



SELF-SERVICE MACHINES SAFETY TIPS



Make sure that the self-service machine has no skimmer (scammers attach them to the card reader for reading information from the card);

Make sure that scammers did not fix keyboard overlay;

When you use ATMs or POS terminals, make sure that no one sees the PIN code that you enter – shield the keyboard with your hand.

- If you got the impression that something is wrong with ATM, we advise to make cash withdrawal via another ATM. Protruding wires or material around the card reader that does not match the color of the rest device - sufficient grounds for suspicion. You may be wrong, but the risk is certainly not worth it.
- Inspect the area around the ATM for mirrors or other suspicious objects. No foreign objects must be in the place where the ATM is installed.
- Look for ATMs under video surveillance. Typically, devices located in the surveillance zone, are better protected from the possibility of installation of the skimmers.
- Beware of ATMs in suspicious places. Skimmers are easier to be installed on devices located back from crowded places and busy streets.
- Do not be afraid to touch the ATM. If you feel that device looks unusual, safely check for skimmer on the ATM. If the fraudsters can remove spyware from the card reader, then you can do it too.
- Do not make transactions with outside help. Fraudsters can disguise themselves as technicians, bank employees, or simply impersonate customers. If a person dressed in an official uniform tells you that your device is being repaired or cleaned and offers assistance in withdrawing funds, simply walk away.



The Bank has all the necessary information and **NEVER**, under **NO** circumstances calls, sends emails, SMS messages, requesting to provide card details, PIN code of the card, and credentials, as well as emails programs and their updates.



In case of compromise of information or detection of unauthorized transactions, you should immediately call the Contact Center: 7111 (toll free), 8(727) 259-07-77 (for Almaty).