CREDO BANK

BANK CARD SECURITY RULES

To enhance your protection against cyber fraud, particularly phishing—a prevalent cybercrime tactic aimed at deceitfully acquiring users' personal data—here are refined recommendations. These guidelines are crucial for safeguarding your information during various transactions, such as using ATMs, making non-cash payments at POS terminals, and engaging in online banking activities.

Enhanced Security Tips for Bank Card Users and Phishing Prevention:

- Exercise Caution with Suspicious Websites: Avoid inputting personal information on websites that appear untrustworthy or have questionable credentials.
- Be Wary of Unsolicited Emails: Disregard emails requesting personal or banking details. Remember, legitimate banks never solicit sensitive information through email.
- Question Urgency in Messages: Treat messages pressuring immediate action with skepticism. Urgency is a common tactic used by cybercriminals to provoke hasty decisions.
- Scrutinize Website Quality: Evaluate the professionalism and accuracy of websites. Poor design or grammatical errors can be indicators of fraudulent intentions.
- Verify Familiar-Looking Requests: Always double-check communications that appear familiar but raise doubts. This vigilance is key to minimizing risks, as cybercriminals often masquerade as trustworthy entities.

By adhering to these enhanced security measures, you can significantly reduce the likelihood of falling victim to cyber fraud and ensure the safe use of your bank card across various platforms.

TERMS AND CONDITIONS FOR CONTACTLESS CARD PAYMENTS

We hereby wish to notify you that, in compliance with the regulations set forth by the National Bank of Georgia, a modification to the verification procedure for contactless payment via payment cards has been implemented as of May 1, 2023. Specifically, it is now mandatory to verify transactions with a PIN code for every consecutive 600 GEL spent in contactless transactions, regardless of the card used.

Please take note of the following details:

- Contactless transactions conducted prior to May 1, 2023 will be considered in the tally.
- The count will reset to zero once the initial PIN code transaction is performed, such as an ATM withdrawal.
- Electronic wallets, including Google Pay and Apple Pay, are exempt from this regulation.
- Transactions in which the amount is not manually adjusted, such as parking fees, will not be factored into the calculation.

- Small transactions, particularly those amounting to 10 GEL or less, will not contribute to the tally.

Contactless payment limit without requiring a PIN verification remains unchanged at 100 GEL.

GENERAL RECOMMENDATIONS

- Never disclose the PIN code of your card to a third person, including relatives, friends, workmates, employees of credit organizations, cashiers and also those who assist you in using the bank card.
- It is recommended to change the PIN code with a combination you can easily remember.
- Never give the card to a third person.
- When receiving an incoming call or email, do not disclose your card details even if a caller has presented himself as an employee of the bank serving you.
- Make sure you have activated the SMS service for transactions.
- In case of loss or theft of the card, block it in time with the help of remote services (the Internet/Mobile Bank) or notify the Bank through the call center +995 32 2 42 42 42.

RECOMMENDATIONS WHEN USING A BANK CARD IN ATMS

- When entering the PIN, make sure that it is not visible for a third person standing near you.
- Outside the county, try to carry out the operation in the TMSs located in bank branches, state organizations, large shopping centers, hotels, airports, etc.
- Carefully read the notice displayed on the ATM (if any) as it may inform you on additional service fees.
- The service provider of an ATM or terminal, independently of CREDO BANK, may offer you to carry out the cash-out transaction in a different currency regardless of the currency the ATM physically dispenses or you have available on the card. If you agree to the offer, the operation will be processed at the rate determined by the ATM which may result in significant costs to you, so be careful with the offered exchange rate and make the desired choice.

RECOMMENDATIONS WHEN USING A BANK CARD IN THE INTERNET

- It is better to use your bank card in the Internet only in your personal computer as there is a risk of remembering confidential information.
- Use your card only on reliable and well-known Internet sites.
- Do not trust unbelievably attractive offers.
- Do not enter the Internet Bank username and password on the web pages opened by clicking on the link.
- Always enter the address of the Internet Bank yourself.

RECOMMENDATIONS WHEN USING A BANK CARD IN SHOPPING UNITS (POS-TERMINAL)

- Never give your card to service personnel, including at restaurants or petrol/gas filling stations.
- Request the card operation to be carried out in your presence to reduce the risk of illegal acquisition of the card data.
- Verify the amount of the withdrawn cash in the SMS or on the receipt

PHISHING

We would like to share to you tips how to protect yourself from online cyber fraud. One of the most common forms of crime is phishing.

Phishing is a form of cybercrime, the purpose of which is to fraudulently obtain personal data of Internet users.

For example: Cyber fraudsters forge websites of well-known companies or sent messages on their behalf through various remote channels, where users are asked to enter personal data (password, card number, etc.).

To protect yourself from the said scam:

- Do not enter your personal information on suspicious websites;
- Do not trust emails where you are asked to enter your personal information or bank details. Your bank will never ask you for sensitive information by email;
- Do not trust messages that require any urgent action from you. Urgency is often a sign that you are facing a cybercriminal;
- Check the website, if it looks less professional or contains errors, the sender may be a cybercriminal.
- Remember that a cybercriminal is trying to deceive you with a familiar image. Therefore, it is necessary to verify everything that seems suspicious to you. You will be able to minimize the risks only in this way.

FOLLOW THE GENERAL SECURITY RULES AND BE CALM AS YOUR CARD IS IN YOUR OWN SAFE HANDS!