Как мошенники получают доступ к личным кабинетам маркетплейсов?

Активное развитие дистанционных платежных сервисов, лежащих в основе бизнес-модели маркетплейсов, постоянно поддерживает интерес мошенников к этим площадкам. В целом, как говорит статистика МВД, количество мошеннических действий с использованием электронных средств платежа сократилось по итогам 5 месяцев 2023 года почти на треть по сравнению с аналогичным периодом 2022 года. Похоже, звучащая «из каждого утюга» установка на то, что ни в коем случае нельзя сообщать посторонним данные своей карты и платежные коды из СМС и чатов, наконец-то начала работать, а приемы социальной инженерии мошенников все чаще дают сбой. Но в случае с маркетплейсами применяются более изощренные схемы обмана, распознать которые сложнее. В результате, по данным одного из крупнейших маркетплейсов страны, 66% клиентов онлайн-магазинов хотя бы раз были обмануты мошенниками. Существует три главных способа обмана. Первый – покупатель переводит деньги по незнакомой ссылке, а продавец перестает выходить на связь. Второй – мошенник представляется сотрудником службы безопасности или службы поддержки и выманивает персональные данные. Третий ¬– злоумышленники различными способами заставляют перейти по ссылке на фишинговый, то есть поддельный, сайт аналогичный сайту онлайн-магазина и через него осуществляют кражу денег.

Как безопасно покупать товары на маркетплейсе и сохранить данные, рассказал интервью РИА Новости руководитель Центра финансовой грамотности НИФИ Минфина России Михаил Сергейчик.

Взлом аккаунта и заказ через него нерационально большого количества товара – явление редкое. Говорить здесь о краже денег не приходится, скорее, может идти речь о недобросовестной конкуренции – в теории недобросовестный предприниматель таким образом может лишить своего конкурента товарного запаса и стать на время монопольным продавцом. В свою очередь представители маркетплейсов утверждают, что в подавляющем большинстве случаев ошибочные покупки совершают маленькие дети невнимательных онлайн-шопоголиков. В любом случае онлайн-шопинг в современном мире требует соблюдения базовых правил кибербезопасности.

К ним можно отнести следующие:

1. Обязательный сложный пароль к своему аккаунту на телефоне, планшете и компьютере (пароль необходимо обновлять регулярно).

2. Нельзя передавать свои электронные устройства в другие руки, в том числе своим детям.

3. Выход «за территорию» мессенджеров электронной площадки и прямое общение с продавцом. С этого шага в большинстве случаев начинаются и классические, и экзотические мошеннические схемы.

4. Переход по сторонним ссылкам от неизвестных. Например, клиент читает отзывы на заинтересовавший его товар и видит комментарий другого клиента со ссылкой на аналогичный товар, но якобы более качественный. Переходить по таким ссылкам опасно. Автоматически может начаться загрузка вредоносного ПО на устройство. В результате злоумышленники могут получить ваши личные данные и возможность входа в ваш личный кабинет.

5. Длительное использование одного и того же пароля. Обычно личный кабинет не только хранит данные клиента, но и дает возможность быстрой оплаты. Поэтому к регулярной смене и выбору пароля от ЛК нужно относиться максимально ответственно. Менять пароль лучше раз в 5-6 месяцев. Причем для разных сервисов нельзя использовать одну и ту же комбинацию цифр и букв. Более надежную защиту ваших данных обеспечит двухфакторная аутентификация: для входа в профиль потребуется ввести не только логин/пароль, но и код из СМС.

6. Онлайн-шопинг через открытые сети Wi-Fi. Если вы совершаете покупки не через защищенную домашнюю сеть, лучше воспользоваться интернетом через мобильную сеть 4G. В идеале – для интернет-серфинга и шопинга использовать виртуальную частную сеть (VPN) в качестве персонального интернет-шлюза.

7. Карта для оплаты товаров. Для расчетов в Интернете лучше использовать отдельную карту: держать ее пустой до момента оплаты и пополнять перед оплатой только на сумму покупки. Кроме того, практически все банковские приложения позволяют установить максимальный лимит расходов по карте.

Что делать, если ваш личный кабинет взломали и от вашего имени оформили и оплатили заказ?

Если такое произошло, нужно как можно скорее отменить заказ и обратиться с жалобой в маркетплейс. В жалобе необходимо подробно описать произошедшее и потребовать возврат средств. Если торговая площадка откажет в возврате, нужно зафиксировать этот факт. Например, сделать скриншот переписки со службой поддержки. Это пригодится для будущих разбирательств.

Вернуть деньги в случае отказа торговой площадки поможет чарджбек (chargeback) – это возможность вернуть деньги через банк. Однако если деньги за товар, который пользователь не заказывал, вернуть удастся, то со штрафом за отказ от покупки – уже сложнее. Избежать списания средств поможет только блокировка банковской карты.

В этом случае взыскать деньги за доставку товара (штраф за отмену) маркетплейс сможет только в судебном порядке. Чтобы отстоять свою правоту в суде, потребителю необходимо доказать, что он не заказывал товар, а аккаунт был взломан.

Каждая ситуация разрешается индивидуально, поэтому необходимо собирать и хранить все возможные подтверждения действий злоумышленников.

Чтобы маркетплейс больше не хранил и не обрабатывал персональные данные пользователя, в том числе – данные карты, которые сохраняются даже после их удаления из ЛК, нужно направить письменный отзыв своего согласия на обработку персональных данных.

Источник: Моифинансы.рф