Автор: Administrator
01.03.2020 00:00 -

После взлома профиля в социальной сети мошенники начинают рассылать сообщения всему списку друзей. Зачастую преступники оказывают психологическое давление или просто пользуются невнимательностью людей. Чтобы не попасться на их удочку, нужно знать самые распространенные схемы.

## Помоги больному ребенку

К рассылкам с просьбами перевести деньги на благотворительность для больных детей нужно относиться с большой осторожностью. Это одна из самых распространенных

схем, которая работает на сиюминутной жалости и доверии. Чаще всего ссылка в посте ведет на фейковую страницу, где мошенник может завладеть не только переведенными деньгами, но и данными банковской карты. В таком сообщении могут содержаться также реквизиты для отправки денежных средств. Разумеется, все они не на помощь детям, а в карман мошеннику.

Защитить себя несложно: в первую очередь необходимо удостовериться, что пишет именно хозяин страницы, а не кто-то посторонний. Задайте несколько наводящих вопросов или позвоните другу. Если окажется, что страница взломана, ее заблокируют после обращения в техническую поддержку.

Любые просьбы перевести деньги на благотворительность нужно проверять на достоверность. Достаточно ввести в любой поисковик имя ребенка, название благотворительной организации и воспользоваться поиском по фото. Мошенники часто используют данные действительно больных детей, деньги на лечение которых собирали несколько лет назад.

Случается и так, что сайт организации может внушать доверие. Не стесняйтесь написать его администрации и попросить подтверждающие документы на осуществление благотворительной деятельности. Честные волонтерские компании не скрывают эту информацию.

## Подпиши петицию против …

Мошенники могут отправлять ссылки на поддельные петиции, воздействуя на сознательность людей. Скорее всего, сайт запросит данные для регистрации: электронную почту, пароль, фамилию и имя. Учитывая, что большинство людей склонны пользоваться похожими или одинаковыми паролями, этого достаточно, чтобы получить доступ к  социальным сетям и аккаунтам на сторонних сервисах, включая банковские.

Если вам неизвестен сайт, на который ведет ссылка, или же вы неуверены в личности отправителя, нельзя вводить никакие личные данные. Оставить жалобу на сайт, занимающийся преступной деятельностью, можно через электронную приемную Роскомнадзора.

## Получи поздравительную открытку

Очень часто можно столкнуться с простой и неприятной схемой вымогательства личных данных: мошенник отправляет ссылку на поздравительную открытку, подарок или набор платных стикеров. Сайт, на который она ведет, может практически не отличаться по оформлению от известных социальных сетей. Он попросит зарегистрироваться, в результате чего данные также будут похищены.

Защититься от такого вредоносного спама очень просто: обращайте внимание на адрес сайта, на который вы переходите. Если он на одну-две буквы отличается от социальной сети, то это фишинговый сайт, который крадет регистрационные данные пользователей.

## У меня умер … , помоги деньгами

Пожалуй, одна из самых аморальных схем мошенничества. Со взломанной страницы пишут друзьям пользователя о смерти близкого родственника и якобы собирают деньги на его похороны. Такое сообщение у неподготовленного человека может вызвать сильный стресс, который притупляет бдительность.

Необходимо сразу же позвонить своему знакомому, с чьей страницы пришло сообщение и уточнить, действительно ли произошла трагедия. Скорее всего, все окажется в порядке. Сообщите другу, что его данными воспользовались для незаконного обогащения. Обращение к модераторам позволит вернуть утраченный доступ и предотвратить неприятные последствия.