BANK OF ISRAEL
Office of the Spokesperson and Economic Information

December 1, 2022

Press Release:

Warning to the Public about Fraud Committed by Posing as the Bank of Israel or Banking Corporations

The Banking Supervision Department is making the public aware that criminal elements are attempting to carry out acts of fraud with the goal of taking money fraudulently from customers by impersonating, among others, representatives of banks, credit card companies, the Bank of Israel, and the Israel Police. Sometimes, the criminal elements send forged documents proving their false identity, such as a Police ID card, or a letter from the Bank of Israel. The attempts at fraud include the criminal elements contacting banking system customers through a range of communication channels such as phone conversation, SMSs, and email. The notices are sent from an address that appears to be that of the institution they are impersonating, such as a bank. During the fraud, use is made of forged addresses and phone books that appear to be that of the bank or Bank of Israel, and at times the notices include a link to a website appearing to be legitimate.

After the criminal element makes contact between and the account holder, the criminal element requests of the account holder to send him or to transfer to him personal details or financial information that allows funds to be withdrawn from his account. The information that the criminal element is liable to request includes: personal details, account details, credit card details, and the code received by the account holder or credit card holder via mobile phone.

Sometimes, the criminal elements request the details while making threats or adopting a strategy of scaring and pressuring the customer, as they claim that the requested information is required to protect the account from the activity of a criminal element or supposed malfunction that occurred at the servers of the bank or credit card company, which requires urgent handling that requires the information requested. Another strategy used by criminal elements is the promise to receive money, notification of winning a lottery, or needing to connect to the bank account in order to make an attractive investment.

The public is requested to increase its vigilance and not to provide personal or classified details. We would like to note that the Bank of Israel, banking corporations, and credit card companies will not contact citizens with a request to send personal and confidential details or financial details including means of authentication and identification sent to the person making contact, such as an SMS containing a personal code.

If you suspect that you have fallen victim to an incident of fraud, we recommend directly contacting the banking corporation's security department or the ombudsman as soon as possible. To the extent that you do not receive a response or that the response is not satisfactory, you can contact the Banking Supervision Department with a complaint on the issue.

Recommendations for securing your bank account:

- Do not connect to your bank account via an SMS or email you receive.
- Examine the website address to which you are connecting, and make sure it is spelled correctly, particularly if you are connecting after searching for the address on a search engine.
- Provide identification details only after calling the banking corporation's call center back using a number that you found on your own on the bank's website.
- Do not provide credit card or identification code details sent to you via SMS or email in order to complete details. The bank or credit card company will not ask you for code details during a phone conversation that the customer does not initiate.
- If you made a mistake and are concerned that you provided details to a criminal element, call the banking corporation immediately and report it to them.
- Make a periodic examination of activity and transactions in your account in order to find suspicious transactions or inconsistencies.
- If there is any doubt, there is no doubt—and it is best not to answer any message or phone call or to click on any link before examining them with the relevant bank or company.