ОСТОРОЖНО, МОШЕННИКИ!

Обмануть или взломать банковскую систему безопасности достаточно сложно, поэтому преступники стараются любыми способами выманить информацию о карте у самого держателя. Для достижения своей цели они используют все доступные ресурсы — телефон, интернет-сайты, онлайн-банк, мобильный банк и прочие каналы.

По телефону

Данный вид мошенничества имеет множество вариаций, которые объединяет то, что владельцу карты звонят с незнакомого номера и под любым предлогом просят сообщить её реквизиты. В большинстве случаев злоумышленники используют следующие схемы:

Выигрыш в лотерею. Преступник представляется менеджером известной компании и сообщает, что клиент стал победителем розыгрыша. Для получения вознаграждения необходимо срочно выслать реквизиты своей банковской карты.

Звонок из службы безопасности банка. Фальшивый «сотрудник» извещает клиента о том, что его карту пытались взломать или совершить операцию по карте и просит уточнить данные для исправления ситуации. Телефонные мошенники всегда говорят уверенно, имеют хорошо поставленный голос, а на любой вопрос клиента имеют заранее подготовленный ответ.

Через СМС

Эта схема имеет много общего с предыдущим способом. Разница заключается в том, что ложная информация приходит в тексте СМС-сообщения. Рассылка осуществляется с незнакомого номера, но мошенники подписываются известной компанией. Распространённый пример подобных фейковых сообщений: «Ваша карта заблокирована. Перезвоните по номеру +7XXX6XXXXXXX. Ваш …...Банк.» Если клиент не реагирует, то преступники могут прислать повторное СМС с угрозой взыскания штрафа или комиссии. Перезвонившего просят сообщить данные карты, провести манипуляции в банкомате или интернет-банке.

Через мобильный банк

Услуга «Мобильный банк» позволяет совершать операции с помощью СМС-команд. Чтобы перевести средства другому клиенту, достаточно отправить сообщение на короткий номер банка с того телефона, который привязан к карте. Мошенники используют данную опцию в следующих случаях:

Телефон был утерян владельцем. До момента блокировки SIM-карты любой человек может списать деньги с карточки с помощью СМС-команд, перечень которых размещён на сайте любого банка.

Клиент отказался от услуг конкретного сотового оператора и не отключил мобильный банк. В этом случае номер телефона попадёт в руки нового абонента, который может оказаться мошенником и списывать деньги посредством СМС-команд.

Благодаря использованию мобильного банка злоумышленник также легко вычислит, в какой организации владелец телефона открыл карту.

Мошенничество с переводом денег на карту

Преступники не всегда преследуют цель узнать реквизиты карты. Самый простой способ незаконного обогащения — это убедить клиента в том, что он должен перевести деньги самостоятельно. Злоумышленники предлагают приобрести товары по выгодной цене и требуют перечисления аванса или всей суммы.

Некоторые мошенники выступают в роли фиктивных компаний, которые предлагают удалённую работу в интернете с хорошим заработком. Соискателю необходимо лишь подтвердить серьёзность своих намерений и перевести определённую сумму на счёт или карту работодателя.

Распространённой схемой аферистов также является «помощь родным». Данный способ чаще всего применяется в отношении пожилых людей, которым звонят и сообщают о том, что их близкие попали в беду. Мошенники представляются сотрудниками правоохранительных органов или медицинскими работниками. Они настоятельно требуют перевести деньги, угрожая необратимыми последствиями для жизни и здоровья близких.

Через банкомат

В этом случае для хищения средств преступники используют такие способы, как:

Скимминг. На банкомат устанавливается специальное оборудование, которое представляет собой накладку на клавиатуру и скиммер (вставляется в картоприёмник и позволяет считать данные магнитной полосы). С помощью полученных сведений мошенники изготавливают дубликат карточки и снимают с неё все средства.

Траппинг. Преступники вставляют в картридер кусок пластика с прорезью в центре. Клиент вводит карточку в банкомат, она попадает в прорезь и остаётся в устройстве. После этого подходит злоумышленник, якобы тоже побывавший в такой ситуации, и советует ввести ПИН-код. Когда это не помогает, клиент уходит, а преступник извлекает карточку с помощью заранее подготовленных инструментов.

Мошенничество на сайтах бесплатных объявлений купли-продажи

Данная процедура проводится следующим образом:

➔ Мошенник звонит автору объявления о продаже чего-либо и представляется заинтересованным покупателем.
➔ Продавец сообщает злоумышленнику номер своей карты для перевода средств в счёт оплаты товара.
➔ Фиктивный покупатель входит в интернет-банк по номеру карточки и списывает деньги со всех счетов. Для доступа требуется одноразовый СМС-пароль, который мошенник с помощью различных уловок выманивает у продавца.
➔ Последний этап может отличаться в зависимости от цели преступника. Некоторые хотят узнать конфиденциальные реквизиты карты, другие — просят провести определённые манипуляции через банкомат якобы для подтверждения платежа. В банкомате клиент под руководством мошенника подключает к своей карте посторонний номер телефона, после чего злоумышленник получает доступ к личному кабинету и мобильному банку.

Махинации с банковскими картами через интернет

Такой вид мошенничества называется фишинг. Аферисты создают поддельный сайт популярного интернет-магазина или онлайн-банка, который внешне похож на оригинал, а его URL-адрес отличается от подлинного одним символом. Для оплаты покупки или входа в систему пользователь вводит на фиктивной странице конфиденциальные данные, которые попадают в руки злоумышленников.

Ссылки на фишинговый сайт под видом акций и спецпредложений мошенники отправляют клиентам на электронную почту, в онлайн-мессенджеры или социальные сети.

Кража банковской карты

Некоторые преступники не хотят использовать изощрённые способы мошенничества, а предпочитают просто украсть карточку. Одни злоумышленники делают это открыто, угрожая жизни и здоровью владельца, другие — дежурят возле банкоматов и забирают потерянные карты. В большинстве случаев устройство возвращает пластик с задержкой. Клиент не дожидается и уходит или, получив наличные, вовсе забывает о карте. После этого мошенник может беспрепятственно её забрать и использовать в своих целях.

Другие способы

Помимо описанного выше, третьи лица воруют деньги с карт при помощи вирусного программного обеспечения. Вредоносная программа под видом полезного приложения устанавливается на компьютер, планшет или смартфон клиента. Её основное предназначение — украсть данные карты или перенаправить пользователя на фишинговый сайт.

Другой популярный вид мошенничества — сговор с сотрудниками предприятий торговли. Кассир может зафиксировать данные карты (например, провести её через скиммер) и передать их посторонним лицам.

В связи с развитием новых технологий меняются и виды краж с банковских карт. С фактами мошенничества всё чаще сталкиваются владельцы пластика с опцией бесконтактных платежей. Для

проведения оплаты по такой карте достаточно приложить её к терминалу. Ввод ПИН-кода не требуется если сумма не превышает 1 000 рублей. При этом количество расходных транзакций не ограничено. Чтобы получить деньги, мошеннику даже не понадобится воровать карту у клиента. Если в общественном транспорте поднести устройство к сумке или карману владельца, то средства спишутся. Для этих целей мошенники изготавливают самодельные переносные считыватели или используют банковские терминалы, оформленные по фиктивным документам.

Злоумышленники продолжают активно использовать фишинг в социальных сетях и онлайн-мессенджерах. Наибольшую выгоду мошенникам приносят махинации через сайты бесплатных объявлений купли-продажи, с помощью которых они получают доступ в онлайн-банк.

Как мошенники снимают деньги с банковской карты?

Способ незаконного вывода средств с карты зависит от того, какой информацией завладел злоумышленник. Основные варианты получения выгоды следующие:

- Если карта считана через скиммер, то жулики изготавливают её дубликат. ПИН-код вычисляется благодаря использованию накладки на банкомат или скрытой камеры на устройстве.
- Зная только номер карточки, преступники проводят процедуру регистрации в онлайн-банке. Остаётся только обманным путём узнать у владельца одноразовый пароль. После входа в систему аферисты переводят на свои счета средства не только с карт, но и со всех вкладов клиента.
- Если мошенник знает реквизиты карты (номер, срок действия и код безопасности), то её можно использовать для оплаты в интернет-магазинах, которые не требуют СМС-подтверждения

Куда обращаться в случае хищения средств?

После выявления факта незаконного списания денег с карты необходимо срочно её заблокировать и обратиться в ближайшее отделение банка-эмитента. Дальнейшая процедура включает следующие этапы:

➔ Клиент пишет заявление о несогласии с конкретной расходной операцией.
➔ Банк проводит служебное расследование по факту хищения средств.
➔ В установленные сроки (до 30 дней) владелец карточки уведомляется о решении.
➔ Банк может вернуть деньги только в том случае, если пользователь не нарушал правила безопасности, то есть добровольно не сообщал конфиденциальную информацию третьим лицам.

Независимо от решения эмитента, владелец карточки имеет право обратиться в правоохранительные органы и написать заявление о краже денег.

Советы по защите своей карты

Чтобы обезопасить себя от действий мошенников, необходимо придерживаться следующих рекомендаций:

1. Не сообщать конфиденциальные данные карты третьим лицам (срок, CVV-код и ПИН-код);
2. Подключить услугу СМС-уведомлений для контроля за счётом;
3. ПИН-код хранить отдельно от карточки и прикрывать рукой клавиатуру банкомата или терминала в момент его ввода;
4. Установить расходные лимиты по карте в том числе в интернет-банке или мобильном приложении;
5. Никогда никому не сообщать код из СМС для подтверждения операции, которую клиент не совершал (сотрудники банка не вправе запрашивать данную информацию);
6. Немедленно блокировать карту в случае утраты, кражи или захвата её банкоматом, а также при утере телефона с привязанным номером.

Ежедневно злоумышленники изобретают новые способы хищения средств с банковских карт, поэтому невозможно предугадать все сценарии развития событий. Однако при соблюдении указанных элементарных мер безопасности любой пользователь сможет предотвратить нанесение ущерба от действий мошенников.