

Памятка для работников «Как уберечься от мошенников»

Схема 1. Звонки из банка

Мошенники представляются сотрудниками банка и сообщают, что кто-то пытается украсть с вашей карты деньги. Чтобы остановить преступление, они просят сообщить им полные реквизиты карты или дать доступ в личный кабинет. Этого делать нельзя.

Что делать **Обратите внимание**

Никогда не сообщайте по телефону незнакомцам свс-код – трехзначный номер на обороте кредитной карты. Эта информация нужна для того, чтобы вывести деньги с карты или безналичным способом

Проверяйте номер, с которого вам звонят. Часто преступники звонят с телефонных номеров, похожих на номера банков – с кодами 495, 499, 8 800. Не сообщайте никому данные ваших кредитных карт: номер, срок действия и свс-код. В банке не станут просить производить какие-либо действия вне отделения банка. Блокировать карту без заявления клиента сотрудники тоже не будут. Из банка могут позвонить только с предложением какой-либо услуги или просьбой пройти опрос.

Если вам позвонили мошенники, не вступайте с ними в переговоры, не реагируйте на угрозы, что сейчас с вашей карты снимут деньги. Их задача – вывести вас из равновесия. Сразу сообщите, что вы сами перезвоните в свой банк или посетите его лично, и повесьте трубку. После этого позвоните в банк по телефону, который указан на официальном сайте, и сообщите о подозрительном звонке, назовите номер телефона, с которого звонили мошенники.

ИСТОРИЯ. У пожилой женщины из Муром лжесотрудники банка похитили 100 000 рублей

В ноябре пенсионерке из Мурома позвонил человек, который представился сотрудником банка и сообщил, что с ее карты кто-то незаконно списал деньги. Чтобы отменить незаконную операцию, он попросил сообщить ему пароль от личного кабинета онлайн-банка. Женщина раскрыла ему пароль. С его помощью злоумышленник зашел в онлайн-кабинет и похитил 100 000 рублей со счета пенсионерки.

Схема 2. Ошибочные переводы

Вам приходит сообщение о том, что на счет поступили деньги. Чуть позже вам звонят и просят вернуть деньги. Скорее всего, СМС о переводе поддельное, и никаких денег вам не приходило. И вы просто «вернете» преступникам собственные средства.

Что делать

Не возвращать деньги, которые вам перевели ошибочно. Если человек действительно ошибся, то он может обратиться в банк и отменить перевод.

ИСТОРИЯ. В Орле злоумышленник украл у мужчины 7000 рублей

Утром Валерий получил СМС о том, что на счет телефона поступил платеж 3000 руб. Через час ему позвонил мужчина с незнакомого номера и взволнованным голосом начал объяснять ситуацию, что деньги положил случайно, хотел себе, но ошибся в цифре номера, поскольку плохо видит. Также поведал историю, что он заблудился в другом городе и ему срочно надо позвонить жене и решить другие срочные вопросы. После попросил перевести ему в ответ хотя бы 2500 руб. и как

консультант салона связи рассказал, какую команду использовать, чтобы это быстро сделать с телефона. Валерий посочувствовал мужчине и выполнил его просьбу. Так со счета пострадавшего списались не только чужие деньги, но 4000 руб. своих, которые в этот момент были на счету.

Схема 3. Просьбы от друзей в соцсетях

Друг в соцсети или в мессенджере пишет, что ему срочно нужны деньги. На вопросы не отвечает или говорит, что попал в сложную ситуацию. Центробанк сообщил, что некоторые мошенники даже записывают голосовые сообщения и имитируют голос знакомого вам человека.

Что делать

Не отправлять деньги, особенно если это малознакомый человек. Скорее всего, его страницу взломали. Если вам пишет ваша подруга, позвоните ей и убедитесь, что это действительно она просит о помощи.

ИСТОРИЯ. Девушка из Томска чуть не лишилась 50 000 руб

К Анастасии в Одноклассниках пришло сообщение от знакомого, с которым она давно не общалась, с просьбой о помощи. Знакомый написал, что позавчера в 02:00 у его дочери остановилось сердце. Благодаря хирургам и реаниматологам ребенка удалось спасти, сердце было запущено. Сейчас дочь находится в реанимации, но потребуется высокотехнологичная и дорогостоящая операция в Германии. На операцию он попросил Анастасию перечислить ему в долг 50 000 руб. Девушка, прежде чем перевести деньги, позвонила приятелю и уточнила, действительно ли это так. Оказалось, что знакомый ей ничего не писал и в семье у него все здоровы.

1,4млрд рублей – похитили у банковских клиентов в России в 2019 году, по данным Центробанка

Схема 4. Сообщение с вирусной ссылкой

Вам приходит СМС или сообщение в соцсети о том, что ваше имущество будет арестовано и ссылка, по которой нужно срочно перейти. Вы переходите по ссылке, а на компьютер или телефон устанавливается программа, которая передает ваши данные карт мошенникам.

Что делать

Не переходить по ссылкам. На компьютер установить антивирусную программу, а на смартфоне обновить операционную систему. Воровство данных таким способом называется фишинг, и эта самая популярная схема этого года, по данным Общероссийского народного фронта.

ИСТОРИЯ. Несколько десятков человек лишились денег, которые у них были на банковских картах

В Оренбурге клиентам Сбербанка и ВТБ-24 на сотовые телефоны пришли сообщения от якобы региональной службы судебных приставов с суммой задолженности, которую надо погасить. Для этого в СМС была ссылка. Люди по ней переходили, запускалась вирусная программа и с карты, которая привязана к номеру телефона, списывались деньги. Вернуть их пострадавшим не удалось.

Схема 5. Ненстоящий подарок

Мошенники звонят от лица крупных компаний, например известного мобильного оператора, и сообщают о подарке или о накопленных бонусах. Жертве предлагают потратить бонусы и оплатить ими часть товаров, или забрать подарок, но оплатить доставку. Обычно мошенники просят сделать это срочно, иначе предложение будет недействительно. Жертва отправляет деньги и ничего не получает взамен.

Что делать

Ничего не покупайте у незнакомых людей по телефону. Даже если они знают ваше имя. Не поддавайтесь на уговоры и заблокируйте этот номер.

ИСТОРИЯ. Мужчина отдал мошенникам 4000 руб. по собственной воле

В конце ноября Алексею позвонила женщина, представилась, обратилась к нему по имени и рассказала, что она из «Бонусного центра», в котором есть информация обо всех его покупках и бонусах. Оказалось, что у Алексея в магазине накопилось баллов на 2000 руб. Использовать эти баллы женщина предложила на современный авторегистратор, который можно купить за 4000 руб. вместо 8000 руб. Уверила, что к регистратору будет приложен гарантийный талон и сертификат качества, а также в подарок – коврик в машину. Посылку мошенники отправили наложенным платежом. В ней оказался самый дешевый регистратор за 1000 руб. и больше ничего.