Урок 1. Безпека в Інтернеті

Вивчення нового матеріалу

Слайд № 1

Наша мета – звести до мінімуму ризики під час роботи в мережі Інтернет.

Отже, зараз розглянемо всі основні мережеві загрози і спробуємо самостійно визначити правила безпечного використання Інтернету.

Проблема безпечного Інтернету наразі дуже актуальна!

Слайд № 2

Кожен день Ви виходите в мережу – спілкуєтеся з друзями, шукаєте інформацію, працюєте і т.д., і навіть не замислюєтеся над тим, що піддаєте свій комп'ютер та мобільні пристрої великому ризику.

Документи, сімейний архів, робоча переписка – все це може зникнути в одну мить через атаку якогось **вірусу**.

Ви вже давно є активними користувачами мережі Інтернет.

Слайд № 3

Різновидів вірусів існує просто безліч. Пропонуємо ознайомитися з найпоширенішими з них.

Завантажувальні віруси, або BOOT-віруси: заражають boot-сектори дисків, де містяться програми, що виконуються під час завантаження комп'ютера.

При звертанні до нового диска вірус копіює себе в його завантажувальний сектор і, таким чином, починає виконуватися під час кожного запуску комп'ютера.

Дуже небезпечні, можуть призвести до повної втрати всієї інформації, що зберігається на диску.

Завантажувальний вірус активізується під час завантаження комп'ютера.

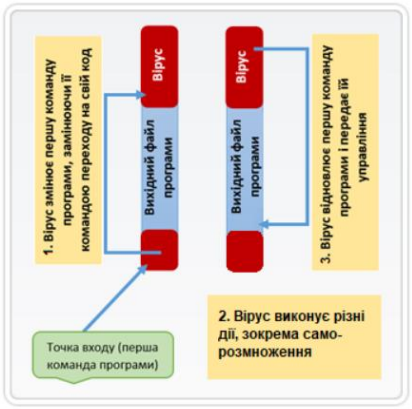
Слайд № 4

Файлові віруси заражають файли, переписуючись з одних файлів у інші.

Як правило, це файли програм. Їх називають також виконуваними файлами, оскільки в них містяться програми, що виконуються комп'ютером.

Стандартний сценарій атаки:

- Після запуску інфікованого файлу починає виконуватися не програма, що в ньому міститься, а вірус.
- Вірус виконує різні дії, до яких обов'язково належить саморозмноження.
- Вірус запускає корисну програму, яка була записана у файлі. Так що власне виконання вірусу користувач може й не помітити.



Вірус може записати свій код на початок, у середину, або в кінець виконуваного файлу.

Слайд № 5

Файлові віруси поділяються на

- віруси, що заражують програми (файли з розширенням **exe**, **com**, **dll**);
- макровіруси: віруси, код яких записано мовою сценаріїв, наприклад JavaScript або Visual Basic. Можуть заражати як файли скриптів із розширенням **js**, так і документи, наприклад файли Word або Excel.

Віруси-невидимки

- приховують свою присутність, фальсифікуючи операції читання з диска, які виконує операційна система і якими може скористатися антивірусна програма.

Файлові віруси — один з перших різновидів шкідливого програмного забезпечення, що отримав найбільшу популярність до 2000 року.

Далі

Слайд № 6

Ретровіруси

- заражують антивірусні програми, намагаючись знищити їх або зробити непрацездатними.

Віруси-хробаки

- хробак — це різновид вірусу, що існує в окремому файлі і саморозмножується, не заражаючи інші файли. Хробак існує на конкретному комп'ютері в одному екземплярі й шукає способи поширитися далі на інші комп'ютери.

Навіть є віруси-жарти, які не завдають шкоди комп'ютеру, а просто саморозмножуються і лякають користувачів.

Слайд № 7

Особливості троянських програм:

Троянський кінь (троян) — це різновид шпигунського ПЗ. Основна особливість троянських програм — це те, що вони не поширюються самостійно, а видають себе за корисні програми, й тому їх запускають та поширюють самі користувачі.

Як правило, мета трояна — замаскований збір конфіденційної інформації та її передача третій стороні. До такої інформації відносять реквізити банківських карт, паролі для платіжних систем, паспортні дані та інші відомості.

Троян – це диверсант, що сидить у засідці і чекає своєї години.

Слайд № 8

А які програми захищають від вірусів і троянів?

Антивірусна програма (антивірус) – спеціалізована програма для знаходження комп'ютерних вірусів та інших шкідливих програм і відновлення заражених ними файлів, а також для профілактики – запобігання зараження файлів чи операційної системи шкідливим кодом.

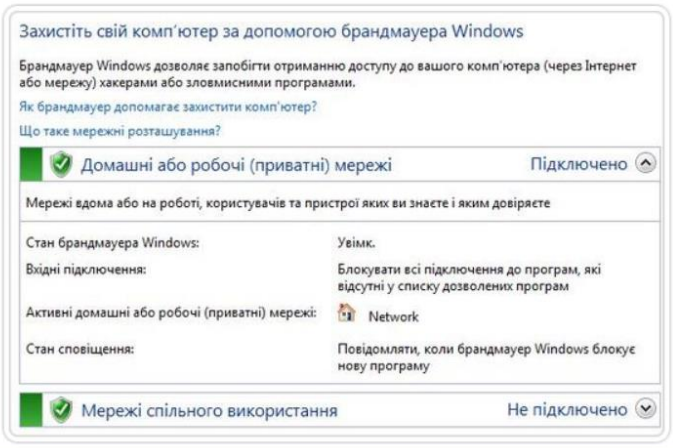
Перші, найпростіші антивірусні програми з'явилися майже відразу після появи вірусів.

Слайд № 9

Окрім антивірусної програми є ще таке поняття, як брандмауер – програма чи пристрій, що захищає комп'ютерні мережі.

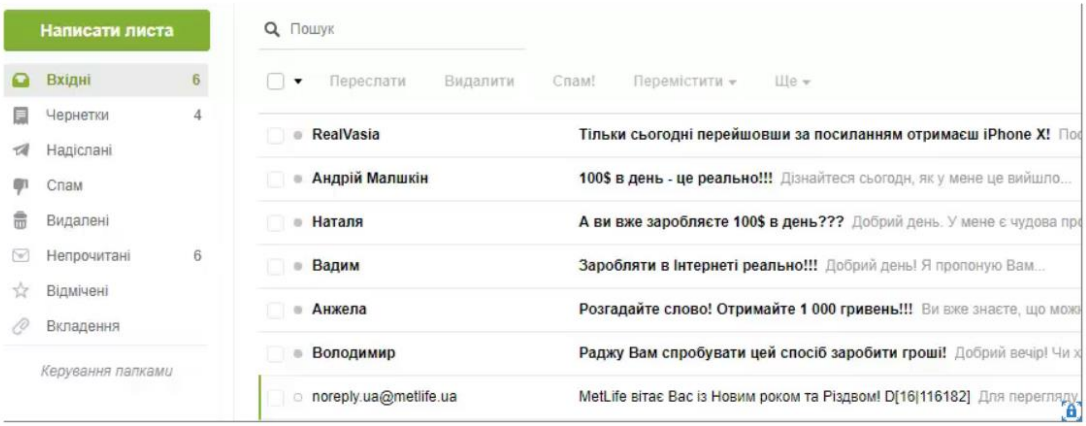
Брандмауер Windows є частиною Центру забезпечення безпеки Windows.

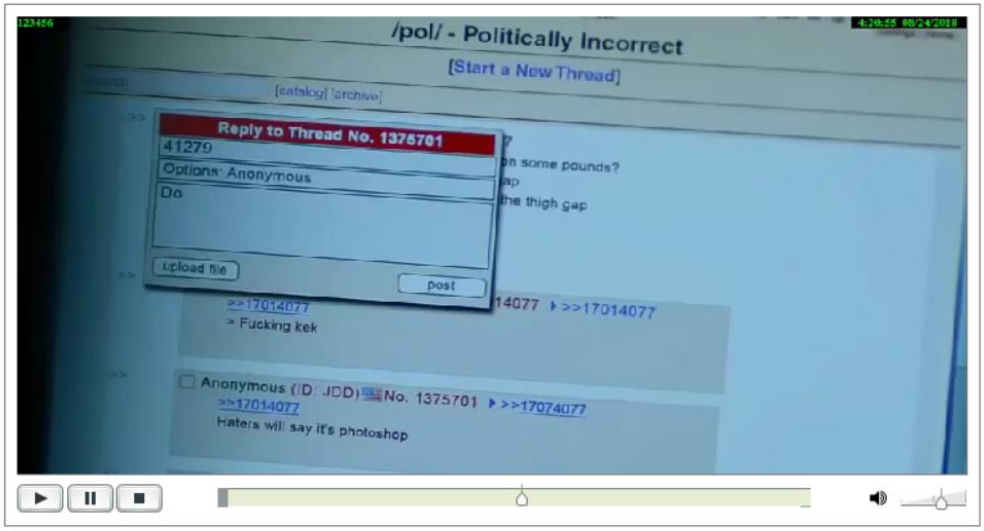
За допомогою брандмауера можна запобігти проникненню на комп'ютер хакерів або зловмисних програм (наприклад, хробаків) через локальну мережу або Інтернет. Крім того, брандмауер запобігатиме надсиланню зловмисних програм із вашого комп'ютера на інші.



Брандмауер Windows не може запобігти виникненню таких проблем, як віруси, що поширюються електронною поштою.

Слайд № 10

	Подивіться уважно на приклади спам-листів, які можуть надходити до електронної скриньки. A Анжела — Раджу Вам спробувати цей спосіб заробити гроші — Добрий вечір. Чи хотіли ви б дізнатися... — 31 бер. B Володимир — ! Розгадайте слово - отримайте 1 000 гривень — Ви вже знаєте, що можна заробляти в Інтернеті! — 30 бер. B Вадим — Заробляти в Інтернеті реально!!! — Добрий день. Я пропоную Вам ефективний метод... — 30 бер. H Наталя — А Ви вже заробляєте 100$ в день? — Добрий день. У мене є чудова пропозиція для Вас... — 30 бер. A Андрій Малкин — 100$ в день - це реально!!! — Дізнайтеся сьогодні як у мене це вийшло... — 29 бер. B Володимир — Бажаєте змінити своє життя? — Добрий день! Я пропоную Вам ефективний спосіб... — 29 бер.  Ці листи однозначно є спамом. Відкриття таких листів не несе ніякої користі і вони можуть містити небезпечні віруси!
Слайд № 11	**Щоб уникнути нав'язливих спам-листів, можна в електронній скринці відразу позначати їх як спам, навіть не відкриваючи!**   Ролик показує, як слід вчиняти з нав'язливими листами.
Слайд № 12	"Майстри" винайшли чимало способів незаконної реклами та інтернет-шахрайства. Серед них – власне реклама, антиреклама, так звані "нігерійські листи" (листи із закликом вислати невеликі гроші, щоб отримати натомість значно більшу суму), фішинг та інше.   **Фішинг** – це технології та дії, які імітують поведінку іншої людини. Метою зловмисників у фішингу є викрадення паролів або пін-кодів, щоб врешті-решт переказати гроші жертви на свій рахунок.  Нові версії браузерів вже оснащені такою функцією, як «антифішинг», яка інформує користувачів про те, що відкривається підозрілий сайт.

Слайд № 13	**Хакери своїми діями намагаються отримати незаконний доступ до комп'ютерних даних іншого користувача.** Наприклад, хакер може зламати комп'ютер користувача, надіславши програму-шпигуна в спамерському листі. Після відкриття такого листа шпигунська програма потрапить на комп'ютер отримувача.   Також на сленгу слово "хакер" вживається у значенні "досвідчений комп'ютерний програміст або користувач".
Слайд № 14	**Перегляньте фрагмент серіалу Homeland, де показано типові дії хакерів.**   Подумайте, що сталося і в чому була помилка жінки.

Слайд № 15	Отже, тенета Інтернету можуть бути дуже небезпечними, але без Інтернету вже не може обійтися жодна сфера діяльності сучасної людини. Треба з особливою обережністю працювати в мережі Інтернет і виконувати правила безпеки, тоді ризик зведеться до мінімуму.   Не забувайте, що, працюючи в Інтернеті, ви відкриваєте себе та свої дані всьому світові.