Правила безопасности при использовании социальных сетей

- Проявляйте осторожность при переходе по ссылкам.
- Контролируйте информацию о себе, которую вы размещаете.
- Не думайте, что сообщение, которое вы получили, было отправлено тем, кого вы знаете.
- Не разрешайте социальным сетям сканировать адресную книгу вашего ящика электронной почты.
- Вводите адрес социальной сети непосредственно в адресной строке браузера или используйте закладки.
- Не добавляйте в друзья в социальных сетях всех подряд.
- Не регистрируйтесь во всех социальных сетях без разбора.
- Все данные, опубликованные вами в социальной сети, могут быть кем-то сохранены.
- Проявляйте осторожность при установке приложений или дополнений для социальных сетей.
- Старайтесь не посещать социальные сети с рабочего места.

Социальные сети — это отличный способ быть на связи с людьми, а малая толика здравого смысла в отношении сведений, предоставляемых другим людям, может сослужить вам хорошую службу в сохранении безопасности и конфиденциальности важной информации.

Используемые ресурсы

- https://pp.vk.me/c320217/v320217375/e583/FwdlaZT5haE.jpg
- http://pro68.ru/wp-content/uploads/2012/02/kids-around-world-graphic8.jpg
- http://www.microsoft.com/ru-ru/security/online-privacy/social-networking.aspx
- http://joomlasecret.ru/wp-content/uploads/2014/01/1291922940_soc.jpg
- http://1webcent.ru/wp-content/uploads/2011/02/socnet.jpg
- http://clck.ru/9Cm7u

ВЛАДИМИРСКИЙ ИНСТИТУТ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ РАБОТНИКОВ ОБРАЗОВАНИЯ ИМЕНИ Л.И. НОВИКОВОЙ

Безопасность в социальных сетях

Социальные сети, такие как Одноклассники, Вконтакте, MySpace, Facebook, Twitter и многие другие, позволяют людям общаться друг с другом и обмениваться различными данными, например, фотографиями, видео и сообщениями. По мере роста популярности таких сайтов растут и риски, связанные с их использованием. Хакеры, спамеры, разработчики вирусов, похитители личных данных и другие мошенники не дремлют.

Владимир 2014

Социальная сеть – это онлайн-сервис, сайт, позволяющий создавать социальные связи, строить взаимоотношения, распространять информацию и др.

Главные особенности социальных сетей:

- практически неограниченные возможности для обмена самой разнообразной информацией;
- индивидуальные профили с максимальным количеством личной информации;
- добавление в "друзья" в первую очередь по принципу наличия реальной связи и во вторую – по принципу схожести интересов.

Сайт социальной сети предоставляет своим пользователям возможность отслеживать связи между своими "друзьями", вступать в различные сообщества, создавать группы, открывать или закрывать для всеобщего доступа информацию своего профиля, комментировать контент, который выкладывают его "друзья" и многое другое.

Риски в социальных сетях

- Потеря персональных данных и информации для доступа к аккаунту.
- Информация, которая появляется в Интернете в отношении тебя, может очень повлиять на тебя сейчас и в будущем.
- Можно заинтересовать не только кибер-, но и других преступников.
- Можно спровоцировать травлю со стороны пользователей сети.
- Возможно заражение компьютера.

Методы получения пароля:

- перебор пароля по словарю или подбор часто используемых простых паролей;
- прямой контакт с жертвой и выяснение, что может быть паролем;
- в интернет-кафе, а также у друзей, которые хотели бы получить пароль;
- получить доступ к профайлу можно через отсылку письма с просьбой перейти по ссылке и там ввести свои данные, или просто выслать свои данные для перерегистрации, представляясь сотрудниками портала;
- программные методы.

Советы по безопасности в социальных сетях

- Ограничьте список друзей.
- Защищайте свою частную жизнь.
- Защищайте свою репутацию.
- Используйте настройки конфиденциальности аккаунта.
- Принимайте запросы в друзья только от тех людей, которых знаете.
- Не используйте веб-камеру для общения с людьми, которых не знаете.
- Если говорите с людьми, которых не знаете, не используйте свое реальное имя и другую личную информацию.
- Если хотите встретиться с человеком, с которым познакомились через Интернет, то договоритесь о встрече в общественном месте, при этом желательно взять с собой кого-то еще.
- Избегайте размещения фотографий в Интернете, где Вы изображены на местности, по которой можно определить местоположение.
- Для социальной сети, почты и других сайтов необходимо использовать разные пароли.
- Не размещайте фотографии и видео со своими друзьями без их разрешения.
- Никогда не открывайте подозрительные ссылки, даже если они пришли от друзей.