Транс — акция: как мошенники обманывают пользователей Wildberries

У клиентов площадки списывают средства за товары, которые они не покупали

Роман Солдатов
3 ноября 2022

Пользователи маркетплейса Wildberries начали сталкиваться с мошенническими схемами: с их банковских карт и расчетных счетов снимают деньги за покупки, которые они не совершали. Одна из пострадавших, с которой поговорили «Известия», таким образом лишилась почти 200 тыс. рублей — мелкими трансакциями по 1 тыс. рублей они переводились фиктивному продавцу. В службе поддержки Wildberries вопросы пострадавшей оставили без ответа. Эксперты считают, что вина за подобные происшествия может лежать на каждой из сторон — засветить данные своей кредитки может сам владелец, или же утечка происходит в той организации, где хранится личная информация клиентов. Как не допустить подобных ситуаций и что делать, если мошенники всё же получили доступ к банковскому счету, — разбирались «Известия».

Маркет и кредит

Дизайнер Оксана Федотова, зайдя на днях в мобильное приложение своего банка, была неприятно удивлена: на ее карте с кредитным лимитом в 180 тыс. рублей в строке баланса значилось -15 588 рублей. Она запросила выписку. Выяснилось, что все 195 тыс. были сняты в течение буквально двух часов мелкими трансакциями в пользу некоего wildberries Podol'sk.

Притом что Оксана, хоть и была зарегистрирована на маркетплейсе, никаких покупок на нем не совершала с августа этого года, а данные кредитной карты на этом сайте вообще не сохраняла.

— В истории трансакций я обнаружила, что с карты списывалось по 1 тыс. рублей чуть ли не каждую минуту, — рассказала «Известиям» Оксана Федотова. — Я сразу же связалась с банком и заблокировала карту. В ответ на мою просьбу разобраться в ситуации в банке мне сказали, что трансакции получили подтверждение, хотя я его не давала.

Потерпевшая отметила, что пыталась связаться и с поддержкой Wildberries, но она ей никак не помогла.

— Мне пришлось воспользоваться своими связями, чтобы получить какой-то ответ. Девушка из маркетплейса сказала, что подобные ситуации бывают. Якобы во всем виноваты мошенники, которые получают доступ к карте и потом списывают с нее деньги. Решить мою проблему можно только через полицию, маркетплейс ответственности не несет, — добавила пострадавшая.

Прежде чем идти к правоохранителям, женщина решила попробовать добиться ответов в официальном чате Wildberries для продавцов, где она состояла. Но, по словам потерпевшей, и там на ее сообщения не среагировали.

— В чате я увидела жалобу на такую же проблему и от другого пользователя — он удивлялся, что с его расчетного счета под видом платежей в пользу Wildberries списывается по 1 тыс. рублей. Никакого решения, как остановить списания и вернуть деньги, сервис не предложил ни мне, ни ему, — отметила она.

Еще одной проблемой для Оксаны Федотовой стало то, что карта, с которой списаны деньги, кредитная, а процентная ставка высокая. В настоящее время ее задолженность составляет 195 тыс. рублей.

— Информация о том, что пользователи Wildberries столкнулись с мошенническими действиями, не соответствует действительности, — заявили в компании в ответ на запрос «Известий». — Мы провели внутреннюю проверку: банковская карта пользователя была привязана с помощью 3ds и смс-верификацией через свой банк. Таким образом, по нашим данным операция была санкционирована пользователем.

По словам представителя сервиса, привязка карт на Wildberries всегда происходят с помощью смс-подтверждения или push-уведомлений, поэтому несанкционированные оплаты возможны только в случае, если покупатель сам передаст свои банковские данные сторонними лицу или установит вредоносное приложение.

В Компании призывали покупателей проявлять бдительность — не предоставлять данные своих банковских карт третьим лицам.

Независимый источник «Известий», знакомый с ситуацией, предположил, что Оксана Федотова стала жертвой мошенников, которые украли данные ее кредитной карты. В итоге они привязали эту карту к ее аккаунту в Wildberries и совершили фиктивные платежи в пользу сторонней фирмы, которая своим названием мимикрировала под маркетплейс.

— Вероятно, сама девушка где-то засветила данные своей карты, или они были украдены. Ей необходимо обращаться в полицию по этому инциденту, — пояснил источник «Известий».

По его словам, только таким образом можно узнать, на чей счет поступили ее деньги. Но, скорее всего, это будет фирма-однодневка, созданная специально для подобных видов мошенничества, предположил собеседник «Известий».

Опять маркетплейс

Утечка личной информации в открытый доступ чаще всего связана с человеческим фактором, рассказал «Известиям» инженер-программист компании «Юнитесс» Владислав Голушко. Например, владелец кредитной карты может зарегистрироваться на фишинговом сайте, даже не поняв этого. Или же личные данные клиентов может передать мошенникам недобросовестный сотрудник банка, онлайн-магазина или сотового оператора.

— Узнать номер карты и CVC нажатием двух клавиш можно только в кино. Для того чтобы получить доступ к такой информации, необходимо, чтобы их засветил владелец карты или слили сотрудники организаций, где хранятся эти данные, — подчеркнул эксперт.

Особо распространенным способом хищения денег с карт и личных данных людей в последние годы стало создание так называемых «зеркал» сайтов маркетплейсов или банковских организаций.

— Человек с базовыми знаниями программирования достаточно легко может создать копию сайта онлайн-магазина. В результате при каждой регистрации ему будут приходить данные банковских карт, — рассказал Владислав Голушко.

Часто мошенники при использовании такой схемы «клонируют» сайт именно Wildberries. Например, Ирине Грачевой на днях позвонили люди, представившиеся сотрудниками маркетплейса, с якобы выгодным предложением — оформить товары с большой скидкой. Когда та заинтересовалась, выслали ей поддельную ссылку на сайт, визуально ничем не отличавшийся от настоящего. Она оформила там покупки, но когда оплатила их, деньги достались мошенникам, а никакие товары, естественно, не пришли. Женщина потеряла порядка 30 тыс. рублей. Об этом говорится в обращении потерпевшей в полицию (документ есть у «Известий»).

Медсестра Наталья Кудакова тоже попалась на удочку мошенников. Они связались с ней по телефону и сообщили о том, что якобы на Wildberries произошел сбой, и необходимо восстановить данные банковской карты. Наталья назвала свои персональные данные, и мошенникам удалось похитить у нее около 30 тыс. рублей.

Если пользователь заметил, что с его карты пропадают деньги, то нужно сообщить о краже не позднее следующего дня, иначе банк имеет право отказать в возврате средств, рассказал «Известиям» управляющий партнер юридической компании AVG Legal Алексей Гавришев.

— В первую очередь необходимо немедленно заблокировать карту. Далее сообщить в банк по горячей линии о краже денег и написать в отделение банка заявление о несогласии с операцией. Всё это нужно сделать не позднее следующего дня после того, как вам пришло сообщение об операции по оплате, которую вы не совершали, — отметил эксперт.

Он добавил, что сам маркетплейс проверяет действительность карты, которая привязывается к счету, но не проверяет количество людей, которые имеют к ней доступ.

— В случае подтверждения мошеннических действий правоохранительными органами сам банк будет также потерпевшей стороной, но всё же его обяжут вернуть средства клиенту, — сказал Алексей Гавришев.

Эксперт подчеркнул, что, если Оксана Федотова напишет заявление о возбуждении уголовного дела, полиция, скорее всего, начнет проверку о возможной утечке данных в Wildberries. Сама потерпевшая сообщила «Известиям», что 2 ноября подала заявление в отдел МВД по району Гольяново города Москвы.

Выводы из подобных историй должны делать и торговые площадки, считает Владислав Голушко. Если пользователи жалуются на утечку информации, звонки от мошенников от имени компании и тем более списание денег, то организации необходимо незамедлительно проверить систему безопасности и сотрудников, которые отвечают за сохранность личных данных клиентов.

Помимо этого, любая крупная компания должна быть сама заинтересована в поиске и принятии мер по блокировке фишинговых сайтов, которые используются для мошеннических схем — ведь таким образом мошенники наносят ущерб деловой репутации компании.