|  |  |
| --- | --- |
| CBRF_vertical_logo_d_=20_rus_SmallSaveZone | Отделение по Кемеровской областиСибирского главного управленияЦентрального банка Российской Федерации650000, Кемерово, ул. Кирова, 1232media@cbr.ru+7 (384-2) 719-219 |

**Защищаем деньги на своей банковской карте**

Жители Кемеровской области все чаще используют банковские карты в расчетах. Так, за 2017 год количество и объем операций по оплате товаров и услуг выросли почти на треть. Однако банковские карты неизбежно привлекают злоумышленников. Цель – узнать их реквизиты и похитить деньги.

Для того чтобы не лишиться своих накоплений, необходимо знать виды и способы мошенничества: от банальной кражи карты до технически сложных способов.

**Сценарий 1 «Социальная инженерия»**

Особую популярность сейчас приобрело так называемое «социальное мошенничество», когда используется психологическое давление на человека. В такой ситуации люди обычно теряют бдительность, начинают паниковать и сами передают мошенникам персональные данные карты. Схема строится на манипулировании желанием быстро разбогатеть, получить что-то даром, купить что-то с большой скидкой. Очень часто аферисты давят на родственные чувства, страх за близкого человека: сообщают, что родственник якобы попал в беду. Особенно подвержены такому воздействию пожилые люди. Также мошенники могут представиться сотрудниками Банка России, прокуратуры, суда, министерства здравоохранения, министерства финансов и других учреждений. Под их именем сообщают о возмещении ущерба от действий мошенников в прошлом. Например, о компенсации за купленные медицинские товары, услуги психологов и экстрасенсов, участие в финансовых пирамидах и т.д. Для получения обещанной компенсации, как правило, предлагается что-то оплатить: налог, банковский сбор, обязательную страховку, госпошлину, комиссию за перевод денег и т.п. Кроме того, преступники просят предоставить банковские реквизиты и паспортные данные.

**Сценарий 2 «Рассылка электронных и sms сообщений»**

Развитие событий зависит от того, кем мошенники представляются.

Злоумышленники не редко прикрываются именем Банка России. Гражданин получает sms с текстом примерно следующего содержания «Ваша банковская карта заблокирована. Информация по телефону: 00000000000. ЦБ РФ». В качестве отправителя может быть указан короткий номер 9-00, номера с кодом 8 800, а также обычный номер телефона, вместо «ЦБ РФ» – «Служба безопасности ЦБ» или Centrobank. Человек звонит по указанному в сообщении номеру, где его убеждают, что в системе произошел сбой и предлагают провести манипуляции с банковской картой. Если выполнить указания мошенников, то деньги с банковской карты будут списаны.

Следует помнить, что Банк России не работает с населением, не блокирует банковские карты, не принимает, не начисляет и не выплачивает денежные средства, включая компенсации.

Sms-сообщение от регулятора может поступить только в одном случае: с просьбой оценить качество и полноту предоставленного Банком России ответа по жалобе.

**Сценарий 3 «Рассылка вредоносного кода»**

Вирус рассылается на компьютер или сотовый телефон с целью хищения персональных данных (данные карты и ее собственника). Обычно мошенники маскируют код под файл или ссылку, кликнув на которые вы запускаете вирус. Подобные письма распространяются через электронную почту, мессенджеры (Viber, WhatsApp, Telegram и пр.), социальные сети и sms. Вредоносная программа похищает логин и пароль онлайн-банка и отправляет их злоумышленникам. Если такую ссылку вы открываете с мобильного устройства – тогда мошенники дополнительно узнают и код подтверждения операции из sms, которое присылает банк.

Чтобы не попасться на уловки мошенников и защитить свои сбережения, необходимо соблюдать несколько простых правил:

1. Берегите свои персональные данные. Большая часть хищений происходит благодаря доверчивости граждан. Не реагируйте на sms и звонки с неизвестных номеров. Не сообщайте третьим лицам номер карты и срок её действия, код подлинности (три цифры на оборотной стороне CVV или CVC), ПИН-код, а также код подтверждения из sms. Для перевода денежных средств достаточно номера карты;
2. Установите антивирус и своевременно обновляйте его. Скачивайте и устанавливайте только лицензированные продукты и приложения с официальных сайтов, не открывайте письма и не переходите по ссылкам, поступившим с подозрительных адресов;
3. Не храните логин и пароль на своем смартфоне: в электронном сообщении, в виде заметки или для «автоматического заполнения» при открытии интернет-сайта или приложения;
4. Подключите функцию sms-информирования о совершении платежа, чтобы сразу узнать о списании средств без вашего согласия;
5. При получении sms-сообщения о блокировке банковской карты немедленно свяжитесь с банком, выпустившим вашу карту. Причем сделайте это по телефонам, указанным на карте, а не в sms;
6. При незаконном списании денег с вашей карты незамедлительно обратитесь в банк, выпустивший карту, для её блокировки
7. При получении sms от родственников, которые якобы попали в беду, позвоните и убедитесь, что помощь нужна именно им;
8. Проявляйте бдительность и не реагируйте на сомнительные предложения незнакомых лиц перечислить деньги для получения разного рода призов, выигрышей, компенсаций.

Если вы считаете, что ваши права как потребителя финансовых услуг нарушены, необходимо обращаться в Банк России через сайт [www.cbr.ru](http://www.cbr.ru) в разделе «Интернет-приемная» или в письменном виде в Отделение Кемерово Сибирского ГУ Банка России по адресу 650000, г. Кемерово, ул. Кирова, 12.