РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ БАНКОВСКИХ КАРТ

1. ТРЕХЗНАЧНЫЙ КОД НА ОБОРОТЕ КАРТЫ, а также ПАРОЛЬ ИЗ СМС могут требоваться для отдельных операций и активации платежных сервисов. Будьте бдительны и НИКОМУ ИХ НЕ СООБЩАЙТЕ, ДАЖЕ СОТРУДНИКАМ БАНКА! Помните, представители Банка, службы безопасности, Центрального банка Российской Федерации, платежной системы или правоохранительных органов НИКОГДА и ни при каких обстоятельствах не попросят назвать эту информацию.

2. ДЛЯ ОФОРМЛЕНИЯ ПЕРЕВОДА **НА** КАРТУ (для зачисления средств Вам, для идентификации Вас как получателя перевода) ДОСТАТОЧНО УКАЗАТЬ ТОЛЬКО ЕЕ ПОЛНЫЙ НОМЕР! Такие РЕКВИЗИТЫ КАРТЫ как срок действия, трехзначный код на обороте карты, дополнительно к номеру карты используются для оформления РАСХОДНЫХ операций по карте, ИХ РАЗГЛАШЕНИЕ ЯВЛЯЕТСЯ НЕБЕЗОПАСНЫМ!

3. БУДЬТЕ БДИТЕЛЬНЫ при получении сообщений или звонков, особенно ЕСЛИ:

   - Вы получили сообщение в СМС, мессенджере или по электронной почте о проведении или отмене операций, которых Вы не совершали;
   - Вас настойчиво и убедительно (с элементами жалости или запугивания) просят совершить действия, которые Вы не планировали совершать или не понимаете их смысл;
   - ЕСЛИ ВАМ ПРЕДСТАВЛЯЮТСЯ РАБОТНИКАМИ БАНКА И ЗАПРАШИВАЮТ КОДЫ И ПАРОЛИ ИЗ СМС якобы для отписки от услуг, аутентификации, отмены операции или разблокировки карты.

   НЕ СОВЕРШАЙТЕ НЕОБДУМАННЫЕ ДЕЙСТВИЯ! НЕ ПЕРЕЗВАНИВАЙТЕ ПО НОМЕРАМ, УКАЗАННЫМ В СООБЩЕНИИ и НЕ ПРОВОДИТЕ ДЕЙСТВИЙ в банкоматах и терминалах по инструкциям, полученным по телефону. ВСЕГДА УТОЧНЯЙТЕ ПОЛУЧЕННУЮ ИНФОРМАЦИЮ ТОЛЬКО ПО ТЕЛЕФОНАМ, УКАЗАННЫМ НА ОБОРОТНОЙ СТОРОНЕ КАРТЫ ИЛИ НА САЙТЕ БАНКА (ТЕЛЕФОНАМ КОНТАКТНОГО ЦЕНТРА ГАЗПРОМБАНКА)[1].

4. Внимательно ИЗУЧАЙТЕ ПОЛУЧЕННЫЕ ОТ БАНКА СООБЩЕНИЯ С ПАРОЛЯМИ, информирующие о характере совершаемой операции. Не разглашайте полученные от Банка коды и пароли. Эта информация конфиденциальна и предназначена для подтверждения Вами операции или активации платежного сервиса. СРОЧНО ЗАБЛОКИРУЙТЕ КАРТУ и свяжитесь с Банком, ЕСЛИ ВЫ НЕ ИНИЦИИРОВАЛИ НИКАКИХ ОПЕРАЦИЙ и не запрашивали активации сервисов.

5. ДЛЯ СРОЧНОЙ БЛОКИРОВКИ КАРТЫ Вы можете выполнить одно из следующих действий:

   - изменить статус карты на «блокирована» в Мобильном банке «Телекард»;
   - направить на один из номеров Банка для получения смс-команд[2] смс в формате BLC <последние шесть цифр номера карты>, например: Blc123456, в ответ должно поступить СМС с подтверждением блокировки (для разблокировки ранее заблокированной карты повторите сообщение, заменив BLC на UBL);
   - обратиться по телефону в контактный центр Газпромбанка.

6. В целях безопасности УСТАНОВИТЕ СУТОЧНЫЙ ЛИМИТ РАСХОДНЫХ ОПЕРАЦИЙ по Вашей карте – Вы можете самостоятельно устанавливать и изменять лимиты операций по карте в Мобильном банке «Телекард» или направив на один из номеров Банка для получения смс-команд СМС в формате LIM <последние шесть цифр номера карты> <пробел> <значение лимита в долл.США>, например: «Lim123456 300». Используйте сервис гео-ограничений операций по регионам и типам операций (через Мобильный Банк «Телекард» или сайт Банка)

7. НЕ ПЕРЕХОДИТЕ ПО НЕЗНАКОМЫМ ССЫЛКАМ! ИЗУЧИТЕ ИНФОРМАЦИЮ о сайте, прежде чем оставить на нем данные своей карты. ИЗБЕГАЙТЕ САЙТОВ, о которых информация в сети Интернет отсутствует либо ее мало, и сайт создан менее месяца назад. Переводите деньги через Мобильный банк «Телекард», банкоматы или проверенные интернет-сервисы.

   > Самые популярные виды МОШЕННИЧЕСКИХ САЙТОВ – сервисы по переводам на карты или кошельки (как правило, с минимальной комиссией или без нее) и сайты по продаже дешевых авиабилетов. Также популярны несуществующие лотереи, в которых Вас оповестят о выигрыше, но попросят осуществить предоплату или оплатить налог.

8. ПРИ ПОЛУЧЕНИИ ОТ БЛИЗКИХ ИЛИ ДРУЗЕЙ СООБЩЕНИЙ С ПРОСЬБОЙ О ФИНАНСОВОЙ ПОМОЩИ – СВЯЖИТЕСЬ с ними ЛИЧНО ПО ТЕЛЕФОНУ! Не переводите деньги, пока не убедитесь, что просьба действительно исходит от них (сообщения могут быть результатом взлома аккаунта или вируса на телефоне).

9. РЕГУЛЯРНО ОБНОВЛЯЙТЕ ПАРОЛИ К ВАШИМ АККАУНТАМ в социальных сетях, мессенджерах и личных кабинетах в сети Интернет, особенно на сайтах, на которых Вы храните карточные данные. Помните о возможности взлома аккаунтов. Пароли от Ваших аккаунтов должны быть сложными. Устанавливайте и регулярно ОБНОВЛЯЙТЕ АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ на Вашем смартфоне, планшете или компьютере.

10. НЕ СООБЩАЙТЕ НИКОМУ СВОЁ КОДОВОЕ СЛОВО, кроме случаев, когда в Банк позвонили Вы сами по телефону, указанному на оборотной стороне Вашей карты.

11. ПОМНИТЕ о том, что ВОЗМОЖНОСТЬ АННУЛИРОВАНИЯ ПЕРЕВОДОВ на карту или кошелек в одностороннем порядке НЕ ПРЕДУСМОТРЕНА. Это также означает, что Вы не сможете в дальнейшем оспорить данные операции через Банк.

12. В СЛУЧАЕ ИЗМЕНЕНИЯ НОМЕРА ТЕЛЕФОНА не забывайте ОПОВЕСТИТЬ ОБ ЭТОМ БАНК – КОНТРОЛЬ сообщений об операциях является одним из ключевых элементов безопасности. В случае внезапного приостановления работы SIM-карты (блокировки SIM-карты) - необходимо в кратчайшие сроки обратиться к оператору мобильной связи и в Банк, поскольку возможно изготовление злоумышленниками дубликата SIM-карты.

---

[1] Телефоны контактного центра Банка: короткий номер *0701 (для абонентов МТС, Билайн, Мегафон, Теле2, Мотив), 8 (800) 100-00-89, бесплатно на территории РФ. 8 (495) 913-79-99, 8 (495) 980-41-41

[2] Номера Банка для получения смс-команд (BLC, UBL, LIM, и др.): +7 (903) 797- 62-22, +7 (926) 240-02-22