**Как защититься 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 не известны); СМС-сообщения Банка отправляются с номера «9002 основной номер, для разных регионов возможна также рассылка с номеров 9000, 9001, 8632, 6470, SBERBANK».

», 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 - 8-495-500-5550 и 8-800-5555550. 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, маскируясь под бренд Сбербанка, как правило, 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 «Сбербанк-ОнЛ@йн», 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: Примеры наименования отправителей в мошеннических сообщениях: Примеры тем сообщений в мошеннических рассылках: − Сбербанк ОнЛ@йн (info@sber.ru) − Сбербанк России (noreply@sber.ru) − Сбербанк Информ (statistics@sber.ru) − и другие − «Сообщение об увеличении задолженности» − «Сообщение об увеличении долга» − «Сообщение об увеличении задолженности на ДД.ММ.ГГГГ»

• письма содержат ссылки на Интернет-сайты, похожие на официальные сайты Сбербанка;

• URL-адрес ссылки в письме отличается от официального адреса (www.sberbank.ru), возможно также появление всплывающих окон на официальном сайте, в котором запрашивается ввод или подтверждение Ваших персональных данных;

• к сообщению прилагается файл-вложение, который Вам настойчиво рекомендуют открыть;

• в тексте содержатся явные опечатки или орфографические ошибки. Обращаем Ваше внимание, что Сбербанк России 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.);

• не отправляет сообщения с формой для ввода Ваших персональных данных;

• не просит Вас зайти в личный кабинет системы «Сбербанк Онлайн» по ссылкам в письмах.

Внимание!

В случае если Вы все же пострадали от мошенничества:

1. 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.

2. По факту мошенничества рекомендуется подать заявление в правоохранительные органы.

Заместитель главы

муниципального образования С.В. Калинина

А.В. Игнатенко

646221