УДК 336.7

В. А. Штефан,
факультет экономики, менеджмента, сервиса и туризма
Омский государственный педагогический университет, Омск
Научный руководитель: канд. биол. наук, доцент Е. В. Алексеенко

Мошенничество в сфере цифровой экономики и методы борьбы с ним

Появление Интернета изменило нашу экономику. К сожалению, оно также позволило злоумышленникам вводить в заблуждение пользователей для хищения их средств, зачастую оставаясь в тени. В данной статье рассмотрены несколько распространенных приемов, которые используют злоумышленники, а также представлены способы борьбы с их деятельностью, доступные рядовому пользователю сети.

Ключевые слова: мошенничество, интернет, доска объявлений, сайты-клоны, спам.

Всемирная сеть Интернет затронула большинство аспектов нашего существования, проникла во все сферы жизни и серьезно повлияла на социальные институты. Не обошло влияние интернета и экономику. Интернет-каталоги известных торговых сетей, онлайн дискаунтеры, электронные кошельки, цифровые лицензии — всех тех благ, которые появились с приходом Всемирной паутины, и не перечислить. Но где появляются блага, там появятся и те, кто попытается их отнять. Речь идет о цифровом мошенничестве. Сегодня число правонарушителей неуклонно растет, а учитывая, что с основами Интернет безопасности знакомы не все, заниматься мошеннической деятельностью становится на порядок проще.

Рассмотрим несколько распространенных способов, используемых мошенниками. Стоит начать со случаев, когда злоумышленникам не требуется специальных средств взлома и программного обеспечения, а нужна лишь анонимность и немалая «доля харизмы». В качестве наиболее распространенного феномена здесь выступает мошенничество на досках объявлений [1]. По данным опроса РОЦИТ, проведенного совместно с интернет-сайтом Avito, уже около 85 % пользователей пользуются досками объявлений. У трети респондентов необходимость использовать доски объявлений возникает более одного раза в месяц (36 %).Такой огромный виртуальный рынок конечно же не обходят вниманием мошенники. Киберпреступники постоянно изобретают новые схемы мошенничества, направленные в первую очередь на кражу персональных данных и денежных средств. И если о сайтах-клонах, рассылке спама и вирусах будет рассказано чуть ниже, так как их создание требует определенных навыков и знаний, то вот на умалчивание о недостатках товара, предоставление ложных сведений о характеристиках, а также на подмену товара посторонними предметами при междугородней пересылке способен практически любой человек, разбирающийся в вопросах розничной торговли на минимальном уровне [2].

По данным РОЦИТ, 59 % пользователей досок объявлений приобретали там технически сложные товары, в том числе электроприборы. Визуально выявить наличие недостатков в таком приборе сложно, а если недостаток является скрытым, то выявить его при первичном осмотре не сможет даже высококвалифицированный специалист. В случае же, если покупатель столкнулся со злоумышленником, который орудует на рынке не первый год, то скорее всего он окажется обманут, даже если внимательно изучит товар и предлагающуюся документацию [3].

Для предотвращения подобных случаев не стоит покупать технически сложные устройства без упаковки, сопроводительных документов, полного комплекта сопутствующих товаров (наушников, блоков питания, шнуров и заглушек). Идеальным вариантом будет запечатанная заводской пломбой упаковка, наличие гарантийной документации, в том числе чеков, а также возможности убедиться, собственно, в наличии самого товара внутри коробки. Однако стоит учитывать, что и стоимость товара в этом случае будет выше. По возможности выбирайте для встречи место работы или проживания продавца, чтобы удостовериться в его благонадежности.

Но даже в этом случае вы можете стать обладателем подделки. Сейчас более дешевые аналоги известных товаров можно увидеть не только на стихийных рынках, но и в магазинах довольно крупных

торговых сетей. Зачастую это, действительно, лишь реплики, которые не используют логотип и название известного бренда, а лишь досконально копируют внешний вид и функции оригинала с существенной потерей качества. Однако есть и такие случаи, когда отличить оригинал от копии сразу невозможно, а продавец заведомо вводит потенциальных покупателей в заблуждение. Тогда речь и заходит о распространении подделок.

Чтобы удостовериться в том, что товар является оригинальным, необходимо тщательно осмотреть его, желательно вживую и непосредственно перед покупкой, так как злоумышленник может добавить в объявление фото оригинала, а в коробку поместить копию. Существует ряд явных признаков поддельного товара, чаще всего это наличие отличий в комплектации, установленных модулях и слотах, материале, наличие подозрительных символов в прошивке и качестве в целом. В телефонах важным моментом являются серийный номер устройства и IMEI код, по которым можно пробить информацию на специализированных сайтах [4].

Также следует воздержаться от покупки товаров из другого города, если продавец отказывается от обоюдного участи в «безопасной сделке», не привязывает к объявлению номер телефона, а представленные фото выглядят стоковыми или на них сложно разобрать детали. Но даже в случае, когда покупатель уверен в благонадежности продавца, ему могут выслать товар, собранный из запчастей или имеющий скрытые дефекты.

Разумеется, доски объявлений — не единственный инструмент, который злоумышленники используют против своих жертв. Далее речь последует о рассылке сообщений через СМС и e-mail. Эти сообщения могут как быть относительно безобидной рекламой платных подписок, так и содержать в себе ссылки на загрузку вирусного ПО, что является уже гораздо более серьезной угрозой.

Существует три основных способа рассылки спама: вручную, с помощью программ автоматической рассылки, а также с помощью троянских программ. В первых двух случаях сообщения приходят с посторонних номеров и адресов, хотя их содержание зачастую замаскировано под сообщения от безымянных родственников или популярных онлайн-компаний, суть которых сводится к тому, чтобы склонить пользователя на переход по вредоносной ссылке или загрузку приложенного файла с вирусом. Эти сообщения без труда отсеиваются встроенными спам-фильтрами, а также самими пользователями и направлены в основном на детей и лиц пожилого возраста.

В третьем случае сообщения могут приходить от проверенных лиц, чьи аккаунты были взломаны (либо чьи устройства были заражены троянским ПО). Такие сообщения могут содержать призывы о помощи, ссылки на якобы выложенные в сеть фото или видео и другие сообщения, призванные воздействовать на эмоции человека и зачастую лишенные конкретики. Чтобы бороться с такой рассылкой, следует иметь дополнительные каналы связи с родными и коллегами, чтобы всегда существовала возможность связаться с ними и уведомить о подозрительной активности на их страницах.

Последней темой, которая будет рассмотрена в данной статье, будет использование сайтов-клонов. Это интернет-страницы, созданные злоумышленником с целью хищения данных пользователей. Они имеют в той или иной степени измененный адрес (от незначительной точки или цифры до полного несоответствия оригиналу), но идентичное или приближенное к оригинальному сайту визуальное оформление. На таких страницах обычно присутствуют поля для заполнения данных карт, логинов, паролей, а также имеются различные ссылки на зараженные файлы. Иногда злоумышленник меняет условия предложений на более выгодные, чтобы склонить пользователя к передаче данных. Вычислить такие страницы можно, найдя в интернете реальный адрес необходимой компании и сравнив домены. Не рекомендуется переход по рекламным ссылкам и баннерам. Так же можно забить подозрительный домен в поиск или проверить его на специализированных ресурсах. Переход на другие разделы подозрительного сайта так же обычно невозможен. В любом случае, если появились подозрения, что данные карты могут быть похищены, следует немедленно заблокировать, связавшись с оператором банка.

Однако, существуют более продвинутые виды сайтов-двойников, где не только собираются данные карт, но и реализуется некачественный товар. Такие сайты обладают более совершенным функционалом, но также обладают и внушительным набором отзывов от обманутых клиентов. Внимательно изучите эти отзывы перед покупкой.

Подводя итоги, стоит признать, что перечисленные способы не являются единственными. Число методов злоумышленников растет с каждым днем, а потому необходимо следить за их появлением и проявлять повышенную бдительность. Только рациональный подход к посещению интернет-ресурсов может уберечь рядового пользователя от риска быть обманутым.

1. *Скворцова А. В.* Обманули на авито: как вернуть деньги гарантировано и по закону. — URL: https://yandex.ru/turbo?text=https%3A%2F%2Fregionfinans.ru%2Fzhiteyskie-voprosy%2Fobman-na-avito.html (дата обращения: 12.01.2020).

2. *Кириенченко Е. Н.* Спам-боты: вскрытие и борьба. — URL: https://xakep.ru/2007/01/19/36312/ (дата обращения: 12.01.2020).

3. *Степанова И. В.* Виды мошенничества на Авито. — URL: http://ugolovnyi-expert.com/moshennichestvo-na-avito/ (дата обращения: 12.01.2020).

4. *Воронцовский К. А.* Как работает спам-фильтр? — URL:https://www.unisender.com/ru/support/about/spam/spam-filters/ (дата обращения: 12.01.2020).