Безопасная работа в социальных сетях: общение, публикация материалов.

Выполнила: Ложкина Екатерина
МБОУ СОШ №54
Ученица 10 класса А
Города Кирова.

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

Вступление.

- Интернет стал существенной частью жизни практически каждого. Помимо электронной почты, ставшей уже привычной, мы заводим персональные странички, блоги, вступаем в сообщества, разыскиваем родных, знакомых, одноклассников и старых друзей, создавая сети, которые могут стать нашей собственной ловушкой.

  Моя презентация поможет вам избежать часто допускаемых виртуальных ошибок. Ваша реальная, личная и профессиональная жизнь, а так же родные и близкие будут в полной безопасности, если вы будете придерживаться простых правил и советов, приведенных на следующем слайде.

Несколько простых правил безопасности:

- Никогда не публикуйте информацию, которую Вы не хотели бы видеть на доске объявлений. Как бы это не банально звучало, но практически любой пользователь может распечатать или сохранить на своем компьютере фотографии, видео, контактные данные и другие оставленные Вами сведения.
- Не добавляйте в «друзья» тех людей, которых Вы не знаете — оставляйте их в подписчиках. За фотографией прекрасной незнакомки, отправившей вам заявку, запросто может прятаться злоумышленник, намеревающийся выведать ценную информацию (например, номер телефона или адрес электронной почты), которая видна только своим.
- И наконец, не регистрируйтесь в тех социальных сетях, которые не собираетесь использовать. Многие люди, поддавшись какому-то сиюминутному энтузиазму, регистрируются везде, но оставив пару сообщений в ленте и не завязав общения с давними друзьями, навсегда покидают свою страничку. Люди приходят и уходят, а их личные данные остаются в сети навсегда…

Что не стоит писать в социальных сетях

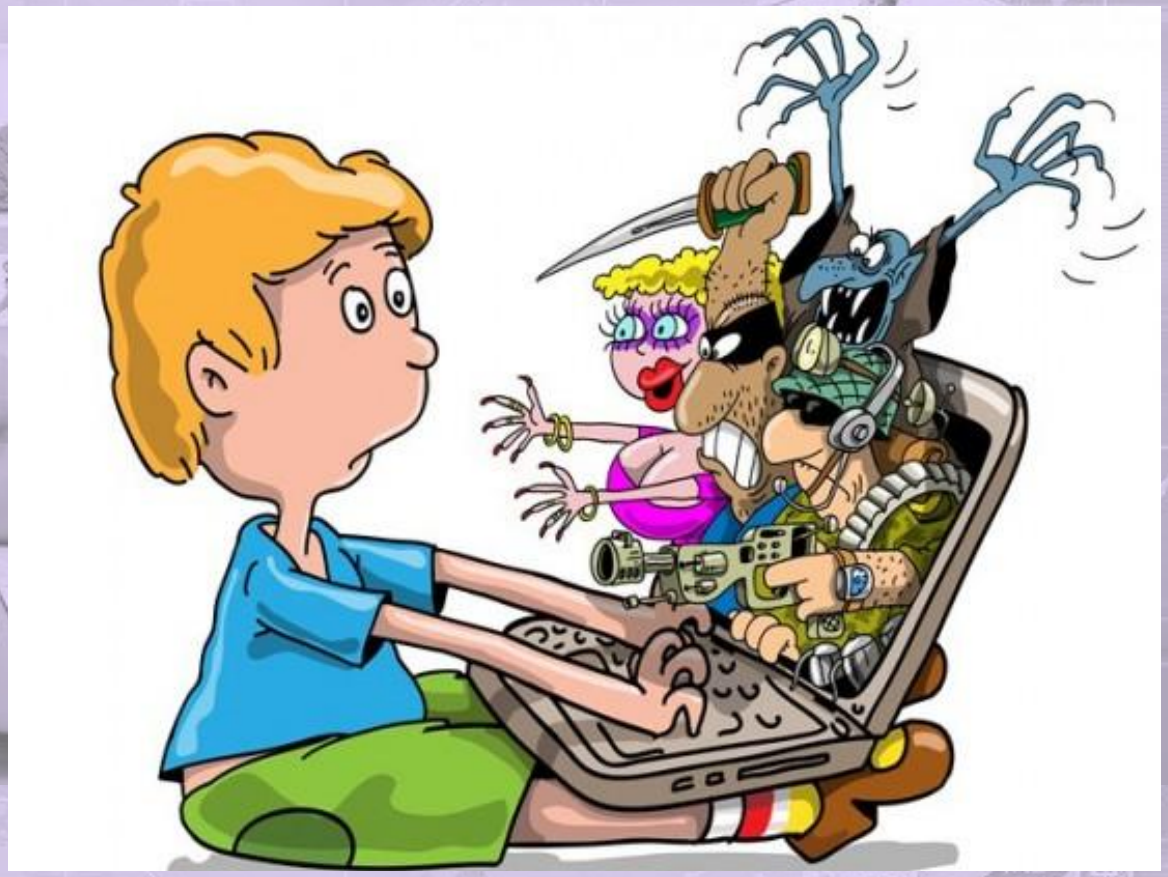
- Явки и пароли. Первыми под запрет попали логины и пароли. Оказалось, что социальные сети используются не только для общения, но и для хранения и обмена секретными данными. Причем некоторые пользователи могут "выставить на всеобщее обозрение" пароль и от самой соцсети. Поэтому особо наивным советуют сразу же сменить пароль, после того, как он попал в чьей-либо чужой ящик.
- Девичья фамилия. Продолжая тему безопасности в сети, нельзя не упомянуть и о кодовых словах, которые используются для возобновления забытого пароля. Ни для кого не секрет, что самыми популярными из кодовых вопросов являются либо девичья фамилия матери, либо номер школы. Именно по этой причине пользователей, желающих предоставить о себе как можно больше информации, предостерегают от афиширования фамилий родственников и номеров учебных заведений.
- "Стена" позора. Следующими в списке запрещенных действий в социальных сетях оказались публикации сообщений личного характера на так называемой "стене". Не надо забывать о том, что шедевры на "стене" видит не только получатель, но и другие пользователи. Поэтому перед тем, как отправить очередное сообщение провокационного содержания, задумайтесь, не навредит ли оно адресату.

- **Приманка для мошенников.** Контактные данные, в частности адрес и телефон, также не стоит оставлять в открытом доступе. Помните, что злоумышленники в любой момент могут использовать эту информацию в незаконных целях, особенно если знают, в какие часы вас не бывает дома.

- **Планы на вечер.** Для обсуждения планов на вечер или выходные лучше использовать личную переписку или создавать закрытые группы. Иначе информация о красочном уикенде может быть использована против вас же самих (смотрите предыдущий пункт).

- **Берегите свой кошелек.** Информация о вашем финансовом положении является, пожалуй, одной из самых секретных. Ни в коем случае нельзя сообщать о размере вашей заработной платы и о том, где вы ее получаете и храните.

- **Детские фотографии.** Безобидные на первый взгляд фотографии детей на самом деле могут сыграть злую шутку с их обладателем. Во-первых, нельзя забывать о людях, больных педофилией, а, во-вторых, информация о том, что ребенок может остаться дома один, может привести к ужасным последствиям.



Эта иллюстрация показывает, что вы общаясь по интернету не знает, точно, кто сидит по ту сторону экрана.

- **Охотники за компроматом.** Информация из вашего профиля также может быть использована другими сервисами и в итоге направлена против вас. Существует немало курьезных случаев, когда человек, отпросившись с работы по причине плохого самочувствия, вместо кабинета стоматолога проводил время на какой-нибудь вечеринке, а работодатель по случайности получал фотографии "тяжело больного сотрудника", танцующего и счастливого.
- **Сам себе враг.** Доверчиво публиковать информацию о себе, понадеявшись лишь только на то, что вряд ли кто-то увидит ее кроме самых близких людей, - ошибка многих пользователей. Помните, что большая часть приложений социальных сетей предназначена для доступа к конфиденциальной информации

Безопасность

Особое и первостепенное внимание стоит уделить вашей личной безопасности. Размещение излишне подробной и полной информации о вас, ваших паспортных данных, адресе, распорядке дня и планах, может спровоцировать мошенников или даже грабителей. Если вы планируете поездку или любое другое долгое отлучение из дома или офиса, постарайтесь не сообщайте об этом публично, ваши близкие друзья и без того будут в курсе всех ваших передвижений и планов.

Вирусы.

- В Интернете могут быть не только злоумышленники и сам человек, который выкладывает в Интернет информацию, но и на вашу безопасность могут повлиять вирусы.
- Вирусы - компьютерные вирусы, сетевые и почтовые черви могут распространяться самостоятельно. Например, если вам приходит подозрительное электронное письмо с вложением – весьма высока вероятность того, что оно содержит компьютерный вирус, который может заразить некоторые файлы на вашем компьютере, испортить или украсть какие-нибудь данные. Троянские программы самостоятельно не распространяются, хотя они могут распространяться с помощью компьютерных вирусов. Их основные цели – красть и уничтожать.

Несколько советов:

- **Защитите свой компьютер**
- Регулярно обновляйте операционную систему.
- Используйте антивирусную программу.
- Применяйте брандмауэр.
- Создавайте резервные копии важных файлов.
  Будьте осторожны при загрузке новых файлов.
- **Защитите себя в Интернете**
- С осторожностью разглашайте личную информацию.
- Думайте о том, с кем разговариваете.
- Помните, что в Интернете не вся информация надежна и не все пользователи откровенны.
- **Соблюдайте правила**
- Закону необходимо подчиняться даже в Интернете.
- При работе в Интернете не забывайте заботиться об остальных так же, как о себе.

Подытожим:

- Виртуальная реальность, как и любое пространство, обладает своими плюсами и минусами. Существование кибер-опасностей так же неоспоримо, как польза и удовольствие от использования Интернет-ресурсов. За безопасностью пользователей следят как государственные структуры, так и сотрудники Интернет сервисов. Тем не менее, ежедневно появляются новые жертвы, чаще всего пострадавшие от собственной неосведомленности.
-

Источники информации:

1. http://uinny.ru/articlessocial.php?id=73
2. http://webtous.ru/poleznye-sovety/pravila-bezopasnosti-povedeniya-v-socialnyx-setyax.html
3. http://softuhitel.com/bezopasnost-v-internete/
4. http://www.openclass.ru/node/431451
5. http://www.azbez.com/safety/internet
6. Картинка с 9 слайда - http://go.mail.ru/search_images?tsq=l&qp=800000&q=%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C+%D0%B2+%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B5&us=7&usln=2&usstr=%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81&usqid=a6a5caae85e81242&hasnavig=0#urlhash=5111626886600815748
7. Картинка с 7 слайда - http://go.mail.ru/search_images?tsq=l&qp=800000&q=%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C+%D0%B2+%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B5&us=7&usln=2&usstr=%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81&usqid=a6a5caae85e81242&hasnavig=0#urlhash=92201374119512229115