Кто и как пытается украсть ваши деньги с банковской карты? Пять мошеннических схем, которые нужно уметь распознавать

На фоне роста популярности использования банковских карт участились случаи мошенничества, связанные с кражей денег со счетов клиентов. Способы обмана людей и кражи денег с их банковских карт разнообразны – от банального подглядывания из-за плеча во время использования клиентом банкомата и последующего хищения его карты до хакерских атак на программное обеспечение. При этом злоумышленники постоянно придумывают новые способы хищения денежных средств, по мере того как старые перестают работать. Именно поэтому важно быть бдительными и соблюдать базовые правила безопасности.

Мы подготовили небольшой обзор самых распространенных на сегодняшний день способов мошенничества с банковскими картами. Надеемся, что знание этих приемов позволит владельцам банковских карт избежать неприятностей при их использовании.

1. **Кража данных карты при расчете.**

Как работает?

В мошеннических схемах могут участвовать не только посторонние злоумышленники, но и те, кому принято доверять: представители сферы торговли и услуг, банковские работники. Терять бдительность нельзя ни при каких обстоятельствах: хищение денег с банковских карт может происходить даже там, где этого никак не ожидаешь.

Часто злоумышленники используют следующую схему. Кассир, официант, заправщик, работник банка или любой другой сотрудник, которому гражданин передал пластиковую карту для расчета, может сфотографировать, переписать ее данные или просто запомнить их, чтобы потом беспрепятственно рассчитаться картой в Интернете.

Это может происходить совершенно незаметно. Например, заранее включается записывающее видеоустройство (это может быть обычная камера видеонаблюдения), 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?

– *Не передавать карту посторонним, рассчитываясь за покупку или предоставление услуг.*

– *Следить за поведением сотрудника, совершающего операцию (нужно насторожиться, если он ведет себя подозрительно – например, фотографирует вашу карту на мобильный телефон под видом набора номера или СМС).*

– *Если есть такая возможность, завести для расчетов через Интернет отдельную карту, которая будет храниться в недоступном посторонним лицам*

месте, а на карте, используемой для покупки через POS-терминалы, заблокировать возможность совершения покупок через Интернет.

2. **Двойная транзакция.**

Как работает?

Еще один простой способ мошенничества с банковскими картами — двойные операции (транзакции). Совершая оплату в торгово-сервисной сети, покупатель передает карту оператору, он проводит ее через считывающее устройство, покупатель вводит ПИН-код (если требуется), 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 СМС-информирования, считая вторую СМС 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 СМС-оповещений по операциям своей карты. Если первая транзакция будет совершена успешно, владелец карты тут же получит соответствующее СМС-сообщение 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.*

3. **Кража денег с карт, оснащенных технологиями бесконтактной оплаты.**

Как работает?

Технологии бесконтактной оплаты разработаны платежными системами Visa (PayWave) и Mastercard (PayPass) для ускорения и упрощения безналичной оплаты покупок. Это комфортный метод, экономящий время покупателей и пользователей различных услуг в местах, где люди не задерживаются надолго. Терминалами бесконтактных платежей чаще всего бывают оснащены торговые автоматы, платные автодороги, турникеты, автозаправки, супермаркеты и кафе. PayPass и PayWave применяются на картах с чипом и магнитной полосой. При расчетах такой картой не нужно вводить ПИН-код, а также ставить подпись на чеке, если сумма покупки небольшая (какая это сумма, зависит от банка-эквайера – банка, который обслуживает платежи, проходящие через конкретный POS-терминал, но она не должна превышать 1000 рублей, данное ограничение введено платежными

системами MasterCard/Visa). При превышении указанной суммы потребуется подтверждение (подпись или ПИН-код), в некоторых случаях платеж может быть отклонен – это решение зависит от банка-эмитента (банка, который выпустил карту). Терминал на расстоянии считывает информацию с карточки и звуковым либо визуальным сигналом дает понять, что необходимая для оплаты сумма списана с нее, а значит, покупка совершена (услуга оплачена).

В Россию эта технология пришла в сентябре 2008 года, и мошенники довольно быстро научились с ней работать. В местах большого скопления людей (переполненном общественном транспорте, на рынках, в магазинах) злоумышленник прислоняет бесконтактный считыватель или POS-терминал к карманам одежды, стенкам сумок и крадет деньги с карт у ничего не подозревающих жертв. Злоумышленнику достаточно приблизить считыватель к карте на расстояние 5–20 сантиметров, чтобы произвести списание. Полученную информацию мошенники могут также записывать на карты-клоны для дальнейшего хищения средств с настоящих банковских карт.

Что делать?

- *Использовать специальные экранированные бумажники (карта кладется в отсек, экранированный фольгой).*
- *Убедиться, что в качестве подтверждения списания суммы более 1000 рублей стоит запрос PIN-кода, а не подпись чека. В случае если вы не планируете оплачивать бесконтактным способом покупки на сумму более 1000 рублей, рекомендуется (при наличии такой возможности у банка-эмитента) установить индивидуальный расходный лимит по карте и ограничить размер возможных транзакций.*

4. Изготовление дубликата сим-карты.

Как работает?

Один из наиболее сложных и наименее очевидных для владельца карточки, а потому наиболее опасных способов кражи денег со счета – изготовление дубликата сим-карты. На первый взгляд, речь идет не о деньгах, но на самом деле таким образом мошенники могут получить полный контроль над счетами жертвы, так как счета банковской карты, как правило, привязаны к номеру телефона и могут управляться дистанционно с его помощью.

Этот способ мошенничества с банковскими картами используется одновременно с другими, после того как злоумышленникам уже удалось завладеть данными карты и им необходимо при помощи кода из СМС подтвердить транзакцию перевода денег на нужный счет. Номер телефона владельца карты злоумышленники могут узнать из социальных сетей, от знакомых, при выполнении своих служебных обязанностей и т.д.

Схема выглядит так. На мобильный телефон поступают звонки с неизвестных номеров и СМС-сообщения от неизвестных людей с просьбой перезвонить. В качестве отправителей сообщений чаще всего указываются «Центробанк России», CentroBank, «Служба безопасности Банка России», Visa, Mastercard, Мир – все эти названия ассоциируются с Центральным банком Российской Федерации (Банком

России) или платежными системами. Если клиент перезванивает по указанному телефону и сообщает свои данные, мошенники могут снять деньги с карты, изготовив ее фальшивый аналог. Теоретически для получения дубликата карты в офисе оператора нужно указать дату первого звонка или остаток на счете, а также предъявить паспорт. На практике работники офисов не всегда бывают скрупулезными, а паспорт мошенники могут предъявить поддельный.

Выдача дубликата сим-карты, как правило, должна быть оплачена, поэтому на телефон держателя карты может поступить сообщение о пополнении счета или списании средств, после чего номер вскоре будет заблокирован.

Затем мошенники переводят деньги с карты своей жертвы на свои карты или рассчитываются за товар в Интернете, подтвердив операции с помощью кода, полученного в СМС. Для потерпевшего ситуация осложняется тем, что исчезновение денег он часто обнаруживает только через несколько дней после происшествия: ведь СМС-сообщение о списании средств он получать уже не может, а о привязке мобильного номера карты к банковскому счету может сразу и не вспомнить.

Что делать?

– *В случае получения внезапного оповещения об изменении состояния счета после звонков с неизвестных номеров или на неизвестные номера немедленно блокировать все свои пластиковые карты, привязанные к этому телефонному номеру, позвонив на горячие линии банков, номера которых указаны на самих картах.*

– *Обратиться к мобильному оператору для разблокировки своей сим-карты и одновременной блокировки дубликата, полученного мошенниками.*

– *Подать заявление в правоохранительные органы.*

5. Социальная инженерия.

Как работает?

В последние годы мошенники начали понимать, что далеко не всегда стоит тратить время и деньги на взлом операционных систем и обход защитных программ. Использование психологических приемов для управления действиями человека часто оказывается намного более простым способом кражи денег с его карты.

Мошенники могут выступать в роли покупателей щенков, автомобилей, земельных участков, гаражей на сайтах бесплатных объявлений или в группах в социальных сетях. Они звонят продавцам и убеждают в своей готовности приобрести предлагаемый товар. Общее у таких «покупателей» одно: они находятся где-то далеко, но для того, чтобы вожделенный товар не приобрел кто-то другой, они готовы перевести часть стоимости или даже полную стоимость немедленно на банковскую карту продавца.

«Покупатель» просит продавца сообщить ему данные карты (код CVV2/CVC2, срок действия, ФИО владельца), чтобы зачислить на нее деньги. После того как доверчивый продавец сообщает мошеннику эту информацию, с его карты начинают списываться деньги за оплату товаров и услуг, осуществляться переводы на другие счета и пр. Мошенники не всегда запрашивают все данные, необходимые для

расчетов: часть сведений может быть им уже известна. В некоторых случаях злоумышленник пытается узнать код из СМС, который приходит на мобильный телефон, — это означает, что с пластиковой картой уже совершают мошеннические действия и не хватает только кода подтверждения транзакции. Получив такие данные, преступники похищают денежные средства.

Что делать?

– *Не сообщать данные карты, персональные данные и коды, присланные в СМС, посторонним лицам.*

– *Ни в коем случае не давать никому доступ к вашей карте через онлайн-банкинг.*

– *В любых подозрительных ситуациях звонить в кредитную организацию, выдавшую карту, по номеру, указанному на оборотной стороне карты.*