البنك المركزي الأردني
CENTRAL BANK OF JORDAN
دائرة حماية المستهلك المالي

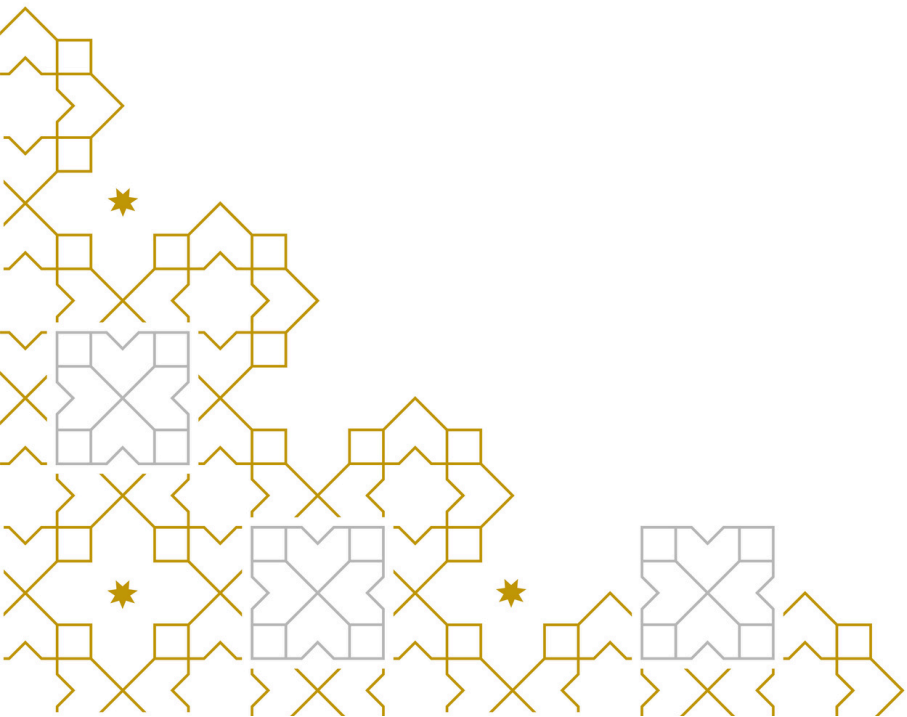
Jo-FinCERT

فريق الاستجابة للحوادث
السيبرانية للقطاع المالي
والمصرفي الاردني

Financial Fraud Awareness Guide:

Using Electronic Methods

V2.0 2025



Introduction

In light of the rapid expansion and diversification of financial services–especially following the COVID-19 pandemic, and the growing reliance on digital financial channels, consumers now benefit from faster, more convenient, and cost-effective ways to manage their finances.

At the same time, this increasing dependence on electronic financial services has accompanied by a rise of sophisticated fraud schemes targeting financial consumers. These schemes have become more advanced and adaptive, exploiting digital platforms and remote channels to deceive individuals into exposing their sensitive and financial information.

In line with its mandate to safeguard financial consumers, the Central Bank of Jordan has developed this Financial Fraud Awareness Guide to raise awareness about common types of financial fraud, outline the tactics used by fraudsters, and provide practical guidance to help consumers protect themselves from such threats.

Table of Contents

Phishing

Phishing URLs are fraudulent web links crafted by cybercriminals impersonating trusted organizations or individuals with the intent to deceive users into revealing sensitive personal or financial information. These URLs are commonly distributed through email, SMS, or social media channels, and are designed to closely resemble legitimate websites, thereby increasing the likelihood that users will be misled into providing confidential data.

Security Tips

- Verify the source before clicking on any link or opening attachments received via email or text message. Use reputable antivirus or endpoint protection solutions to scan attachments and validate URLs before interacting with them.

- Access your bank or financial institution's website directly by typing the official address into your browser, especially when requested to provide confidential information. Confirm that the website uses HTTPS and displays a secure lock icon in the address bar before entering any sensitive data.

- Carefully inspect website URLs and domain names included in emails or messages for subtle misspellings or unusual characters. These are common indicators of phishing attempts designed to impersonate legitimate entities.

Vishing - Caller ID Spoofing

Vishing is a form of telephone fraud in which scammers impersonate trusted entities to deceive individuals into revealing sensitive personal or financial information. These calls may involve false claims such as winning a prize, verifying bank details, or resolving a non-existent issue, with the goal of exploiting the victim's trust or uncertainty in order to obtain confidential data.

Common Indicators of Vishing :

- Fake prize-winning notifications.
- Calls requesting bank account verification or Update Account Information.
- Appeals for assistance with non-existent technical or financial issues.

Security Tips

- Banks and financial institutions do not request sensitive information such as usernames, passwords, One-Time Passwords (OTPs), or card verification codes (CVV) over the phone under any circumstances.

- If you receive a call urging immediate action or requesting unusual payments, do not comply. Always contact the bank or financial institution directly using its official communication channels to verify the legitimacy of the request.

Public free Wi-Fi

Cyberattacks via public Wi-Fi networks occur when fraudsters exploit unsecured wireless connections, commonly available in cafés, airports, and hotels, to intercept user communications or compromise connected devices. Although these networks may appear convenient, they often lack essential security controls.

Threat actors can monitor network traffic to obtain sensitive information such as login credentials, financial details, or personal files. In some cases, attackers may deploy rogue access points, or install malware without the user's awareness. Such compromises can ultimately result in fraudulent activities, privacy violations, or identity theft.

Security Tips

- Avoid connecting to public or free Wi-Fi networks, even those requiring a password, unless you fully trust the provider and have confirmed that network is properly secured.

- Disable automatic Wi-Fi connection on your device. Connect manually only to verified and trusted networks to reduce the risk of unauthorized access or data interception.

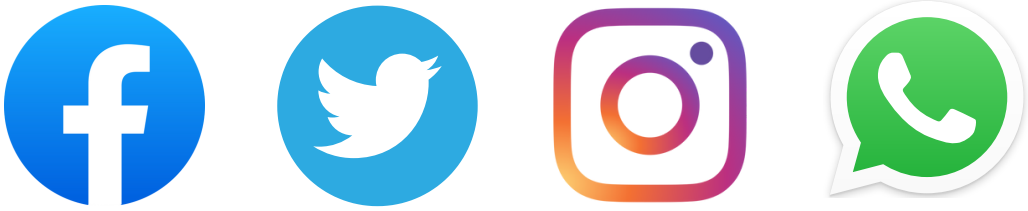
Social Engineering

Social engineering occurs when fraudsters manipulate individuals into sharing sensitive information, transferring money, or carrying out risky actions by exploiting human trust rather than technical flaws. Fraudsters often pose as trusted individuals or organizations — such as coworkers, banks, or service providers — and use phone calls, emails, text messages, or online platforms to appear legitimate.

After establishing contact, fraudsters apply pressure by creating urgency, fear, authority, or promising rewards. As a result, victims may be persuaded to disclose personal data, click on malicious links, or transfer funds. The obtained information is then used for fraud, blackmail, identity theft, or larger cyberattacks.

Common Red Flags:

- Unexpected messages or calls requesting sensitive information
- Urgent appeals for money, help, or immediate action
- Requests for passwords, PINs, or one-time password (OTP).
- Offers, links, or attachments that seem suspicious or “too good to be true”



Security Tips

- Always confirm the identity of anyone requesting money, even if they claim to be a friend, colleague, or relative. Use trusted communication channels to verify the request before taking any action.

- Do not send money to unknown individuals online, regardless of how credible their profiles may appear.

- Avoid sharing personal or confidential information publicly, as such information can be exploited for impersonation, scams, or extortion.

Malicious QR Code

Malicious QR codes are used by threat actors to deceive individuals by disguising harmful links or fraudulent payment destinations as legitimate QR codes. While QR codes are commonly used for quick access to websites, payments, and digital services, attackers may tamper with authentic codes or generate fake ones to redirect users to malicious platforms.

Once scanned, these QR codes may direct users to phishing websites, initiate unauthorized financial transactions, or prompt the disclosure of sensitive information, thereby posing risks of data theft, financial fraud, or device compromise.

Common Exploitation Methods:

- Replacing legitimate QR codes in public places.
- Embedding malicious links in printed advertisements or stickers.
- Creating fraudulent payment requests that mimic real vendors.

Security Tips

- Avoid scanning QR codes from unknown or unverified sources, particulary in public locations or unsolicited messages.
- Always preview the destination URL before opening it. Most modern devices display the link, verify its legitimacy before proceeding.
- Use QR scanner apps with security features, such as malicious link detection or URL filtering.
- Inspect physical QR codes for signs of tampering, overlays, or mismatched branding that may indicate manipulation.
- Never enter sensitive information—such as login credentials or payment details unless the source is trusted and verified.

Fake or Malicious Mobile Applications

Cybercriminals develop fake or malicious apps that imitate legitimate services—such as VPNs or banking apps—to steal personal data, login credentials, or gain access sensitive information.

These apps may appear on official app stores or be distributed through unofficial links. Once installed, they can allow attackers to access the device's contents, including messages, stored data, and One-Time Passwords (OTPs).

Scammers often deceive users into downloading these apps by presenting them as trusted services or urgent updates.

Security Tips

- Do not download applications from unverified or unknown sources, or from links shared by unknown individuals. Applications should only be installed from trusted and official app stores.

- Before downloading any application, verify the identity of the publisher or developer. Review app ratings, user feedback and download counts. An unusually low number of reviews or vague developer information can indicate a fraudulent app.

- Examine the permissions requested by the app prior to installation. Exercise caution with applications that request access to sensitive features—such as SMS, contacts, or device storage—if such access is not necessary for the app's stated purpose.

Malicious Charging Cable

Malicious charging cables are designed to appear as standard accessories but contain embedded malicious components. Fraudsters use these cables to steal data or install malware when they are connected to a device.

Once plugged in, such cables can silently transmit information to a remote system or inject harmful code, granting attackers unauthorized access to personal data, credentials, or device controls.

Security Tips

- Avoid using charging cables provided in public areas, such as airport or café charging stations, as these cables may have been tampered with to compromise your device or extract sensitive information without your knowledge.

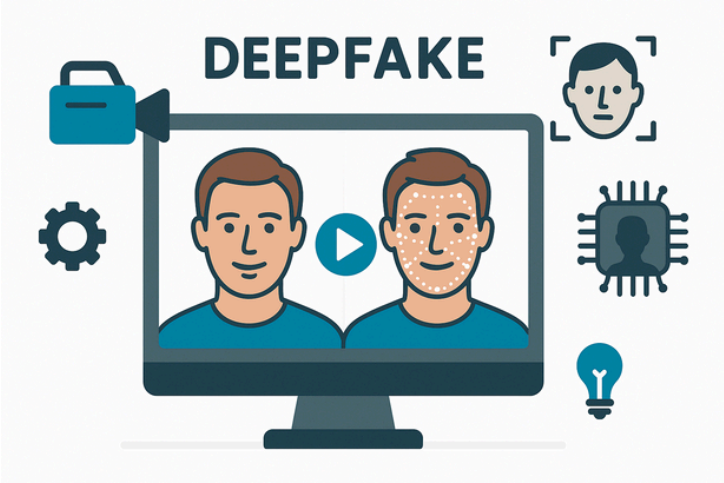
Deepfake

Deepfakes refer to the use of artificial intelligence (AI) to generate highly realistic yet fabricated videos or images that impersonate real individuals. These media are created using advanced machine learning techniques to manipulate content, making it appear as though a person has said or done something they never actually did.

This technology poses a growing threat across multiple domains, including identity theft, social engineering, and disinformation. By undermining trust in digital content and can be used to mislead individuals or institutions.

Common Misuse Scenarios:

- Fake video calls mimic executives or public figures
- Voice recordings used to deceive victims or authorize transactions
- Forged imagery employed in verification or reputational attacks



Security Tips

- Unusual or urgent requests: Be cautious when receiving video messages—especially from familiar individuals that request suspicious actions such as fund transfers or the disclosure of confidential information. Such messages may be artificially generated.

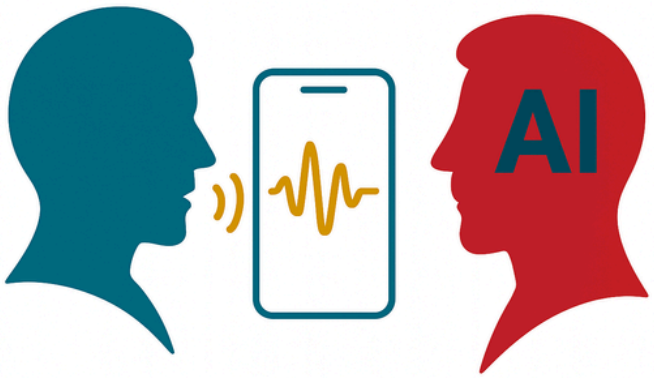
- Visual inconsistencies: look for subtle anomalies, including unnatural facial expressions, inconsistent lighting, mismatched lip-sync, or robotic speech patterns. These are common indicators of deepfake manipulation.

- Out-of-character behavior: If the message content appears implausible or deviates significantly from the sender's typical tone or behavior, treat it with suspicion and verify the request independently.

AI Voice Impersonation

Fraudsters are increasingly leveraging artificial intelligence to replicate human voices with high precision, producing synthetic audio that is nearly indistinguishable from that of a real speaker. This capability enables them to convincingly impersonate trusted sources—such as senior executives, coworkers, or family members—and manipulate victims into taking unintended actions.

Common malicious scenarios include fake calls impersonating senior management, voice messages mimicking relatives in distress, or spoofed verbal instructions authorizing transactions. This convergence of AI-driven voice cloning and spoofed caller identities dramatically amplifies the success rate of funds transfer fraud, the disclosure of sensitive information, and the circumvention of verification controls posing a severe risk to financial institutions and individuals.



Security Tips

- **Unexpected or urgent requests:** Remain alert if you receive a phone call from someone you trust—such as a colleague or family member—requesting unusual or time-sensitive actions like transferring money or sharing sensitive data.

- **Subtle voice inconsistencies:** Pay close attention to minor deviations in speech patterns, tone, pacing, or emotional inflection. AI-generated voices may sound realistic but often miss natural nuances.

- **Absence of personal context:** Synthetic voices may fail to reference shared experiences, known facts, or conversational cues that a real person would naturally include. This lack of contextual familiarity can be a key warning sign.

E-Commerce Fraud

E-commerce fraud refers to deceptive activities carried out through online shopping platforms, where fraudsters exploit consumers by creating fake websites or establishing fraudulent seller accounts on legitimate platforms. These scams may involve counterfeit offers, undelivered products, or theft of payment information, ultimately resulting in financial loss to the buyer.

Common Forms of E-Commerce Fraud:

- Fake product listings or discount offers designed to attract and mislead shoppers.
- Theft of payment data during the checkout process via unsecured or fraudulent websites.
- Non-delivery of purchased goods, despite successful payment confirmation.

Security Tips

- Exercise caution when buying or selling through online marketplaces. Fraudulent listings and impersonated sellers are common tactics used to deceive users.

- Never provide your password or personal identification number (PIN) to receive payments. Legitimate transactions do not require this information.

- Before making a purchase, verify the seller's credibility. Review feedback, ratings, and buyer comments to identify any history of fraud or unethical conduct.

Fraud through Trading Platform

Fraud through trading platforms refers to deceptive practices conducted via unauthorized or unregulated trading applications, particularly those dealing in digital assets or cryptocurrencies. These platforms often permit users to deposit funds but lack secure, and transparent mechanisms for withdrawal. Consequently, users' funds are exposed to high risks, with little to no legal protection.

In some cases, fraudulent brokers may engage in unauthorized trading activities or manipulate funds through informal agreements and unverified transactions, leading to significant financial loss or outright theft.

Common Risks Associated with Fraudulent Trading Platforms:

- Inability to withdraw deposited funds
- Absence of legal protections or regulatory oversight
- Undocumented or manipulated trading activities

Security Tips

- Be cautious when dealing with individuals or entities that promise unrealistically high returns in a short period of time. Such claims are a common tactic used in fraudulent trading schemes particularly those involving digital currencies and may lead to significant financial losses.

Lottery Scam

Lottery scams are a form of online fraud that exploit individuals' desire to win large sums of money. Victims are misled into believing they have won a lottery or prize draw, often through falsified results or unsolicited communications. In reality, no prize exists; and the objective is to obtain funds or steal personal information.

Scammers frequently require that the supposed "winner" to pay upfront charges—such as taxes, processing fees, or legal costs to claim the prize. Once payment is made, the fraudster cease contact, and the victim receives nothing.

Key Characteristics of Lottery Scams:

- Unsolicited notifications claiming you've won a large prize
- Requests for payment prior to the release of the prize.
- Lack of legitimate contact or a verifiable lottery source.

Security Tips

- Be cautious of unsolicited messages or calls claiming you have won a lottery you did not enter, as these are frequently fraudulent attempts to obtain your personal or financial information.

- Do not make any payments or disclose sensitive data in response to such claims; legitimate prizes do not require advance fees or banking information.

Recruitment Fraud

Recruitment fraud involves deceptive practices designed to exploit job seekers by obtaining personal or financial information under the pretense of legitimate employment opportunities. Fraudsters often impersonate established companies or create fake job postings and websites to gain applicants' trust.

These scams typically involve the collection sensitive information such as CVs, identity documents, and banking details. In many cases, scammers conduct staged interviews and later request applicants to transfer money, claiming it is required for application processing, work permits, or onboarding procedures.

Common Tactics in Recruitment Fraud:

- Fake job postings on fraudulent recruitment platforms
- Impersonation of legitimate companies
- Requests for payment during or after a staged interview

Security Tips

- Always research the company before engaging with any job offer. Confirm that the opportunity is genuine and the organization is reputable.

- Use trusted sources and official websites to verify the company's existence and legitimacy. Be cautious of vague contact details or unverified domains.

Impersonation of CBJ-Licensed Finance Companies

This type of fraud involves scammers impersonating finance companies licensed by the Central Bank of Jordan (CBJ) through phone calls, text messages, or spoofed emails. Victims are misled into believing they are receiving a legitimate loan or financing offer—often advertised with low interest rates, flexible repayment terms, or no collateral requirements.

Once a customer engages, the fraudster provides forged contracts and requests payment of various fees or commissions under the pretext of processing loan processing. After these payments are made, the scammer ceases contact, leaving the victim without funds or legal recourse.

Common Red Flags:

- Unsolicited messages promoting easy-access financing
- Pressure to pay upfront “fees” before receiving any funds
- Absence of verifiable documentation or use of unofficial company channels

Security Tips

- Do not rely on loan or financing offers communicated solely through phone calls or messages.

- Always verify that the offering entity is licensed by the Central Bank of Jordan. Use the CBJ’s official website to cross-check the institution, and where possible, visit a physical branch listed on the verified website.

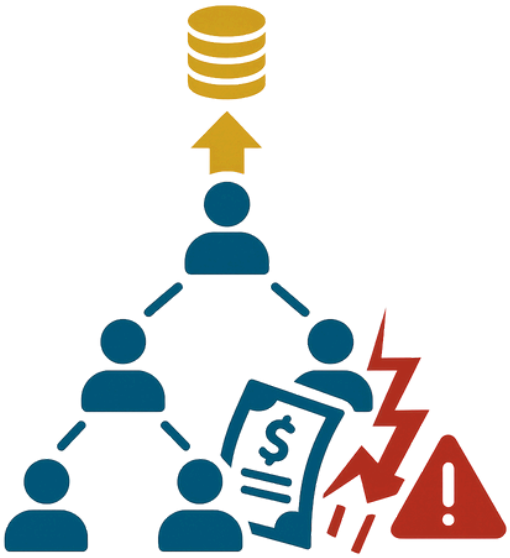
Ponzi Scheme/Pyramid Marketing

Ponzi schemes and pyramid marketing scams are fraudulent investment operations in which individuals are persuaded contribute relatively small amounts of money with promises of high returns and minimal risk. Participants are often incentivized to recruit others into the scheme in exchange for commissions or a share of anticipated profits.

Rather than generating legitimate earnings, early returns are paid using funds collected from newer recruits, creating the illusion of a profitable and sustainable business model. Eventually, when recruitment slows or ceases, the scheme collapses. At that point, the fraudsters disappear with the accumulated funds, leaving most participants to bear significant financial losses.

Common Characteristics:

- Promises of unusually high or guaranteed returns
- Incentives or pressure to recruit additional participants into the scheme
- Absence of transparent, and verifiable business activities.



Security Tips

- Be cautious when encountering any company or individual promising to double your money within an unreasonably short period. Such claims are a hallmark of Ponzi and pyramid schemes and often result in serious financial loss.

Financial Transactions Warnings

General Security Tips

- **Verify Source Authenticity:** Always confirm the legitimacy of any entity before sharing personal or financial information. Verify the company's or institution's identity through its official website and contact details published by authorized sources.

- **Avoid Untrusted Links & Downloads:** Be cautious when browsing unfamiliar websites. Do not click on suspicious links or download unverified attachments. Only enter sensitive information on websites that use secure HTTPS connections.

- **Protect Sensitive Information:** Do not share personal or financial details via phone, email, or untrusted platforms. Use strong, unique passwords and ensure your device’s security software is regularly updated.

- **Ignore Suspicious Emails:** Never respond to unsolicited emails, especially those containing links or attachments. These may lead to phishing websites or introduce malware aimed at stealing your data.

- **Update Contact Information Promptly:** Immediately update your bank or e-wallet with any changes (e.g., phone number). This ensures delivery of OTPs and transaction alerts to the correct device.

- **Avoid International Scam Calls:** Avoid answering unexpected calls from international numbers. Such tactics are frequently used in fraudulent schemes.

Protect Your Devices

- **Update and change passwords frequently:** Update your passwords periodically and use strong, unique combinations for each account.
- **Install and keep antivirus up to date:** Ensure antivirus programs are properly installed, activated, and kept up to date. Apply all operating system security patches promptly.
- **Be cautious when using external devices:** Do not use unknown USB drives without scanning them first with updated security tools.
- **Secure your devices physically:** Never leave your computer or mobile device unattended and unlocked. Always use lock screens and set strong device passcodes.
- **Enable automatic screen lock:** Configure your devices to lock automatically after a period of inactivity to prevent unauthorized access.
- **Avoid installing unverified or untrusted software:** Avoid downloading or installing applications or programs from unofficial or unknown sources.
- **Avoid storing sensitive information unless it is encrypted and securely protected:** Avoid saving passwords, banking details, or personal identifiers directly on your device.
- **Maintain regular backups of critical data:** Regularly back up critical files to secure external storage or encrypted cloud services to safeguard against data loss.

Safe Internet Browsing

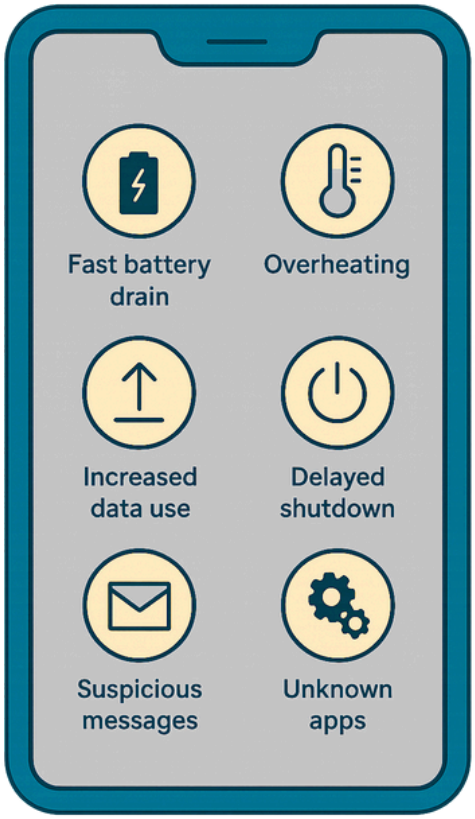
- Avoid accessing untrusted or suspicious websites.
- Refrain from using unfamiliar or unverified web browsers.
- Never enter personal or sensitive information on unsecured websites or shared/public devices.
- Do not disclose financial information to anyone—especially through social media or unverified contacts.

Safe Online Banking

- Log out immediately after completing any online banking session.
- Update your passwords regularly, and ensure they are strong and unique.
- Do not reuse the same passwords for email and online banking accounts.
- Avoid conduct financial transactions on public or shared devices (e.g., internet cafés), unless absolutely necessary.

"Indicators" of Potential Phone Surveillance

- Fast Battery Drain.
- Overheating.
- Increased Data Use.
- Delayed Shutdown.
- Suspicious Messages.
- Installation of Unknown Apps.



Actions to Take Following a Fraud

- Block your payment card and freeze your bank account balance or any e-wallet linked to the card by visiting your bank branch or contacting the official customer service number listed on the bank's or financial company's website. Additionally, verify and ensure the security of other banking channels such as internet banking, the bank's mobile application on your smartphone, and the e-wallet application.

- File a formal complaint with the bank or financial company, as well as with the Central Bank of Jordan.

- Report the fraud to the Cybercrime Unit.

- Perform a factory data reset on your mobile phone (Settings-Reset-Factory Data) to secure your device in cases where the fraud may have resulted from data leakage.

What TO DO !!!

Precautions Regarding Debit/Credit Cards

- You should deactivate optional features on your payment card—such as online purchases (both domestic and international) when they are not needed. If you do not plan to use the card for an extended period, consider temporarily disabling it via your bank's official app or platform.

- If your card is not in regular use, it's advisable to disable the contactless payment feature.

- Always verify the transaction amount displayed on the POS terminal screen before entering your PIN or using contactless payment.

- Never allow merchants to take your card out of your sight when processing a transaction.

- Stay alert and exercise caution when entering your PIN at ATMs or POS terminals to avoid shoulder surfing or skimming.

Safe Password

- Use strong passwords consisting of at least 14 characters, combining uppercase and lowercase letters, numbers, and special characters (e.g., @, #, !).
- Avoid using personally identifiable information (PII) in your passwords, such as your name, date of birth, or the names of relatives.
- Enable two-factor authentication (2FA) or multi-factor authentication (MFA) wherever available, especially for sensitive accounts.
- Change your passwords regularly and avoid reusing the same password across multiple platforms.

Warnings when Depositing

- When depositing funds at a bank, always request a printed receipt confirming the transaction.
- Ensure the receipt is properly completed, including:
  - The deposit amount in both numbers and words
  - The date of the transaction
  - The depositor's name
- This documentation serves as proof of payment and supports dispute resolution if needed.

Submit Complaints

- If you encounter any issues with banks or non-banking financial institutions, you have the right to file a complaint with the Central Bank regarding all institutions under its supervision, including banks, microfinance companies, exchange companies, and payment service companies.

- Initially, you should file the complaint with the bank or financial institution concerned. If you do not receive a response, or if the response is unsatisfactory, you may escalate the matter by submitting a complaint to the Central Bank or resort to legal action.

- You can file a complaint to the Central Bank of Jordan through the following channels:

- Contact the Financial Consumer Protection Department at:
  - Telephone: 06-4630301, subsidiary numbers: 1113 / 1515 / 4825
  - Website: www.cbj.gov.jo
  - Email: fcp@cbj.gov.jo

- Visit the Central Bank headquarters, or its branches in Irbid and Aqaba.

  - Fax: 06-4602482
  - Postal address: P.O. Box 37, Amman 11118, Jordan

- For complaints related to insurance companies, you can contact the Insurance Supervision Department through the following channels:

- Contact the department, including the Insurance Dispute Resolution Department, at the following subsidiary numbers: 4649 / 4969 / 4968 / 4972
- Email: Insurance.Supervision@cbj.gov.jo

Glossary of Terms

(URL)	Uniform Resource Locator
(PIN)	Personal Identification Number
(OTP)	One-Time Password
(HTTPS)	Hypertext Transfer Protocol Secure
(CVC)	Card Verification Code
(SMS)	Short Message/ Messaging Service
(USB)	Universal Serial Bus