Кибермошенники

Автор: Редакция
08.06.2017 10:32 -

Сегодня мы почти каждый день – на экранах телевизоров, или в сети Интернет, или на расклеенных объявлениях – видим призывы собрать деньги на лечение больных детей или читаем просьбы перечислить посильные суммы в благотворительные фонды.
Как сделать доброе дело и при этом не попасть в лапы мошенникам?
Благотворительные фонды всё чаще сталкиваются с киберпреступниками, которые подделывают сайты фондов или собирают деньги на спасение несуществующих людей. Поймать и обезвредить мошенников бывает почти невозможно, но, если знать, как они действуют, и соблюдать несколько простых правил, можно не попасться на их удочку.
«Червь» в телефоне
- Мы уже второй год получаем запросы из МВД, - рассказывает исполнительный директор фонда «Подари жизнь» Григорий Мазманянц. - Люди пишут заявления в полицию и утверждают, что с их карточек снимаются деньги в пользу нашего фонда. Всё это клиенты одного крупного банка.
Получив несколько таких запросов, руководители фонда написали письмо в банк и выяснили, что с осени прошлого года его клиенты получали на свои телефоны вирус, который списывал со счетов деньги через мобильный банк. Сколько людей пострадали от этого вируса, неизвестно.

Компьютерные вирусы - проблема не только благотворительных фондов. Мошенники могут действовать от имени любой организации и взломать любой сайт, где совершаются платежи. Вирус может подменить данные в окне браузера - когда человек совершает платёж, его перекидывает на другую страницу, где деньги переводятся мошенникам, а не на счёт фонда.
«Черви» могут делать в вашем телефоне всё то же, что делаете вы: читать переписку, распоряжаться банковским счётом в мобильном банке. Иногда «трояны» умеют даже удалять сообщения, так что можно долго не замечать, что со счёта снимаются деньги. И всё это потому, что нам часто не хватает бдительности. Мы устанавливаем бесплатный фитнес-трекер или фонарик, а он запрашивает доступ к записной книжке и платёжной системе. Фонарик - это приложение, которое позволяет всем пользователям использовать своё мобильное устройство в качестве яркого и мощного фонарика. Зачем ему наши контакты? Но мы часто не задаём себе этот вопрос, а просто пролистываем окно и нажимаем «ОК», чтобы поскорее установить программу.
Мир поменялся, а мы оказались к этому не готовы. Многие по-прежнему думают, что киберпространство - это что-то не совсем реальное, а при этом в наших телефонах хранится куда больше важной информации, чем в кошельках и в сумках. Мы ведь всегда закрываем дверь, когда выходим из дома. Но при этом готовы доверить фонарику информацию о своём местоположении и оставить номер банковской карты на непонятном сайте. Пора бы уже относиться к киберпространству так же, как к реальному.
Что делать

Используйте антивирусы на всех устройствах и регулярно их обновляйте. Думайте, что за ссылку вы открываете и готовы ли установить приложение, которое получит доступ к вашей личной информации. Приложения из неавторизованных источников вообще не стоит устанавливать - почти все они вредоносные. Заведите себе отдельную банковскую карту для интернет-платежей и храните на ней только небольшие суммы денег или переводите средства прямо перед тем, как что-то купить или оплатить в Интернете. Номер основной карты, где хранятся ваши сбережения, нигде никогда не вводите.

Благо дарить?

В последнее время интернет-мошенничество, связанное с благотворительностью, встречается всё чаще. «Третий сектор» - то есть некоммерческие организации - в России достиг высокого уровня, и некоторые благотворительные фонды собирают больше миллиарда рублей в год, так что они стали очень привлекательны для мошенников. У некоммерческих предприятий, как и у любых других, есть свои бренды. И бренд благотворительных фондов - это доверие. Именно этим и пользуются мошенники. Они могут создать отдельный сайт, который выглядит почти так же, как сайт какого-то фонда, или создать группу в социальной сети. Для правдоподобности преступники часто берут фотографии и истории с настоящих страниц фондов. Иногда их полностью копируют, а иногда смешивают - например, фотография одного ребёнка, а текст про другого. Мошенники специально выбирают истории и фотографии, которые вызывают у пользователей больше эмоций. Доверчивые пользователи сами вовлекаются в эту схему, когда начинают делать репосты в соцсетях и призывать друзей тоже пожертвовать деньги. В итоге деньги попадают не туда, а настоящие фонды страдают от этого. Ведь у людей, попавших на удочку преступников, подрывается доверие ко всему «третьему сектору» в целом. При этом, если бы удалось выдворить из интернета всех мошенников, благотворительные фонды получали бы куда больше пожертвований, чем сейчас.

Что делать

Никогда не нужно переводить деньги в благотворительные фонды впопыхах, под воздействием эмоций. Как правило, жертвами мошенников становятся те, кто впервые совершают благотворительный перевод. Они читают ленту в соцсети, видят историю, которая задевает их за живое, и тут же отдают деньги, потому что им хочется сделать доброе дело.

На сайте настоящего фонда всегда есть отчётность, где отражены все поступления и траты. В идеале - копии платёжных поручений. Нужно следить, на какой счёт вам предлагают перевести деньги. «Если это банковский счёт частного лица или «Яндекс. Кошелёк», лучше сразу уходите с такого сайта.

Проявляя бдительность, вы добьётесь того, что ваши деньги пойдут на доброе дело, а не пополнят кошелёк киберпреступника.

Подготовила Т. НИКОЛАЕВА