Memo

Compliance with security measures to prevent remote fraud

- A real bank employee will never ask you to provide him with any of your bank card details. You can call the code word only if you call the bank's hotline yourself.
- If you received a call and were told that your relative was in trouble, the first thing you should do is call your relative back.

- Any payments to pensioners are made only by the assigned social worker.
- If you receive an SMS about winning a prize or winning a lottery, do not respond to the received SMS message, do not call or write to an unknown number.
- Do not transfer funds to strangers under any pretext.
- Always check the information and be careful

If your bank card is lost:

1. Block the card.
2. Check recent transactions.
3. Contact your bank to issue a new card

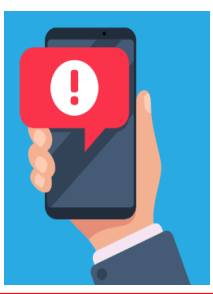
In case of theft of funds from a bank account:

1.Contact the bank immediately and describe the situation

2.Go to the police and report or call 102 (from mobile 112).

3.Send a notification coupon to the bank about the accepted application in the police station.

In case if you lost your phone:

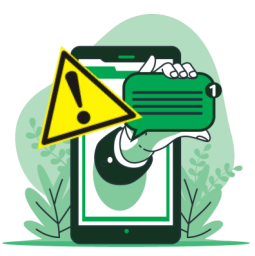


1.Contact your bank to block the banking application and delete your bank card data from your mobile device.

2.Contact your mobile operator to block your SIM card.

3.Check the latest transactions on bank cards and accounts.

REMEMBER:



1. Do not tell anyone your bank card details, SMS codes, PIN code, three-digit code on the back of the card, do not enter any dubious combinations on your mobile device and do not follow unknown links.
2. Do not rush to trust the caller, even if he introduced himself as "an employee of the bank, including the security service." If you receive a suspicious call from the "bank", without continuing the conversation, without answering the questions, immediately stop the conversation and call the bank back yourself using the official number - it is on the Bank website or the back of the card, having clarified the information you received from the caller, do not call back by calling the number of the caller, you can get scammers again.
3. Do not tell strangers details about yourself on social networks: last name, first name, patronymic, place and year of birth, passport details.
4. Do not install unknown applications on your phone at the request of a "bank employee" or "financial advisors."
5. Use the bank's official services "Transaction Notifications".
6. Do not transfer mobile devices with banking applications installed into the hands of unknown persons, including those involved in payment chains for certain goods and services. Do not store card details on your phone: number, expiration date, verification code and card PIN.

7. Do not use an ATM in the presence of suspicious people and do not accept help from strangers, give preference to ATMs installed in secure places (for example, in bank offices, government agencies, large shopping centers), and cover the keyboard with your hand when entering the PIN code.
8. Ensure the safety of bank cards, in particular those providing contactless payment methods.
9. Make purchases, access the bank's website or banking applications only from your personal computer, tablet and phone. Set passwords for all your gadgets.
10. Do not trust information from callers, as well as from SMS, with offers of free provision of various services, such as medical services, investing money, making contributions to any investment projects, in particular under the pretext of making further profits, you pay compensation, do not follow the messages sent unknown links

If illegal actions are committed against you and your loved ones,

call 102:

from mobile 112