Міністерство освіти і науки, молоді та спорту України
Інститут інноваційних технологій та змісту освіти
Компанія "Майкрософт Україна"

Навчальний курс "Основи безпечної роботи з ІКТ в навчальному закладі"

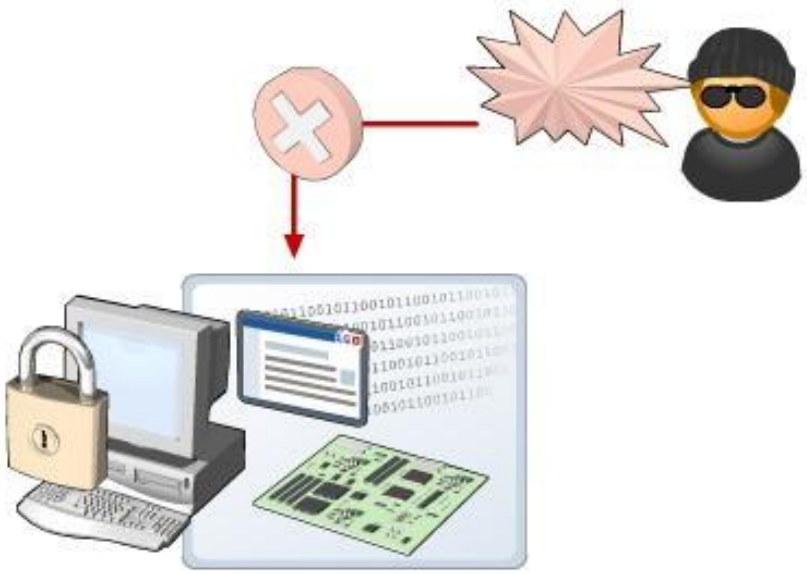
- 1.1. «Огляд безпеки та конфіденційності комп`ютера»

Артур Кочарян,
Координатор програми
"Онляндія – безпека дітей в Інтернеті"
2011 р.

Microsoft Partners in Learning

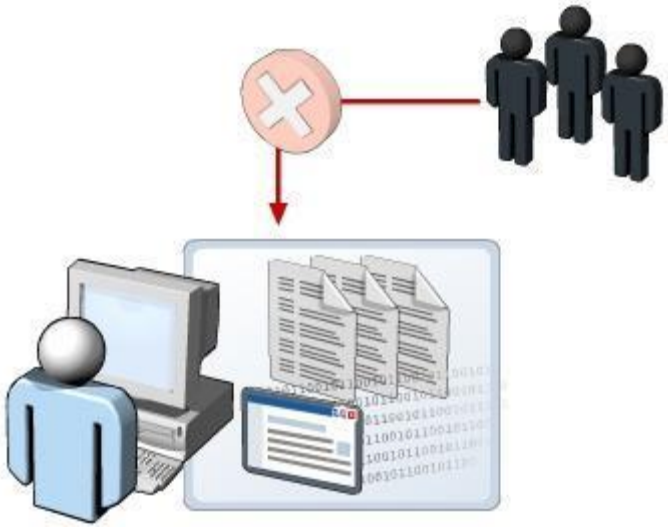
Microsoft

Вступ до безпеки та конфіденційності комп'ютера



- Обладнання комп'ютера може пошкодитися через недбалість людини або природні стихії, наприклад землетруси, повені й урагани. Крім того, дані та програмне забезпечення на комп'ютері слід захищати від випадкової або навмисної втрати та підроблення. Безпека комп'ютера стосується заходів, які можна здійснити для попередження подібного пошкодження комп'ютера та його даних.

Вступ до безпеки та конфіденційності комп'ютера



- Конфіденційність комп'ютера означає, що до даних, наприклад особистих файлів і повідомлень електронної пошти, без вашого дозволу не отримає доступу будь-яка інша особа. Конфіденційність комп'ютера стосується заходів, які можна здійснити для обмеження доступу до ваших даних. Конфіденційність комп'ютера також стосується обачності під час надання особистих відомостей через Інтернет.

Загрози для комп`ютера

- **Надмірне тепло або холод**. Більшість компонентів усередині комп'ютера розроблено для функціонування в межах певного діапазону температур. У разі впливу надмірного тепла або холоду деякі компоненти комп'ютера можуть почати неналежно працювати, тому їх слід буде замінити. Якщо комп'ютер перебував надворі та зазнав впливу екстремальних температур, перед запуском занесіть його до приміщення з кімнатною температурою.

- **Проблеми з напругою – сплески та стрибки напруги**. Сплески або стрибки напруги – це несподіване збільшення напруги живлення, яке може остаточно пошкодити деякі компоненти комп'ютера. Наприклад, раптове збільшення напруги може зруйнувати системну плату комп'ютера. Сплеск напруги може також трапитися через блискавку, при ударі якої виділяється значна кількість електричного заряду. Цей заряд може потрапити до комп'ютера через лінії електропередач або телефонні лінії та пошкодити компоненти всередині нього.

Загрози для комп`ютера

- **Фізична крадіжка**. Будь-який користувач може вкрасти ваш комп'ютер або його компоненти, якщо матиме доступ до них. У зв'язку з підвищенням популярності портативних комп'ютерів, наприклад лептопів, фізичні крадіжки комп'ютерів набули надзвичайного поширення.

- **Віртуальна крадіжка**. Можна стати жертвою віртуальної крадіжки, що стають більш поширеними в разі підключення комп'ютерів до Інтернету. Одним із прикладів віртуальної крадіжки є *викрадення особистих даних*, коли хакер може викрасти ваші особисті відомості для привласнення вашої особи. За допомогою цих підробних особистих даних хакер може отримати доступ до ваших фінансових рахунків або виконати незаконні дії. Іншим прикладом віртуальної крадіжки є *програмне піратство*, яке стосується викрадення комп'ютерних засобів або програм. Воно також може стосуватися несанкціонованого розповсюдження та використання комп'ютерної програми.

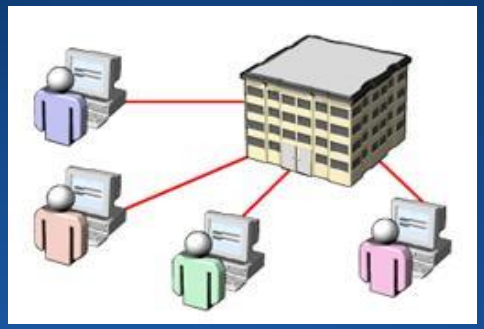
Загрози для комп`ютера

- **Шпигунське програмне забезпечення**. Так називаються програми, які інсталюються на комп'ютер без вашого відома. Вони можуть таємно надсилати відомості про перегляд вами веб-сторінок або інші особисті відомості на інший комп'ютер через мережу.

- **Злодії в мережі**. Злодії в мережі – це особи, які заохочують будь-яку людину в онлайні до непристойних і неетичних стосунків. Жертвами злодіїв у мережі можете стати ви або члени вашої родини. Злодії в мережі встановлюють контакт із своїми жертвами за допомогою електронної пошти або спілкування в чатах.

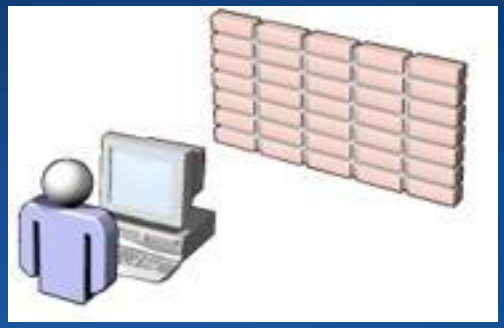
- **Інтернет-шахрайства**. Використовуючи Інтернет, можна отримати деякі привабливі пропозиції через повідомлення електронної пошти або під час спілкування в чатах. Слід бути надзвичайно обачними, перш ніж приймати подібні пропозиції, оскільки вони можуть бути частиною добре спланованих шахрайств, які можуть призвести до фінансових збитків.

Захист



Установіть ім`я користувача та пароль

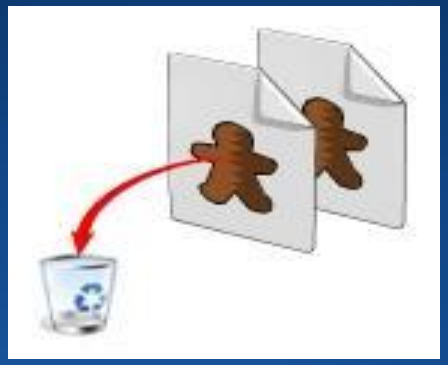
Слідкуйте за захистом свого паролю



Інсталюйте захисне програмне забезпечення

Захист

Періодично очищуйте журнал і кеш



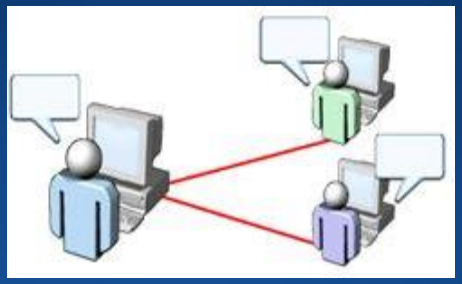
Періодично видаляйте файли cookie

Настройте компоненти безпеки за допомогою центру безпеки Windows

Захист

Захистіть себе від фішингу

Не відповідайте на небажані повідомлення



Спілкуйтеся в чаті лише з відомими вам особами

Почніть вже зараз!

Microsoft®
Partners in Learning

Microsoft