

На сегодняшний день практически каждый человек знаком с понятием «социальная сеть». Многие из нас зарегистрированы в той или иной социальной сети, и в виртуальном пространстве создаются группы и сообщества, объединяющие людей с самыми разными интересами.

Однако существуют опасности, которые подстерегают любого пользователя социальных сетей: ваша личная информация, изображения, привычки и пристрастия, о которых вы рассказываете, информация о ваших близких – все это может быть использовано не с добрыми намерениями, использовано «против вас».

Чтобы не оказаться в какой-либо неприятной ситуации, прочтите и запомните простые правила безопасного поведения в социальных сетях.

Подготовлено по материалам источников:

1. Болсуновская Н. Этикет в Интернете: Правила сетевой культуры / Н. Болсуновская, О. Решетникова // Школьный психолог. – 2012. - №5. – С. 50
2. Детская безопасность в Интернете: технологии и рекомендации в помощь учителям и родителям // Школьная библиотека. - 2012. № 4-5. – С.28-73.
3. Как обеспечить безопасность своих данных в соцсети: Правила безопасности при использовании социальных сетей [Электронный ресурс] // Режим доступа: <http://www.microsoft.com/ru-ru/security/online-privacy/social-networking.aspx> - 23.01.13

Составитель: Мартынова Е.Р., психолог

Наши адреса и телефоны:

600028, г. Владимир,
пр-т Строителей, 23
(остановка «ул. Красноармейская»)
тел.: (4922)33-64-66

600009, г. Владимир, ул. Мира, 51
(остановка «ул. Полины Осипенко»)
тел.: (4922)33-37-00

Наш сайт: www.detmobib.ru

E-mail: pchelkaodb@mail.ru

ДЕПАРТАМЕНТ ПО КУЛЬТУРЕ АДМИНИСТРАЦИИ
ВЛАДИМИРСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ КУЛЬТУРЫ
ВЛАДИМИРСКОЙ ОБЛАСТИ
«ВЛАДИМИРСКАЯ ОБЛАСТНАЯ БИБЛИОТЕКА
ДЛЯ ДЕТЕЙ И МОЛОДЕЖИ»

ДЕТИ И СОЦСЕТИ: ПРАВИЛА ПОВЕДЕНИЯ



ПОДРОСТКАМ И МОЛОДЕЖИ

Владимир, 2013

Не регистрируйтесь во всех социальных сетях без разбора.

Оцените сайт, который вы планируете использовать, с точки зрения секретности. Узнайте, существует ли на сайте контроль информации, которая публикуется его пользователями. К сайтам, на которых вы оставляете свои персональные данные, необходимо относиться с той же серьезностью, которой требуют сайты, где вы совершаете какие-либо покупки при помощи кредитной карты.

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.

Контролируйте информацию о себе, которую вы размещаете.

Для установки 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 будет легко найти, если вы опубликуете эти сведения на своей странице в какой-либо популярной социальной сети. Злоумышленники смогут использовать эту информацию для взлома учетной записи. Поэтому при установке секретных вопросов необходимо придумывать их самостоятельно (если сайт, на котором вы регистрируетесь, это позволяет) или не использовать личные сведения, которые легко найти в сети.



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 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.

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.

