:04/04/2025 Date of final acceptance:13/07/2025 Date of publication :September

#### Abstract :

Financial fraud constitutes a serious economic offense, exacerbated by the increasing digitalization and the rapid expansion of financial technologies. This crime encompasses various schemes, including phishing, cryptojacking, and fraudulent initial coin offerings (ICOs). These deceptive practices present complex challenges, prompting jurisdictions to adopt legal frameworks such as the General Data Protection Regulation (GDPR) in Europe, the Computer Fraud and Abuse Act (CFAA) in the United States, and the Budapest Convention. Additionally, Interpol and Europol play a critical role in facilitating international cooperation, enabling cross-border enforcement against cyber-enabled financial fraud.

**Keywords:** Financial Fraud, Phishing, Cryptojacking, Cybersecurity, Data Protection.

ملخص:

يشكل الاحتيال المالي جريمة اقتصادية خطيرة في ظل التحول الرقمي وتطور التكنولوجيا المالية. وهو يشمل عدة أساليب مثل التصيد الاحتيالي، والمخططات الاحتيالية المتعلقة بالعملات الرقمية كالتعدين الخفي وعمليات الطرح الأولى للعملات الرقمية الوهمية، وغيرها من الأساليب الأخرى التي تشكل تحديات استجابت لها الدول بوضع أطر قانونية، مثل اللائحة العامة لحماية البيانات (GDPR) في أوروبا، وقانون الاحتيال وإساءة استخدام الحاسوب (CFAA) في الولايات المتحدة، واتفاقية بودابست ووكالات مثل الإنتربول ويوروبول لمكافحة الاحتيال الإلكتروني عبر الحدود.

**الكلمات المفتاحية:** الاحتيال المالي، التصيد الاحتيالي، تعدين العملات المشفرة غير المشروع، الأمن السيبراني.

Auteurcorrespondant : Farah Aicha

## Introduction

Financial fraud is increasingly recognized as a grave economic crime that significantly undermines national economies. Its repercussions are profoundly detrimental, affecting individual and institutional integrity as well as overall economic stability. Moreover, in an era marked by rapid technological progress and widespread d

igital adoption, the risk associated with financial fraud has escalated, further complicated by the pervasive use of electronic payment methods and the advent of fintech innovations.

Consequently, “financial fraud” now encompasses a broad range of deceptive practices aimed at securing unlawful financial advantages. In essence, it involves any attempt to circumvent or manipulate financial systems to derive illegal profits. These practices include, but are not limited to, falsifying financial records, disseminating misleading information, and directly deceiving stakeholders for illicit gains.

For clarity, the U.S. Securities and Exchange Commission (SEC) categorizes financial fraud as any activity that manipulates financial data to mislead investors or regulatory authorities, including altering figures or crafting spurious reports.<sup>1</sup>

Similarly, the American Institute of Certified Public Accountants (AICPA) defines it as intentional malfeasance by individuals or groups intended to secure personal financial benefits through fraudulent means, such as manipulation or outright deception<sup>2</sup>.

The World Bank, in turn, describes financial fraud as any conduct involving unlawful or deceptive practices to evade financial obligations or illegally acquire assets<sup>3</sup>. On a broader scale, financial fraud is a scheme that employs deceit or falsehoods to secure financial benefits at the expense of another party<sup>4</sup>. It is evident that with technological advancements and the inevitable digitalization of critical sectors—particularly finance—the modalities of financial fraud have evolved, becoming more sophisticated and interconnected with digital methodologies, thereby amplifying its potential impact on both individual and institutional levels.

The adverse effects of financial fraud are manifold, affecting individuals through significant financial loss and extending to broader economic consequences such as eroding trust in financial institutions, triggering corporate bankruptcies, and tarnishing business reputations. Furthermore, at the macroeconomic level, fraudulent activities can inflict substantial fiscal losses, precipitate economic downturns, and degrade public confidence in the financial system.

The evolution of financial fraud has kept pace with technological innovations, leading to the emergence of a novel form known as cyber financial fraud. This development poses one of the most pressing challenges for contemporary

technological governance, necessitating robust legal frameworks and rigorous enforcement mechanisms to mitigate its pervasive threats.

The pervasive spread of financial fraud is largely driven by unchecked greed, prompting individuals to exploit technological advancements for illicit financial schemes. This raises a fundamental question: **To what extent have contemporary national and international legal and regulatory frameworks proven effective in addressing the evolving forms of cyber-enabled financial fraud in the digital era?**

This study adopts a descriptive and analytical methodology grounded in comparative legal analysis. It begins by identifying and categorizing the most prevalent forms of digital financial fraud (namely phishing and cryptocurrency-based schemes) by examining how these operate in practice and why they have proliferated. In the second phase, the study evaluates national and international legal responses through a comparative lens, focusing on selected Arab, European, and American legal systems. Doctrinal sources, statutory texts, and international conventions are critically assessed, alongside reports from global enforcement agencies, to determine the strengths and limitations of existing legal frameworks.

To provide a comprehensive analysis, this study is structured into two main sections. The first section examines the primary typologies of financial fraud in the digital age, exploring the evolving tactics employed by perpetrators to circumvent regulatory controls. The second section assesses the measures adopted at both domestic and international levels to combat financial fraud, evaluating the efficacy of legislative instruments, regulatory enforcement, and cross-border cooperation in addressing the growing sophistication of digital fraud schemes.

## **Section One: The Evolution of Financial Fraud Techniques in the Digital Age**

Financial fraud manifests in various forms, all ultimately serving the same objective: illicit financial gain, either through direct monetary theft or by unlawfully acquiring sensitive information that facilitates financial exploitation. In the era of digital transformation, fraud schemes have become increasingly sophisticated, leveraging technological advancements to deceive victims more effectively. Among the most prevalent forms of digital financial fraud are phishing schemes (Subsection One) and fraud related to digital assets (Subsection Two).

### **A) Financial Fraud Through Phishing**

Phishing—referred to in French as *hameçonnage*—constitutes a well-documented cybercrime technique designed to illicitly obtain confidential data by masquerading as a legitimate entity. This fraudulent practice exploits digital communication channels such as email, text messaging, and counterfeit websites to manipulate victims into disclosing sensitive credentials, including login details, credit card information, and other personally identifiable data. The success of phishing

hinges on the perpetrator's ability to convincingly imitate trustworthy sources, thereby circumventing traditional security measures<sup>5</sup>.

The execution of phishing fraud unfolds in three distinct stages (2) and relies on various strategies (1).

### **1- Stages of Phishing**

Phishing fraud, an increasingly prevalent form of cybercrime, unfolds through a three-stage process. Initially, the fraudster establishes trust with the target through emotionally charged communications that skillfully mimic legitimate institutions. Once trust is gained, the victim is directed to a counterfeit platform that mirrors authentic online services. The final stage involves the victim unknowingly submitting personal and financial details, which the fraudster then exploits to access financial accounts.

#### **1.1. Initial Attack Phase**

Phishing fraud begins with an orchestrated deception, wherein the perpetrator sends an email or message that appears to originate from a reputable entity, such as a financial institution, government agency, or multinational corporation. This initial contact is carefully crafted to manipulate the recipient's emotions—typically by instilling a sense of urgency, fear, or false opportunity—to coerce compliance. Fraudsters rely on sophisticated social engineering techniques, exploiting psychological vulnerabilities to induce the victim into disclosing confidential data or granting access to their financial assets.

A particularly effective method of deception involves corporate impersonation, where fraudsters unlawfully appropriate the name, logo, and branding of a well-established institution, such as a commercial bank or regulatory authority. By creating communications that closely resemble official correspondence, cybercriminals deceive victims into believing they are interacting with a legitimate entity. Given that high-profile financial and governmental institutions are generally perceived as credible and secure, many victims fail to recognize the fraudulent nature of these communications, unwittingly providing sensitive information.

#### **1.2. Redirection to a Fraudulent Digital Platform**

Once trust has been established, the victim is directed to a counterfeit website via an embedded link in the fraudulent message. These deceptive platforms are engineered to replicate the user interfaces of legitimate websites, often incorporating authentic design elements, domain structures, and login functionalities to enhance their credibility. Victims, believing they are accessing an official online portal, are prompted to enter personal credentials such as banking login details, credit card information, or multi-factor authentication codes.

### 1.3. Data Harvesting

The final phase involves the unauthorized exfiltration of the victim's data. Once submitted, the compromised credentials are immediately transmitted to cybercriminal networks, where they may be used for direct financial theft including credit card fraud, and even cryptocurrency-based fraud.

## 2- Phishing Techniques

Phishing insidious success relies on deceptive communications that meticulously emulate trustworthy sources. This exploitation is predominantly orchestrated by entities masquerading as reputable institutions such as banks or major corporations, which solicit personal information under the pretense of service verification or security enhancements. Such requests are carefully crafted to create an illusion of legitimacy, compelling individuals to disclose sensitive data. Once acquired, this data facilitates unauthorized access to banking accounts and digital identities, catalyzing a spectrum of fraudulent activities, including illicit financial transactions and identity theft.

The sophistication of phishing scams has advanced significantly, keeping pace with technological advancements and continually challenging existing cybersecurity measures. These methods include<sup>6</sup>:

- **DNS Spoofing:** This involves altering the domain name system settings to redirect users to counterfeit websites, where cybercriminals harvest personal credentials.
- **Content Injection:** Here, attackers insert malicious scripts into legitimate websites, creating fake login prompts to steal user data.
- **Man-in-the-Middle Attacks(MITM):** These occur when attackers intercept and manipulate data transmitted between two parties without their knowledge, often in real-time.
- **Obfuscation Techniques:** Using complex coding to mask malicious URLs, attackers make them appear harmless to unsuspecting users and even sophisticated security systems.
- **Malware Phishing:** By covertly installing spyware or key loggers, attackers gain prolonged access to a victim's personal and financial information.
- **Search Engine Phishing:** Fraudsters manipulate search engine algorithms to boost the ranking of phishing sites, misleading users into believing these are legitimate.
- **Popup Phishing:** These attacks involve sudden, unsolicited popups that deceive users into entering personal information under the guise of security checks or software updates.

- **Fake Address Bar Displays:** Cybercriminals manipulate browser interfaces to show legitimate URLs while directing users to fraudulent sites.<sup>7</sup>

## **B) Financial Fraud Involving Cryptographic Assets**

The digitization of financial transactions has precipitated the advent of what are popularly known as virtual currencies or cryptocurrencies. This emerging domain has become fertile ground for distinctive forms of financial fraud, notably cryptojacking (1) and deceptive initial coin offerings (ICOs) (2).

### **1- Cryptojacking**

Cryptojacking represents a sophisticated type of financial cyber fraud. In this scheme, the fraudster covertly uses a victim's computing resources to mine cryptocurrency without their consent. This deceit begins with the victim being duped into clicking a seemingly benign link that activates a malicious script. This script then commandeers the computing power of the victim's device to mine crypto currency, surreptitiously depleting the device's resources and electricity. As a result, the unwitting victim bears the hidden costs of both the electrical<sup>8</sup> and computational resources exploited in the mining process, often without any indication of the ongoing deceit until the device's performance deteriorates or energy bills surge.

### **2- Fraudulent Initial Coin Offerings (ICOs)**

The rapid development of initial coin offerings (ICOs) has created an attractive environment for fraudsters, who launch fraudulent projects under the guise of legitimate cryptocurrency ventures. In reality, many ICOs have been revealed to be outright scams<sup>9</sup>. As with all financial fraud schemes, the first stage of an ICO scam involves gaining the victim's trust.

## **Section Two: National and International Responses to Electronic Financial Fraud**

Given the profound implications of electronic financial fraud on both national economies and individual security, a significant number of countries have fortified their legal frameworks with robust statutes aimed at mitigating this pervasive criminal phenomenon (A). The inherently global nature of electronic financial fraud, propelled by the digitization of financial transactions and reliance on cutting-edge communication and internet technologies, necessitates a paradigm of transnational legal cooperation to effectively address these challenges (B).

### **A- National Strategies to Counter Electronic Financial Fraud**

Around the world, jurisdictions have been proactive in crafting and implementing comprehensive legislation specifically designed to combat the multifaceted aspects of electronic financial fraud. These laws typically extend beyond traditional fraud

prohibitions, addressing contemporary threats such as unauthorized access to computer systems, identity theft, online fraud, and the distribution of malware.

In a bid to deter such crimes, legal systems globally have introduced stringent penalties, encompassing both severe criminal liabilities and punitive fines. This subsection will explore seminal legislations from various legal traditions—Arab, European, and American—that have been pivotal in shaping the defenses against the electronic manipulation of financial systems.

## **1- Arab Legal Frameworks on Electronic Financial Fraud**

The Arab world currently lacks specific codifications that address electronic financial fraud within its legislative corpus, which necessitates a thorough examination of the general fraud provisions in existing penal codes to assess their applicability to the digital sphere. This gap in the law raises significant questions regarding the classification of electronic financial fraud as a distinct category within the broader spectrum of cybercrimes.

### **1.1. Penal Code Provisions**

Although the Algerian legislator has not delineated a discrete offense for fraud within its penal code, it has articulated the constituent acts and attendant circumstances that comprise such conduct. Article 372 specifies that:<sup>10</sup>

“Any person who, through deceit, obtains or attempts to obtain money, movable or immovable property, securities, financial documents, releases from obligations, or any other benefits, and does so with the intent of depriving another of their assets—whether partially or wholly—utilizing false or fictitious names, misrepresenting financial credentials, or creating false expectations of gain or fear of loss through imaginary events or circumstances, shall be subject to criminal penalties.”

The Algerian legislative framework, as articulated in its Penal Code, characterizes financial fraud in broad strokes<sup>11</sup>, encompassing traditional constructs of fraud that include the unlawful acquisition of money, movable property, securities, financial documents, and various other contractual obligations.

Notably, the law delineates the acts constitutive of fraud, such as obtaining assets under false pretenses or through the deployment of deceitful tactics.

However, this statutory language conspicuously omits specific references to information or personal data as objects of fraud, a gap that beckons scholarly scrutiny and judicial interpretation.

This lacuna in the legislative text prompts a critical question of whether the scope of the fraud provisions can be judicially interpreted or legislatively

amended to include digital information and data as potential subjects of fraudulent acts

Similarly, the Lebanese Penal Code addresses fraud under Article 655, as amended by Legislative Decree No. 112 dated December 16, 1983, which states:

Any person who, through fraudulent maneuvers, deceives another into handing over movable or immovable property, securities, or any document containing a commitment or release, and appropriates such property, shall be punished with imprisonment from six months to three years and a fine ranging from 100,000 to 1,000,000 Lebanese pounds.

fraudulent maneuvers include:

- Conduct that misleads the victim about the existence of a non-existent venture or instills unwarranted fear of prospective harm.
- The creation of fabrications that the victim accepts as true, often reinforced by the endorsement of a third party, regardless of whether the third-party acts in good faith or as a result of circumstances manipulated by the perpetrator.
- Unauthorized control over movable or immovable assets by individuals lacking the legal right or authority, or misuse of such authority by rightful holders to extort financial benefits.
- The adoption of a pseudonym or false attributes to deceive or influence the victim. The same penalties apply to attempted acts of fraud.

A significant jurisprudential debate has emerged regarding whether the fraudulent acquisition of information—without the physical transfer of tangible assets—can be classified as financial fraud. Traditional penal codes do not explicitly criminalize the misappropriation of data, leading to divergent interpretations among legal scholars.

In France, one school of thought advocates for an expansive interpretation of financial fraud, arguing that fraudulently obtaining information should be equated with the unlawful acquisition of financial assets<sup>12</sup>. Conversely, a more restrictive legal perspective contends that fraud, by its classical definition, requires a transfer of a tangible asset or the voluntary surrender of financial resources by the victim.

According to this interpretation, the intangible<sup>13</sup> nature of information precludes its classification as an object of fraud, since the legal concept of delivery necessitates a material exchange. Acknowledging the evolving nature of financial crime, the French legislature revised its penal code to address this issue. The new Article 313(1)<sup>14</sup> adopted a broader legal formulation, replacing the exclusive enumeration of assets with the phrase "or any property".

Against this backdrop, it is incumbent upon Arab legislators to account for the unique attributes of electronic financial fraud, which often entails the appropriation of digital information and data—a concept that does not align with conventional notions of tangible documents. Legislative initiatives must therefore incorporate provisions specifically tailored to the challenges posed by the digital age, while avoiding an unwarranted expansion of the classical legal definitions underpinning criminal law<sup>15</sup>.

Saudi Arabia has taken a proactive approach by enacting a dedicated legal regime for financial fraud and breach of trust, which came into effect on April 22, 2021. Article 1 of the Saudi Law on Financial Fraud and Breach of Trust establishes severe penalties for fraudulent financial conduct, stipulating:

Anyone who unlawfully appropriates another's property through fraudulent means—including deception, misrepresentation, or misleading inducement—shall be subject to imprisonment for up to seven years and a fine not exceeding five million Saudi riyals, or one of these penalties.<sup>16</sup>

## 1.2. Cybercrime Legislations

Many legal systems now regulate technology-driven offenses, including hacking, phishing, and online fraud, under cybercrime statutes. These laws establish criminal liability for individuals who engage in fraudulent financial activities through digital platforms, prescribing penalties commensurate with the gravity of the offense.

In Algerian legislative discourse, Law No. 09-04, enacted on August 5, 2009, addresses the prevention and mitigation of crimes associated with information and communication technologies<sup>17</sup>. This pivotal statute serves as a cornerstone in Algeria's efforts to combat cybercrime, with a pronounced focus on safeguarding computer systems and personal data against fraudulent schemes, notably phishing.

Law No. 09-04 establishes comprehensive procedural guidelines designed to enhance the efficacy of cybercrime countermeasures. This is complemented by Executive Decree No. 15-261, issued on October 8, 2015, which delineates the structure, organization, and operational directives of the National Authority for the Prevention of Crimes Related to Information and Communication Technologies. The regulatory framework for this authority was further refined under Presidential Decree No. 20-183, dated July 13, 2020<sup>18</sup>.

## 2- European Legislative Frameworks

At the European level, pivotal legislations like the General Data Protection Regulation (GDPR) and the Directive on Security of Network and Information Systems (NIS Directive) form the bulwark against electronic financial fraud.

- **The General Data Protection Regulation (GDPR)** (*Règlement Général sur la Protection des Données*). While not explicitly targeting phishing, the GDPR mandates strict data protection measures, requiring organizations to implement robust security protocols to safeguard personal information. Companies that

fail to uphold these obligations may be subject to significant financial penalties, particularly if data breaches occur as a consequence of phishing attacks.

- **The Network and Information Security (NIS) Directive.** This directive serves as a foundational cybersecurity framework within the European Union, compelling Member States to develop and implement national cybersecurity strategies. It mandates preventive measures against a broad spectrum of cyber threats, including phishing and other forms of electronic financial fraud.

### **3- The U.S. Legal Framework**

In the United States, the legal framework for combating cyber-enabled financial deceit includes:

- **The Computer Fraud and Abuse Act (CFAA).** This legislation is a cornerstone of U.S. cybersecurity enforcement, criminalizing unauthorized access to computer systems, online fraud, and other cyber offenses. It provides federal authorities with broad prosecutorial powers to pursue individuals and entities engaged in phishing schemes.
- **The Identity Theft Enforcement and Restitution Act.** Recognizing that identity theft is a frequent byproduct of phishing fraud, this statute specifically criminalizes the unlawful acquisition and exploitation of personal data obtained through fraudulent means. It prescribes severe penalties for perpetrators who engage in identity-based financial crimes.

### **B- International Cooperation in Combatting Electronic Financial Fraud**

Phishing, characterized by its transnational nature, necessitates a comprehensive framework of international cooperation to effectively mitigate its impact. The concerted global efforts prioritize the alignment of legal systems, enhance the exchange of crucial information, and streamline the prosecution of perpetrators across national boundaries. Among the key instruments in this international strategy is the Budapest Convention on Cybercrime (Part One), complemented by the pivotal roles that Interpol and Europol play in fostering collaborative measures to combat these digital threats (Part Two).

#### **1- The Budapest Convention on Cybercrime**

Established as the first international treaty aimed specifically at addressing criminal activities conducted via the internet and other computer networks, the Budapest Convention on Cybercrime, ratified in Budapest on November 23, 2001, is regarded as the cornerstone of international legal standards for cybercrime legislation. This convention is particularly influential in shaping laws related to cybercrimes, including phishing.

Article 8 of the Budapest Convention stipulates that each participating state is required to implement the necessary legislative and ancillary measures to criminalize actions in their national laws when carried out deliberately and without rights, which result in damage to another person's property. These actions include:

- The unauthorized alteration, deletion, or deterioration of computer data;
- The intentional interference with computer system functions, perpetrated with the intent of illicitly securing an economic benefit for oneself or another<sup>19</sup>.

## **2- The Role of Interpol and Europol in Combating Financial Fraud<sup>20</sup>**

In the contemporary landscape of globalized finance, the scourge of electronic financial fraud, particularly phishing, transcends national borders, necessitating an escalated level of international cooperation. Within this framework, both Interpol and Europol play pivotal roles, serving as linchpins in the robust network of global efforts aimed at curtailing cybercrime. These organizations facilitate a critical exchange of intelligence and technical support, enhancing the efficacy of multinational law enforcement efforts.

Europol has notably advanced its commitment to this cause through the establishment of the European Cybercrime Centre (EC3). This initiative is strategically positioned to bolster member states in the combat against organized cyber threats, including expansive phishing operations and other sophisticated forms of financial fraud.

## **Conclusion**

As digital financial activities become increasingly indispensable in the modern world, they also become more susceptible to the sophisticated tactics of cybercriminals. This paper initially discusses various prevalent methods of financial fraud that have emerged alongside digital innovations. However, it is crucial to recognize that electronic financial fraud is not limited to the forms specifically discussed herein.

For example, credit-card fraud—the unauthorized use of stolen card details for illicit transactions—remains rampant. Such fraud can occur through cyber-hacking, data skimming via illicit devices, or other unauthorized data-capture techniques. Additionally, the digital sphere has seen a rise in charity fraud, where perpetrators create fictitious entities to solicit funds deceitfully. These instances exemplify the broader spectrum and evolving nature of electronic financial fraud, indicating a vast array of tactics that extend beyond this paper's scope.

To confront these challenges effectively, legal frameworks at both national and international levels have been progressively strengthened. While national laws are instrumental in delineating and prosecuting fraudulent acts and safeguarding victims, international cooperation is crucial for the seamless execution of cross-

border legal processes. This dual approach not only facilitates the rigorous enforcement of laws but also ensures that preventive measures keep pace with the rapid evolution of cyber-fraud tactics.

Beyond the foundational role of legislation in curbing financial malfeasance, the contributions of financial institutions and regulatory agencies—including oversight bodies and central banks—are paramount. Central banks regulate the banking sector, impose rigorous standards to oversee financial flows, and preemptively thwart fraudulent activities.

Governments therefore advocate robust governance practices aimed at enhancing transparency and accountability within financial institutions. Such frameworks typically include independent boards of directors and dedicated audit committees, which are crucial in ensuring the integrity of financial operations. Moreover, technology serves as a critical ally in fraud detection, underpinning the financial-control systems that regulators leverage to monitor transactions and identify suspicious activities. In this digital age, artificial intelligence and big-data analytics play pivotal roles in early detection, analyzing patterns and behaviours that may indicate fraud.

In light of the findings presented in this study, it is evident that addressing financial fraud in the era of digital transformation requires a multifaceted, forward-looking approach. First, legislatures must modernize their legal frameworks to define and criminalize digital forms of financial fraud, including phishing, cryptojacking, and fraudulent ICOs. A pivotal step involves recognizing digital data and personal information as legal assets protected under fraud statutes. Additionally, specialised judicial and prosecutorial bodies trained in cybercrime are essential to enhance enforcement.

To ensure regional coherence, efforts should be made to harmonize cybercrime laws across Arab states, drawing inspiration from instruments such as the Budapest Convention. At the institutional level, financial entities should invest in advanced technologies—particularly artificial intelligence and big-data analytics—to detect and prevent fraud in real time. Public-awareness campaigns and digital-literacy programmes must also be intensified to equip individuals and businesses to resist evolving cyber threats.

Finally, robust international cooperation remains a cornerstone in combating transnational financial fraud. Greater integration of Arab countries into global cybersecurity frameworks, and enhanced collaboration with entities such as Interpol and Europol, will strengthen cross-border enforcement capabilities. In parallel, fintech firms and digital platforms must assume greater responsibility by adhering to

stringent compliance and transparency standards, thereby contributing to a more secure and resilient financial ecosystem.

Nevertheless, the efficacy of these technological and regulatory strategies must be bolstered by comprehensive awareness programmes and adaptive preventive measures designed to counteract the continually evolving cyber-threat landscape. To this end, governments and financial institutions must deploy extensive educational initiatives to help individuals and businesses avoid falling prey to fraud; these programmes are vital in increasing public understanding of fraudsters' tactics.

<sup>1</sup>[SEC.gov | Guide to Identifying and Avoiding Securities Fraud](https://www.sec.gov/edu/guide-to-identifying-and-avoiding-securities-fraud)

<sup>2</sup>[AU Section 316 - Consideration of Fraud in a Financial Statement Audit | PCAOB](https://www.pcaob.org/au/section-316-consideration-of-fraud-in-a-financial-statement-audit)

<sup>3</sup><https://www.worldbank.org/13/02/2025>

<sup>4</sup>De Zabihollah Rezaee, Richard Riley, *Financial Statement Fraud: Prevention and Detection*, 2<sup>nd</sup> Edition, John Wiley & Sons, Inc., Hoboken, New Jersey, 2010.

<sup>5</sup>Al-Ghathir, Khalid bin Suleiman, and Suleiman bin Abdulaziz bin Hisha. *Electronic Phishing: Methods and Countermeasures*. Preface by Zaban bin Othman Al-Huqail. First edition. Riyadh: King Fahd National Library, 2009.P.38.

<sup>6</sup>Avinash Gupta Desetty, Vinay Dutt Jangampet, Srinivas Reddy Pulyala, "Phishing Attacks: Evolving Techniques, Emerging Trends, and Countermeasure Strategies", *International Journal for innovative engineering and management research*, Volume 09 Issue 12 Dec 2020, p.986.

<sup>7</sup>[https://www.researchgate.net/publication/376645699\\_Phishing\\_Attacks\\_Evolving\\_Techniques\\_Emerging\\_Trends\\_and\\_Countermeasure\\_Strategies](https://www.researchgate.net/publication/376645699_Phishing_Attacks_Evolving_Techniques_Emerging_Trends_and_Countermeasure_Strategies)

<sup>8</sup>For more details refer to:Al-Ghathir, Khalid bin Suleiman, and Suleiman bin Abdulaziz bin Hisha. *Electronic Phishing: Methods and Countermeasures*. Preface by Zaban bin Othman Al-Huqail. First edition. Riyadh: King Fahd National Library, 2009. last accessed October 29, 2020.p.58.

<sup>9</sup>Menassera Youssef, *Financial Fraud in the Cryptocurrency Sector*, *Journal of Legal Discourse*, vol. 10, no. 1, January 2024, p. 362.

<sup>10</sup>The Coincheck exchange incident in Japan serves as a prime example of fraud perpetrated through initial coin offerings (ICOs), where 200,000 users were affected, and approximately \$530 million was illicitly appropriated based on asset valuations at the time of the breach. See:Menassera Youssef, *op. cit*.

<sup>11</sup>Ordinance No. 66-156, enacted on June 8, 1966, containing the Penal Code (as amended and supplemented).

<sup>12</sup>Ben Bouaziz Assia, Miloud Bin Abdelaziz. "The Crime of Electronic Fraud in the Era of Information Technology." *Journal of Financial, Accounting, and Administrative Studies*, vol. 09, issue 01, June 2022, p. 1369.

<sup>13</sup>Naeem Mghabeghab, *Protection of Computer Programs: A Study in Comparative Law*, 2nd ed. (Halabi Legal Publications, Beirut, 2009).P, 157

<sup>14</sup>Ibid

<sup>15</sup>LUCAS De Leyssac (Marie-Paul), *droit de l'informatique et de l'internet*, Press. Universitaires de Paris, 2001, p.51

<sup>16</sup>Naeem Mghabeghab,Op.cit

<sup>17</sup>Government of Saudi Arabia. *Law on Combating Financial Fraud and Breach of Trust*. Issued April 22, 2021. Accessed October 23, 2024, at 16:18. <https://www.boe.gov.sa>.

<sup>18</sup>Law No. 09-04 of August 5, 2009, on the Prevention and Suppression of Offenses Related to Information and Communication Technologies.

<sup>19</sup>Presidential Decree No. 20-183 of July 13, 2020, restructuring the National Authority for the Prevention and Suppression of Cybercrime.

<sup>20</sup>Council of Europe. *Convention on Cybercrime (Budapest Convention)*. Signed November 23, 2001. Accessed October 30, 2024, at 16:48. <https://rm.coe.int/budapest-convention-in-arabic/1680739173>.

<sup>21</sup>Interpol : Organisation internationale de police criminelle créée en 1923, Europol : Dans le même esprit organe de coordination des policiers européens a été créé (convention signée à Bruxelles le 26 juill.1995). voir : Christiane FERAL-SCHUHL, *CYBERDROIT Le droit à l'épreuve de l'internet*, Dalloz, Paris, 2010, p.1014

—

—

– **Bibliography:**

**A- Books:**

- Al-Ghathir, Khalid bin Suleiman, and Suleiman bin Abdulaziz bin Hisha. *Electronic Phishing: Methods and Countermeasures*. Preface by Zaban bin Othman Al-Huqail. First edition. Riyadh: King Fahd National Library, 2009. last accessed October 29, 2020.
- De Zabihollah Rezaee, Richard Riley, *Financial Statement Fraud: Prevention and Detection*, 2<sup>nd</sup> Edition, John Wiley & Sons, Inc., Hoboken, New Jersey, 2010.
- Christiane FERAL-SCHUHL, *CYBERDROIT Le droit à l'épreuve de l'internet*, Dalloz, Paris, 2010.
- LUCAS De Leyssac (Marie-Paul), *droit de l'informatique et de l'internet*, Press. Universitaires de Paris, 2001.
- Naeem Mghabeghab, *Protection of Computer Programs: A Study in Comparative Law*, 2nd ed. Halabi Legal Publications, Beirut, 2009.

**C - Newspaper articles:**

- Ben Bouaziz Assia, Miloud Bin Abdelaziz. "The Crime of Electronic Fraud in the Era of Information Technology." *Journal of Financial, Accounting, and Administrative Studies*, vol. 09, issue 01, June 2022, p. 1369.
- Avinash Gupta Desetty, Vinay Dutt Jangampet, Srinivas Reddy Pulyala, "Phishing Attacks: Evolving Techniques, Emerging Trends, and Countermeasure Strategies", *International Journal for innovative engineering and management research*, Volume 09 Issue 12 Dec 2020, p.985. [https://www.researchgate.net/publication/376645699\\_Phishing\\_Attacks\\_Evolving\\_Techniques\\_Emerging\\_Trends\\_and\\_Countermeasure\\_Strategies](https://www.researchgate.net/publication/376645699_Phishing_Attacks_Evolving_Techniques_Emerging_Trends_and_Countermeasure_Strategies)

**D - Websites:**

- Council of Europe. *Convention on Cybercrime (Budapest Convention)*. Signed November 23, 2001. Accessed October 30, 2024, at 16:48. <https://rm.coe.int/budapest-convention-in-arabic/1680739173>.
- Government of Saudi Arabia. *Law on Combating Financial Fraud and Breach of Trust*. Issued April 22, 2021. Accessed October 23, 2024, at 16:18. <https://www.boe.gov.sa>.
- [SEC.gov](https://www.sec.gov) | [Guide to Identifying and Avoiding Securities Fraud](https://www.sec.gov/edu/guide-to-identifying-and-avoiding-securities-fraud)(consulted on 12/12/2024)
- [AU Section 316 - Consideration of Fraud in a Financial Statement Audit | PCAOB](https://www.pcaob.org)(consulted on 24/12/2024)
- <https://www.worldbank.org>(13/02/2025) (consulted on 24/03/2025)