Пре тему: “Безпека в інтернеті”

Підготував учень
1(5)-А класу
Конотопської гімназії
Конотопської міської ради
Сумської області
Бабенко Антон

- Кожен користувач Інтернету повинен мати чітке уявлення про основні джерела безпеки, що йому загрожують. Це насамперед діяльність хакерів, а також віруси та спам.

Способи проникнення Хакерів до чужих систем

Троянські коні.

Перевантаження сайту або мережі.

Підміна адрес.

Аналіз пакетів.

Соціотехніка. .

Підміна веб-сторінки.

Віруси та хробаки

- Існують програми, що мандрують Інтернетом та, потрапивши на комп'ютер чи до локальної мережі, завдають тієї чи іншої шкоди. Особливо небезпечними є два види таких програм — віруси та хробаки.
- **Віруси.** Програми названі на ім'я біологічних організмів, бо вони досить малі, розповсюджуються, роблячи копії з самих себе, та не можуть існувати без носія.
- **Хробаки.** Хробак схожий на вірус тим, що розмножується, роблячи власні копії, але на відміну від останнього він не потребує носія й існує сам по собі.

Спам

- Спамом називають небажану електронну пошту, тобто пошту, що надходить без вашої згоди.

Хто за мною спостерігає?

- Крім програм, за допомогою яких певні люди намагаються проникнути до вашої системи, існують також засоби, що застосовуються для спостереження за вами. Це насамперед програмне забезпечення, яке зазвичай називають adware та spyware, шпигунські програми, програми для батьківського контролю, блокуючі програми тощо.

Як уберегтися від непроханих візитерів?

- Отже, ви мали змогу впевнитись, що є багато людей, які намагаються отримати доступ до чужих комп'ютерів. Проте існують засоби, що утруднюють цей процес або навіть унеможливлюють його. Найпоширеніші з них — брандмауери, а також антивірусне та антиспамове програмне забезпечення. Велике значення має також дотримання користувачами правил безпеки під час роботи в Інтернеті.

Антивірусне програмне забезпечення

- Однією з найбільших загроз для комп'ютерних систем є віруси. Для боротьби з ними можна придбати програмне забезпечення, що називається антивірусним.

Як уберегти персональну інформацію від викрадення?

- Правила безпеки, яких слід дотримуватися під час передавання інформації Інтернетом
- Ніколи не надсилайте персональну інформацію незнайомим людям.
- Не надавайте більше інформації, ніж потрібно. Захищені сайти зазвичай вимагають введення імені користувача та пароля. Робіть його довжиною щонайменше вісім символів, комбінуючи букви та числа.

Висновки

- Основними причинами, що провокують ріст мережної злочинності є недосконалі методи і засоби мережного захисту, а також різні уразливості у програмному забезпеченню елементів, що складають мережну інфраструктуру.
- Основними джерелами небезпек для користувачів Інтернету являється діяльність хакерів, вірусів та спамів. Існують засоби, що утруднюють доступ до чужих комп'ютерів – це брандмауери, антивірусне та антиспамове програмне забезпечення. Велике значення також має дотримання користувачами правил безпеки під час роботи в Інтернеті.
- Для отримання персональної інформації, небезпечні особи використовують чати, системи обліку миттєвими повідомленнями та сайти знайомств. Дотримання простих правил в спілкуванні через мережу Інтернет, дозволить захистити користувача від недобрих намірів зловмисників.

Інформація взята з сайтів:

- http://school.xvatit.com/index.php?title=%D0%9F%D1%80%D0%B5%D0%B7%D0%B5%D0%BD%D1%82%D0%B0%D1%86%D1%96%D1%8F_%D0%B4%D0%BE_%D1%82%D0%B5%D0%BC%D0%B8:_%D0%91%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0_%D0%B2_%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D1%96
- http://images.yandex.ua/yandsearch?text=%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0%20%D0%B2%20%D1%96%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D1%96%20%D1%84%D0%BE%D1%82%D0%BE&stype=image&lr=20553&noreask=1&source=wiz