**Основы безопасности в сети интернет**

Основная проблема социальных сетей – это доверие к тем, кто внесен в список «друзей». Бездумное предложение «дружбы» от неизвестных или малоизвестных людей может привести к драматическим последствиям. Очевидно, что уровень доверия к тем, кто находится в списке «друзей», по определению всегда будет выше, чем к случайным людям. С одной стороны, это хорошо, так как формирует лояльную аудиторию вокруг человека, но с другой стороны, открывает двери для злоумышленников.

«Дружеский» стиль общения, распространенный в социальных сетях, обманчив. Он может создать ложное ощущение, что вокруг только друзья и доброжелатели, с которыми можно делиться любой информацией.

Общение в сети, точно такое же общение, как и в обычной жизни, с той лишь разницей, что дети порой доверяют «виртуальным друзьям» гораздо больше, чем реальным. Особенно это обостряется в тот момент, когда у подростка возникают проблемы в реальной жизни или в общении со сверстниками. В сети очень быстро находятся «сопереживающие» и «советующие».

Зачастую злоумышленники ведут очень долгую и дружескую переписку, находят слабые места, втираются в доверие, становятся лучшим другом или подругой, делают вид, что понимают собеседника лучше всех на свете, а потом, понемногу начинают склонять к тем либо иным действиям, манипулировать или шантажировать. Преследуя эти цели, злоумышленники порой используют фотографии «друзей» из профиля подростка, чтобы создать дубликат страницы этого «друга» и якобы от его имени уже вести переписку.

Обезопаситься от этого можно лишь развивая критичное отношение к собеседникам в сети и их словам, проявляя не меньшую осторожность, чем в обычной жизни. Не следует выставлять всю свою жизнь напоказ, гонясь за мнимой известностью, «лайками» и комментариями и, конечно же, следует понимать, что слова, написанные в личных сообщениях, отправленное фото и иные сведения, могут стать инструментом, который позволит манипулировать собеседником.

Вторая угроза связана со взломом пользовательских записей социальных ресурсов. И это происходит не потому, что использовались простые пароли (что конечно тоже бывает) или они записывались где-то, грубо говоря «на бумажке» и кто-то мог их «подсмотреть».

Проблема носит более масштабный характер. Источников утечки персональной информации о логинах и паролях пользователей данной социальной сети крайне много и в большинстве случаев вина лежит на самих пользователях, которые осуществляли авторизацию на иных ресурсах или в приложениях через свои учетные записи в социальных сетях. Например, для скачивания музыки или видеофайлов, получения мнимого выигрыша. Часть из данных ресурсов были созданы именно для сбора персональной информации.

Посредством взлома злоумышленник может проникнуть в социальную сеть, разослать по ее списку друзей фишинговое (или заведомо ложные) сообщение и получить деньги либо мотивировать получателей к каким-либо негативным действиям. Например, пройти по указанной ссылке и запустить вредоносный код.

Таким образом, после совершения несанкционированного доступа к аккаунтам, в течение первых суток развиваются следующие сценарии:

1. Злоумышленник рассылает всем виртуальным «друзьям» потерпевшего просьбу под различными предлогами сообщить реквизиты банковской платежной карты. Это может быть ее фото или просто номер, срок действия и иные реквизиты. При этом хоть школьники банковских карт не имеют, но желая помочь «другу», очень часто используют карты своих родственников и друзей. Порой преступники просят просто номер мобильного телефона либо пытаются похитить со счета деньги или наоборот используют его как промежуточное звено, направляя на этот счет чужие деньги, переводя их затем дальше, чтобы запутать свои следы. Практически во всех случаях хищения денежных средств со счетов мобильных телефонов потерпевшие сообщали преступнику персональные коды, приходящие в виде смс-сообщений на телефон.

Чтобы обезопасить себя от этого вида преступлений, не стоит сообщать никому реквизиты доступной банковской платежной карты или номер мобильного телефона и содержание смс-сообщений, поступающих для подтверждения совершения операции.

2. Злоумышленник изучает содержание переписок потерпевшего и использует их содержание в качестве инструмента для вымогательства денежных средств. Таким образом, инструментом вымогательства становятся личные диалоги на откровенные темы, фотографии, содержащиеся на странице и иные личные данные. Обычно, перед тем как связаться с потерпевшим, преступник делает скриншот списка всех его друзей и близких. Избежать подобного возможно лишь путем регулярной чистки своих диалогов и удаления из сети всей информации, компрометирующего характера.

3. Злоумышленник начинает рассылать различного рода порочащую информацию от имени владельца страницы иным пользователям.

В случае обнаружения «взлома» аккаунта, прежде всего, следует попытаться восстановить доступ наиболее привычным способом, путем отправки сообщения на «привязанный» номер мобильного телефона или электронную почту, кроме этого, следует оповестить друзей и знакомых об инциденте, используя иные социальные сети и мессенджеры. Также, чтобы в какой-то мере обезопасить себя от взлома, специалисты рекомендуют «привязать» страницу социальной сети именно к номеру мобильного телефона, а не к адресу электронной почты. Помимо этого, в настройках страницы в разделе «Безопасность» подключить услугу «Подтверждение входа». При этом вход на Вашу страницу с неизвестного компьютера или мобильного телефона будет не возможен без знания кода, который автоматически будет выслан на указанный при регистрации страницы номер.