Мошенники на маркетплейсах: как не попасть в ловушку

Евгений не любит ходить по магазинам, поэтому давно заказывает на маркетплейсах практически все – от носков до бытовой техники. Ему неоднократно доводилось сталкиваться там с мошенниками и иногда он даже терял деньги. Рассказываем, какие ловушки могут поджидать покупателей маркетплейсов и как в них не попасться.

Маркетплейсы защищают от взлома свои мобильные приложения и онлайн-кабинеты покупателей. Но порой обойти все эти барьеры преступникам помогают сами пользователи.

Разбираем пять популярных схем обмана на маркетплейсах, с помощью которых мошенники пытаются завладеть паролями от аккаунтов, реквизитами банковских карт и кодами из уведомлений. Все для того, чтобы обчистить чужие счета.

1.Умопомрачительные скидки по ложной ссылке

Евгений получил рассылку от маркетплейса о распродаже в черную пятницу. Он давно присматривал робот-пылесос, но откладывал покупку из-за цены. А теперь нужная модель продавалась со скидкой 50%.

По ссылке из письма Евгений сразу оказался на странице с пылесосом. Положил его в корзину и кликнул «оплатить». Открылась форма, где нужно было вбить данные карты. Он удивился, так как уже привязывал ее к личному кабинету, но решил, что просто сбились настройки. Ввел реквизиты, код подтверждения. Деньги списались.

На следующий день он зашел в кабинет на маркетплейсе, чтобы проверить статус заказа, но не нашел никаких следов покупки. Написал в техподдержку и узнал, что никакого заказа не было. Евгений предъявил доказательства — чек из онлайн-банка. Тут и выяснилось, что платеж ушел не маркетплейсу, а компании с похожим названием.

В чем суть обмана: мошенники часто рассылают людям заманчивые предложения по электронной почте, через соцсети и мессенджеры — обычно они активизируются перед праздниками и в периоды распродаж. В их сообщениях всегда есть ссылка, по которой можно купить товар с дополнительной скидкой. Но вместо сайта реального магазина она ведет на сайт-двойник. С его помощью преступники воруют деньги и данные карт доверчивых покупателей.

Если бы Евгений присмотрелся к адресу отправителя и вложенной ссылке, то заметил бы, что они отличаются от настоящих.

Как стоит поступать: когда вы получаете сообщение от знакомой компании, внимательно проверьте отправителя. Аватарка с логотипом компании не гарантирует, что вам пишет представитель настоящего магазина.

А если адрес хотя бы одним символом отличается от официальной почты организации, письмо лучше сразу удалить.

Не торопитесь переходить по ссылкам от незнакомцев. Вы рискуете попасть на фишинговый сайт — клон настоящего магазина.

Как отличить подлинную страницу магазина от фальшивой, читайте в статье «Безопасные покупки в интернете».

Лучше всего самому зайти в приложение или на официальный сайт магазина — персональные скидки вы увидите после авторизации. При этом ни по каким ссылкам переходить не придется.

Если вы все же оказались на поддельном сайте и ввели там реквизиты карты — лучше немедленно ее заблокировать и перевыпустить. Иначе велика вероятность, что мошенники снимут с нее все деньги. При этом банки не компенсируют потери, так как вы сами нарушили правила безопасности и передали данные карты мошенникам.

2.Заботливая, но фальшивая техподдержка

Вскоре Евгений чуть было не угодил еще в одну ловушку. Один из маркетплейсов по ошибке списал с его счета больше денег, чем нужно. Не только плату за сам товар, но и комиссию за возврат, которого он не делал. Возмущенный Евгений зашел на официальную страницу магазина в популярной соцсети и высказал недовольство в комментариях.

Через несколько минут в той же соцсети ему пришло личное сообщение от аккаунта с логотипом маркетплейса. Собеседник представился менеджером службы поддержки, извинился и предложил быстро уладить ситуацию. Обещал, что Евгению компенсируют списанную комиссию в двойном размере.

Собеседник прислал ссылку: в специальной форме надо было ввести реквизиты карты, на которую вернутся деньги. Все выглядело как обычный сервис банковских переводов. Но в этот раз Евгений сразу заметил, что в адресной строке некоторые буквы в названии банка повторяются два раза. После этого он прекратил переписку.

В чем суть обмана: в группах маркетплейсов в соцсетях преступники выискивают людей, которые жалуются на проблемы с заказами, и точечно обрабатывают таких покупателей. Евгений не сразу догадался, что в личных сообщениях ему ответил вовсе не сотрудник магазина — мошенник просто поставил себе на аватар логотип торговой площадки.

«Получила уведомление от маркетплейса: «Доставка задерживается на две недели». Решила отменить. Ждала ответа от службы поддержки три часа, не выдержала и написала гневный коммент в канале маркетплейса. Тут же получила сообщение: предложили отменить заказ и начислить 10% бонусами...»

Форма возврата, которую присылают аферисты, на самом ведет на поддельную страницу банка. Поскольку они не просят денег, а наоборот — обещают возврат, люди теряют бдительность и выдают секретные реквизиты карты.

Как стоит поступать: общайтесь со службой поддержки только в проверенных каналах — в чате приложения или сайта маркетплейса. Если решите использовать дополнительные каналы связи, используйте только те, что указаны на официальной странице магазина.

Не передавайте никому полные данные карты — срок действия, три цифры с оборота — ни в каких соцсетях и мессенджерах. Тщательно проверяйте адреса сайтов, на которых вас просят ввести свои данные. Какую информацию безопасно рассказывать посторонним, читайте в статье «Какие банковские реквизиты можно и нельзя сообщать другим».

3.«Угон» аккаунта

Евгений только проснулся и увидел в смартфоне целый ворох уведомлений о списании с карточки. Каждое на небольшую сумму — до 1000 рублей, но в целом денег ушло довольно много, и все – за покупки на маркетплейсе.

Он попытался зайти в личный кабинет на сайте интернет-магазина, но не смог. Попробовал авторизоваться с помощью электронной почты и обнаружил, что в нее войти тоже не получается.

Когда удалось восстановить доступ к ящику, Евгений увидел, что ночью приходили письма о смене пароля от кабинета на маркетплейсе. Вернув доступ к профилю в интернет-магазине, он обнаружил десяток заказов: это были странные товары вроде насадки с цветной подсветкой на кран для воды.

В чем суть обмана: преступники взломали почту Евгения и с ее помощью вошли в его аккаунт на маркетплейсе. Набрали фейковых заказов в своей фирме-однодневке. Все оплатили картой Евгения, которая была в его аккаунте. А так как каждая покупка не превышала 1000 рублей, коды подтверждения операций от банка им не потребовались. Аферисты рассчитывали обмануть как можно больше покупателей и скрыться до того, как интернет-магазин начнет разбираться в ситуации и удалит их фирму из списка продавцов.

Как действовать: когда заказы оформлены от вашего имени на настоящем маркетплейсе, просто отмените их. По закону вы вправе отказаться от товара в любое время до его получения. Продавец должен перечислить вам деньги в течение 10 дней с момента, как вы потребуете их вернуть. Он может только удержать комиссию за обратную доставку вещи. Но если вы вообще не делали заказ — напишите в поддержку и подробно расскажите, что произошло. Требуйте проверить поставщика и полностью вернуть оплату.

Возникнут проблемы с возвратом — подайте жалобу на маркетплейс в Роспотребнадзор. Если это не поможет, остается обращаться в суд.

Чтобы избежать подобных проблем, используйте для электронной почты сложный пароль. Лучше брать комбинации не меньше восьми символов — с цифрами, прописными и строчными буквами. Для каждого

аккаунта на сайтах магазинов, банков и других организаций создавайте свой пароль.

Стоит завести отдельную карту для интернет-покупок и каждый раз переводить на нее нужную сумму прямо перед оплатой. Или вообще не сохранять данные карты для оплаты в разных сервисах и магазинах — просто вводить их перед каждой покупкой.

И уж точно не нужно привязывать к сайтам кредитки. Если профиль с такой картой взломают, есть риск остаться не просто без денег, но и в долгах.

4.Кража денег с карты маркетплейса

Маркетплейсы нередко предлагают дополнительные скидки при оплате картой партнерского банка. Евгений решил оформить такую карту.

Оплатил ей новую покупку — умную колонку по хорошей цене. Вскоре в приложении маркетплейса пришло сообщение от продавца: «Для доставки заказа напишите менеджеру в мессенджере» – и телефон для связи. Евгений уже знал, что нельзя переходить в сторонние приложения для оплаты товара. Но речь шла только о доставке. Поэтому он решил, что ничем не рискует, и отправил сообщение.

Продавец ответил, что не сможет привезти товар по выбранному адресу, но можно переоформить заказ на соседний пункт выдачи. Евгений был не против. Нужно было только переслать продавцу код из уведомления от маркетплейса.

Код пришел с привычного номера интернет-магазина, Евгений передал цифры собеседнику, но заподозрил неладное и написал в поддержку маркетплейса — не опасно ли выдавать кому-то присланный код. Чат-бот магазина не смог ответить на вопрос.

При этом Евгению пришло уведомление, что заказ отменен и деньги вернулись на карту. А продавец в мессенджере уже просил новый код «для переотправки» заказа в другой пункт. На телефон действительно упало еще одно сообщение от маркетплейса с цифрами.

Пока Евгений мешкал, продавец написал в мессенджере: «Вам должен прийти второй код. Не говорите его мне. Просто отправьте эти цифры в чат техподдержки в приложении магазина». Евгений не увидел в этом никакой опасности — ведь он сообщит код боту маркетплейса, а не продавцу-незнакомцу.

Но как только он написал цифры в чате поддержки, деньги с карты маркетплейса ушли неведомому Геннадию Петровичу В. Причем как раз та сумма, которую Евгений отдал за колонку.

В чем суть обмана: в этом случае мошенники снова зарегистрировались на маркетплейсе как продавцы. Когда Евгений написал им в мессенджере, они узнали его номер телефона — он же логин для входа на маркетплейс. Так как пароль от кабинета они не знали, то для авторизации запросили код —

именно он пришел Евгению в первом уведомлении, а вовсе не код для смены адреса доставки.

Когда преступники вошли в аккаунт покупателя на маркетплейсе, они отменили заказ, и деньги вернулись на карту Евгения.

«Выбирала смартфон на маркетплейсе, остановилась на самом выгодном предложении. Оформила заказ, но он отменился. Со мной связался продавец: «Товар закончился на складе маркетплейса. Можем отправить его с другого склада через сервис быстрой доставки»…»

Обычно клиенты интернет-магазинов могут входить в чат со службой поддержки одновременно с нескольких устройств. Этим и воспользовались мошенники. Они не только видели, что пишет Евгений, но и сами отправляли туда сообщения, а Евгений в суматохе принял их слова за инструкции техподдержки и не обратил внимания, что все сообщения в чате были от его имени. В частности, они написали в чат: «Бот маркетплейса: Введите 4-значный код для переоформления заказа».

Евгений так и сделал — ввел второй код в чат. Но на самом деле этот код в СМС пришел вовсе не от маркетплейса, а от его банка. Он был нужен аферистам, чтобы войти в профиль Евгения в онлайн-банке и получить доступ к его карте. Как только они получили этот код, они перевели деньги со счета одному из своих сообщников.

Как быть: если с карты списали деньги без вашего согласия, немедленно свяжитесь со своим банком и просите ее заблокировать. На всякий случай смените пароль от интернет-банка, если он у вас есть.

Когда в ваш аккаунт на маркетплейсе вошли посторонние, поищите в настройках личного кабинета опцию «Завершить сессии на подключенных устройствах» или «Выйти на всех устройствах» и воспользуйтесь ею. Как можно скорее сообщите о происшествии в техподдержку маркетплейса. Если не получится отключить мошенников самостоятельно, это сделают сотрудники сервиса.

Попросите маркетплейс помочь вам вернуть деньги. Возможно, он сам свяжется с продавцами-мошенниками и убедит их добровольно компенсировать вам украденное. Или сообщит вам их данные, чтобы вы обратились в полицию и сразу приложили к заявлению все известные реквизиты преступников.

Когда выбираете товары, обращайте внимание, давно ли продавец работает на этой площадке, высок ли его рейтинг, какие отзывы от покупателей.

Лучше никогда не переходить на общение с продавцами в мессенджерах и соцсетях. Но если маркетплейс предлагает вам связаться насчет доставки с партнерами напрямую, ни в коем случае не называйте им никакие коды и пароли.

Всегда внимательно читайте, что за коды вам приходят и от кого. Получив код, который не запрашивали, не сообщайте его никому ни под каким предлогом. Если у вас есть личный кабинет в этой организации — как можно скорее зайдите в него через сайт или приложение,

прекратите все сеансы на сторонних устройствах и смените пароль. Не получится сделать это самостоятельно — обратитесь в техподдержку организации. Контакты берите только на официальном сайте компании.
На некоторых интернет-площадках есть возможность оплачивать товар не заранее, а при получении — используйте эту опцию.

5.Легкий заработок

Однажды Евгению предложили подзаработать на любимом маркетплейсе. Вакансия пришла в мессенджере от незнакомого человека. Обязанности были прописаны невнятно, зато кандидатом мог стать любой человек старше 20 лет. Доход обещали от 5 000 до 20 000 рублей в день.

Евгений сразу понял, что это очередной развод: никто не будет платить такие деньги за легкую работу людям без всякого опыта. Но из интереса решил поболтать с аферистами. Представился Игорем Катамарановым, сказал, что работает в НИИ, но его интересует дополнительный доход.

«Менеджера» это устроило. Оказалось, что они ищут «трейдера маркетплейса», в обязанности которого входит «увеличение конверсии и объема транзакций». По словам собеседника, это только кажется сложным — всему научит куратор.

Для начала достаточно зарегистрироваться на маркетплейсе по специальной ссылке от куратора. Там же нужно внести депозит. Если отправить 500 рублей — вернется столько же плюс 30%. За 1000 рублей — уже 50%, а за 3000 рублей — все 70%.

Евгений даже не стал уточнять, о каких «транзакциях» и «конверсиях» идет речь. И выяснять, за счет чего он получит такую бешеную прибыль. Сделал вид, что со всем согласен, и тут же получил ссылку.

Сайт, на который он попал, копировал дизайн настоящего маркетплейса. Но картинки на нем были растянуты, баннеры наезжали друг на друга, на главной странице встречались опечатки. Конечно, Евгений не стал вводить там свои данные и уж тем более отправлять деньги.

В чем суть обмана: преступники часто завлекают людей в свои сети обещаниями дистанционной работы и высоким заработком. Задачи могут быть самыми разными, – к примеру, оформлять заказы на сайте маркетплейса, затем отменять их. Якобы это повышает рейтинги выбранных продавцов и самой торговой площадки, и маркетплейс готов оплачивать такие услуги.
«Мне предложили работу на известном маркетплейсе, от 5000 рублей в день. Нужно просто заказывать товары, чтобы он поднялись в рейтинге. Деньги за покупку вернут и доплатят бонус сверху…»

Чтобы убедить человека, что работа настоящая, мошенники могут поначалу даже перечислить ему небольшую «зарплату». Но как только жертва пополнит «депозит» на крупную сумму — эти деньги уже не вернутся.

Как действовать: не верьте обещаниям высокого заработка за неквалифицированный труд без опыта работы. Обращайте

внимание на список обязанностей: расплывчатые формулировки — явный признак обмана.

Если потенциальный работодатель выходит с вами на связь в мессенджере или через соцсети, уточните, есть ли информация о вакансии на сайте компании или популярных ресурсах для поиска работы. Впрочем, иногда даже на известных рекрутинговых сайтах попадаются ненастоящие объявления — так что не теряйте бдительности на собеседованиях.

И, главное, не связывайтесь с людьми и компаниями, которые просят внести плату за регистрацию в их сервисах, перечислить «страховой взнос» или купить что-то, чтобы начать работать. Почти наверняка это мошенники.