

Памятка по противодействию несанкционированным операциям (мошенничеству)

Уважаемый клиент ПАО «НИКО-БАНК»!

В связи с высоким уровнем объема и количества операций без согласия клиентов, совершаемых, в том числе с применением методов социальной инженерии (в особенности, телефонного мошенничества), рекомендуем Вам проявлять осмотрительность в отношении сохранности информации, используемой в целях совершения банковских операций, в частности перевода денежных средств.

Предупреждаем Вас о недопустимости сообщения посторонним лицам информации (например, персональных данных, данных банковской карты, пароля из СМС, кодовых слов и т.д.), использование которой указанными лицами может привести к совершению перевода денежных средств без согласия их владельца.

Общие рекомендации по снижению риска несанкционированного перевода денежных средств:

1. Никогда не сообщайте посторонним лицам информацию, используемую для совершения банковских операций - персональные данные, данные банковской карты, логин и пароль от системы «Интернет-Банк», пароли из СМС, кодовое слово и т.д. Мошенники могут использовать полученную информацию для совершения переводов денежных средств с Ваших счетов без Вашего согласия. При получении просьбы, в том числе со стороны сотрудника банка, сообщить вышеуказанные данные или совершить какие-либо операции, перезвоните в банк и сообщите о данном факте (в целях информационного взаимодействия с банком рекомендуется использовать только реквизиты средств связи, которые указаны в документах, полученных непосредственно в банке).

2. ПИН-код Вашей карты необходимо запомнить или в случае, если это является затруднительным, хранить его отдельно от карты в неявном виде и недоступном для третьих лиц месте.

3. Никогда ни при каких обстоятельствах не передавайте карту для использования третьим лицам.

4. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с Вашего счета целесообразно установить суточный лимит на сумму операций по карте и одновременно подключить услугу оповещения о проведенных операциях.

5. Не рекомендуется отвечать на электронные письма, в которых от имени банка предлагается предоставить персональные данные. Не следуйте по «ссылкам», указанным в письмах (включая ссылки на сайт банка), т.к. они могут вести на сайты-двойники.

6. В случае если карта, мобильный телефон и данные для входа в систему «Интернет-Банк» были утрачены, необходимо немедленно обратиться в банк и следовать указаниям сотрудника банка.

7. Осуществляйте операции с использованием Устройств самообслуживания, установленных в безопасных местах (например, в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.). Перед использованием Устройства самообслуживания осмотрите его на наличие дополнительных устройств, не соответствующих его конструкции и расположенных в месте набора ПИН-кода и в месте (прорезь), предназначенном для приема карт (например, наличие неровно установленной клавиатуры набора ПИН-кода). В указанном случае воздержитесь от использования такого Устройства самообслуживания.

8. Набирайте ПИН-код карты таким образом, чтобы люди, находящиеся в непосредственной близости, не смогли его увидеть. При наборе ПИН-кода прикрывайте клавиатуру рукой.

9. В случае если Устройство самообслуживания работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается), следует отказаться от использования такого Устройства самообслуживания, отменить текущую операцию, нажав на клавиатуре кнопку «Отмена», и дождаться возврата карты.

10. Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с картой в Устройствах самообслуживания.

11. Не используйте карты в организациях торговли и услуг, не вызывающих доверия.

12. Требуйте проведения операций с картой только в Вашем присутствии.

13. Не используйте ПИН-код при заказе товаров и услуг через сеть Интернет, а также по телефону.

14. Пользуйтесь интернет-сайтами только известных и проверенных организаций торговли и услуг. Обязательно убедитесь в правильности адресов интернет-сайтов, к которым подключаетесь и на которых собираетесь совершить покупки, т.к. похожие адреса могут использоваться для осуществления неправомерных действий.

15. Рекомендуется совершать покупки и осуществлять переводы только со своего компьютера/смартфона в целях сохранения конфиденциальности персональных данных и (или) информации о карте (счете).

16. Установите на свой компьютер/смартфон антивирусное программное обеспечение и регулярно производите его обновление и обновление других используемых Вами программных продуктов (операционной системы и прикладных программ), это может защитить Вас от проникновения вредоносного программного обеспечения.

17. При обнаружении Вами попыток несанкционированного доступа к Вашим счетам или в случае мотивированных опасений, что такие попытки могут быть осуществлены, просим Вас:

- немедленно сообщить об этом в ПАО «НИКО-БАНК» по одному из следующих телефонов: (3532) 34-90-32; (3532) 20-55-42;

- заблокировать карты и систему «Интернет-Банк».

Соблюдение вышеуказанных рекомендаций существенно повышает сохранность Ваших денежных средств!