

Количество IT-преступлений ежегодно растет. К сожалению, эффективных инструментов борьбы с мошенниками пока не изобрели. Поэтому, чтобы не стать их жертвой, следует знать основные виды и понимать, как не попасться на их уловки.

РАСПРОСТРАНЁННЫЕ ВИДЫ МОШЕННИЧЕСТВ

1. Покупки через «Интернет»

Мошенники заманивают покупателей фальшивыми объявлениями, обычно с заниженной ценой. После этого они переводят общение с клиентом в сторонние мессенджеры якобы «для удобства» или под каким-то другим предлогом. Уже там они отправляют покупателю ссылку на фальшивый сайт, который внешне напоминает сайт известного бренда. Клиент проводит там оплату, вводит данные своей карты и лишается денег.

На что следует обратить внимание?

1. **Низкая цена.** Если вы нашли объявление или магазин, предлагающий товары по ценам существенно ниже рыночных, имейте в виду, что мошенники часто используют данный прием для привлечения жертв.

Как распознать мошенничество?

Посмотрите стоимость аналогичных товаров в других Интернет-магазинах, она не должна отличаться слишком сильно. Не поддавайтесь на слова «акция», «количество ограничено», «спешите купить», «реализация таможенного конфиската», «голландский аукцион».

2. **Требование предоплаты.** Если продавец предлагает перечислить предоплату за товар, особенно с использованием анонимных платежных систем, электронных денег или при помощи банковского перевода на карту, выданную на имя частного лица, нужно понимать, что данная сделка является опасной.

Как распознать мошенничество?

Учитывайте риски при совершении Интернет-покупок. Помните о том, что при переводе денег в счет предоплаты вы не имеете

никаких гарантий их возврата или получения товара. Если вы решили совершить покупку по предоплате, проверьте рейтинг продавца в платежных системах.

3. **Отсутствие возможности курьерской доставки и самовывоза товара.** Данные факторы вынуждают покупателей пользоваться для доставки товара услугами транспортных компаний и, соответственно, вносить предоплату.

Как распознать мошенничество?

Выбирая из нескольких магазинов, следует отдать предпочтение тому, в котором есть возможность забрать товар самостоятельно. Злоумышленники могут предоставить поддельные квитанции об отправке товара транспортной компанией.

4. **Неточности или несоответствия в описании товаров.** Если в описании товара присутствуют явные несоответствия, следует осторожно отнестись к подобному объявлению.

Как распознать мошенничество?

Внимательно прочитайте описание товара и сравните его с описаниями на других Интернет-ресурсах.

5. **Излишняя настойчивость продавцов и менеджеров.** Если в процессе совершения покупки менеджер магазина начинает торопить вас с заказом и оплатой товара, убеждая в том, что если не заказать его сейчас, то цена изменится или товар будет снят с продажи, не поддавайтесь на уловки и трезво оценивайте свои действия.

Как не стать жертвой мошенников?

Злоумышленники часто используют временной фактор для того, чтобы не дать жертве оценить все нюансы сделки. Тщательно проверьте платежную информацию и при наличии любых сомнений откажитесь от сделки.

2. Заработок на бирже

Одна из встречающихся схем обмана — это мошенничество, связанное с заработками на бирже. На примере типичных случаев расскажем о способах, которыми пользуются аферисты, и о том, как не попасться на их уловки.

Как распознать мошенника, который представляется сотрудником брокерской компании?

1. Навязчивые звонки в любое время суток.

2. Звонки поступают с мобильного или скрытого номера.

3. Обещание баснословной прибыли от вложенных денежных средств в короткие сроки — 10–20% и более в неделю или месяц.

4. Отказ называть адрес сайта брокерской компании.

5. Отказ предоставить информацию о лицензии или ее отсутствие.

6. Брокер отказывается встретиться в офисе и заключить брокерский договор. Предлагает быстро открыть счет без проверки ваших документов и заверяет, что достаточно оформить личный кабинет.

3. Взлом социальных сетей

У большинства из нас много аккаунтов — в соцсетях, электронной почте, всевозможных сервисах и онлайн-магазинах. Узнать, что какой-то из них взломали — тот еще стресс. Особенно если вы активно пользуетесь этим аккаунтом.

Что делать, если не получается войти в аккаунт?

1. Первым делом попробуйте сбросить пароль: есть шанс, что взломщики не успели отвязать от аккаунта вашу почту.

2. Предупредите о взломе как можно больше знакомых.

3. Если мошенники обратились до аккаунта в платежной системе или к учетной записи была привязана кредитка, позвоните в банк или платежный сервис, чтобы тот заблокировал ваш аккаунт или карту.

4. Составьте список самых важных сервисов, которые привязаны к взломанному аккаунту.

5. Попробуйте получить логин в эти сервисы и отвязать их от взломанной учетной записи.

6. Напишите в поддержку сервиса о случившемся.

Как не стать жертвой взломщиков?

1. Используйте надежные и уникальные пароли.

2. Включите двухфакторную аутентификацию.