Памятка держателям банковских карт АО «Севастопольский Морской банк» (Банк)

1. Мошенничество с использованием SMS - рассылки

SMS мошенничество является примером использования методов социальной инженерии и основано на доверии клиентов к сообщениям банка. Мошенники могут рассылать сообщения следующего содержания:

** «Ваша банковская карта заблокирована, перезвоните по номеру телефона +7 (XXX) XXX-XX-XX или обратитесь в службу банка по телефону +7(XXX)XXX-XX-XX».*

В случае обращения по указанному номеру мошенники будут требовать для разблокировки карты конфиденциальные данные: полный номер карты, срок действия карты, CVC/CVV, PIN-коды. Также мошенники могут предложить пройти к ближайшему банкомату, перезвонить на указанный в сообщении номер и для разблокировки карты потребуют перевести деньги с вашей банковской карты на электронный кошелек, карту стороннего банка или телефон.

Обратите внимание: Сотрудники Банка не запрашивают конфиденциальные данные клиентов в телефоном режиме!

** «Оплата покупки с вашей банковской карты на сумму XXX рублей прошла успешно. Если вы не совершали покупку, перезвоните по номеру +7 (XXX) XXX-XX-XX или обратитесь в службу банка по телефону +7(XXX) XXX-XX-XX».*

В случае обращения по указанному номеру мошенники могут представиться работниками службы безопасности банка или технической поддержки банка. Для отмены операции и возврата денежных средств обратно на карту мошенники запросят у вас код подтверждения из СМС-сообщения.

Обратите внимание: Сотрудники Банка не запрашивают информацию о коде подтверждения операции. Для отмены операции код подтверждения не требуется!

** «Вам одобрен кредит в размере XXX рублей, его возможно получить, не обращаясь в Банк. Указанную сумму доставит курьер после оплаты на карту компании Х-% от суммы кредита. После того, как необходимая сумма будет получена, кредит можно будет получить, не подавая никаких заявок и не подписывая кредитную документацию».*

В случае обращения по указанному номеру мошенники могут потребовать перевести денежные средства на карту стороннего банка и запросить конфиденциальную информацию.

Обратите внимание: услуги кредитования в АО «Севастопольский Морской банк»» могут быть предоставлены только при личном обращении в отделения Банка.

Также вы можете получить от мошенников SMS–сообщение с требованием обновления персональных данных или данных мобильного банка. Для вашего «удобства» в сообщении будет форма для ввода необходимых данных или ссылка для перехода в мобильный банк.

Обратите внимание: Сотрудники Банка не запрашивают информацию, содержащую конфиденциальные сведения, персональные данные клиентов в режиме SMS-сообщений!

2. Мошенничество с использованием рассылки по электронной почте

Аналогичные сообщения о блокировке карты, банковского счета, увеличении задолженности по кредиту, о каком-либо выигрыше или получении наследства мошенники могут направлять и по e-mail. В сообщениях также могут содержаться ссылки на сайты, на которых вам будет предложено ввести свои персональные данные, логин и пароль для входа в мобильный банк, кодовые слова, реквизиты карты или счета. Подобные письма могут содержать вложенный файл с вирусом или ссылку на сайт с вредоносным программным обеспечением, заражающим компьютер при открытии страницы, **которые Вам не следует открывать** в целях соблюдения мер безопасности.

Обратите внимание: Банк не использует e-mail клиентов-держателей банковских карт для запроса информации, содержащей конфиденциальные сведения, персональные данные клиентов!

3. Предупредительные меры безопасности

В целях безопасности очень важно отличать официальные уведомления Банка от уведомлений мошенников. Обращайте внимание: с какого номера телефона или адреса направлено уведомление; соответствуют ли данные отправителя данным из ранее получаемых сообщений/писем от Банка. Мошенникам не известен номер вашей банковской карты, номер счета, поэтому в сообщении будет указано: «Ваша карта», «Ваш счет».

При любых сомнениях по вопросам безопасного использования банковской карты/реквизитов карты обращайтесь в Банк по официальным телефонам, номера которых размещены на оборотной стороне карты или на официальном интернет сайте Банка www.morskoybank.com

Единый информационный центр АО «Севастопольский Морской банк»:

+7- 978-777-3-111 (время работы с 9:00 до 17:00, понедельник – пятница)

Круглосуточная служба поддержки держателей карт: +7- 978 - 842 - 70 - 39

4. Рекомендуемые меры защиты от мошенничества и предосторожности при использовании банковской карты/реквизитов карты

- В случае получения подозрительного сообщения от имени Банка (например, «Ваша карта заблокирована»), содержащего номер мобильного телефона, с требованием / просьбой перезвонить на указанный номер, никогда не перезванивайте на указанный номер.
- В случае получения SMS-сообщения о каких-либо финансовых операциях по Вашим банковским картам, которые Вы не совершали, обязательно перезвоните в службу поддержки по круглосуточному телефону **+7-978-842-70-39** (указан на обратной стороне Вашей карты). Оператор проверит операции по Вашей карте и заблокирует ее при подозрении в мошеннических действиях третьих лиц.
- В случае входящего звонка на Ваш мобильный телефон никогда не называйте все реквизиты Вашей карты (номер, срок действия, CVV-код и пр.) и не предоставляйте все Ваши персональные данные (серия и номер паспорта, адрес регистрации, контактные телефоны, данные о счетах).
- В случае поступления входящего звонка на Ваш мобильный телефон с сообщением о том, что Ваша карта заблокирована и для ее разблокировки необходимо установить Вашу личность через банкомат – не осуществляйте требуемых действий и не сообщайте реквизиты Вашей карты (номер, срок действия, CVV-код и пр.).
- Никогда не называйте все реквизиты Вашей карты (номер, срок действия, CVV-код и пр.) и не предоставляйте все Ваши персональные данные (серия и номер паспорта, адрес регистрации, контактные телефоны, данные о счетах).
- Обращаем Ваше внимание на то, что владелец карты не может передавать свою карту и / или называть PIN-код другим лицам. В целях безопасности владелец карты обязан хранить номер PIN-кода отдельно от карты. Операции с использованием PIN-кода признаются совершенными владельцем и оспариванию не подлежат.
- Никогда не сообщайте реквизиты Вашей карты третьим лицам и не передавайте ее в руки незнакомым людям, в том числе официантам, продавцам в магазинах и пр.
- Помните о том, что сотрудники Банка никогда не запрашивают у Вас номер Вашей карты, CVV-код, PIN-код или коды, которые поступают в SMS-сообщениях от Банка для подтверждения совершения операций лично, по телефону или через SMS-сообщения.
- При смене номера мобильного телефона или какой-либо иной личной информации (фамилия, адрес постоянной регистрации и пр.) оперативно сообщите Банку актуальные данные.

Ознакомиться с правилами безопасного использования/хранения банковских карт можно на официальном банка сайте Банка: http://www.morskoybank.com/files/safety_rules_cards.pdf