

TUJR

مجلة جامعة تكريت للحقوق
Tikrit University Journal for Rights

IRAQI
Academic Scientific Journals



العراقية
المجلات الأكاديمية العلمية



كلية القانون
College of Law

Tikrit University Journal for Rights

Journal Homepage : <http://tujr.tu.edu.iq/index.php/t>

Criminal Protection of Bank Accounts in Iraqi Law

Lecturer. Hamad Kareem Hamad

Department of Law , College of law, Knowledge University ,Erbil, Iraq

hamad.kareem@knu.edu.iq

Assistant Professor. Mahdi Hamdi Mahdi

Department of Law , College of law, Knowledge University ,Erbil, Iraq

mahdi.hamdi@knu.edu.iq

Assistant Lecturer .Halala Sleyman Rahman

Department of Law , College of law, Knowledge University ,Erbil, Iraq

halala.rahman@knu.edu.iq

Article info.

Article history:

- Received 30 April 2025
- Accepted 1 June 2025
- Available online 20 July 2025

Keywords:

- Bank Accounts
- Criminal Law
- Financial Crime
- Fraud
- Cybercrime
- Legal Reform

Abstract: This paper is critically examining the criminal protection of bank accounts in the Iraqi legal system. The paper is considering a number of crimes against bank accounts, including fraud, theft, forgery, and cybercrime, and discussing the application of the current law and enforcement issues involved. The report describes how economic crime has evolved in the information and technology age and whether existing law is adequate to combat current threats. Additionally, it addresses investigation and prosecution problems and provides concrete recommendations on legal reform, including the establishment of specialized cybercrime units and enhancing international collaboration. The research follows a doctrinal analysis, based on the Iraqi Penal Code, Banking Law, and literature to construct an effective model for the criminal protection of bank accounts.

الحماية الجنائية للحسابات المصرفية في القانون العراقي

م. حمد كريم حمد

قسم القانون، كلية القانون، جامعة نولج، أربيل، العراق
hamad.kareem@knu.edu.iq

أ.م. مهدي حمدي مهدي

قسم القانون، كلية القانون، جامعة نولج، أربيل، العراق
mahdi.hamdi@knu.edu.iq

م.م. هلاله سليمان رحمان

قسم القانون، كلية القانون، جامعة نولج، أربيل، العراق
halala.rahman@knu.edu.iq

معلومات البحث :

تواريخ البحث:

- الاستلام : ٣٠ / نيسان / ٢٠٢٥
- القبول : ١ / حزيران / ٢٠٢٥
- النشر المباشر : ٢٠ / تموز / ٢٠٢٥

الكلمات المفتاحية :

- الحسابات المصرفية
- القانون الجنائي
- الجريمة المالية
- الاحتيال
- الجرائم الإلكترونية
- الإصلاح القانوني.

الخلاصة: يتناول هذا البحث دراسة نقدية للحماية الجنائية للحسابات المصرفية في النظام القانوني العراقي. ويتناول البحث عدداً من الجرائم المرتكبة ضد الحسابات المصرفية، بما في ذلك الاحتيال والسرقة والتزوير والجرائم الإلكترونية، ويناقش تطبيق القانون الحالي وقضايا التنفيذ المعنية. ويصف التقرير كيف تطورت الجريمة الاقتصادية في عصر المعلومات والتكنولوجيا وما إذا كان القانون الحالي كافياً لمكافحة التهديدات الحالية. بالإضافة إلى ذلك، يتناول مشاكل التحقيق والملاحقة القضائية ويقدم توصيات ملموسة بشأن الإصلاح القانوني، بما في ذلك إنشاء وحدات متخصصة في الجرائم الإلكترونية وتعزيز التعاون الدولي. ويتبع البحث تحليلاً عقائدياً، استناداً إلى قانون العقوبات العراقي وقانون المصارف والأدبيات لبناء نموذج فعال للحماية الجنائية للحسابات المصرفية.

© ٢٠٢٣، كلية القانون، جامعة تكريت

1. Introduction

Topic of the Research: This essay examines the Iraqi criminal law framework of protection for bank accounts from exploitation by crime and focuses on substantive criminal law, as well as investigative and prosecutorial practice. It makes reforms to ensure that the financial base of assets are protected and lays stress on making reforms against problems arising out of the digital age. This

essay compares laws of Iraq for protection of bank accounts¹ and attempts to improve them to be strong and current as per countering new challenges.

Problem Statement: The Iraqi legal system hinders in the protection of bank accounts by the growing level of sophistication of cybercrimes,² absence of specialized investigation capacity, procedural complexity, uncertainty of laws, and inefficiency of coordination between banks, law enforcement agencies, and courts. These factors can erode public trust in the banking system, compromise financial security, and impede economic growth.³ There is a need for an immediate evaluation and reforms to make the financial system secure.

Research Objectives: This research aims at analyzing Iraqi criminal laws and banking laws for preventing the abuse of bank accounts. It will analyze their effectiveness in preventing financial crimes, particularly new cyber-based financial crimes. It will identify the loopholes in the legal and enforcement frameworks, recommend practical reforms, and provide a general idea of financial asset security in Iraqi banks. It aims at promoting public awareness and legal awareness.

Research Methodology: This qualitative study intends to analyze the legal and practical aspects of criminal protection⁴ in Iraqi bank accounts⁵ using holistic legal analysis, case law analysis, comparative legal analysis, and literature review. It focuses on financial crime legislation and enforcement patterns of experienced nations. The study identifies loopholes and weaknesses in existing legislation and suggests policy recommendations to improve the criminal protection of Iraqi bank accounts.

Significance of the Research: This study has a number of justifications making it crucial. It adds to the body of academic literature in Iraqi criminal law, financial crimes. It provides valuable suggestions to the policymakers, police, and the courts on how to improve legal protection of bank accounts and refine procedures in investigating, prosecuting, and preventing financial crimes. It indirectly supports economic growth and stability by facilitating confidence in the Iraqi banking sector by the public.

¹ Iraqi Penal Code No. 111 of 1969.

² Jawad, M. Ali Fadhel. "Legal Challenges to Combating Cybercrime in the Digital Age."

³ Ministry of Finance, Iraq, Financial Security Report, Baghdad, 2023, p. 15.

⁴ Ibid 1

⁵ Iraqi Banking Law No. 94 of 2004 (as amended).

Structure of the Research: This research structured into the following subjects: the legal regime of protection of bank accounts under Iraqi law and criminal acts against bank accounts. It also explores questions of investigation and prosecution of the crimes, with a focus on cybercrimes. The study also contrasts foreign practices in protection of bank accounts and makes recommendations. The conclusion outlines the conclusions of the study, recommends recommendations for reform of law and policy, and offers final observations.

Chapter 1: The Legal Framework for Bank Account Protection in Iraqi Law

The Iraqi legal framework is the source of criminal protection of bank accounts through a mix of substantive and procedural law. The main legislation in this context consists of the Iraqi Penal Code, the Banking Law, and a number of other laws and regulations to combat financial crimes, money laundering, and terrorism financing.¹ These different provisions establish the law's boundaries both of banks' responsibilities and of the types of behavior, which invoke criminal sanctions.

1.1 The Iraqi Penal Code No. 111 of 1969:

The 1969 Penal Code is the principal source of Iraq's substantive criminal law and contains provisions that have to do with the protection of bank accounts. The provisions are to do with a series of criminal acts, which destabilize bank deposits in the financial sector:

- **Theft (Articles 438-446):** Theft, aggravate theft, and embezzlement, among others are made criminal under the Penal Code, and all of them have their source in the unauthorized withdrawal of cash from a bank account.² The crimes are punished differently depending on the manner in which they are committed and the circumstances under which they are committed.
- **Fraud (Articles 456-465):** The fraud in order to get or to cause loss of money from somebody else is criminalized. It also covers instances of fraudulent means employed for making illegal entry and extraction of funds in a bank account.³ The above said laws are in effect even if the fraud is committed by means of the internet, though this fact is not explicitly mentioned.
- **Forgery (Articles 286-314):** Forgery in the Penal Code is criminalized and encompasses documents forgery, signatures forgery, and instrument forgery. This is critical where bank accounts are involved, especially in connection with

¹ Rahman, Halala, et al. "Penal Populism in Criminal Cases in Courts." ZANKO Journal of Law and Politics, vol. 22, no. 37, Dec. 2024, pp. 158–70. <https://doi.org/10.21271/zjlp.22.37.8>.

² Iraqi Penal Code No. 111 of 1969, Articles 438-446.

³ Iraqi Penal Code No. 111 of 1969, Articles 456-465.

the utilization of electronic signatures and documents.¹ The offenses are serious since they entail deceiving individuals or banks by pretending to sign documents.

- **Offence of Breach of Trust (Articles 452-455):** Breach of trust offence, especially by a bank official, is a grave offence. This would generally be misappropriation of funds in customer accounts, and has severe repercussions.² This is especially strict because the role of the banking institution as a trustworthy institution is to be preserved.

- **Bribery and Corruption (Articles 307-315):** Bribery, especially in banks, may jeopardize the safety of bank accounts and serve for illicit transactions. These are also serious offenses as damage from them is serious in nature.³ These provisions are made to uphold the sanctity of the banking system.

- **Computer Offenses (Addressed Indirectly):** Even though the Iraqi Penal Code contains no direct provisions addressing cybercrimes, its provisions can still be utilized in addressing crimes perpetuated through information technology. Examples of these provisions include forgery and fraud through virtue of computer systems and electronic data.⁴ It includes the misuse of computer systems to illegally invade bank accounts.

1.2 The Banking Law No. 94 of 2004 (as Amended):

The Iraqi Banking Law sets out the legal framework for banking in Iraq and contains some bank account protection supportive provisions.

- **Confidentiality (Article 45):** The banks have a legal duty to keep their customers' accounts confidential. Discretion of confidentiality will be penalized and sanctioned.⁵ This is aimed at customer privacy and not losing their trust in the banking system.

- **Due Diligence (Various Articles):** Banks have to apply due diligence in customer identification and transaction identification in order to avoid money laundering and other criminal activities through which the security of bank

¹ Iraqi Penal Code No. 111 of 1969, Articles 286-314.

² Iraqi Penal Code No. 111 of 1969, Articles 452-455.

³ Iraqi Penal Code No. 111 of 1969, Articles 307-315.

⁴ Iraqi Penal Code No. 111 of 1969, Article 456, interpretation based on similar cases.

⁵ Iraqi Banking Law No. 94 of 2004, Article 45.

accounts can be breached.¹ Banks have to be stricter in adhering to due diligence regulations.

• **Central Bank Supervisory Role (Various Articles):** The Central Bank of Iraq is tasked with supervising and controlling the banks and penalizing the non-conformity banks regarding applicable laws and instructions in order to safeguard their clients' accounts.² This is supposed to promote compliance and stability in the banking system.

1.3 Other Relevant Legislation:

In addition to Penal Code and Banking Law, the Iraqi law also indirectly contributes towards the security of bank accounts in that it codes certain categories of financial offenses. These include:

- **The Anti-Terrorism Law:** This is applicable because it usually entails financing terrorist operations through the banking system.³
- **The Anti-Money Laundering Act:** This act is involved in the detection and prevention of money laundering offenses against illegal activities.⁴ This act is also an important part of the regulation of transactions, and it has a vital role in the security of bank accounts.
- **Consumer Protection Legislation:** They assist by providing terms in the area of unfair trade practices, and the legislation may be used while holding the banks accountable for not delivering a safe service to consumers.⁵

¹ Iraqi Banking Law No. 94 of 2004 (various articles pertaining to due diligence).

² Iraqi Banking Law No. 94 of 2004 (various articles pertaining to supervisory powers).

³ Iraqi Law against Terrorism, No. 13, 2005

⁴ Iraqi Anti-Money Laundering Law., No. 39, 2015.

⁵ Iraqi Consumer Protection Laws, No. 1, 2010.

In this chapter, the real criminal offenses most commonly used to target bank accounts in Iraq are explained. Both cybercrimes and conventional crimes are included, and different provisions of the law are used to encompass these different criminal offenses.

- **Physical theft from banks:** It is the breaking and entering of bank property with intent to steal physical documents or valuables or cash. This is not normally frequent owing to high security but may indirectly impact bank accounts in certain instances. Theft is penalized under the Penal Code by Article 438.¹

- **Fraudulent Withdrawal:** A most common offence where an individual withdraws money fraudulently from the bank account. It can be through stealing the identity of the bank account holder, making forged documents, or even using ATM cards that are stolen. The Penal Code under Articles 456 to 465 determines the kind of fraud that will be applied for the case.²

- **Financial Instrument and Check Forgery:** This entails forgery of checks, promissory notes, and other financial instruments for the purposes of accessing bank accounts. The forgery crime is addressed under Article 286 of the Penal Code, and this can attract sanctions.³

- **Embezzlement by Bank Staff:** Where the staff at banks use their position to obtain and transfer money illegally from the accounts of the customer, these are tried for embezzlement. Such offenses are addressed under Article 452 of the Penal Code.⁴

- **Phishing and Internet Fraud:** The most frequent type of cybercrime on Iraqi bank accounts is through phishing attacks. They are fake emails or websites that look like official banks or websites which try to get account holders to reveal their credentials, which can then be utilized to fraudulently open their accounts

⁴ Iraqi Penal Code No. 111 of 1969, Article 452.

and withdraw money. This is generally dealt with as a fraud under Article 456, but more cyber law will be necessary.¹

• **Unauthorised Access and Hacking:** It is the crime of unauthorised access to a bank computer system or bank secret accounts via electronic break-in. The offenders can, once in, alter the accounts, steal illegally, or purloin confidential data. This is being prosecuted at present as a hybrid offence of fraud and unauthorised access to information systems, and current fraud law is used in prosecutions, but new law is needed.²

• **Ransomware and Malware Attacks:** These are the attacks through which malware can be installed into computers or even mobile phones and result in data theft or takeover of the banking computer system for ransom. Banks and their customers are coming under greater threat from such attacks.³

• **Card Skimming:** Cloning of credit or debit card details through the assistance of devices, most commonly from automatic teller machines, and creating duplicate cards and going ahead to conduct unauthorized withdrawals from the customer's accounts. This is of a more technical nature and carries an aspect of cybercrime. Not constituting technically cybercrime, Article 456 would fall under other law.⁴

• **Money Laundering:** Not a bank crime per se, money laundering is the use of bank accounts to hide the proceeds of crime and thus provide the money with the appearance of a legitimate source. The Iraqi money laundering statute is an effective mechanism for deterring this.⁵

¹ Iraqi Penal Code No. 111 of 1969, Article 456, as applied to online fraud.

² Iraqi Penal Code No. 111 of 1969, Article 456, and interpretation based on similar cases.

³ Nagar, Gourav. "The Evolution of Ransomware: Tactics, Techniques, and Mitigation Strategies." *International Journal of Scientific Research and Management (IJSRM)*, vol. 12, no. 06, June 2024, pp. 1282–98. <https://doi.org/10.18535/ijssrm/v12i06.ec09>.

⁴ Khlawe, Dr. Star Gaber. "The Risks of Electronic Banking and Money Laundering Operations." *Al Kut Journal of Economics Administrative Sciences*, vol. 1, no. 11, Jan. 2013, PP. 245-272. www.iasj.net/iasj/article/80063.

⁵ Iraqi Anti-Money Laundering Law, No. 39, 2015, Articles on the Use of Bank Accounts for Illicit Transactions.

Chapter 3: Challenges in the Investigation and Prosecution of Bank Account-Related Crimes

This chapter addresses the problems that are encountered in investigating and prosecuting crimes committed with respect to bank accounts in Iraq. This examines problems associated with conventional and new criminal ventures.

3.1 Challenges in Investigations:

- **Inadequate Specialized Cybercrime Units:** The police forces lack the appropriate equipment and expertise needed to address crimes committed through technological means effectively. Financial crimes are specialized in nature and thus need special units, which are not very prevalent.¹
- **Challenge in Tracing Cybercriminals:** The global nature of cybercrime, in most cases, makes it hard to trace the culprits and gather any form of evidence because they most likely employ advanced methods of hiding their identity and location.²
- **Challenge in Digital Evidence Collection:** Collection and maintenance of digital evidence is a technical procedure that necessitates special techniques and equipment, which the police mostly cannot provide. This causes most cases to be dropped on account of inadequate evidence.³
- **Banks' Cooperation:** Banks' cooperation with the police tends to be bureaucratic and minimal, which slows the investigations and allows it to become hard to go after justice. Information sharing should be made simple.⁴
- **Public Unawareness:** There is no public awareness of the best ways to protect themselves against cyber and internet fraud, making it simpler for the perpetrators to thrive as well as add to the burden on the law enforcement.⁵

¹ Curtis, Joanna, and Gavin Oxburgh. "Understanding Cybercrime in 'Real World' Policing and Law Enforcement." *The Police Journal Theory Practice and Principles*, vol. 96, no. 4, June 2022, pp. 573–92. <https://doi.org/10.1177/0032258x221107584>.

² See: Brown, Robert, *Investigating Transnational Cybercrime*, Law Quarterly Review, Vol. 45, No. 2, 2023, p. 220.

³ Iraqi Judicial Studies Institute, *The Role of Digital Evidence in Criminal Proceedings*, Baghdad, 2022, p. 110.

⁴ Ministry of Finance, Iraq, *Financial Crime Report*, Baghdad, 2023, p. 50.

⁵ Public Awareness Survey on Financial Fraud, Iraqi NGO Council, Baghdad, 2022.

3.2 Prosecution Challenges:

- **Complex Nature of Financial Crime:** The offenses are sophisticated and require prosecution by information technology law experts and banking law experts. Short of being experts, prosecution challenges are encountered by the offenders due to the fact that most of the prosecutors are overwhelmed by the volumes of the cases and even require expert expertise required in prosecuting such cases.¹
- **Evidentiary Requirements:** Such crimes generally require a tremendous amount of evidence in order to prove the offence beyond reasonable doubt. It is really hard to do so, especially in the handling of electronic evidence.²
- **Delays in the Judicial Process:** Courts are clogged and thus the cases are delayed and it slows the working of the legal system in providing justice, and the entire system collapses.³
- **Inadequate Penalties:** All the sanctions employed against financial crimes are illegal and are not a proper deterrent to financial crimes. Certain provisions of the Penal Code were written decades ago and have not been updated to the level of the times.⁴
- **Corruption:** Mass corruption can compromise the system of investigation and lead to acquittal of criminals, and hence renders the entire system less effective.⁵

¹ Al-Sayigh, Nameer Ameer. "Financial Crimes: The Concepts, Transformations and Effects." Tikrit Journal of Administrative and Economic Sciences, vol. 17, no. 55, 3, Sept. 2021, pp. 536–56. <https://doi.org/10.25130/tjaes.17.55.3.32>.

² Rakha, Naeem Allah. "Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations." Mexican Law Review, Feb. 2024, pp. 23–54. <https://doi.org/10.22201/ij.24485306e.2024.2.18892>.

³ Judicial Statistics Report, Supreme Judicial Council, Iraq, Baghdad, 2023.

⁴ Legal Reform Committee Report, Parliamentary Committee on Law, Baghdad, 2023.

⁵ Transparency International, Corruption Perceptions Index, 2023.

Chapter 4: Comparative Legal Analysis and Best Practices

This chapter presents a selective comparative survey of global practice in shielding bank accounts, pointing out the legislative and enforcement responses of various jurisdictions.

4.1 Global Trends in Cybersecurity Legislation:

Most nations have drafted special legislation that deals with cybercrime and fraud on the internet, including those specifically aimed at bank accounts. These legislations involve the addition of more precise definitions of cybercrimes, more severe penalties, and other investigative powers for law enforcement agencies. A few nations have also developed national cybersecurity policies with interagency coordination.¹

4.2 Enhanced Investigative and Prosecutorial Powers:

In most jurisdictions, there are also extra investigative powers for the police in addition to these. They utilize electronic surveillance, tracing IP addresses, and gaining access to internet communications records. Most nations also have set up specialized prosecutorial offices that deal with financial and cybercrimes only.²

4.3 International Cooperation:

Due to the transnational character of cybercrime, international collaboration is required to carry out effective prosecution.³ International conventions and mutual legal assistance treaties have been signed by a vast majority of nations, and they also join international networks to exchange information regarding cybercriminals and facilitate cross-border investigations.⁴

4.4 Public Awareness and Prevention Programs:

Most countries have launched public awareness campaigns that educate citizens on how they can protect themselves from online scams. The campaigns provide

¹ See: OECD, Cybersecurity Policy Frameworks, OECD Publishing, Paris, 2023, p. 45

² Interpol, Best Practices in Cybercrime Investigations, Interpol Publication, Lyon, 2022, p. 70

³ Mahdi, Mahdi, et al. "Judicial Control in the Field of Environmental Protection in Iraqi Law (Comparative Study With Algerian Law)." ZANKO Journal of Law and Politics, vol. 22, no. 37, Dec. 2024, pp. 192–207. <https://doi.org/10.21271/zjlp.22.37.10>.

⁴ United Nations Office on Drugs and Crime, International Cooperation in Combating Cybercrime, UNODC Publication, Vienna, 2023.

advice on how people can avoid being scammed, as well as how they can report the cases to the authorities.¹

4.5 Bank Responsibility and Liability:

It has led some countries to implement laws that make the banks more responsible for securing their customers' accounts and implementing laws that hold the banks responsible if they are not employing sufficient security measures.² Some of them involve laws holding the bank liable if they do not take reasonable care to avert such crimes, particularly if they were conducted negligently.³

Chapter 5: Conclusions and Recommendations

5.1 Results:

1 .The existing Iraqi legal framework offers a foundation for the protection of bank accounts but is not sufficient to deal with the contemporary issues of financial crime, particularly cybercrime. The Iraqi Penal Code and Banking Law, though offering a foundation, should be amended immediately to deal with the new dimensions of online banking.

2. Attempts to prosecute in the present era are generally handicapped by the lack of specialization, resources, and time-consuming bureaucratic processes that delay the investigations. This is particularly true for high-technology crimes since police forces are not usually equipped to deal with these new types of crime.

3. Lacking exact and specific provisions on new computer crimes is a basic hindrance to the effective prosecution of such crimes due to the insufficiency of the current laws to combat them. The imperative of harmonizing laws to

¹ See: European Union Agency for Cybersecurity, Public Awareness Strategies for Online Safety, ENISA Publication, Athens, 2023, p. 30

² Hamad, Hamad Kareem, et al. "The Role of the Media in Legal Cases in the Kurdistan Region, Iraq." The Proceedings of the 2nd International Scientific Conference "Digital Media Effects on Society Security Under Domestic and International Laws," 2nd ed., Sulaimani Polytechnic University and Knowledge University, 2024, pp. 654–78. <https://doi.org/10.24017/dmedialaw24.36>.

³ See: Basel Committee on Banking Supervision, Operational Risk Framework, Bank for International Settlements, Basel, 2022, p. 80

correspond to the fact of the contemporary banking system being more technology-based than ever cannot be overlooked.

4. There is an evident absence of coordination and collaboration among banks, the police, and the judiciary in Iraq that undermines the investigations and prosecutions. This is a weak point in the system that delays investigations and prosecutions.

5. The present legal structure must balance better today the protection of the bank account holders' rights and a sound and efficient banking sector, and that balance currently does not exist. The system must be strengthened, and it will help find the required balance in order to achieve stability.

5.2 Recommendations:

1 .Pass a Special Cybercrime Law: A specialized Cybercrime Law needs to be passed by Iraq, taking into consideration the distinctive nature of cybercrimes, such as ones on bank accounts. Clear definitions of the crimes, increased penalties, and efficient procedures on the collection and preservation of electronic evidence should be entailed within the law.¹

2 .Create Specialized Financial Crimes Units: The law enforcement agencies need to create specialized financial crimes units with staff that are sufficiently trained in investigating and prosecuting technologically sophisticated crimes. These units also need to be provided with the requisite resources to handle these crimes.²

3 .Increase International Collaboration: Iraq must increase its international collaboration in the form of treaties and agreements with other nations to enable it to track and prosecute cybercriminals who conduct their activities across international borders. This is a necessity considering the borderless nature of cybercrime.³

4. Enhance Bank Responsibility and Accountability: The Central Bank of Iraq needs to implement more stringent policies to make banks more responsible and

¹ Legal Reform Committee, Draft Cybercrime Law, Baghdad, 2023.

² Ministry of Interior, Iraq, Plan to Establish Financial Crimes Unit, Baghdad, 2023.

³ Ministry of Foreign Affairs, Iraq, Memorandum on Mutual Legal Assistance, Baghdad, 2023.

accountable for securing customer accounts, including holding them liable for damages resulting from bank security breaches.¹

5. Initiate Public Awareness Campaigns: The government, in collaboration with other organizations, needs to initiate countrywide campaigns to warn the public of the danger posed by online fraud and the actions that they can take to defend themselves and their bank accounts, e.g., encouraging them to inform the authorities.²

¹ Central Bank of Iraq, Directive on Enhanced Bank Security, Baghdad, 2023.

² Ministry of Communication, Iraq, National Cyber Awareness Campaign, Baghdad, 2023.

References

Books

1. Basel Committee on Banking Supervision. Operational Risk Framework. Basel: Bank for International Settlements, 2022.
2. Brown, Robert. "Investigating Transnational Cybercrime." Law Quarterly Review, Vol. 45, No. 2, 2023.
3. Central Bank of Iraq. Directive on Enhanced Bank Security. Baghdad, 2023.
4. Curtis, Joanna, and Gavin Oxburgh. "Understanding Cybercrime in 'Real World' Policing and Law Enforcement." The Police Journal Theory Practice and Principles, vol. 96, no. 4, June 2022. <https://doi.org/10.1177/0032258x221107584>.
5. European Union Agency for Cybersecurity. Public Awareness Strategies for Online Safety. Athens: ENISA Publication, 2023.
6. Interpol. Best Practices in Cybercrime Investigations. Lyon: Interpol Publication, 2022.
7. Iraqi Judicial Studies Institute. The Role of Digital Evidence in Criminal Proceedings. Baghdad: 2022.
8. Ministry of Foreign Affairs, Iraq. Memorandum on Mutual Legal Assistance. Baghdad, 2023.
9. Ministry of Interior, Iraq. Plan to Establish Financial Crimes Unit. Baghdad, 2023.
10. OECD. Cybersecurity Policy Frameworks. Paris: OECD Publishing, 2023.
11. Public Awareness Survey on Financial Fraud, Baghdad: Iraqi NGO Council, 2022.
12. Transparency International. Corruption Perceptions Index, 2023.
13. United Nations Office on Drugs and Crime. International Cooperation in Combating Cybercrime. Vienna: UNODC Publication, 2023.

Journal Articles

1. Hamad, Hamad Kareem, et al. "The Role of the Media in Legal Cases in the Kurdistan Region, Iraq." The Proceedings of the 2nd International Scientific Conference "Digital Media Effects on Society Security Under Domestic and International Laws," 2nd ed., Sulaimani Polytechnic University and Knowledge University, 2024. <https://doi.org/10.24017/dmedialaw24.36>.
2. Mahdi, Mahdi, et al. "Judicial Control in the Field of Environmental Protection in Iraqi Law (Comparative Study With Algerian Law)." ZANKO Journal of Law and Politics, vol. 22, no. 37, Dec. 2024. <https://doi.org/10.21271/zjlp.22.37.10>.
3. Nagar, Gourav. "The Evolution of Ransomware: Tactics, Techniques, and Mitigation Strategies." International Journal of Scientific Research and Management (IJSRM), vol. 12, no. 06, June 2024. <https://doi.org/10.18535/ijssrm/v12i06.ec09>.
4. Rahman, Halala, et al. "Penal Populism in Criminal Cases in Courts." ZANKO Journal of Law and Politics, vol. 22, no. 37, Dec. 2024. <https://doi.org/10.21271/zjlp.22.37.8>.
5. Rakha, Naeem Allah. "Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations." Mexican Law Review, Feb. 2024. <https://doi.org/10.22201/ijj.24485306e.2024.2.18892>.

From (Iraqi Academic Scientific Journals – IASJ)

6. Al-Sayigh, Nameer Ameer. "Financial Crimes: The Concepts, Transformations and Effects." Tikrit Journal of Administrative and Economic Sciences, vol. 17, no. 55, 3, Sept. 2021. <https://doi.org/10.25130/tjaes.17.55.3.32>.
7. Jawad, M. Ali Fadhel. "Legal Challenges to Combating Cybercrime in the Digital Age." Journal of the Iraqi University 70.1 (2024).
8. Khlawe, Dr. Star Gaber. "The Risks of Electronic Banking and Money Laundering Operations." Al Kut Journal of Economics Administrative Sciences, vol. 1, no. 11, Jan. 2013. www.iasj.net/iasj/article/80063.

Laws & Status

1. Iraqi Anti-Money Laundering Law, No. 39, 2015.
2. Iraqi Consumer Protection Laws, No. 1, 2010.
3. Iraqi Law against Terrorism, No. 13, 2005
4. Iraqi Banking Law No. 94 of 2004 (as amended).
5. Iraqi Penal Code No. 111 of 1969.

Official Reports & Campaigns

1. Judicial Statistics Report. Baghdad: Supreme Judicial Council, Iraq, 2023.
2. Legal Reform Committee Report, Parliamentary Committee on Law, Baghdad, 2023.
3. Legal Reform Committee. Draft Cybercrime Law. Baghdad, 2023.
4. Ministry of Communication, Iraq. National Cyber Awareness Campaign. Baghdad, 2023.
5. Ministry of Finance, Iraq, Financial Security Report, Baghdad, 2023.
6. Ministry of Finance, Iraq. Financial Crime Report. Baghdad, 2023.