**Схемы мошенничества на маркетплейсах: как защититься**

**Согласно исследованию аналитического агентства НАФИ 69% россиян делали заказы на маркетплейсах за последние три месяца. При этом аудитория онлайн-площадок для продажи товаров растет. Средняя ежемесячная выручка российских продавцов маркетплейсов в 2023 году увеличилась почти на 40% и превысила отметку в 761 тысячу рублей. К сожалению, этим каналом пользуются не только добросовестные продавцы, но и мошенники. О том как безопасно покупать на маркетплейсах в** [**интервью ТАСС**](https://tass.ru/obschestvo/24427601) **рассказала эксперт проекта НИФИ Минфина "Моифинансы.рф" Мария Иваткина.**

**Звонок от лица сотрудников маркетплейсов:** Преступники действуют под видом сотрудников пунктов выдачи заказов (ПВЗ) популярных маркетплейсов. Под предлогом доставки товара на дом они запрашивают конфиденциальную информацию: СНИЛС, ИНН, а также коды из СМС. Получив данные, злоумышленники переходят к следующему этапу: жертве звонит другой человек, заявляющий о взломе аккаунта на "Госуслугах" и угрозе деньгам. Под давлением жертву вынуждают перевести средства на "безопасный счет" или отдать наличными "сотрудникам полиции".

**Обман продавцов:** Мошенник, прикидываясь покупателем на площадках объявлений, просит прислать фото товара в мессенджер (ссылаясь на технические проблемы), обещает оплату через платформу и требует "подтвердить" оплату. Жертва получает фишинговое письмо/сообщение, стилизованное под площадку. Переход по ссылке ведет на поддельную страницу, где ввод реквизитов карты и СМС-кода приводит к хищению средств.

**Ложные курьеры/складские работники:** Используя общедоступные данные (имя, телефон), аферист сообщает о готовности заказа к отправке и уточняет адрес ПВЗ или доставки. Эта классическая социальная инженерия рассчитана на тех, кто действительно ожидает посылку. Собранные сведения могут использоваться для дальнейшего мошенничества.

**Сценарий "найденной посылки":** Представившись сотрудниками склада, мошенники сообщают об обнаружении "утерянной" посылки и просят продиктовать код из СМС якобы для её пересылки. На деле этот код предназначен для сброса паролей банковских приложений или мессенджеров, что ведет к краже средств.

**Многоступенчатый сценарий:** После звонка "сотрудника маркетплейса" может последовать звонок от "представителя службы безопасности" или "правоохранителя", который якобы "пресек" аферу. Под видом "защиты счетов" или "восстановления доступа" вымогаются конфиденциальные данные и СМС-коды.

**Доход за лайки:** Маскируясь под сотрудников маркетплейсов, мошенники рассылают голосовые сообщения. Для того, чтобы расположить к себе потенциальную жертву, они переводят небольшую сумму якобы за выполнение заданий. Далее следует требование оплатить "выкуп товара" или купить "премиум-аккаунт" для увеличения заработка — после чего мошенники исчезают с деньгами.

Ключевые правила безопасности:

1. Сотрудники маркетплейсов никогда не запрашивают по телефону или в мессенджерах СМС-коды, пароли, полные банковские реквизиты, СНИЛС или ИНН.
2. Уточнение адреса доставки происходит исключительно через личный кабинет или официальное приложение платформы. Курьеры не звонят с личных номеров для уточнения адреса.
3. При малейших сомнениях или подозрительных звонках/сообщениях немедленно прервите разговор. Все вопросы решайте только через официальную поддержку маркетплейса в чате на сайте или в приложении.