Презентация подготовлена для конкурса «Интернешка»

Безопасная работа в социальных сетях: общение, публикация материалов

* 1. Используйте **надежный пароль**: он должен содержать не менее 8-ми символов и состоять из букв в верхнем и нижнем регистре, цифр, спец. символов.
* 2. Обращайте внимание на ссылки, по которым переходите, контролируйте **правильность написания URL** социальной сети! Сегодня в Интернет существуют десятки клонов сайтов Вконтакте, Facebook и пр.
* 3. По возможности, включайте передачу данных по зашифрованному **протоколу HTTPS**, особенно если выходите в Интернет из публичных сетей.
* 4. Включите **двухфакторую авторизацию**. Помимо стандартной связки из логина и пароля, при входе в систему такой вариант защиты будет требовать еще и PIN-код.
* 5. Никогда **не публикуйте информацию**, которую Вы не хотели бы видеть на доске объявлений.
* 6. **Контролируйте информацию о себе**, которую вы размещаете.
* 7. Не разрешайте социальным сетям сканировать адресную книгу вашего ящика электронной почты.
* 8. Не добавляйте в «друзья» тех людей, которых Вы не знаете — оставляйте их в **подписчиках**.
* 9. Проявляйте осторожность при **установке приложений или дополнений** для социальных сетей.

Безопасность в соц. сетях

* **Правила безопасности при работе 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.
* Одна из ключевых проблем социальных сетей – открытость большинства учетных записей. В частности, по различным оценкам, порядка 500 миллионов пользователей социальных сетей по всему миру держат свою частную информацию в открытом доступе, а эта информация может собираться с помощью автоматизированных решений. К примеру, подобный функционал может быть встроен во всевозможные приложения, которыми славится один из самых популярных подобных сервисов – Facebook.
* Ни для кого не секрет, что в социальных сетях хранится много нежелательной информации: экстремистской, призывы к разжиганию национальной ненависти, порнография и т.п.

Защита собственной информации от несанкционированного доступа

Несанкционированный доступ –чтение, обновление или разрушение информации при отсутствии на это соответствующих полномочий.

Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи.

Защита от несанкционированного доступа

* Для защиты информации от несанкционированного доступа применяются:
* 1) организационные мероприятия;
* 2) технические средства;
* 3) программные средства;
* 4) щифрование.

Компьютерные вирусы

* Компьютерные вирусы — это одна из наиболее широко известных опасное для сетей. Подобно живым микроорганизмам, они распространяются, заражая здоровые программы. Заразив систему, они проникают в каждый исполняемый или объектный файл, размещенный на машине. Более того, некоторые вирусы заражают загрузочные сектора дисков, а это значит, что вирус проникнет и в машины, загружающиеся с зараженного диска.
* Большинство вирусов распространяется одним из двух методов: заражая файлы или загрузочные сектора.
  Файлы данных не могут быть заражены вирусом. Однако существуют так называемые макровирусы, которые распространяются с помощью файлов шаблонов.
  В Internet существует значительное количество «мнимых» вирусов.

Заражения вирусами

* Простейшие вирусы заражают файлы следующим образом:

1. Прежде всего пользователь должен загрузить зараженный файл в память компьютера. Этот файл может попасть в компьютер с помощью флоппидиска, локальной сети или через Internet. После его запуска вирус копирует себя в память компьютера
2. Разместившись в памяти, вирус ожидает загрузки следующей программы.

* 3. После запуска следующей программы вирус помещает свое тело внутрь жертвы. Кроме того, вирус помещает свое тело и внутри копии программы, хранящейся на диске.
* 4. Вирус продолжает заражать программы до тех пор, пока не заразит их все или пока пользователь не выключит компьютер. Тогда расположенный в его памяти вирус пропадает.
* 5. После включения компьютера и загрузки зараженной программы вирус снова начинает свою «невидимую» жизнь в памяти системы. И так до бесконечности.

Типы вирусов

* **Троянские кони**
* **Полиморфные вирусы**
* **Стелс-вирусы**
* **Медленные вирусы**
* **Ретро-вирусы**
* **Файловые вирусы**
* **Макровирусы**
* **Черви**

Антивирусные программы

* **Антивирус** – это программа, цель которой найти и обезвредить вирусы на компьютере пользователя.
* *Во-первых*, вы можете не знать и чаще всего и не знаете о наличии вирусов на вашем компьютере.
* *Во-вторых*, если вы и найдёте какой-то подозрительный объект на компьютере и это окажется вирус и вы его попытаетесь удалить как обычную программу, то ни к чему хорошему это не приведёт. Вирус, как правило где-то на компьютере остаётся, затем снова восстанавливается и продолжает вредить вашему компьютеру.

Работа антивирусов

* Диагностика
* Лечение
* Профилактика

Правовые и этические аспекты использования интернета

Информационная безопасность - защищенность информационной системы (ИС) от случайного или преднамеренного вмешательства в нормальный процесс функционирования, а также от попыток хищения, модификации или разрушения ее компонентов.