

«Черный треугольник»: как мошенники заставляют людей платить незнакомцам и почему жертвой может стать каждый

С развитием онлайн-торговли мошенники постоянно совершенствуют свои схемы. Если раньше злоумышленники просто просили перевести деньги за несуществующий товар, то сегодня они используют более сложные методы, которые затрудняют выявление преступников и запутывают следы денежных переводов.

Одна из таких схем получила название «Черный треугольник» или «треугольное мошенничество». Ее особенность в том, что в преступной цепочке участвуют сразу три стороны, при этом никто из потерпевших зачастую не понимает, что стал частью мошеннической схемы.

Как работает схема

В классической мошеннической схеме участвуют три стороны: мошенник, покупатель и третье лицо, которое даже не подозревает, что стало частью обмана. Суть схемы заключается в том, что злоумышленник использует чужие банковские реквизиты и чужой товар, чтобы получить выгоду и скрыть свою личность.

Обычно схема развивается следующим образом:

Шаг 1. Мошенник размещает в интернете объявление о продаже популярного товара, например смартфона, игровой приставки, бытовой техники или другого востребованного товара по цене значительно ниже рыночной. Это помогает быстро привлечь внимание потенциальных покупателей.

Шаг 2. Покупатель связывается с «продавцом», уточняет детали и соглашается на покупку. Мошенник может торопить с оплатой, ссылаясь на высокий спрос или наличие других желающих.

Шаг 3. Для оплаты злоумышленник отправляет банковские реквизиты. Однако счет принадлежит не ему, а совершенно другому человеку — реальному продавцу, который в этот момент продает свой товар на другой площадке.

Шаг 4. Третье лицо — настоящий продавец ожидает перевод от своего покупателя и **не подозревает о мошеннической схеме**. Получив деньги, он считает оплату подтверждением сделки.

Шаг 5. Покупатель переводит деньги третьему лицу, думая, что оплачивает товар мошенника.

Шаг 6. После получения оплаты настоящий продавец отправляет свой товар по адресу, который указывает мошенник, либо передает его подставному получателю.

В результате покупатель остается без оплаченного товара и денег, настоящий продавец невольно становится участником мошеннической схемы, а злоумышленник получает товар или денежную выгоду и исчезает, оставаясь вне прямого контакта с переводом средств.

Как это выглядит на практике

Представим ситуацию. Алия разместила объявление о продаже смартфона за 250 000 тенге. Мошенник копирует объявление и публикует его от своего имени уже за 200 000 тенге. Ерлан находит это объявление и связывается с мошенником. Тот объясняет, что телефон находится у его «сестры» Алии, которая покажет устройство, а деньги нужно перевести ему. Одновременно мошенник сообщает Алие, что телефон приедет посмотреть его «брат», а оплату он произведет сам. В итоге Ерлан переводит деньги мошеннику, а тот исчезает. Покупатель остается без денег, а Алия становится невольным участником обмана.

Другой пример. Покупатель приходит в строительный магазин, выбирает товар на 120 000 тенге и просит выставить счет для удаленной оплаты. После поступления денег он забирает товар и получает чек. На следующий день в магазин звонит незнакомая девушка и говорит: «Вчера мы перевели вам 120 000 тенге за юрту. Почему вы ее не отправили?». Оказывается, мошенник использовал реквизиты магазина для получения денег от третьих лиц под видом продажи другого товара.

В обоих случаях добросовестные граждане и предприниматели становятся невольными участниками мошеннической схемы, не подозревая об этом до момента обращения потерпевших.

Почему схема опасна

Главная цель злоумышленников — скрыть свое участие в финансовой операции и максимально усложнить отслеживание движения денег. Для этого мошенники используют счета и данные посторонних людей, которые не связаны с преступлением напрямую.

В результате денежные средства проходят через чужие банковские карты и переводы, из-за чего установить связь между мошенником и полученными средствами становится значительно сложнее. Такая схема **позволяет злоумышленникам оставаться «в тени»** и снижает риск их быстрого обнаружения.

При этом некоторые участники цепочки могут даже не подозревать, что стали **частью мошеннической схемы**. Настоящие продавцы уверены, что получили обычную оплату за товар, а покупатели считают, что переводят деньги продавцу. Однако впоследствии именно этим людям нередко приходится подтверждать происхождение переводов, предоставлять переписки, банковские выписки и участвовать в разбирательствах с банком или правоохранительными органами.

В отдельных случаях подобные схемы используются не только для обмана покупателей, но и для вывода или обналичивания похищенных денежных средств (дропперство), когда мошенники используют банковские счета третьих лиц для сокрытия следов преступления и транзита незаконных средств.

Какие признаки должны насторожить

Существует несколько тревожных сигналов, которые могут указывать на мошенническую схему:

- имя получателя платежа не совпадает с именем продавца или владельца аккаунта;
- деньги просят перевести родственнику, знакомому, «бухгалтеру», «менеджеру» или «партнеру»;
- продавец избегает оплаты на собственные банковские реквизиты и объясняет это различными причинами;
- стоимость товара значительно ниже средней рыночной цены;
- собеседник торопит с переводом денег, создает ощущение срочности или давления;
- продавец отказывается от безопасных способов оплаты и настаивает только на переводе;
- у аккаунта отсутствуют реальные отзывы, история продаж или подтвержденные данные;
- продавец уклоняется от видеосвязи, дополнительных фотографий товара или личной встречи.

Даже один из таких признаков — повод проявить осторожность и провести дополнительную проверку. Чем больше совпадений, тем выше риск столкнуться с мошенничеством. В подобных ситуациях лучше отказаться от поспешного перевода денег и убедиться, что получатель платежа действительно связан с продавцом и товаром.

Как защитить себя

Чтобы не стать жертвой «черного треугольника», рекомендуем соблюдать **несколько простых правил**:

1. Переводите деньги только человеку или организации, с которыми заключаете сделку.
2. Проверяйте, совпадают ли данные продавца и получателя платежа.
3. Не соглашайтесь на объяснения вроде «это карта родственника», «счет бухгалтера» или «карта друга».
4. Используйте безопасные способы оплаты и сервисы с защитой покупателя.
5. Не совершайте предоплату незнакомым продавцам без проверки информации о них.
6. Сохраняйте переписку, чеки и подтверждения переводов.

Перед любым переводом важно помнить простое правило: если деньги просят отправить третьему лицу, которого нет в сделке, это серьезный повод остановиться и еще раз проверить всю информацию.

Материал подготовлен при помощи www.fingramota.kz