**Преступления, совершаемые с использованием сайтов бесплатных объявлений**

20.11.2020 Киберпреступность

**С каждым годом мошеннические схемы становятся все изощреннее, а выявить злоумышленников — все труднее и труднее. Новые технологии только играют преступникам на руку. А самое неприятное то, что жертва сама отдает свои деньги аферистам, даже не задумываясь о последствиях.**

Интернет-мошенничество процветает, пока мы смотрим очередное видео, ищем вторую половинку на сайте знакомств, общаемся в социальных сетях, просто серфим сайты в поисках чего-то особенного. Практически во всех обманных схемах жулики играют на наших чувствах: любопытстве, жадности и страхе. Мошенники в сети ищут и находят способы получить данные банковских карт, электронных счетов и даже наличные деньги.

*Одним из новых способов мошенничества является хищение денежных средств с использованием сайтов бесплатных объявлений.*

Мошенники создают поддельные сайты, похожие на сайт бесплатных объявлений и его сервисы, чтобы похитить деньги со счетов граждан с использованием их платежных карт. Заметить подмену неподготовленному пользователю будет сложно — страницы полностью копируют дизайн официального сайта и сервисов. Домены (адреса страниц) также пытаются замаскировать под страницы народной площадки объявлений.

— На сайте бесплатных объявлений переслать фишинговую ссылку нельзя — ее блокирует система безопасности, поэтому мошенники всеми силами и под любыми предлогами пытаются перевести общение в мессенджеры. Поэтому, если в мессенджере или в почте вам присылают ссылку на сайт бесплатных объявлений, не переходите по ней. Используйте официальное мобильное приложение сайта или вбейте нужный адрес руками.

— В своей работе мошенники используют 6 основных схем, успешно опробованных в России. В зависимости от того, насколько доверчивый собеседник попадается мошеннику, одна схема может перетекать в другую или изменяться, чтобы не вызывать подозрений.

Мошенники хорошо чувствуют эмоции собеседников, играют на доверчивости и открытости белорусов. Могут рассказывать, что попали в сложную жизненную ситуацию и продают вещь за бесценок потому, что нужно оплатить лечение родственнику, учебу ребенку или спасти бизнес, пострадавший от кризиса. Все, что находит отклик в сердце другого человека может и будет использовано ради наживы.

*Какие схемы используют мошенники*

**Для продавцов. Предоплата №1.**

* преступник находит продавца на площадке объявлений, копирует его контактные данные, но на площадке не пишет, — заблокируют. Ищет номер продавца в мессенджерах, представляется якобы покупателем и говорит, что готов купить товар по предоплате;
* высылает продавцу ссылку на поддельную страницу предоплаты, где продавцу нужно ввести номер своей карты для того, чтобы получить деньги от покупателя;
* естественно, никаких денег продавец не получит — как только он введет данные своей карты, преступник получит доступ к его счету.

**Для продавцов. Предоплата №2 (Продвинутая)**

* если предыдущая схема успешно сработала, мошенник может повторно сам связаться с покупателем или представиться службой поддержки и сказать, что произошла ошибка;
* чтобы вернуть ошибочно переведенные средства, он предложит перейти на фишинговый сайт и ввести данные своей карты;
* если продавец это сделает, мошенник повторно спишет деньги.

**Для покупателей. Доставка №1 (Базовая)**

* преступник выставляет товар по крайне выгодной цене;
* когда потенциальный покупатель пишет ему, убеждает перейти в мессенджер. Уговаривает покупателя на предоплату или доставку под любым предлогом: уехал из города, боится встречаться во время эпидемии коронавируса, нет времени;
* чтобы развеять сомнения покупателя, говорит о новой услуге холдирования средств: если доставки не будет, сайт автоматически вернет средства на карту;
* высылает покупателю ссылку на поддельную страницу, которая имитирует страницу сайта Доставки, где нужно ввести данные карты, чтобы совершить предоплату;
* как только пользователь вводит данные своей карты, с нее списываются деньги, посылка не приходит.

**Для покупателей. Доставка №2 (Продвинутая)**

* после того, как предыдущая схема полностью реализована, и покупатель начинает подозревать, что его обманули, мошенник повторно связывается с покупателем;
* говорит, что произошла ошибка, товар уже забрали (или передумал подавать), готов вернуть деньги;
* высылает ссылку на поддельную страницу возврата средств, где покупателю нужно ввести данные своей карты и точную сумму, которую ему должны вернуть;
* после того, как покупатель повторно вводит данные своей карты, с него повторно списывается та же сумма (если повезет) или все деньги.

**Для покупателей. Доставка №3 (Наглая).**

* после того, как мошенник реализовал схему Доставка 1.0, он пишет пострадавшему покупателю, представляется службой поддержки сайта;
* говорит, что посылка не была доставлена, извиняется и рассказывает про возможность возврата средств за посылку;
* присылает ссылку на фишинговую страницу, где покупателю нужно вбить данные своей карты и сумму, которая соответствовала сумме предыдущего списания;
* после того, как покупатель повторно вводит данные своей карты, мошенник повторно похищает деньги с банковского счета.

**Для покупателей. Доставка №4 (Мошенничество с накладными)**

* преступник выставляет товар по очень выгодной цене;
* когда потенциальный покупатель пишет ему, под любым предлогом предлагает перейти в мессенджер;
* уговаривает отправить товар по почте. При этом мошенник специально создает ажиотаж вокруг объявления. Он может говорить, что буквально на днях уезжает из города, или что товар готовы купить другие покупатели;
* продавец говорит, что можно оплатить товар уже после того, как он его отправит, при этом готов предоставить доказательства;
* если покупатель соглашается, в качестве доказательства отправки мошенник высылает ссылку поддельную страницу трекинга посылки или скан поддельного документа об оплате. Минимальное знание фотошопа позволяет преступнику сымитировать квиток любой службы доставки, будь то СДЭК, Белпочта или любая другая компания;
* после того, как покупатель поверил, что посылка отправлена, мошенник присылает ссылку на фишинговую страницу, где нужно оформить перевод суммы за товар;
* как только пользователь вводит данные своей карты, с него списываются деньги, посылка не приходит.

*Чтобы обезопасить себя от хищения денежных средств, не переходите по подозрительным ссылкам, также заведите несколько карт для разных целей: для платежей в интернете, для походов в магазин, для накоплений. И не храните на картах для расчетов лишние средства.*

**Роман Романенко,
начальник управления по противодействию киберпреступности УВД**