# **Чем опасны социальные сети**

Социальные сети, такие как Одноклассники, Вконтакте, Одноклассники, Facebook, Twitter и многие другие позволяют людям общаться друг с другом и обмениваться различными данными, например, фотографиями, видео и сообщениями. Сегодня миллионы людей разной национальности и разного возраста имеют свои странички в социальных сетях. По мере роста популярности таких сайтов растут и риски, связанные с их использованием.

Социальные сети дают человеку возможность обрести новых друзей любого пола и возраста. Вот только будет ли общение с ними доверительным и глубоким?

Главный недостаток виртуального мира – это полное отсутствие непосредственного общения. Мы не видим эмоций, жестов и мимики собеседника, а значит, не может быть уверены в искренности и положительном настрое человека к нам.

Сейчас вместо улыбки мы можем поставить смайлик, но он не несёт в себе столь уж серьёзной функции. В будущем это может привести к тому, что люди не будут понимать, что происходит вокруг. Серьёзное отношение будет восприниматься как шутка, и наоборот.

Сейчас психологи уже вывели такое понятие, как «**зависимость от Интернета**». Специалистов больше всего пугает тот момент, что данный вид зависимости развивается гораздо быстрее, чем привыкание к алкоголю и курению.

Серьёзная проблема школьников, живущих в Сети, это безграмотность. Общение со сверстниками не требует грамотности, поэтому дети пишут с ошибками, не обращая внимания на подчёркивания редактора. Кроме того, сейчас стало модным писать сообщения нарочито неправильным языком.

* Проникновение социальных сетей в жизнь человека предоставляет для него серьёзную опасность.

Часто мы размещаем о себе много личной информации (домашний адрес, телефон, социальный статус), которая легко может быть использована злоумышленником против нас. Помните, что любой человек в Сети может скрываться под маской друга, а на деле быть опасным кибер-преступником.

**Правила безопасности при использовании социальных сетей**

* **Проявляйте осторожность при переходе по ссылкам, которые вы получаете в сообщениях от других пользователей или друзей.** Не следует бездумно открывать все ссылки подряд - сначала необходимо убедиться в том, что присланная вам ссылка ведет на безопасный или знакомый вам ресурс.
* **Контролируйте информацию о себе, которую вы размещаете.** Обычно злоумышленники взламывают учетные записи на сайтах следующим образом: они нажимают на ссылку "Забыли пароль?" на странице входа в учетную запись. При этом для восстановления или установки нового пароля, система может предлагать ответить на секретный вопрос. Это может быть дата вашего рождения, родной город, девичья фамилия матери и т.п. Ответы на подобные вопросы можно легко найти в сведениях, которые вы опубликовали на своей странице в какой-либо популярной социальной сети. Поэтому при установке секретных вопросов необходимо придумывать их самостоятельно (если сайт, на котором вы регистрируетесь, это позволяет) или старайтесь не использовать личные сведения, которые легко найти в сети.
* **Не думайте, что сообщение, которое вы получили, было отправлено тем, кого вы знаете, только потому, что так написано.** Помните, что хакеры могут взламывать учетные записи и рассылать электронные сообщения, которые будут выглядеть так, как будто они были отправлены вашими друзьями. Если у вас возникло такое подозрение, будет лучше связаться с отправителем альтернативным способом, например, по телефону, чтобы убедиться в том, что именно этот человек отправил вам данное сообщение. Точно также необходимо относиться и к приглашениям зарегистрироваться в той или иной социальной сети.
* **Чтобы не раскрыть адреса электронной почты своих друзей, не разрешайте социальным сетям сканировать адресную книгу вашего ящика электронной почты.** При подключении к новой социальной сети вы можете получить предложение ввести адрес электронной почты и пароль, чтобы узнать, есть ли в этой сети пользователи, с которыми вы уже поддерживаете отношения при помощи электронной переписки. Используя эти данные, сайт может рассылать электронные сообщения (например, приглашения присоединиться к этой сети от вашего лица) всем пользователям из вашего списка контактов. Социальные сети должны указывать то, что эти адреса электронной почты будут использованы для этой данной, но зачастую не делают этого.
* **Вводите адрес социальной сети непосредственно в адресной строке браузера или используйте закладки.** Нажав на ссылку, которую вы получили в электронном сообщении или нашли на каком-либо сайте, вы можете попасть на поддельный сайт, где оставленные вами личные сведения будут украдены мошенниками.
* **Не добавляйте в друзья в социальных сетях всех подряд.** Мошенники могут создавать фальшивые профили, чтобы получить от вас информацию, которая доступна только вашим друзьям.
* **Не регистрируйтесь во всех социальных сетях без разбора.** К сайтам, на которых вы оставляете свои персональные данные, необходимо относиться очень серьезно. Кстати, эксперты признали "ВКонтакте" самой опасной социальной сетью для детей.
* **Учитывайте тот факт, что все данные, опубликованные вами в социальной сети, могут быть кем-то сохранены.** На большинстве сервисов вы можете в любой момент удалить свою учетную запись, но, не смотря на это, не забывайте, что практически любой пользователь может распечатать или сохранить на своем компьютере фотографии, видео, контактные данные и другие оставленные вами сведения.
* **Проявляйте осторожность при установке приложений или дополнений для социальных сетей.** Довольно часто Фприложения используются для кражи личных данных, поэтому к их использованию необходимо относиться также серьёзно, как и к установке на свой компьютер программ, которые вы можете найти в Интернете.

Но не все так печально на самом деле, не все социальные сети опасны, да и кроме социальных сетей в Интернете есть много чего интересного. В Интернете есть много познавательных сайтов, которые ведут интересные и умные люди. Кстати, вы сами можете создать свой сайт, хотя лучше поручить создание сайта профессионалам.

Педегог-психолог – Зайчикова М.В.

