Приложение

**Банк России предупреждает о совершенствовании мошенниками схем кражи денег граждан с использованием банковских карт**

Банковские карты – это очень удобно. Не нужно держать в кармане или в кошельке большие суммы денег. При потере карточки вы не теряете деньги: достаточно позвонить в банк, выдавший «пластик», заблокировать карту, и злоумышленники не смогут снять ваши кровные в ближайшем банкомате, вы же сможете снимать деньги со своего счета в банке по паспорту.

Однако деньги можно потерять, и не теряя карту. Причем люди зачастую сами помогают мошенникам опустошить их счета, сообщая данные своих платежных карт. Жертвой может стать любой человек, поэтому не лишне еще раз напомнить о том, как обезопасить свои сбережения на банковских картах.

*Виды мошенничества:*

**«Ваша банковская карта заблокирована»**

На номер абонента приходит sms о том, что его карта заблокирована. Отправителем как правило значится «Банк России« «Центробанк России», CentroBank, «Служба безопасности Банка России». В сообщении предлагается связаться с «сотрудником» банка, который объяснит, что нужно сделать, чтобы деньги не были списаны с карты.

Если получатель сообщения перезванивает по указанному номеру, мошенники, пытаются выяснить у него данные карты, включая PIN-код, либо предлагают адресату предпринять некоторые действия с использованием банкомата, следствием чего станет списание денег со счета.

*Что делать?*

Не следует ни при каких обстоятельствах сообщать никому PIN-код карты, CVC (последние 3 цифры на ее оборотной стороне) Даже сотрудники банка не имеют права спрашивать PIN-код. Не рекомендуется записывать код на бумаге и хранить ее рядом с картой.

Кроме того, нужно помнить, что Банк России не работает с физическими лицами и не занимается рассылкой sms. Если у вас возникают какие-либо вопросы или сомнения относительно судьбы своих денег на счете, звоните в банк по телефону, указанному на оборотной стороне карт или на его сайте.

**Хищение с использованием сайтов в сети Интернет**

Преступники стали активно использовать в своих целях сайты бесплатных объявлений. К примеру, они размещают объявления о продаже товара или оказании услуг. Доверчивые граждане делают заказ и оплачивают покупку, переводя аванс на номер сотового телефона или электронного кошелька, после этого «продавцы» исчезают.

Но чаще всего злоумышленники представляются покупателями. Мошенническая схема, получившая в последнее время широкое распространение, выглядит следующим образом: аферисты звонят людям, разместившим объявление в интернете, и сообщают, что им понравился товар (это может быть дом, квартира, автомобиль и другое), но, чтобы никто другой не приобрел его, они готовы перечислить предоплату на банковскую карту продавца.

Для этого мошенники сначала «выпытывают» данные банковской карты, а затем под предлогом «что-то перевести не получается» и код безопасности, который банк отправляет держателю карты по sms. В итоге беспечный покупатель не только не получает никакой предоплаты, но и лишается денег с принадлежащей ему банковской карты.

*Что делать?*

Не стоит совершать покупки, если у Вас требуют предоплату. Если вещь подозрительно дешевая, то это, возможно, мошенничество, и следует отменить сделку.

Не сообщайте данные своей карты людям на другом конце провода, даже если они сулят Вам предоплату за Ваш товар.

**«Ваш сын (дочь) совершил преступление»**

Вам поступает звонок, во время которого мошенник выдает себя за близкого родственника. Взволнованным голосом он сообщает о том, что задержан за совершение преступления (ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений), и ему срочно нужны деньги. Очень часто шокированный таким сообщением человек не способен реально оценить ситуацию и готов передать деньги. Злоумышленник также может представиться работником правоохранительных органов или знакомым ваших близких.

«Полицейский» уверенным тоном сообщает, что уже не раз помогал людям таким образом. Но, если раньше деньги привозили непосредственно ему, то сейчас этого делать нельзя, так как он боится «потерять погоны». «Безопаснее всего» деньги отправить на указанный счет с помощью электронной системы переводов или онлайн-кошельков.

Как правило, мошенники используют «одноразовые» номера мобильных, оформленные на подставных лиц, чтобы потом их было сложнее вычислить, или пользуются «антиопределителями» номера, скрывающими от абонента номер звонящего.

*Что делать?*

При поступлении таких звонков, попросите перезвонить через пару минут, сославшись на плохую слышимость, после чего сразу же попытайтесь связаться с близким человеком или с его знакомыми и друзьями. Главное, не терять самообладания и не паниковать, особенно если речь идет о полиции.

Если звонящий представляется сотрудником полиции, выясните его фамилию, имя, отчество, звание или должность, место работы и телефон подразделения полиции, попросите время на обдумывание, позвоните в это подразделение по телефону, найденному в интернете, и уточните, есть ли у них такой сотрудник, и задерживали ли они Вашего родственника.

Схем мошенничества по телефону очень много, и преступники могут очень тщательно подготовить «речь» и отрепетировать ответы на вопросы. Однако ко всему они подготовиться не могут, тем более обычно они не настроены на долгое выяснение ситуации.

**Хищения денег с банковских карт при расчетах**

В данном случае мошенниками могут оказаться представители сферы торговли и услуг, банковские работники. Принимая для расчета банковскую карту от клиента, они могут сфотографировать, перезаписать или запомнить ее данные, чтобы потом рассчитаться картой в интернете.

Происходить это может совершенно незаметно. Например, заранее включается записывающее видеоустройство, на записи, с которого карта видна с обеих сторон. В этом случае мошенникам остается лишь отмотать запись на нужное время и переписать данные карты.

*Что делать?*

При расчете, передавая карту другим людям, не упускайте ее из виду. Необходимо вводить PIN-код так, чтобы он не был виден посторонним.

Следите за поведением сотрудника, совершающего операцию. Нужно насторожиться, если он ведет себя подозрительно, например, фотографирует вашу карту на мобильный телефон под видом набора номера или sms.

Если есть такая возможность, заведите отдельную карту для расчетов через Интернет и через POS-терминалы и храните на ней лишь небольшую часть Ваших средств.

**Хищения денег при двойной транзакции**

Еще один способ мошенничества с банковскими картами – двойные операции (транзакции). Совершая оплату в магазине или кафе, покупатель передает карту продавцу или официанту, он проводит ее через считывающее устройство, покупатель вводит ПИН код, и сотрудник сообщает, что произошла ошибка. Затем действия повторяются еще раз, и транзакция выполняется успешно, а спустя какое-то время владелец карты обнаруживает, что деньги за покупку списаны дважды.

При этом многие держатели карт не замечают этого даже при наличии sms-информирования, считая вторую sms о списании средств ошибкой или дублем, так как суммы совпадают. Такие транзакции легко опротестовать и вернуть свои деньги, однако виновных сложно привлечь к ответственности, так как все можно списать на сбой в системе или ошибку оператора.

Тем не менее, стоит учитывать, что двойная транзакция действительно может оказаться не мошенничеством, а сбоем в работе платежного терминала. Подобные ситуации возникают нередко, и от них практически никто не застрахован.

*Что делать?*

Подключить опцию sms-оповещений по операциям своей карты. Если первая транзакция будет совершена успешно, владелец карты тут же получит соответствующее sms и сможет продемонстрировать его сотруднику, настаивающему на повторной транзакции, в качестве подтверждения уже произведенной оплаты.

Если вам поступило два сообщения о списании одной и той же суммы, стоит сразу же позвонить в банк и проверить, действительно ли произошло двойное снятие средств со счета.

Пресс-служба Южного главного управления Центрального банка Российской Федерации