РАСПОЗНАЁМ МОШЕННИКОВ

Как справиться с атаками мошенников

или

Жизненные истории о мошеннических схемах

ПРИМЕР 1

САЙТ ЧАСТНЫХ ОБЪЯВЛЕНИЙ

Вы продаете какой-либо товар на сайте частных объявлений, и вам звонит покупатель, желая перевести деньги/предоплату за товар. Покупатель запрашивает у вас номер карты, срок действия, трехзначный код и даже код из СМС-сообщения для подтверждения пополнения.

ГОВОРИТЬ?

Нет. Это мошенник! Если кто-то хочет перевести вам деньги, достаточно знать номер карты или телефона. В случае если требуют больше информации о карте и ваших счетах – кладите трубку.

ПРИМЕР 2

ЗВОНОК ИЗ БАНКА

Вам поступил звонок из «банка» от сотрудника службы безопасности с информацией о мошеннических действиях по вашей карте. Сотрудник «банка» предлагает отменить операции, в целях безопасности заблокировать все карты, открытые в разных банках, и переключает звонок на Центробанк РФ. В свою очередь, сотрудник Центробанка может предложить закрыть вклады и вывести все деньги на «безопасный» счет в Центробанке, запрашивая при этом коды из СМС.

ВЕРИТЬ?

Не верьте! Это самая простая мошенническая схема, но она часто срабатывает! Если звонит настоящий сотрудник банка, у него и так есть все данные по карте, он не просит снять деньги в банкомате или перевести на другой счет, а также не переключает на сотрудников Центробанка. Кроме того, Центробанк не отменяет операции, а «безопасного» счета для спасения ваших средств в Центробанке не существует. Прервите разговор и сами перезвоните в свой банк по официальному номеру телефона.

ПРИМЕР 3

ОПЛАТА ПО ССЫЛКЕ

Вы опоздали на автобус, взяли проезжающее мимо такси, а наличных денег с собой нет. Таксист подготовлен к таким ситуациям: у него нет терминала для оплаты, но есть ссылка, которую он сразу же прислал вам в СМС. Пройдя по ссылке, вы засомневались, потому что нужно ввести полный номер карты, срок действия и трехзначный код на обороте карты, а затем подтвердить оплату кодом из СМС.

ОПЛАЧИВАТЬ?

Нет! Опасно совершать оплату по сомнительным ссылкам, информация о карте может попасть в руки мошенников. Безопасней перевести деньги в мобильном приложении своего банка или найти ближайший банкомат и снять наличные.

КАК ОТЛИЧИТЬ СОТРУДНИКОВ БАНКА ОТ МОШЕННИКОВ

СОТРУДНИК БАНКА	МОШЕННИК
ЗАДАЕТ ВОПРОСЫ, НЕ ТОРОПИТ И НЕ ДАВИТ	*ВЫНУЖДАЕТ ЧТО-ТО СДЕЛАТЬ С ВАШИМИ ДЕНЬГАМИ, ТОРОПИТ И НЕ ДАЁТ ПОДУМАТЬ*
Общается спокойно, терпеливо, вежливо	Говорит быстро, напористо, побуждает к действию, торопит принять решение
Не запрашивает коды из СМС, полный номер карты, срок действия, трехзначный код на обороте карты	Запрашивает коды из СМС, полный номер карты, срок действия, трехзначный код на обороте карты
Может запросить для идентификации клиента паспортные данные/ кодовое слово /последние операции по карте	Может запросить информацию о наличии карт других банков, обвиняет банки в утечке информации и сговоре с преступниками
Не побуждает сделать перевод, закрыть вклад, пройти к банкомату	Вынуждает для защиты средств перевести их на "безопасный" счет в Центробанке
Не переключает на сотрудников службы безопасности Центробанка, другого банка или правоохранительных органов	Высылает ссылку для оплаты, где требуется ввести все реквизиты карты и коды из СМС
Задает вопросы, чтобы удостовериться, что клиент совершает операции сознательно, а не под действием мошенников	Подталкивает установить «программу для защиты» и другие сторонние приложения, пытается удаленно подключиться к телефону

КАК УБЕРЕЧЬ ДЕНЬГИ ОТ МОШЕННИКОВ

ТРИ ЗОЛОТЫХ ПРАВИЛА

1. **НЕ** раз**ДАВАЙТЕ** реквизиты карты, со**ХРАНИТЕ** информацию в тайне!

2. Не ра**СКРЫВАЙТЕ** код-пароль, полученный в СМС-сообщении!

3. По**СПЕШИТЕ** за**БЛОКИРОВАТЬ** карту в личном кабинете «Кубань Кредит Онлайн» или в Контакт-центре банка, если есть подозрение на мошенничество.

КАК ПРЕДОТВРАТИТЬ МОШЕННИЧЕСТВО

Подключите сервис «СМС-инфо» или «E-mail-инфо», которые своевременно проинформируют вас обо всех операциях по карте, в том числе неуспешных. Если мошенники попытаются расплатиться вашей картой, вы сразу об этом узнаете: банк пришлет СМС /ПУШ и e-mail уведомление.

Внимательно проверяйте реквизиты для оплаты/ перевода и сумму операции в СМС-сообщении от банка с кодом ее подтверждения.

Используйте карту с отдельным счетом для оплаты товаров / услуг в интернете. Держите на ней минимальное количество денег или переводите на неё необходимую сумму перед совершением операции.

Установите лимиты (ограничения) на сумму операций по карте при оплате товара/услуги в сети Интернет и переводов с карты.

Не переходите по случайным ссылкам, найденным в интернете или полученным в сообщении от незнакомых адресатов. Эти ссылки могут вести на поддельные сайты.

Для оплаты телефонной связи, интернета, коммунальных услуг, перевода денежных средств и т.д., используйте сервис «**Кубань Кредит Онлайн**» - это безопасно, быстро и не требует посещения банка.