**Что делать людям, столкнувшимся с мошенничеством с пластиковыми картами**

Банковские карты – удобное современное средство платежа, с их помощью граждане каждый год оплачивают товары и услуги на триллионы рублей. Но технологиями в финансовой сфере научились пользоваться и мошенники. Только с начала этого года с банковских карточек ими было украдено более 1,65 млрд рублей.

Чаще всего жертвами мошенников становятся люди с низким уровнем образования, а также граждане преклонного возраста. Впрочем, простейшие правила кибербезопасности следует помнить и соблюдать всем без исключения, ведь преступники делают ставку именно на нашу невнимательность, доверчивость, легкомыслие или жажду наживы.

Вот несколько самых элементарных норм безопасности, которыми всегда надо руководствоваться при пользовании банковской картой.

Никогда не сообщайте незнакомцам данные своей карты (ее номер, пин-код, кодовое слово и т.д.), даже если они представляются работниками банка или госструктур. Как только речь заходит о деньгах, например, вам предлагают какие-то призы, выплаты, компенсации, сообщают о блокировке карты или списании денег с нее и предлагают помочь решить эту проблему, проявите бдительность и не забывайте, что бесплатный сыр бывает только в мышеловке.

Центральный банк России не работает с гражданами - не принимает вклады и не дает кредиты, не открывает и не закрывает банковские счета, не блокирует карты, не выплачивает никакие компенсации, выигрыши. Кроме того, Банк России не рассылает SMS-сообщения. Поэтому, если вы получили сообщение якобы от имени Банка России, – просто проигнорируйте его и ни в коем случае не перезванивайте по указанному в нем телефонному номеру.

**Наиболее распространенные виды мошенничества:**

**1. Кража данных карты при расчете**

Мошенниками могут оказаться представители сферы торговли и услуг. Принимая для расчета банковскую карту от клиента, они могут сфотографировать, переписать или запомнить ее данные, чтобы потом рассчитаться картой в Интернете.

*Совет:*

При расчете, передавая карту другим людям, не упускайте ее из виду. Вводите ПИН-код так, чтобы он не был виден посторонним, по возможности не записывайте ПИН-код нигде и ни в коем случае не храните его в кошельке или вместе с картой. Обращайте внимание на подозрительное поведение тех, кому вы передаете карту для расчета.

**2. Двойная транзакция**

При оплате картой c помощью POS-терминала (*прим.: тут нужно фото или изображение POS-терминала – далеко не все люди, а тем более пенсионеры, знают, что аппарат для приема платежей через карты называется именно так*), сотрудник утверждает, что оплата не прошла и просит повторно ввести ПИН-код. Делая это, вы рискуете заплатить за один и тот же товар/услугу два раза.

*Совет:*

Чтобы избежать обмана, подключите функцию СМС-информирования о совершении платежа. Даже если СМС-сообщение о платеже не пришло сразу, оно придет через 1–2 минуты. Стоит учитывать, что двойная транзакция может оказаться не мошенничеством, а действительно сбоем в работе. Чтобы убедиться в том, что произошла ошибка, попросите у сотрудника распечатанное на POS-терминале уведомление о сбое. В том случае, если платеж прошел успешно, POS-терминал также печатает соответствующее уведомление, которое продавец должен Вам дать.

**3**. **Кража денег с карт, оснащенных технологиями бесконтактной оплаты** (*примеч. для пресс-службы: этот способ мошенничества пока не является массовым в России, поэтому можно особенно внимание на нем не акцентировать. Однако этот вид мошенничества распространен на Западе, поэтому есть вероятность, что скоро он дойдет и до нашей страны*)

Карты с системой бесконтактной оплаты позволяют совершать платежи до определенного лимита без ввода ПИН-кода – вы просто касаетесь ими платежного терминала.

В местах большого скопления людей злоумышленник может похитить деньги с такой карты, прислонив считыватель или POS-терминал к карманам одежды, сумкам. Мошенники также могут записывать полученную информацию на карты-клоны для дальнейшего хищения средств с настоящих банковских карт.

*Совет:*

Чтобы не стать жертвой этого вида мошенничества, храните карты с технологией бесконтактной оплаты в экранированных фольгой отсеках кошелька или сумки.

**4. Покупатель из Интернета**

Мошенники могут выступать в роли покупателей на сайтах бесплатных объявлений или в соцсетях. Они звонят и убеждают в своем намерении приобрести товар, заявляя о готовности перевести аванс вам на карту, чтобы товар не купил кто-то другой. Для этого «покупатель» просит вас сообщить ему данные карты: номер, код CVC2, срок действия, ваши ФИО. В некоторых случаях злоумышленник пытается узнать код из СМС для подтверждения транзакции. Получив такие данные, преступники похищают денежные средства.

*Совет:*

Чтобы избежать обмана, не сообщайте незнакомцам данные своей карты ни под каким предлогом.

**5. Рассылка СМС от имени родственников и друзей**

Популярным способом мошенничества является рассылка СМС якобы от имени родственников (обычно детей), которые попали в беду и им необходимы деньги для того, чтобы из нее выбраться. Реакция на возможную угрозу, как правило, весьма бурная, поэтому в порыве эмоций некоторые родители переводят деньги злоумышленникам.

*Совет:*

Чтобы не стать жертвой этого вида мошенничества, при получении СМС подобного содержания позвоните на телефон родственнику или другу, от имени которого оно пришло, и убедитесь, что с ним все в порядке.

**6. Скимминг**

При этом виде мошенничества хищения осуществляются с помощью специального оборудования, которое преступники устанавливают на банкоматы для съема информации с карт. На щель приема карты банкомата устанавливают скиммер, который при прохождении карты считывает данные с магнитной ленты. После этого мошенники легко изготавливают копию банковской карты. Но для того чтобы воспользоваться такой картой-копией, преступники должны знать ПИН-код. Считывают этот код при помощи видеокамеры, установленной неподалеку, или при помощи тонкой накладной клавиатуры, устанавливаемой на клавиатуру банкомата.

Сейчас в России используются карты, оснащенные чипами, поэтому актуальность скимминг-атак существенно снизилась. При этом Банк России предупреждает, что злоумышленники изучают и разрабатывают варианты скиммингового оборудования, которое считывает информацию с чипов. Поэтому вполне вероятно, что в скором времени этот вид мошенничества вновь наберет обороты.

*Совет:*

Чтобы не стать жертвой мошенничества, старайтесь снимать деньги в проверенных банкоматах, стоящих на охраняемой территории без доступа посторонних лиц. Внимательно следите, чтобы на банкоматах не было установлено никаких подозрительных устройств. Если вы до сих пор пользуетесь картой с магнитной полосой, замените ее на карту с чипом. Это можно сделать бесплатно в отделении вашего банка.

**7. Сайты-двойники**

Суть этого вида мошенничества заключается в том, что злоумышленники создают фишинговые сайты (сайты-двойники). Они предлагают продукты и услуги от лица различных организаций для хищения денег у граждан.

Для этих целей используется наименование сайта, похожее на имя действующей организации, элементы ее фирменного стиля. Расчет прост: не все люди внимательно смотрят на адресную строку браузера и не все понимают, что сайт только похож на привычный сайт, на самом деле являясь совершенно другой страницей. К примеру, вы, желая узнать, есть ли у вас штрафы в ГИБДД или как оформить кредит онлайн, попадаете на такой фишинговый сайт и вводите на нем свои персональные данные. Эти данные становятся доступны преступникам, которые либо сами используют их для незаконного обогащения, либо продают другим злоумышленникам.

*Совет:*

Чтобы не быть обманутыми, внимательно изучите название и содержание сайта, на который зашли, чтобы убедиться, что это не сайт-двойник. Не вводите свои персональные данные на сайтах, которые вызывают подозрения.

**8. Письма с вирусами и ссылками на вредоносное программное обеспечение**

На ваш электронный почтовый ящик или на страницу в соцсетях с незнакомого адреса может прийти письмо с вложенным файлом или ссылкой. Открыв это письмо или перейдя по ссылке, вы рискуете загрузить на свой компьютер вирус, который позволит злоумышленникам захватить контроль над ним и получить доступ к персональным данным, например, он-лайн банку. Вы также рискуете, скачивая сомнительные мобильные приложения, которые по факту могут оказаться носителями вируса.

*Совет:*

Чтобы избежать обмана, скачивайте только лицензированные продукты и приложения с официальных сайтов, не открывайте письма и ссылки, поступившие с подозрительных адресов. Установите антивирус на свой компьютер и мобильный телефон.

**9. Мошенничество с компенсационными выплатами пенсионерам**

В январе 2017 года все пенсионеры получат компенсационную выплату в размере 5000 рублей. Мошенники, зная про это, могут звонить и просить назвать реквизиты карты и другие персональные данные якобы для перевода этих денег.

*Совет:*

Не сообщайте никому реквизиты банковской карты, пенсионного счёта и другие персональные данные. Выплата 5000 рублей будет производиться одновременно с январской пенсией. Никакого заявления для этого не требуется.

**10. Виды мошенничества с использованием имени Банка России**

**- Телефонные звонки**

Граждане могут получать звонки от мошенников, которые представляются сотрудниками Банка России, Прокуратуры, суда, Министерства здравоохранения, Министерства финансов и других учреждений и сообщают о положенном 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 мошенники, как правило, предлагают что-то оплатить: подоходный налог, налог на прибыль, банковский сбор, обязательную страховку, госпошлину, комиссию за перевод денег и т.п. Кроме того, преступники требуют предоставления паспортных данных и банковских реквизитов. Очевидно, что после перевода денег никаких компенсаций не следует.

**- Письменные уведомления**

Похожая схема мошенничества – поддельные уведомления о выплатах и компенсациях.

Гражданин получает по почте на бланке с некоторыми реквизитами Банка России уведомление о том, что судом принято решение о выплате компенсации за приобретение в мошеннических организациях лекарств, биодобавок, медицинских приборов или за оплату услуг экстрасенсов и психологов. В фальшивом уведомлении указывается контактное лицо и номер телефона. Для большей убедительности мошенники предупреждают свою жертву о том, что в случае игнорирования письма компенсация перейдет в пользу государства.

Гражданин, поверивший такому письму, попадает к сети к аферистам, которые далее действуют по схеме, аналогичной первой.

**- СМС-сообщения**

Мошенничества с использованием СМС-сообщений — также одна из наиболее распространенных схем, в которых аферисты прикрываются именем Банка России.

Гражданин получает СМС-сообщение с текстом примерно следующего содержания: «Ваша банковская карта заблокирована. Информация по телефону: 00000000000. ЦБ РФ». В качестве отправителя может быть указан короткий номер 900, а также номера с кодом 8800. Вместо «ЦБ РФ» может быть указано «Служба безопасности ЦБ», или «Centrobank», или «Сбербанк».

Гражданин, позвонивший по указанному в сообщении номеру, попадает в фальшивую службу безопасности якобы Банка России или Сбербанка, где его убеждают в том, что в системе произошел сбой и предлагают:

* подойти к ближайшему банкомату и провести операции, которые ему укажут;
* сообщить данные своей карты для того, чтобы ее можно было разблокировать (возможны и другие варианты).

Если человек выполнит указания мошенников, с его карты будут списаны деньги.

*Совет:*

Чтобы не стать жертвой обмана, ни в коем случае не реагируйте на сообщения государственных структур, если вас просят совершить какие-либо платежи.

**Что делать людям, столкнувшимся с мошенничеством?**

В случае если с банковской карты без согласия ее держателя списаны деньги, следует:

1) незамедлительно позвонить в банк, выпустивший карту, сообщить о мошеннической операции и заблокировать карту; номер телефона указан на обороте карты, на официальном сайте банка и в договоре о выпуске и обслуживании карты.

2) обратиться в отделение банка, запросить выписку по счету и написать заявление о несогласии с операцией, экземпляр заявления с отметкой банка о приеме оставить у себя.

3) обратиться в правоохранительные органы с заявлением о хищении.

В соответствии с законом, заявление рассматривается банком не более 30 дней со дня его получения, при осуществлении международных операций – не более 60 дней. Банк информирует держателя карты о результатах рассмотрения заявления способом, определенным договором о выпуске и обслуживании карты. По требованию держателя карты банк обязан предоставить письменный ответ.

**Могут ли пострадавшие рассчитывать на компенсацию?**

После получения заявления клиента банк проводит служебное расследование, по результатам которого принимает решение о возмещении ущерба.

На возмещение можно рассчитывать, если держатель карты не нарушал условия ее использования, в том числе соблюдал меры по безопасности, и обратился в банк не позднее дня, следующего за днем получения от банка уведомления о совершении операции. Имейте в виду, если кража денег с карты стала следствием вашей собственной неосмотрительности, если вы сами сообщили преступникам свои персональные данные, банк может не возвращать деньги.