СДМБАНК
Генеральная лицензия Банка России №1637

Круглосуточная справочная служба: +7 (495) 705 90 90
Для звонков по России (бесплатно): 8 (800) 200 02 23
Сайт банка www.sdm.ru
125424, г. Москва, Волоколамское шоссе, 73

Защита от СМС и e-mail мошенничества

Мошеннические СМС-сообщения, как правило, информируют о блокировке банковской карты, о совершенном переводе средств или содержат другую информацию, побуждающую перезвонить на указанный в СМС-сообщении номер телефона для уточнения информации. Затем мошенники представляются сотрудниками службы безопасности, специалистами службы технической поддержки и **в убедительной форме** предлагают срочно провести действия по разблокировке карты, по отмене перевода и т.п., в зависимости от содержания СМС-сообщения.

В случае получения подобных СМС-сообщений настоятельно рекомендуем Вам:

- **не перезванивать** на номер телефона, указанный в СМС-сообщении;
- **не предоставлять информацию** о реквизитах карты (номере карты, сроке ее действия, ПИН-коде, CVV2/CVC2 коде, контрольной информации по карте), или об одноразовых паролях, в т.ч. посредством направления ответных СМС-сообщений;
- **не проводить** через банкоматы и иные устройства самообслуживания никакие операции по инструкциям, полученным по телефону.

В ряде случаев Банк рассылает информационные СМС-сообщения, при этом:

- в СМС-сообщениях, направляемых Банком по операциям, проведенным с использованием Вашей карты, обязательно указываются последние 4 цифры номера Вашей карты (мошенникам они обычно не известны);
- СМС-сообщения Банка отправляются с номера SDM-BANK, в них указываются только официальные телефоны Банка, опубликованные на официальном сайте или указанные на оборотной стороне Вашей банковской карты.
- СМС-сообщения Банка не рассылаются с официальных номеров Контактного Центра Банка .

Если полученное СМС-сообщение вызывает любые сомнения или опасения, необходимо обратиться в Контактный Центр Банка по телефонам, указанным на обратной стороне банковской карты, и следовать указаниям специалиста.

Мошеннические e-mail-рассылки, обычно предназначены для заманивания получателей сообщений на сайты - «ловушки», на которых под различными предлогами мошенники попытаются получить персональные данные (идентификатор и пароль для входа в систему «Мобильного банка», контрольную информацию по банковским картам, номера банковских карт, ПИН-коды, CVV и иную информацию) или принуждения под различными предлогами на открытие файла-вложения, содержащего вирус, или переход по ссылке для загрузки вирусного файла. Часто на таких сайтах размещаются вирусы, заражающие компьютеры при открытии страниц.

Признаки того, что e-mail-сообщение является мошенническим:

- сообщения замаскированы под официальные письма Банка и требуют от Вас каких-либо быстрых действий или ответа;
- адрес отправителя и тема сообщения замаскированы под обращения от имени Банка.

Например: «Сообщение об увеличении задолженности», «Сообщение об увеличении долга»

- письма содержат ссылки на Интернет-сайты, похожие на официальные сайты банка;
- URL-адрес ссылки в письме отличается от официального адреса (www.sdm.ru);
- к сообщению прилагается файл-вложение, который Вам **настойчиво рекомендуют** открыть;
- в тексте содержатся явные опечатки или орфографические ошибки.

Обращаем Ваше внимание, СДМ-Банк никогда:

- не отправляет сообщения с просьбой подтвердить, обновить или предоставить персональные данные (ФИО, данные документа, удостоверяющего личность, номер мобильного телефона, информацию банковской карты, CVV, ПИН-код, контрольную информацию и пр.), кроме случаев, когда требуется обновление данных в отделении Банка или в системах ДБО;
- не отправляет сообщения с формой для ввода Ваших персональных данных;
- не просит Вас зайти в личный кабинет систем ДБО по ссылкам в письмах.

Внимание! В случае если Вы все же пострадали от мошенничества:

- Необходимо немедленно обратиться в Контактный Центр Банка для блокировки карты, реквизиты которой были сообщены посторонним или по которой были совершены несанкционированные операции, и следовать рекомендациям специалиста.

- По факту мошенничества рекомендуется подать заявление в правоохранительные органы.