Central Bank of Jordan

Awareness Guide on Financial Fraud

Using Electronic Means

2023

Financial Consumer Protection Department (FCP Dep.)

The Unit of Financial Computer Emergency Response Team (Jo-FinCERT)

Contents

Introduction

There has been an expansion and diversification in the financial services, the importance of which has become clearer since the outbreak of COVID-19 pandemic, and an increased spread of electronic financial services driven by the rapid technological developments, which have proven their advantages to clients in terms of being fast, easy to use, secure and of a reasonable cost.

As well, there is a continuous increase in the usage of electronic services, which resulted in the occurrence of fraud techniques that affect the financial consumer and expose him/ her to the risks of becoming a victim of scams and fraud. And owing to the Central Bank of Jordan's (CBJ's) role to raise the awareness of the financial consumer, the CBJ issues this awareness guide that aims to promote the financial consumer's awareness regarding fraud and the tactics used by scammers and how to handle them.

The CBJ emphasizes that the financial consumer should never share any personal data, especially the financial data, with any untrustworthy party.

Handling Procedures and Precautionary Measures

Phishing Links

Phishing links are links that look suspicious and mostly appear through e-mails, text messages and social media. These links aim at deceiving individuals to click on them, thus redirecting them to fake websites that are similar to the legitimate ones, and usually these websites require their users to log in or provide personal or sensitive financial information.

Forms of phishing links:

- Fraudulent e-mail messages.
- Fraudulent mobile phone text messages (Smishing).
- Social Media.

Warning

- Before clicking on any link or opening any attachment in an- email or text message, make sure that it is safe and trustworthy. You may use anti – malware software to check whether the attachments and links are safe.
- Visit the official website of the bank or the financial company that you are dealing with, and carefully check the details of the website, especially when it requires entering data or confidential data. Additionally, check if the website address begins with the (https) sign and the lock symbol before entering any data or confidential data.
- Check the website address's (URL) and the domain name included in the e-mail messages for any spelling mistakes.

Vishing Calls

Voice phishing or vishing calls are phone calls that are used by scammers to deceive people into revealing sensitive personal or financial information. There are many forms of phishing calls including fake claims to win a prize, verifying bank account data, or requesting assistance in a fake issue. Scammers aim at taking advantage of the lack of trust or confusion of people and persuading them to deal with them.

Forms of vishing calls:

- Prize- winning calls.
- Bank account verification calls.

Warning

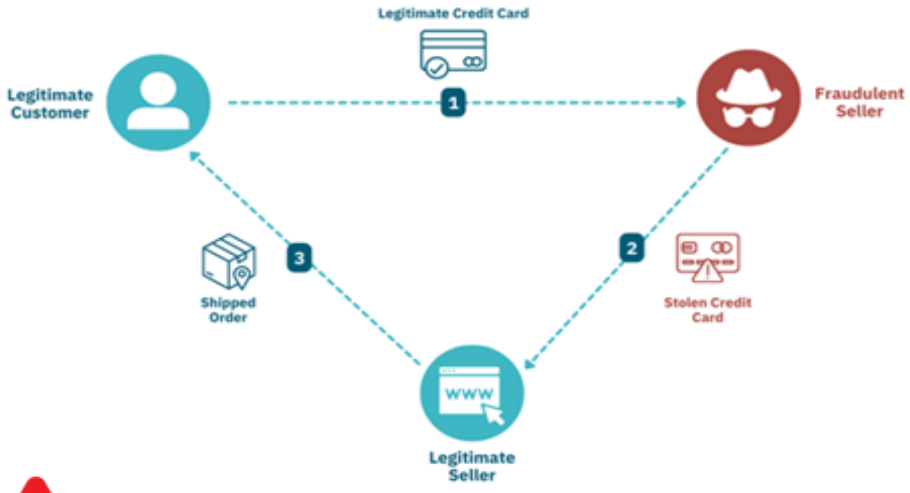
- Know that neither banks nor financial companies ask clients to share any confidential data such as a username, password, or details of client's payment cards (one- time passwords (OTP), Card Verification Value (CVV code)).
- In case you receive a call asking you to implement an unusual procedure or instantly pay an amount of money, make sure to verify the authenticity of the phone call by calling the bank or the institution mentioned during the call using the official contact information and verify the caller's request.

Online Shopping Platforms Fraud

Online shopping platforms frauds are types of frauds that target consumers who shop online. These frauds are implemented by creating fake websites or fake accounts on popular shopping platforms, which enables scammers to trick buyers through fake products and offers, stealing payment data, or not delivering the requested products.

Forms of online shopping platforms frauds:

- Fake selling.
- Payment data theft.



Warning

- Always be cautious when buying or selling products through online shopping platforms.
- Always remember that there is no need to enter your personal identification number/ password anywhere to receive money.
- Before implementing any purchase process through online shopping platforms, search thoroughly and verify the store or seller's reputation. Reading reviews and comments of other users may reveal previous fraudulent behavior or illicit dealing.

Mobile Applications Fraud

- Fake mobile applications are applications claiming to be providing certain services, while actually used to obtain personal information of the users or to access sensitive financial data.
- Scammers deceive the client to open these links, which results in downloading fake applications once the application is downloaded. The scammer might get full access to the client's device including confidential data stored in the device, messages, as well as OTPs received before and after installing these applications.

Warning

- Do not download an application from any unverified/ unknown source, or which was sent by an unknown person.
- As a rational practice before installation, verify the application's publisher/ owner, and check the users' ratings and so on.
- Check the permissions needed by the application before installing it, and make sure it does not require any permission that does not fit the application's functions.

ATM Skimming

- Payment card data breach (prepaid, debit and credit cards): this type of fraud occurs when fraudsters install skimming devices (skimmer) on ATMs. These devices are used to steal the card information and its password.
- Fraudsters may also install a fake keypad on the ATM or a small hidden camera to capture the PIN.

Sometimes fraudsters pretend to be using the ATM and stand beside the client to reach the PIN when the client enters it in the ATM. These data are used later to clone the card and withdraw money from the client's account.

Warning

- Always check the ATM for signs of an additional device that is connected to, or installed close to, the card reader space, or the keypad, before executing any transaction.
- Cover the keypad with your other hand when entering the PIN.
- Do not write your PIN on your payment card.
- Do not enter your PIN in the presence of any other/ unknown person.
- Do not give your payment card to anyone.
- Do not follow the instructions given to you by any unknown person, or ask for help/ guidance from unknown people when using the ATM.
- If the cash was not dispensed from the ATM, press the "Cancel" button, and wait until the screen is back to home screen before leaving the ATM.

VPN Scams

- Virtual private network (VPN) applications are applications used for the purposes of creating connections to intermediate servers between the user and the required websites through a computer or smartphone. Usually these applications are used to access locally blocked websites or applications.
- Some of these applications are insecure, and are used for the purpose of accessing the smartphone data within the permissions related to the application.
- They are also used in fraud in case of insecurely signing in the bank's or wallet's application when activating connection through an insecure VPN as stealing the login information related to the application, or the payment card details registered on the smartphone.

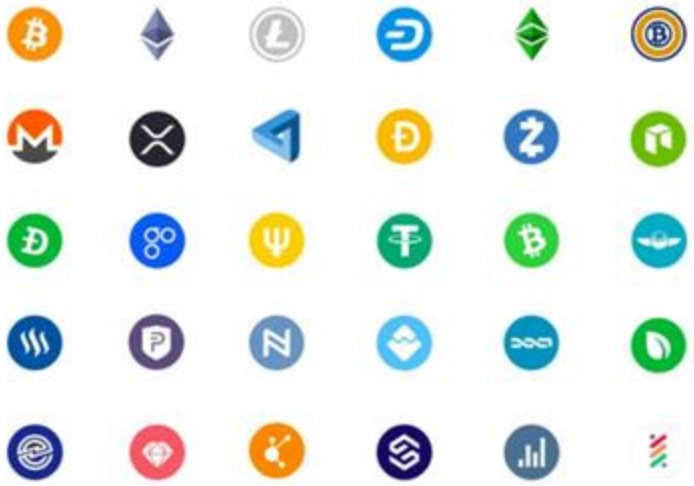
Warning

- Avoid using free VPN applications that could be unreliable and may cause user data leak.
- Do not execute a bank transaction when you are connected to a VPN application to prevent your banking data theft.
- Do not provide the VPN application with sensitive information such as your payments cards details and passwords.

Trading Platforms and Brokerage Fraud

Users of trading apps are often scammed, especially when trading digital currencies which, being unauthorized, is executed through brokers to withdraw or deposit funds, thus imposing risk on the transferred money for not being subject to any clear policy or laws, in addition to being illegal as well.

Fraud is also done through brokers when they operate funds through trading, as when it is agreed to deposit the capital by the first party, and to trade for earning money by the second party, with no written or no documented agreement, which results in the first party losing the deposited money, or the money being stolen by the second party.



Warning

- Be careful not to deal with companies or individuals who claim that they are capable of unrealistically doubling your money within a short period in order to avoid being scammed and the risk of losing your money through digital currencies trading.

Social Media Impersonation

- Impersonation occurs when someone uses the personal information or identity of another person on social media websites. This information can be used to create a fake account, provide false information, or send scam messages in the name of the person being impersonated.
- Scammers, pretending to be your friends, send you a request asking you for money for medical emergencies, pay for some basic needs, etc.
- Scammers also use fake details to contact some users of these applications and earn their trust throughout a period of time. In case the users share their personal data, scammers use these data to blackmail them and get money from them.

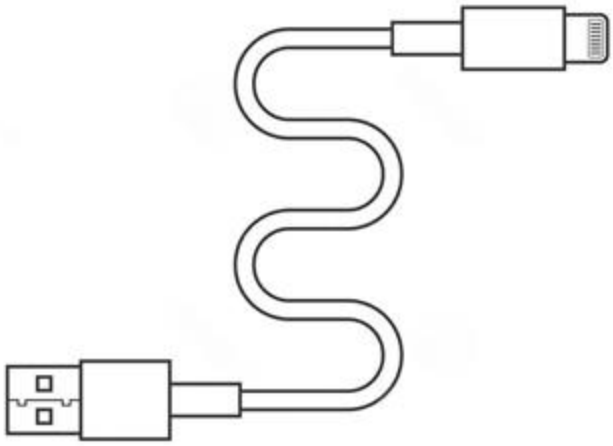
Warning

- Always verify whether the person who is asking you for money is a friend or relative by confirming through a phone call or in person to make sure he/ she is not being impersonated.
- Do not pay money for unknown people through the internet.
- Do not share your personal or confidential information on social media platforms.

Charging Cable Fraud

Charging cable fraud refers to using fake or modified charging cables with the purpose of stealing your personal information, or infecting your device that is being charged with malicious programs. The cables are modified to allow unauthorized access of attackers to your device or record your sensitive information without your Knowledge.

These could be charging cables or stations in public places.



Warning

- Avoid using charging cables that are available in public places such as public charging stations, as you cannot know whether these cables were modified or not, thus imposing risks to your device and information.

Lottery Fraud

- Lottery fraud is considered a type of online fraud that targets people's ambition to win large prizes through lottery. Victims are tempted to participate in fake lotteries, as the results are falsified and the victim is told about his/ her big win, while actually they do not receive any prize, and their money is stolen or exploited illegally.
- Fraudsters ask you to pay taxes or handling fees etc. upfront to receive the lottery.

Warning

- Beware of any unknown messages or phone calls announcing that you won a lottery that you did not participate in; as such messages might be fraudulent and seek steeling your personal information.
- Do not execute any payment transactions or share your financial data in response to any calls or emails.

Online Job Fraud/ Employment Scam

- Online job fraud refers to using illegal or misleading practices to deceive people seeking jobs and steal or exploit their personal information. Fraudsters use a variety of methods to attract their victims and convince them to provide sensitive information such as the Curriculum Vitae, identification documents, and financial information with the aim of using them for suspicious purposes like financial fraud or identity theft.
- Fraudsters contact their victims through job search websites that are created for attracting job seekers.
- Fake interviews are conducted with job seekers, who are later induced to transfer funds to the fake company's accounts to complete the hiring procedures.

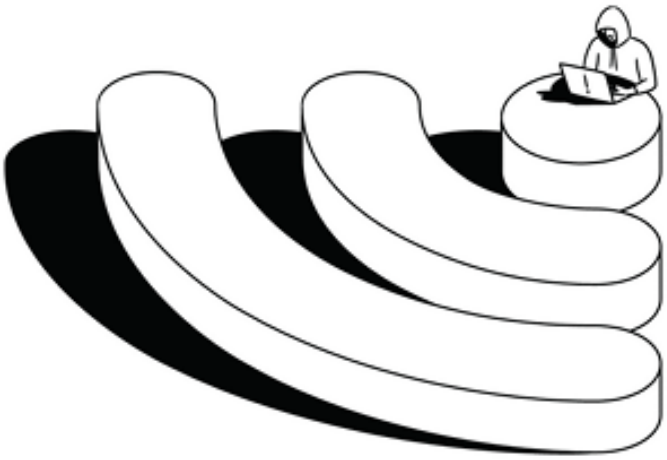
Warning

- Before interacting with any job offer, do some research regarding the employing company to confirm the accuracy of the provided information.
- Use reliable websites and sources to verify the existence of the company and its credibility.

Public Wi-Fi Networks Scam

Public Wi-Fi networks are networks that are available in public places and offer internet connection. They seem to be a free service to access internet. However, they might be used to access the information on the devices that try to connect to the public network.

Through the public network, scammers can get access to the information related to the device such as the information stored on the device or uploading profile files to the device without the user's knowledge.



Warning

- Do not connect to any public network or free network whether or not it requires a password for logging in.
- Turn off automatic Wi-Fi connection: turn off automatic Wi-Fi connection on your device to prevent it from connecting to public Wi-Fi networks. Instead, manually connect to trusted networks only.

Impersonating a Finance Company Licensed by the Central Bank of Jordan (CBJ)

- Calling or sending text messages or e-mails impersonating a finance company, and misleading the clients pretending to grant them a loan/ financing, as these companies offer low interest rates, and/ or flexible repayment options and/or no collateral requirement.
- In case the client responds, he/ she is provided with fake contracts, and several commissions and fees are charged. After these commissions and fees are paid, the fraudster disappears.

Warning

- Do not believe offers provided by people themselves whether through calls or messages.
- It is necessary to verify the identity of the company offering the loan/ financing in case the company was licensed by the CBJ. It is also preferable to visit one of the company's branches, as published on their website, which is listed on the CBJ's website.

Fake Ponzi Schemes/ Pyramid Marketing

- Fraudsters convince clients to invest an amount of money, as it is possible that the amount is small, and the fraudsters promise that the return on the investment will be huge.
- Fraudsters offer the client to market this investment and add new members for a return and a commission for each client added through them into the chain.
- After adding more members, fraudsters terminate the scheme and get all the funds invested by clients.

Warning

- Beware of dealing with companies that claim to be able to, unrealistically, double your money in a short period of time to avoid being scammed and the risk of losing your funds.

Warnings Regarding Financial Transactions

General Warnings

- Before providing any personal or financial information or carrying out any financial transaction, always ensure the authenticity and credibility of the source. Verify the identity of the company or institution and verify its actual existence by using official websites, calling the announced phone numbers, and verifying the concerned parties.
- Be careful when dealing with untrusted websites and avoid opening unknown links or downloading illegal attached files. Make sure that the website uses a secure connection (HTTPS) before entering any personal or financial information.
- Avoid sharing your sensitive personal or financial information via phone, email, or untrusted websites. Update the protection software on your electronic devices and use strong and varied passwords.
- Do not reply to emails from unknown sources because they may have attachments containing malware to steal your data or phishing links.
- Always make sure to update your information with the bank or e-wallet provider immediately if it changes, such as the phone number, because messages related to your account (transaction messages or one- time passwords (OTP)) will be sent to your phone number registered with the bank or e-wallet provider.
- Do not answer incoming calls on your phone if they are of international sources, as fraud is usually conducted through such ways.
- Do not share any personal photos or pictures of your identity proof (personal identity card or passport) with any party.

Protecting the Device/ Computer or Phone

- Change the passwords frequently.
- Install antivirus software on your devices, update it regularly, and make sure to download the latest security updates for your phone's operating system.
- Always test unknown USB Flash Drives before use.
- Do not leave your computer open and do not leave your phone unlocked.
- Set an automatic lock mechanism on your phone/ device after a specified period.
- Do not install any unknown applications or programs on your phone/ computer.
- Do not save passwords or confidential data on the devices.
- Keep a copy of your important data on the device with a backup copy on an external hard drive or through cloud storage services platforms.

Browse the Internet Safely

- Avoid visiting unsafe/ unknown websites.
- Avoid using unknown browsers.
- Avoid entering your personal data on unknown websites/ public devices.
- Do not share your financial data with anyone, especially unknown people on social media.

Obtaining Safe Online Banking Services

- Always use the virtual keyboard on public computers, in light of the existence of hacking mechanisms that capture the keyboard input log.
- Log out of online banking services directly after using.
- Update passwords periodically.
- Do not use the same passwords for email and online banking.
- Try as much as possible to avoid using public devices (such as an Internet café) to conduct financial transactions.

Factors that indicate that Your Phone is Being Spied on

- Your phone's battery is draining faster than usual.
- Your phone overheating could be a sign that someone is spying on you.
- An unusual increase in the amount of data consumption can sometimes be a sign of spyware running.
- Spyware applications can sometimes interfere with the phone shutdown process so that your device fails to shut down properly or takes longer than usual.
- Spyware and malware can use text messages to send and receive data.
- There are applications on the device that you have not downloaded, or active applications on the device that you have not clicked on.

Measures to be taken after Being Exposed to Fraud

- Block the payment card and freeze the balance in the bank account/ e- wallet linked to the card by visiting your branch or calling the official customer service number available on the bank's/ financial company's website. In addition, check and ensure the integrity of other banking channels such as online banking and the bank's application on your mobile phone, as well as the e-wallet application.
- File a complaint with the bank/ financial company and the Central Bank of Jordan.
- Call or report the fraud through the Anti- Cybercrimes Unit.
- Reset your mobile phone (Setting-Reset-Factory Data) to reset your phone in case a fraud occurs due to data leakage from it.

Precautions Regarding Payment Cards

- You must deactivate the various features of the payment card in your local and international online transactions, and if you do not use the card for a period of time, you must deactivate it online.
- If you are not using your card, you must deactivate your card's contactless feature.
- Before entering the personal identification number at any point of sale (POS) site or while using the card with the contactless feature, you must carefully check the amount displayed on the vending machine screen.
- Do not let the merchant take the card out of your sight to swipe it while conducting the transaction.
- Be careful and pay attention while entering the personal identification number at the point of sale site/ ATM.

Email Account Protection

- Do not open links sent via emails from unknown parties.
- Avoid opening emails on public networks.
- Do not store your data/ passwords of your financial accounts, etc. in emails.

Password Security

- Use a combination of alphanumeric characters and special characters in your password, and it must consist of at least (14) characters.
- Maintain two- factor authentication for all your accounts, if available.
- Change your passwords periodically.
- Avoid choosing any personal data when specifying the password, such as your date of birth and the name of a member of your family.

Precautions to be taken by Depositors

- When depositing your money, be careful to obtain the receipt for each deposit you make at banks.
- The receipt must be duly signed, and must contain the value of the deposit, its date, the name of the depositor, and the amount in words and numbers.

Filing Complaints

If you encounter any problem with the banks or non- banking financial institutions that you are dealing with, you have the right to file a complaint to the CBJ against all banks and financial institutions subject to its supervision: banks, microfinance companies, exchange companies, and payment service companies.

First, you must submit the complaint to the bank/ financial institution you are dealing with, and in the event of no response or dissatisfaction with the response, you can submit your complaint to the CBJ or resort to the courts.

You can file a complaint to the CBJ through the following means:

Contact the Financial Consumer Protection Department: 06 4630301

On the following extension numbers: 1113 / 4825 / 1515

The website of the CBJ: www.cbj.gov.jo

Financial Consumer Protection Department's e-mail: fcp@cbj.gov.jo

Personal attendance to the Central Bank's main building and its two branches in Irbid and Aqaba.

Fax: 06 4602482

P.O. Box 37 Amman 11118 Jordan

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

Contact the department/ the Insurance Disputes Resolutions Division on the following extension numbers: 4649/4969/4968/4972

Insurance Supervision Department's e-mail Insurance.Supervision@cbj.gov.jo

Abbreviations List

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