Мошенничество в Интернете!

В период стремительного развития цифровой экономики и глобальной информатизации общество столкнулось с очень серьезной и злободневной проблемой – мошенничеством в Интернете. В последнее время в Беларуси зафиксирован рост количества преступлений, связанных с хищениями денежных средств посредством обманных действий в Интернете и с использованием компьютерной техники. О способах защиты своих интересов от интернет-мошенничества сообщалось неоднократно многими средствами массовой информации, банками, правоохранительными органами. Эта статья, в первую очередь, о том, что делать, если Вы уже стали жертвой мошенников.

На сегодняшний день наиболее распространенными формами мошенничества в Интернете являются:

• рассылка (СМС, e-mail, в мессенджерах) предложений об участии в проектах, для вступления в которые необходима уплата взноса или сообщение личных данных, распространение сведений о выигрышах в конкурсах и акциях, для получения которого необходимо перевести определенную сумму или сообщить данные банковской карты;

• рассылка вредоносных писем и сообщений, содержащих ссылки на установку вредоносного ПО под видом лицензионного, которое впоследствии «вытягивает» персональные данные из девайса;

• «сайты-фальшивки» — на первый взгляд внешне не отличимые от искомых веб-сайтов (аналогичная структура и оформление, сходный до степени смешения домен), на которых не подозревающий пользователь вводит свои персональные данные;

• взлом аккаунтов в соцсетях для распространения просьб о материальной помощи на благотворительные цели (например, под видом перевода денег для больных родственников, детских домов, приютов и тд.);

• взлом и блокировка аккаунтов с большой аудиторией, для восстановления доступа к которым мошенники требуют перевода денег;

• звонки от имени компетентных представителей обслуживающего банка, требующих под различными предлогами сообщить им данные банковской карты и иные персональные данные (вишинг)

- просьбы одолжить денег

Друг просит в долг? Взломав чью-то учетную запись, злоумышленники первым делом пытаются разослать сообщения друзьям жертвы со срочной просьбой об одолжении денег в надежде найти сочувствующего друга, прежде чем обман будет раскрыт.

- опросы, тесты и конкурсы для сбора данных

Сегодня мы часто можем увидеть призывы пройти платный опрос, по итогу которого нужно лишь оставить данные банковской карты, чтобы оплатить небольшую комиссию за получение вознаграждения. Это мошенничество. Относитесь к подобным вещам скептически, даже если они рекламируются в социальных сетях.

- кликбейт

Это может быть страницей входа на сайт через аккаунт на Facebook или ВКонтакте. Вас может смутить тот факт, что нужно заново выполнить вход, но вы можете просто сделать это машинально. Они надеются, что вы сделаете это, ведь если вы все-таки введете учетные данные для входа, они завладеют страницей.

- сокращенные URL-адреса

Сокращенные URL-адреса выглядят короткими и симпатичными, начинаясь, например, с bit.ly (популярный сервис для сокращения ссылок), но злоумышленники используют их для скрытия подозрительных сайтов, распространяя подобные ссылки в социальных сетях и мотивируя перейти по ним.

Такие сокращенные URL-адреса могут маскироваться под официальные сайты, поэтому, прежде чем переходить по ним, проверьте эти адреса с помощью сервисов вроде CheckShortURL на наличие вредоносных программ.

- Запросы от людей, которые уже были в списке друзей

Вы получаете запрос на добавление в друзья от пользователя, который уже есть в вашем списке контактов, легко объясняете это как его новую страницу или странный сбой в системе и добавляете пользователя. Это ведь ваш друг. На деле это не всегда так. Это прием социальной инженерии в ее самом ужасном проявлении, рассчитанный на то, что вы сами без задней мысли добавите мошенника и будете считать, что на другом конце — ваш знакомый.

Что необходимо делать, если Вы попались на уловку злоумышленников:

1. БЛОКИРУЕМ КАРТУ

Если Вы понимаете, что стали жертвой мошенничества, а злоумышленники заполучили доступ к Вашим персональным данным, то немедленно заблокируйте банковские карты. Заблокировать карту можно следующими способами: • позвонить в круглосуточный контакт-центр обслуживающего банка (обычно номер указан на обороте пластиковой карты); • позвонить напрямую в круглосуточную сервисную службу Банковского процессингового центра (8-(017)-299-25-26); • через мобильный или интернет-банкинг; • через SMS-банкинг; • в отделении банка.

2. ФИКСИРУЕМ ИНФОРМАЦИЮ

При наличии возможности необходимо «по горячим следам» зафиксировать всю имеющуюся информацию о злоумышленнике: скриншоты (веб-сайта, социальной сети, переписки), имена, адреса, информацию, озвученную в ходе диалога, иные характерные особенности. В дальнейшем такие сведения могут быть очень полезны для установления и поиска виновных лиц.

3.ОБРАЩАЕМСЯ В ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ

Не стоит думать, что раз Вы не знаете ничего о злоумышленнике, то дело безнадежно. За время существования интернет-мошенничества правоохранительные органы выработали эффективные меры расследования подобных дел. Также не стоит отказываться от обращения в милицию по причине небольшой суммы похищенных денег: любые сведения о злоумышленниках помогают в раскрытии преступлений. Вполне вероятно, что вы не единственная жертва противоправных действий.