Как распознать мошенничество на сайте объявлений и не потерять деньги

Злоумышленники постоянно придумывают новые способы обмана на сайтах объявлений, торговых площадках и маркетплейсах. Мы собрали самые популярные схемы и советы, как не попасться на уловки мошенников

40% случаев, когда мошенники крадут деньги с карты, связаны с попыткой купить или продать товары на сайтах объявлений. Рассказываем, как не попасть в эту статистику.

Коротко про обман в объявлениях

Если покупаете или продаете товары на сайтах объявлений, соблюдайте несложные правила. Изучите их, если нет времени читать всю статью:

никому не сообщайте номер паспорта, банковской карты и другие персональные данные;

не переходите по ссылкам, которые присылают другие пользователи;

не соглашайтесь обсуждать детали покупки или продажи в сторонних мессенджерах;

не соглашайтесь на предоплату, особенно — переводом на карту;

остерегайтесь слишком выгодных предложений;

обращайте внимание на дату регистрации профиля: если аккаунт создан 1—2 месяца назад, это могут быть мошенники;

с подозрением относитесь к аккаунтам, у которых мало или совсем нет отзывов и которые ничего еще не продавали.

А теперь расскажем подробнее.

Пишут мало подробностей о товаре

В интересах продавца выставить много фотографий и написать детальное описание товара, которое снимет все вопросы потенциальных покупателей: так товар купят быстрее. Если описания нет, оно короткое или слишком общее и при этом цена товара ниже, чем в других предложениях, это должно вызвать подозрения.

Например, ответственный продавец телефона напишет, в каком году купил устройство, как часто использовал, есть ли царапины на экране или корпусе, насколько изношена батарейка, приходилось ли ремонтировать смартфон. А если в описании есть

только пара общих предложений вроде «смартфон в хорошем состоянии, возможен торг», лучше поискать другие объявления.

✓ Признаки ответственного продавца

«Купил 3 года назад»

«На задней крышке небольшой скол — есть на фото»

«Батарейку держит на 80%, но этого хватает, чтобы слушать музыку, переписываться в мессенджерах и при этом не заряжать телефон сутки»

«Не был в ремонте, все запчасти оригинальные, кроме шнура — оригинал вскоре после покупки погрызла собака, пришлось покупать замену»

«Меняли экран. Гарантийный талон из сервисного центра предоставлю»

✕ Повод насторожиться

«Состояние хорошее, торг»

«Пользовалась мало, царапин нет»

Короткое описание не обязательно означает, что товар продает мошенник. Но риск, что такое объявление выложил злоумышленник, а не реальный продавец, намного выше.

Как не попасться. Свяжитесь с продавцом и расспросите его о товаре. Задавайте вопросы, на которые может ответить только владелец, например, откуда появилось повреждение на корпусе телефона и сколько часов он работает без подзарядки.

Правда, мошенники могут выдумать ответы, поэтому попросите продавца прислать фото гарантийного талона, чека или снимки товара с других ракурсов: так вы поймете, действительно ли общаетесь с владельцем. Не стесняйтесь уточнять детали — заинтересованный продавец постарается ответить на все вопросы.

Если продавец уходит от ответа, у товара нет описания или оно слишком общее — будьте внимательны. Обычно мошенники ленятся писать подробный текст и не хотят выдумывать реалистичные детали.

Выкладывают объявления с нового профиля

В профиле на сайтах объявлений обычно указаны рейтинг пользователя на основе отзывов, есть фотография и список товаров, которые он продавал или покупал на площадке. Но все эти поля мошенники стараются заполнять правдоподобно: выбирают вымышленное имя, загружают фотографию, а иногда даже

накручивают себе рейтинг. Сделать это несложно: у мошенников есть несколько профилей, они ставят друг другу лайки и на пять звезд оценивают несуществующие сделки.

Главное, что не могут подделать злоумышленники, — это дата регистрации профиля, поэтому в первую очередь обращайте внимание именно на нее. Если пользователь зарегистрировался на сайте недавно, будьте внимательнее: он может быть как реальным человеком, так и мошенником.

Как не попасться. Обращайте внимание на имя, рейтинг продавца, отзывы других пользователей. Но особенно — на дату регистрации профиля продавца: если аккаунт создали 1—2 месяца назад, нужно быть осторожным, даже если у пользователя высокий рейтинг.

Не обязательно сразу отказываться от покупки или продажи: если у пользователя нет оценок или низкий рейтинг, возможно, это просто новичок. Но к сделкам с такими пользователями нужно относиться настороженно. Поэтому всегда выбирайте безопасную сделку и доставку через сервисы объявлений, общайтесь только в чате платформы.

Просят предоплату за товар

Злоумышленники просят перечислить часть или всю сумму покупки до отправки заказа, якобы чтобы забронировать товар или перебить цену другого покупателя. Если покупатель соглашается, они могут придумать новые поводы, чтобы выманить больше денег: попросят оплатить доставку или курьера. Мошенники будут просить деньги до тех пор, пока покупатель не поймет, что его обманывают.

Иногда мошенники просят внести предоплату не переводом, а через сервис онлайн-оплаты. Для этого они присылают ссылку для оплаты — она может быть очень похожа на настоящую, но на самом деле только имитирует ее. Мошенники копируют интерфейс и адрес известных сервисов для оплаты в интернете или даже самого сайта, где вы хотите купить товар. Это называется «фишинг».

Например, вам могут прислать ссылку на популярный сервис оплаты yoomoney.ru, но с одной «о». Отличить такую ссылку от настоящей сложно. Если покупатель переходит по ней и вводит данные карты, он передает мошенникам конфиденциальные данные.

Как не попасться. Никогда не вносите предоплату, если это не предусмотрено самой площадкой, которая гарантирует

безопасность сделки. И тем более не соглашайтесь на предоплату с помощью обычного перевода на карту физлицу.

Не переходите по ссылкам, которые присылают другие пользователи. Особенно остерегайтесь ссылок, которые начинаются с http, а не с https: этот протокол для шифрования не так надежно защищен.

Проверьте, правильно ли указан адрес сайта, на который вам предлагают перейти. Для этого уточните его реальный адрес в интернете и сравните со ссылкой, которую вам прислали. Если одна или несколько букв в адресе сайта отличаются, переходить на него опасно.

Что выдает фишинговый сайт

Ошибки в имени домена или использование поддомена

Адрес сайта начинается с http://

Грамматические или орфографические ошибки, опечатки в текстах на сайте

Устаревший дизайн сайта или элементы дизайна, которые очень похожи на оригинальные, но отличаются от них — другие шрифты, толщина линий

Если все же перешли по фишинговой ссылке, не паникуйте, не вводите личные данные и не давайте согласия на скачивание сторонних программ. Просто закройте сайт.

Предлагают перейти в мессенджеры

У сайтов объявлений есть свои чаты, встроенные в сервис. Там безопасно переписываться с продавцами и покупателями: в таких чатах есть механизмы распознавания подозрительных фраз, они не дают отправить ссылки на сторонние площадки. Например, если вам напишут «переведите деньги» или пришлют ссылку на другой сайт, сервис автоматически заблокирует эти сообщения.

Чтобы обойти системы защиты торговой площадки, мошенники просят перейти в сторонний мессенджер. Они могут объяснить это тем, что сидят в интернете с телефона или редко заходят на сайт и боятся пропустить сообщение.

В мессенджере злоумышленники могут присылать любые сообщения и не бояться, что диалоги или ссылки на подозрительные сайты заблокируют.

Если покупатель оплатит заказ по фишинговой ссылке, в лучшем случае мошенник получит деньги, а покупатель просто не получит товар, а в худшем — украдут и данные карты.

Как не попасться. Скройте свой номер в настройках профиля — так он не попадет в открытый доступ и с вами не смогут связаться мошенники.

Не соглашайтесь обсуждать детали сделки в мессенджере или по телефону. Все, что можно обсудить в чате сайтов объявлений, лучше обсуждать именно там.

Как не попасть в ловушку телефонных мошенников

Ставят слишком низкую цену

Если видите, что кто-то продает свежий флагманский смартфон не за 100 000—120 000 ₽, а за 55 000 ₽, это повод насторожиться. Часто злоумышленники выставляют популярный товар по цене гораздо ниже рыночной.

Соблазн написать таким продавцам высок, но, скорее всего, товары, которые они предлагают, бракованы, сломаны или продавец просто хочет украсть ваши деньги.

Как не попасться. Вряд ли товар в хорошем состоянии получится купить в два раза дешевле обычного. Зато высока вероятность, что внимание покупателя пытается привлечь мошенник. Как только ему удастся связаться с потенциальной жертвой, он попытается ее обмануть: будет просить внести предоплату или прислать данные карты, пришлет вредоносную ссылку. Лучше обходить слишком выгодные предложения стороной — даже если очень хочется сэкономить.

Пытаются узнать данные карты

У мошенников есть десятки объяснений, для чего им нужны данные вашей карты. Причем неважно, покупатель вы или продавец.

К конфиденциальным данным относятся:

номер из 16 цифр (иногда 18);

CVV/CVC-код — трехзначный код безопасности на обратной стороне;

срок действия карты;

ПИН-код, одноразовый пароль для подтверждения операции, который приходит в СМС или пуш-сообщении, ответ на контрольный вопрос.

Чаще всего мошенники убеждают, что данные карты нужны им, чтобы перевести деньги за покупку. Если пользователь

не соблюдает правила безопасности, злоумышленникам удается узнать срок действия и CVV/CVC-код и украсть деньги.

Как не попасться. Никогда не сообщайте данные карты посторонним людям — даже если они обещают, что заплатят за товар в два раза больше, чем вы просите.

Что делать, если мошенники узнали данные карты
Что делать, если столкнулись с мошенничеством

Если злоумышленникам все же удалось вас обмануть — можно обезопасить других пользователей и попробовать вернуть деньги.

Свяжитесь с администрацией сайта. Расскажите, как действовал мошенник, как списали деньги, прикрепите ссылки на товар и профиль мошенника, скриншоты ваших переписок с ним. Попросите модераторов заблокировать профиль мошенника, чтобы он не украл деньги у кого-то еще.

Обратитесь в свой банк с заявлением о возврате средств. Если вы оплатили товар или услугу онлайн по карте, а не переводом, не сообщали мошенникам код из СМС и нигде его не вводили, вероятность, что деньги удастся вернуть, выше.

Но если злоумышленники просили отправить деньги на личную карту или электронный кошелек, на возврат списания полагаться не стоит: если клиент перевел деньги сам и ввел код подтверждения, процедура не поможет.

Как работает чарджбэк

Напишите заявление в полицию. Укажите, как мошенники связались с вами, с какой карты и когда списали деньги. Обратитесь в поддержку Т-Банка, чтобы собрать данные об операциях по карте для расследования. К заявлению приложите скриншоты переписки с указанием даты и времени.

Свяжитесь с банком мошенника. Расскажите о случившемся службе безопасности банка, которым пользуется мошенник, и передайте им всю информацию. Чтобы понять, какой у него банк, наберите его номер телефона или первые шесть цифр номера карты в разделе переводов денег в приложении любого банка