Payment System

Expand Hide

Press releases Press room

30.10.2019

Recommendations for increasing safety in the use of a payment card

Recommendations for the safe use of payment cards in a physical environment

	Managing the PIN code and other codes/passwords	Keep your PIN, CVV2 / CVC2 / CID code or any other password related to the payment card secret: — Do not tell your PIN number to anyone, not even to the members of your family (nobody has the right to demand your PIN, CVV2/CVC2/CID code or any other password); — Try to remember the PIN number without writing it on the payment card or any other support; — Even if you wrote the PIN number somewhere, make sure that this information is kept safe, separately from the payment card; — Keep the card and the file containing sensitive authentication data received from the bank at the time of receipt of the card (PIN, CVV2/CVC2/CID) separately, to exclude their simultaneous possession, in case of unauthorized use. — Enter the PIN number in a discreet way when making payments at POS terminals or at withdrawal of cash from banks' ATMs, in order to avoid their reproduction and fraudulent use by third parties; — Modify the PIN number[1] periodically. — Do not use a combination of figures/common password for accessing all payment instruments; — Contact immediately the bank and change the PIN number in case of suspicion regarding the unauthorized possession of the card by other persons.
	Applying certain value limits of daily transactions made with the payment card	— In order to prevent fraud situations, activate the option of setting value limits for transactions made with the card. The limit represents the maximum value of transactions or a maximum number of operations that can be carried out daily/weekly/for a certain period, from the payment account attached the card.
	Applying precautionary measures when using the payment card	— Check your bank's website frequently for security measures when using the payment card and the bank's contact details if necessary. — In case of loss, theft or other suspicious situations, inform the bank immediately and request the locking of the card. Bankcard support services are available 24/7/365. — Check the sum indicated on the screen of the POS terminal/ATM before the validation of the transaction.
	Activation of notification services regarding the transactions performed	— Activate the SMS-notification service[2] to be immediately informed about the transactions made with the payment card. — In the event of a payment card transaction failure, promptly check the balance of the account attached to the payment card, by viewing the content of notifications received or through internet-banking, mobile-banking applications or other means offered by the issuing bank in this respect.

	Safe maintenance/use of payment card and keeping the confirming documents	— Keep the card in pertinent conditions to avoid damage, loss and theft, or compromise of data from the card; — Sign the card on the reverse side, immediately upon receipt; — Do not give the card to third parties; — Ask to perform the operations at the merchant/bank's counter only in your presence, do not allow its photographing or making copies by persons who are not authorized for such actions, to avoid the theft of data registered on the card that can be used when conducting transactions in the online environment; — Avoid to store/send confidential information by phone, mail and/or other means of communication through unsecured channels; — Ask for confirming documents or visualize the received notification after every transaction performed by a special device (ATM, POS terminal) and check carefully the information highlighted on the card (date, card number, first / last name, transaction amount, transaction currency); — Keep all confirming documents related to the transactions so that you can compare them with the transactions described in the statement of account.

1. This service is provided by banks, both at ATMs and via the automated remote service systems (internet-banking, mobile-banking, etc.).
2. This service offers the possibility to receive notifications on the mobile device without having internet connection.

Recommendations for the safe online use of the payment card

	Check the security of online merchants	— Check the presence of 3D-Secure symbols on the e-commerce platforms (Mastercard Secure Code, VERIFIED by VISA, American Express SafeKey). These symbols are usually displayed at the bottom of the web page of the merchant; — Check if the website of the merchant is secured through the presence of the SSL logo[3] or if its address starts with "https://", which indicates the encryption of the transmitted information; — Never provide the PIN number when making online transactions because it is not necessary. No online merchant is entitled to ask you to introduce the PIN number in a box on the e-commerce platform; — Avoid using the option "keep data" which offers the possibility to make future transactions without the need to enter the data of the payment card.
	Use a safe environment for making payments	— Avoid using Wi-Fi public networks to perform online transactions, as they can be used to capture the transmitted data; — Protect your computer by activating the security updates provided by software producers (usually for free) and install an antivirus or antimalware program[4], which will contribute to the detection of fraudulent programs, aimed to capture the personal data entered, of websites created by criminals in order to obtain confidential data, etc.; — Avoid accessing suspect links from emails, social networks, instant message delivery programs, especially in cases where personal data or card information is required; — In case of online transactions, we recommend you to use a virtual card[5], where you can transfer the sum necessary for the transaction; — Keep all confirmation documents of the operations performed until the final settlement of sums from the account of the card.

	Management of CVV2 / CVC2 / CID codes and one-time passwords	— Do not give to anyone your CVV2 / CVC2 / CID code or any other one-time password received from your bank to authorize a payment or to subscribe to internet-banking/mobile-banking systems.

3. Security standard for the connection between the browser and the server.
4. Protection program developed specifically to counteract software that is designed to infiltrate or damage the computer system without the consent of the owner.
5. Card that allows only online transactions, which has a separate payment account. The lack of the magnetic strip and the chip do not allow the payments in a physical environment.

Tags
safe use of payment cards [1]
increasing safety [2]
payment cards in a physical environment [3]
safe online use of the payment card [4]

Source URL:
http://bnm.md/en/content/recommendations-increasing-safety-use-payment-card

Related links:

[1] http://bnm.md/en/search?hashtags[0]=safe use of payment cards [2] http://bnm.md/en/search?hashtags[0]=increasing safety [3] http://bnm.md/en/search?hashtags[0]=payment cards in a physical environment [4] http://bnm.md/en/search?hashtags[0]=safe online use of the payment card