Правила безопасности в социальных сетях

Сегодня социальные сети становятся все более популярными, каждый день новые пользователи регистрируются в таких сетях как Вконтакте, Одноклассники, Фэйсбук, Твиттер и другие. В социальных сетях люди могут общаться, обмениваться фотографиями и видеозаписями. И чем популярнее становятся такие ресурсы, тем больше интереса к ним проявляют мошенники, и тем опаснее становится их использовать. Чтобы не нарваться на хакеров, спамеров и мошенников, которые похищают персональные данные, нужно знать правила безопасности в социальных сетях.

1. При регистрации в социальной сети лучше придумать случайный пароль, состоящий не менее чем из 6-7 знаков. Пароль от вашего аккаунта в социальной сети и пароль от электронной почты не должны совпадать, это затруднит задачу хакерам. А если пароли будут разными, то на почту можно будет выслать пароль от своей учетной записи. Лучше всего, если для каждого сайта в сети у вас будут разные пароли.

2. Для выхода в социальные сети используйте только распространенные и доказавшие свою надежность браузеры. Не забывайте также устанавливать обновления для своей операционной системы и для браузера. То же самое относится к брандмауэру и антивирусу – все эти меры предосторожности помогут вам повысить свой уровень безопасности в социальных сетях.

3. Никогда не принимайте и не устанавливайте неизвестные файлы от людей, которых не знаете. Не открывайте подозрительные сообщения, в которых находятся ссылки на неизвестные ресурсы, и никогда не переходите по этим ссылкам. Мошенники могут пообещать вам все, что угодно, включая фотографии голых знаменитостей, не попадайтесь на их удочку.

4. Не устанавливайте приложения для социальных сетей, которые якобы позволяют найти работу, скачать музыку, видео и другое, если вы не уверены в безопасности этих приложений. Часто при установке они запрашивают логин и пароль от вашего аккаунта – все это ухищрения хакеров, которые пытаются заполучить доступ к вашему аккаунту.

5. Старайтесь не заходить на свои аккаунты в социальных сетях с чужих компьютеров. Даже если вы доверяете этому человеку, может случиться так, что на его компьютере находится троян, который отправит хакеру данные о вашем аккаунте.

6. Осторожнее размещайте информацию о себе в социальных сетях. Часто мошенники взламывают аккаунты с помощью кнопки «Забыли пароль?», которая предлагает ответить на секретный вопрос. Эти вопросы стандартные, и ответы на них пользователь может сам по неосторожности разместить на своей странице. Поэтому, если социальная сеть позволяет, лучше придумать свой, оригинальный секретный вопрос.

7. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение.

8. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее.

9. Иногда сообщения, отправленные вам якобы вашими друзьями, могут быть отправлены злоумышленниками, которые взломали их аккаунты. Поэтому если сообщение кажется вам подозрительным или содержит подозрительную ссылку, свяжитесь с другом напрямую или по телефону, чтобы убедиться, что сообщение действительно пришло от него.

10. Не позволяйте социальным сетям сканировать адресную книгу вашей электронной почты, чтобы не раскрывать адреса своих друзей.

11. Чтобы зайти в социальную сеть, используйте непосредственно адресную строку браузера или закладку. Если вы перейдете в социальную сеть по случайной ссылке из интернета, то можете попасть на поддельный сайт, который крадет личные данные.

12. Следите за тем, кого вы добавляете в друзья. Часто мошенники стараются таким образом узнать данные, которые доступны только для ваших друзей.