**Распространенные способы мошенничеств в социальных сетях**

В настоящее время наличные денежные средства все больше уступают безналичным платежам, прогулки по рынкам и магазинам заменяют просмотры сайтов Интернет-магазинов, реальное общение переходит в виртуальное.

К сожалению, эру информационных-телекоммуникационных технологий не смогли оставить без внимания мошенники, а социальные сети огромный плацдарм для осуществления преступной деятельности. Существует огромное количество видов и способов мошенничеств в социальных сетях, но остановимся на самых распространенных «схемах».

1. Сбор денежных средств в несуществующих благотворительных фондах.

Многие помогают нуждающимся, попавшим в сложное материальное положение людям, через различные благотворительные фонды. В целях хищения денежных средств, мошенники создают «фейковые» группы с несуществующими историями людей, постановочными фотографиями.  При переводе денежных средств по реквизитам, указанных на таких сайтах, они поступают на счет злоумышленников, а не в помощь нуждающимся. Осуществляйте благотворительность только через проверенные фонды, с «прозрачностью» поступления денежных средств и отчетами по результатам оказания помощи.

2. Просьбы помочь от близких друзей

Нередки случаи, когда от друзей и знакомых Вам в социальных сетях приходят сообщения с просьбами о помощи либо займе денежных средств. Немаловажную роль играет посыл в данных сообщениях, когда они

сопровождаются какими-либо тревожными фактами (попадание в дорожно-транспортное происшествие, близкие в больнице, кража имущества, нет связи). В большинстве случаев от их имени Вам пишут мошенники, которые взламывают аккаунты в социальных сетях Ваших знакомых.

В указанных случаях Вам следует связаться с этим человеком по имеющимся у Вас его контактам, либо связаться с его родственниками и выяснить причины случившегося. Переводить денежные средства, пока Вы не убедитесь, кто находится по ту сторону экрана не следует.

3. Фишинговые приложения и сайты

Фишинг – это вид интернет-мошенничества, при котором данные пользователя попадают к злоумышленникам через фальшивые сайты, которые в точности повторяют интерфейс и дизайн оригинала.

Зачастую переход на фишинговые сайты популярных социальных сетей происходят, когда потерпевшие ищут сайт социальных сетей посредством поисковиковых страниц: (яндекс, гугл, майл.ру). При переходе на сайты социальных сетей обращайте внимание на правильное название сайтов, на которые переходите. Современные браузеры предупреждают пользователя о переходе на подозрительный сайт.

Кроме того, во избежание перехода на «фейковый» сайт, не переходите в социальные сети по ссылкам на сторонних сайтах.

4. Выигрыш призов или лотерей

Участились случаи, когда Вам в социальные сети приходят сообщения о выигрыше в розыгрыше или лотерее, и для его получения нужно лишь оплатить доставку, либо налог. В данном случае Вам следует вспомнить, заполняли ли Вы ранее купоны или анкеты для участия в розыгрышах и обратиться на тот сайт, где это происходило, чтобы проверить результаты конкурсов. Также не переходите по ссылкам, полученным в сообщениях от незнакомых лиц. Это может привести к попаданию стороннего программного обеспечения на Ваш смартфон/компьютер и в дальнейшем, посредством мобильного банка, могут быть произведены неправомерные списания с Ваших счетов.

Будьте бдительны при использовании и общении в социальных сетях, никому не сообщайте пароли от банковских карт. В случае, если в отношении вас совершено преступление, необходимо в обязательном порядке обратиться в органы полиции.