Безопасная работа в социальных сетях: общение, публикация материалов.

"Презентация подготовлена для конкурса "Интернешка" http://interneshka.org/".

Учащимся 9 класса МБОУ «Надеждинской СОШ» Кайбицкого района РТ

Салатовым Константином

Многообразие социальных сетей

- Общение:
  - блоговые сервисы (Blogger, LiveJournal, Open Diary, и др.);
  - микроблоги (Twitter, Yammer, Qaiku и др.);
  - соц. сети (Facebook, Vkontakte, Одноклассники, LinkedIn, Ning, Orkut и др.)
  - сети событий (Eventful, Upcoming и Meetup).

Многообразие социальных сетей

- Мультимедиа:
  - социальные видеохостинги (YouTube, Vimeo и Zideo);
  - сервисы обмена фото (Instagram, deviantArt, Picasa и Zooomr);
  - сервисы обмена музыкой (MySpace Music, Last.fm, ShareTheMusic и ccMixter);
  - Интернет-службы вещания в прямом эфире (Justin.tv, Skype, Ustream.tv, OpenCU);
  - виртуальные службы обмена презентациями (Scribd и Slideshare).

Многообразие социальных сетей

- Сотрудничество:
  - справочники (Wikipedia, Wetpaint и PBworks);
  - социальные закладки (Delicious, Google Reader, News2.ru, Bobrdobr.ru и др.);
  - новостные службы (Digg, NowPublic, Reddit и Mixx).

  Обзоры и авторские точки зрения:
  - сервисы потребительских обзоров товаров и услуг (MouthShut.com, Epinions.com и др.);
  - службы по бизнес-деятельности (Yelp.com и Customer Lobby);
  - социальные порталы популярных вопросов и ответов (WikiAnswers, Yahoo!Answers, Google Answers, Askville и др.).

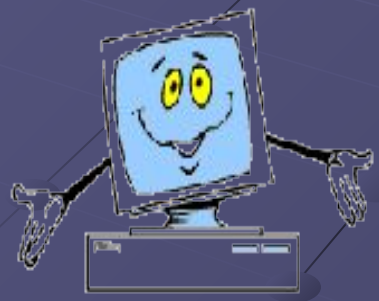
Многообразие социальных сетей

- Развлечения:
  - развлекательные платформы (Cisco Eos);
  - онлайн-игры (Аллоды, Троецарствие, World of Warcraft, The Sims Online и др.);
  - сервисы обмена играми (Kongregate и Miniclip).

Дополнительно подразделим социальные сети еще на несколько видов

- По доступности:
  - Открытые (Facebook);
  - Закрытые (бизнес-сети).
- По региону:
  - Мир (hi5);
  - Страна (Qzone).

  Территориальная единица



- • Без региона (InterNations).

Правила безопасной работы

- Социальные сети, такие как Facebook, Одноклассники, ВКонтакте, пользуются большой популярностью. Это привлекает мошенников. Используя *механизмы* социальных сетей, злоумышленники распространяют вредоносное *программное обеспечение*, собирают *персональные данные* о пользователях.

Вот несколько рекомендаций, которые позволят повысить *безопасность* работы в социальных сетях.

- **Ответственно подходите к выбору социальной сети.**
  Не следует регистрироваться во всех найденных социальных сетях. Перед регистрацией ознакомьтесь с правилами социальной сети. Обычно ссылку на правила можно найти на первой странице регистрации. Ознакомьтесь с информацией о социальной сети. Регистрируйтесь только в том случае, если правила сети вас устраивают.
- **При регистрации используйте сложный пароль.**
  Учетные записи пользователей социальных сетей представляют повышенный интерес для злоумышленников. Надежный пароль – один из главных факторов защиты учетной записи. Пароль должен содержать в себе буквы в разных регистрах, цифры и специальные символы. Чем длиннее пароль и чем менее осмысленным он является, тем лучше.

- **Никогда никому не сообщайте пароль для доступа к странице в социальной сети.**

  Администрация сети никогда не попросит вас сообщить пароль.
- **При завершении работы в социальной сети выполняйте процедуру выхода.**

  Если не следовать этой рекомендации, а, например, просто закрывать страницу, доступ к ней могут получить другие люди, которые работают за тем же компьютером.
- **Осмотрительно подходите к выбору друзей.**

  Не добавляйте в их список всех подряд. "Друзья" – это пользователи, с которыми установлены доверительные отношения. Обычно они обладают повышенным уровнем привилегий по отношению к вам – например, могут просматривать данные, закрытые от других пользователей, комментировать ваши записи, отправлять вам сообщения. Мошенник, находящийся в друзьях, сможет узнать о вас то, что вы не хотели бы делать общедоступной информацией.

- **Не переходите по ссылкам, отправленным в сообщениях, если вы не уверены в безопасности ссылок.**

  Ссылка на какой-либо сайт, полученная от человека, которого вы знаете, причем в сообщении, текст которого соответствует стилю общения этого человека, обычно безопасна. Однако, если вы получили сообщение, даже от известного человека, которое вызывает малейшие подозрения (стиль отличается от его обычного стиля, сообщение кажется бессмысленным, в сообщении имеется лишь ссылка), не переходите по такой ссылке.
- **Будьте внимательны, переходя на сайт социальной сети, проверяйте адрес в адресной строке браузера.**

  Злоумышленники создают сайты, по внешнему виду напоминающие сайты социальных сетей. Их основная задача – ввести пользователя в заблуждение и украсть его пароль. Поэтому для перехода на сайт социальной сети пользуйтесь закладками или, если вы хорошо помните адрес, вводите его непосредственно в адресной строке браузера.

- **Помните о том, что данные о себе, которые вы размещаете в социальной сети, могут попасть в руки злоумышленников.**

  Даже если вы установили ограничение на просмотр некоторых данных, злоумышленник может попасть в число тех, кто может получить к ним доступ.
- **С осторожностью устанавливайте приложения, ориентированные на работу с социальными сетями.**

  Подобные приложения могут собирать данные о вас, либо, если они созданы злоумышленниками, содержать вредоносный код, который может быть использован для кражи учетных данных в социальной сети.
- **Если вы подозреваете, что кто-то узнал ваш пароль к учетной записи, как можно скорее смените пароль.**

Принимая во внимание эти рекомендации, вы значительно повысите уровень безопасности и конфиденциальности при работе в любых социальных сетях.

Использованные материалы

http://smo-i-seo.ru/vneshnee-smosmm/vidy-socialnyx-setej.html

http://www.intuit.ru/studies/courses/3462/704/lecture/19435

http://smayls.ru/animashki-komputeri.html

2015 г.