КАК ОБМАНЫВАЮТ МОШЕННИКИ

Узнайте о распространённых приёмах злоумышленников и не дайте им себя обмануть

Ситуация 1. Звонок из службы безопасности банка

Вам звонит незнакомец

Номер входящего звонка очень похож на номер банка, а звонящий представляется «сотрудником службы безопасности банка».

У вас просят конфиденциальные данные

Мошенник сообщает, что «банк выявил подозрительную операцию» или «в системе произошел сбой». Он просит у вас полные данные карты, CVV- или CVC-код, код из СМС или пароли от СберБанк Онлайн. Это нужно якобы «для сохранности ваших денег».

Злоумышленники могут поменять одну цифру в номере, которую вы не заметите и подумаете, что это банковский номер.

Как защитить себя

Запишите номер банка 900 в адресную книгу своего телефона. Если звонок будет с другого номера, то на экране телефона он отобразится как комбинация цифр, которая отличается от 900.

Не совершайте никаких операций по инструкциям звонящего. Все операции для защиты карты сотрудник банка делает сам.

Сразу заканчивайте разговор. Работник банка никогда не попросит у вас коды безопасности с обратной стороны карты (CVV/CVC), логин от СберБанк Онлайн, коды из СМС, номер банковской карты.

Проверьте, не было ли сомнительных операций за время разговора. Если успели что-то сообщить мошенникам, сразу позвоните в банк на номер 900 и сообщите о случившемся.

Ситуация 2. Перевод по ошибке

Вы оставили своё имя и номер телефона на сайте бесплатных объявлений

Вскоре кто-то присылает вам с мобильного телефона СМС, подделанное под банковское сообщение об операции. Затем с другого номера приходит СМС с просьбой вернуть деньги.

Мошенники исчезают после перевода

Если вы самостоятельно сделали перевод, деньги вернуть не получится.

Как защитить себя

Проверьте номер, с которого пришла СМС. Помните: банк присылает СМС только с номеров 900 или 9000.

Проверьте баланс своей карты, чтобы убедиться, действительно ли деньги поступили на счёт.

Если баланс не изменился, проигнорируйте СМС и сообщите нам номер телефона мошенника. Мы примем меры.

Для удобства запишите номера банка в телефонную книгу.

Ситуация 3. Брокерские или дилерские услуги

Выгодные инвестиции

Вам звонит незнакомец, который называет себя представителем брокерской или дилерской компании, предлагает инвестировать деньги и обещает высокий доход. Вы соглашаетесь открыть счёт и самостоятельно переводите деньги на карту третьего лица. Мошенники пропадают, вернуть деньги невозможно.

Бинарные опционы

Вы регистрируетесь на сайте бинарных опционов. После пополнения баланса вы получаете уведомление о получении «бонусных доходов». Чтобы вывести эти деньги, вам нужно повысить «торговый статус». Для этого вы вносите на счёт дополнительную сумму. Мошенники пропадают, вернуть деньги невозможно.

Как защитить себя

Проверьте лицензию. Прежде чем переводить деньги брокерской компании, убедитесь, что у неё есть лицензия. Список компаний с лицензиями на брокерскую и дилерскую деятельность есть на сайте Центробанка.

Проверьте реквизиты. Настоящие брокерские или дилерские компании никогда не попросят перевести деньги на карту обычного человека — это должен быть именно счёт компании.

Если баланс не изменился, проигнорируйте СМС и сообщите нам номер телефона мошенника. Мы примем меры.

Ситуация 4. Опрос от СберБанка

Вы получаете письмо или СМС о том, что СберБанк проводит лотерею. Вам предлагают пройти опрос по ссылке, вы кликаете и попадаете на

фишинговый сайт. Вы проходите «опрос» на сайте, и за это вам обещают крупную сумму вознаграждения, например, 150 тысяч рублей.

Но для подтверждения карты и перечисления бонусов вас просят перечислить «закрепительный платёж» в размере 150 рублей. Вы отправляете деньги, а потом не можете связаться с мошенниками.

*Фишинговый сайт — сайт, на котором у вас пытаются выудить секретную информацию, например, пароль от личного кабинета***.**

Как защитить себя

Настройте блокировку фальшивых сайтов в своём браузере. Когда оплачиваете покупки в интернете, проверяйте адрес сайта. Если домен не совпадает в точности с официальным названием сайта, не вводите данные.

Выбирайте защищённое интернет-соединение. Адрес сайта должен начинаться с букв https, а не с http, а в адресной строке должен отображаться значок в виде закрытого замка.

Подключите уведомления по карте и получайте сообщения об операциях по вашим картам, вкладам и счетам.

Ситуация 5. Автоматизированные кол-центры

Вам звонит робот — будто бы от банка. Он сообщает, что ваша карта «заблокирована в связи с подозрительной операцией», просит вас перезвонить для выяснения подробностей и диктует номер. По этому номеру отвечает мошенник под видом сотрудника службы безопасности — пугает вас потерей денег и настойчиво предлагает их «спасти», переведя на «безопасный счёт», либо старается выманить секретные данные (например, логин от СберБанк Онлайн или код из СМС).

Важно: иногда вам может позвонить настоящий голосовой помощник от банка — в том случае, когда банк подозревает мошенничество. Но это делается лишь для подтверждения, что операцию проводили вы сами. Ни сотрудник банка, ни голосовой помощник никогда не просят называть цифры и коды или звонить на номер, который отличается от официального.

Как защитить себя

Запишите номер банка 900 в адресную книгу своего телефона. Если звонок будет с другого номера, то на экране телефона он отобразится как комбинация цифр, которая отличается от 900.

Не совершайте никаких операций по инструкциям звонящего. Все операции для защиты карты сотрудник банка делает сам.

Сразу заканчивайте разговор.

Работник банка никогда не попросит у вас коды безопасности с обратной стороны карты (CVV/CVC), логин от СберБанк Онлайн, коды из СМС, номер банковской карты

Проверьте, не было ли сомнительных операций за время разговора. Если успели что-то сообщить мошенникам, сразу позвоните в банк на номер 900 и сообщите о случившемся.

Ситуация 6. Звонок из прокуратуры

Мошенник звонит и сообщает, что некий сотрудник банка с доступом к вашему счёту находится под подозрением и в его отношении ведутся следственные действия. На следующий день мошенник звонит вам под видом «представителя прокуратуры». Он сообщает, что вам необходимо выполнить гражданский долг — помочь следствию, а также убеждает вас перевести свои деньги на «специальный счёт» для гарантии их сохранности.

Как защитить себя

Запишите номер банка 900 в адресную книгу своего телефона. Если звонок будет с другого номера, то на экране телефона он отобразится как комбинация цифр, которая отличается от 900.

Не совершайте никаких операций по инструкциям звонящего. Все операции для защиты карты сотрудник банка делает сам.

Сразу заканчивайте разговор. Работник банка никогда не попросит у вас коды безопасности с обратной стороны карты (CVV/CVC), логин от СберБанк Онлайн, коды из СМС, номер банковской карты.

Проверьте, не было ли сомнительных операций за время разговора. Если успели что-то сообщить мошенникам, сразу позвоните в банк на номер 900 и сообщите о случившемся.

Ситуация 7. Приложение-кошелёк с «защищённой» картой

Злоумышленник звонит от имени банка и говорит, что для вас выпущена новая, особо защищённая карта. Такую карту якобы нужно добавить в мобильное приложение-кошелёк и перевести на неё деньги с других карт «для сохранности». Если вы под диктовку мошенника привяжете к приложению-кошельку свою карту и пополните её, деньги уйдут мошеннику.

Дело в том, что в такое приложение можно добавить любую, даже чужую карту, а имя поставить какое угодно — мошенники этим пользуются.

Как защитить себя

Запишите номер банка 900 в адресную книгу своего телефона. Если звонок будет с другого номера, то на экране телефона он отобразится как комбинация цифр, которая отличается от 900.

Не выполняйте инструкции звонящего и положите трубку.

Позвоните в банк на номер 900 и сообщите о случившемся.