Презентація на тему:

Керування безпекою комп'ютера

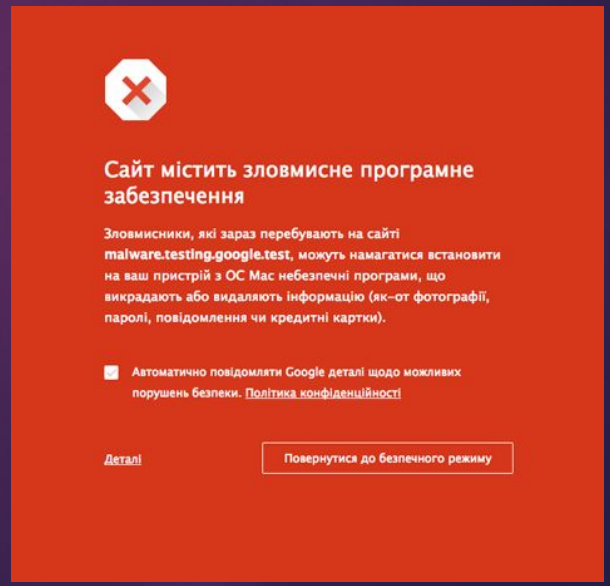
Якщо комп'ютер підключений до Інтернету,або користувач використовує файли спільно з іншими, слід ужити заходів для захисту комп'ютера від потенційної загрози. Чому? Тому, що на комп'ютер можуть вчинити напад комп'ютерні злочинці (іноді їх називають хакерами). Напад може бути безпосередній – зловмисники проникають у комп'ютер через Інтернет і викрадають особисту інформацію – або опосередкований, коли зловмисники створюють шкідливі для комп'ютера програми.

На щастя, можна захистити себе, вживши кілька простих запобіжних заходів. У цій презентації описано можливі загрози та способи запобігання ним.

Ознаки наявності зловмисного програмного забезпечення

Ознаками присутності на комп'ютері зловмисного програмного забезпечення можуть бути:

- *спливаючі оголошення;*
- *небажані панелі інструментів;*
- *недоречні результати пошуку Google або оголошення;*
- *переспрямування із сайту, який ви хочете відвідати, як-от із вашої домашньої сторінки або Google;*
- *пошукова система, яка нагадує Google, але її логотип і URL-адреса інші;*
- *отримання результатів з іншої пошукової системи.*



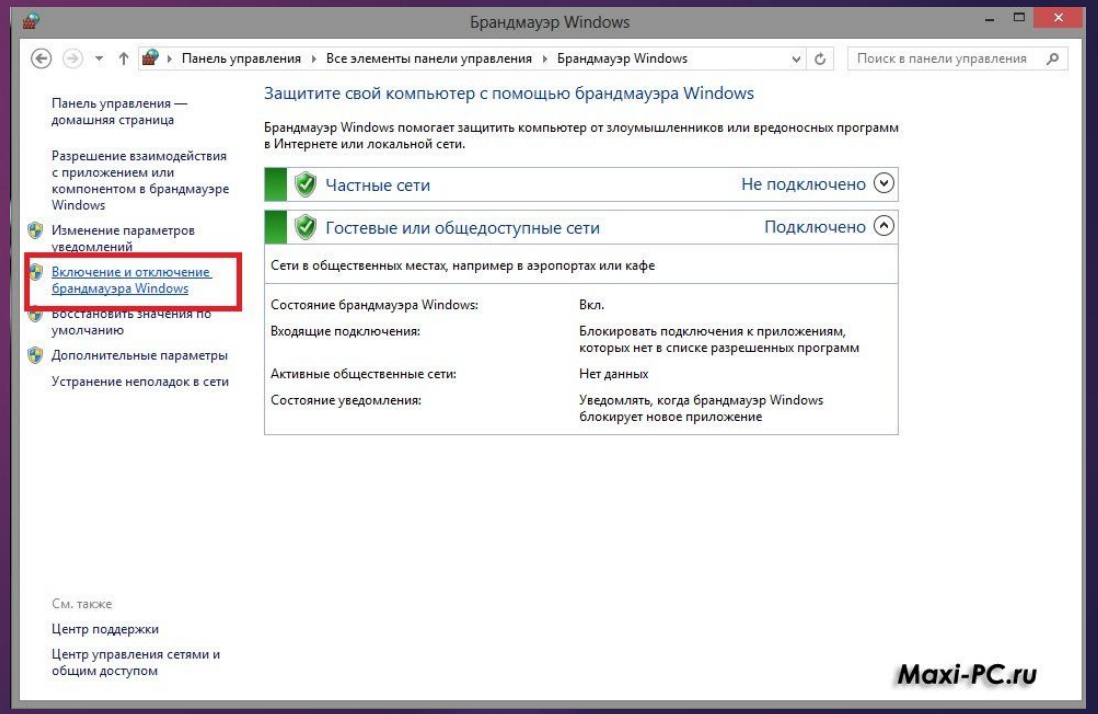
Захистити комп'ютер від потенційних загроз можуть такі засоби:

- *Брандмауер. Брандмауер допомагає захистити комп'ютер, не даючи змоги хакерам або зловмисним програмам отримати до нього доступ.*
- *Захист від вірусів. Антивірусне програмне забезпечення допомагає захистити комп'ютер від вірусів, хробаків та інших небезпек.*
- *Захист від шпигунських та інших зловмисних програм. Антишпигунські програми допомагають захистити комп'ютер від шпигунських та інших потенційно небажаних програм.*
- *Windows Update. Windows може регулярно перевіряти наявність оновлень для вашого комп' ютера й автоматично інсталювати їх.*

Використання брандмауера

Брандмауер - це програма або пристрій, який перевіряє дані, що надходять з Інтернету або мережі, та на основі поточних параметрів приймає рішення, потрібно їх пропускати чи ні. Таким чином брандмауер блокує доступ до вашого комп'ютера для хакерів і зловмисних програм.

Брандмауер Windows вбудований у систему Windows та вмикається автоматично.



Використання захисту від вірусів

Віруси, хробаки та троянські коні - це програми, створені хакерами, які використовують Інтернет для зараження комп'ютерів. Віруси та хробаки можуть самостійно переписуватись із комп'ютера на комп'ютер, а троянський кінь потрапляє до комп'ютера, сховавшись у звичайній на позір програмі, такій як заставка. Деструктивні віруси, хробаки та троянські програми можуть стерти інформацію з жорсткого диска або повністю вивести комп'ютер із ладу. Інші не завдають прямої шкоди, але знижують продуктивність і стабільність комп'ютера.

Антивірусні програми перевіряють електронну пошту та інші файли комп'ютера на наявність вірусів, хробаків і троянських програм. Якщо такі будуть знайдені, антивірусна програма переміщує їх у карантин (ізолює) або повністю видаляє до того, як буде заподіяно шкоду комп' ютеру та файлам.

Використання захисту від шпигунських програм

Шпигунськими називають програми, які можуть відображати рекламні повідомлення, збирати інформацію про вас або змінювати параметри на комп'ютері, зазвичай, без вашого відома. Наприклад, шпигунські програми можуть інсталювати небажані панелі інструментів, посилання або вподобання у браузері, змінювати встановлену за промовчанням домашню сторінку або часто відображати спливаючі рекламні оголошення. Деякі шпигунські програми нічим не виказують своєї присутності, а таємно збирають конфіденційні відомості (наприклад, введений текст або список відвіданих веб-сайтів). Більшість шпигунських програм інсталюються разом із безплатним програмним забезпеченням, завантаженим вами, проте подеколи навіть просте відвідування веб-сайту спричиняє зараження шпигунською програмою.

Автоматичне оновлення Windows

Microsoft регулярно розробляє важливі оновлення для Windows, які допомагають захистити комп'ютер від нових вірусів та інших загроз, що порушують його безпеку. Щоб забезпечити якнайшвидше отримання цих оновлень, увімкніть автоматичне оновлення. Таким чином вам не доведеться перейматися тим, що критичні виправлення в роботі Windows будуть відсутні на вашому комп'ютері.

Оновлення завантажуються приховано, коли ви підключені до Інтернету. Оновлення інсталюються о 3:00, проте ви можете встановити інший час для цього. Якщо ви вимикаєте комп'ютер до цього часу, оновлення можна інсталювати перед вимкненням. Інакше, Windows інсталює їх після наступного ввімкнення комп'ютера.