Інформаційна безпека.
Загрози при роботі в Інтернеті і їх уникнення.

Потреба в захисті дуже висока в наш час. Через те, що інформацію котра була вивільнена вами, і змінила носій з головного мозку на інший уже є мало захищеною.

І що ж таке ця безпека інформації?

Інформаційна безпека — це стан захищеності систем передавання, опрацювання та зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність даних.

Конфіденційність включає в себе доступність (забезпечення доступу до загальнодоступних даних усім користувачам і захист цих даних від блокування зловмисниками) та цілісність (захист даних від їх зловмисного або випадкового знищення чи спотворення).

Стосовно України то указом Президента в лютому 2017 року було прийнято Доктрина інформаційної безпеки України. Головними тезами якої є:

- Захист українського суспільства від агресивного впливу деструктивної пропаганди.
- Захист українського суспільства від агресивного інформаційного впливу, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України.
- Всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірних та об'єктивних відомостей.

Серед основних загроз використання комп'ютерних мереж для користувачів, виділяють: комунікаційні, контентні, споживчі та технічні ризики.

Комунікаційні ризики - - ризики, що пов'язані зі спілкуванням у мережі та використанням онлайн-ігор:

- ✓ БУЛІНГ - залякування, приниження, цькування, переслідування, компрометація людей з використанням особистих або підробних матеріалів, розміщених в Інтернеті, надсилання повідомлень з використанням різних сервісів;
- ✓ КОМПРОМЕТУВАТИ – виставляти в негарному вигляді, шкодити добрій славі;
- ✓ КІБЕР – ГРУМІНГ - входження в довіру людини для використання її в сексуальних цілях;
- ✓ ОНЛАЙН – ІГРИ – надмірне захоплення може призвести до втрати реальності, нерозуміння та несприйняття норм і правил людського співіснування, комп'ютерної залежності.

Контентні ризики - ризики, що пов'язані з доступом до матеріалів, розміщених у мережі, матеріалів шкідливого характеру або таких, що не відповідають віковим особливостям розвитку дитячої психіки.

Такі матеріали як правило містять:

- ✓ сцени насилля, жорсткої поведінки з людьми та тваринами;
- ✓ пропаганду расової або національної ненависті;
- ✓ рекламу або пропаганду використання тютюну, алкоголю та наркотиків, азартних ігор;
- ✓ пропаганду релігійних вірувань, заборонених законодавством, або спільнот, що не мають офіційних дозволів на свою діяльність;
- ✓ пропаганду шкідливих лікарських засобів і методів боротьби з хворобами, відмови від лікування;
- ✓ нецензурну лексику;
- ✓ матеріали для дорослих.

Споживчі ризики - ризики, що пов'язані з порушенням прав споживачів:

- ✓ реклама та продаж через мережу інтернет-магазинів низькоякісної продукції;
- ✓ купівля підроблених товарів відомих виробників;
- ✓ втрата коштів через невиконання обіцянок надіслати товар, невідповідність товару за якістю або за виробником (шахрайство);
- ✓ викрадання персональних даних для зняття коштів без відома користувача з його рахунків.

Технічні ризики - ризики, що пов'язані з роботою шкідливих програм:

- ✓ Віруси
- ✓ Хробаки (черв'яки)
- ✓ Трояни
- ✓ Скрипт-віруси
- ✓ Дропери
- ✓ Боти
- ✓ Руткіти
- ✓ Експлойти
- ✓ Бекдори
- ✓ Шпигунські програми
- ✓ Рекламні модулі або Adware

Отже, існує досить багато загроз. Основні з них:

- Отримання несанкціонованого доступу до секретних або конфіденційних даних
- Порушення або повне припинення роботи комп'ютерної інформаційної системи
- Отримання несанкціонованого доступу до керування роботою комп'ютерної інформаційної системи
- Знищення та спотворення даних
- Потрапляння в інформаційну систему шкідливого програмного забезпечення: вірусів, троянських програм, мережевих хробаків, клавіатурних шпигунів, рекламних систем
- Атаки хакерів
- BotNet - це комп'ютерна мережа, що складається з деякої кількості хостів, із запущеними ботами — автономним програмним забезпеченням.
- DdoS - атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні (англ. DoS attack, DDoS attack, (Distributed) Denial-of-service attack) — напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена.
- Крадіжка особистості

При використанні смартфонів основні небезпеки це визначення вашого місця розташування, читання смс та заволодіння банківською інформацією.

Та яка б не захищена була система всеодно завжди є простий шлях її взломати – через людину (соціальну інженерія).

Серед заходів безпеки, яких повинен дотримуватися кожен користувач, перше місце займає його особиста організованість і відповідальне ставлення до зберігання важливих даних.

Розрізняють три шляхи захисту даних:

1. Захист доступу до кмп'ютера
2. Захист даних на дисках
3. Захист даних в Інтернеті

Захист доступу до комп'ютера

Для запобігання несанкціонованому доступу до даних, що зберігаються на комп'ютері, використовують ***облікові записи***.

Пуск → Панель управления → Учетные записи пользователей → Управление другой учетной записью → Создание учетной записи

При щоденній роботі за комп'ютером використовуйте обліковий запис Windows без прав адініструтора. Це простий, безкоштовний і доступний кожному спосіб захисту від більшості шкідливих програм.

Захистити конфіденційну інформацію можна також шляхом архівування та встановлення пароля на архів. Такий спосіб захисту доцільно використовувати й під час листування.

Захист даних на дисках

Для зберігання даних та їх захисту від пошкодження варто розділити жорсткий диск на кілька логічних розділів.

На кожний диск, папку та файли локального комп'ютера, а також комп'ютера, підключеного до локальної мережі, встановлюються певні права доступу (повний, тільки читання, доступ за паролем).

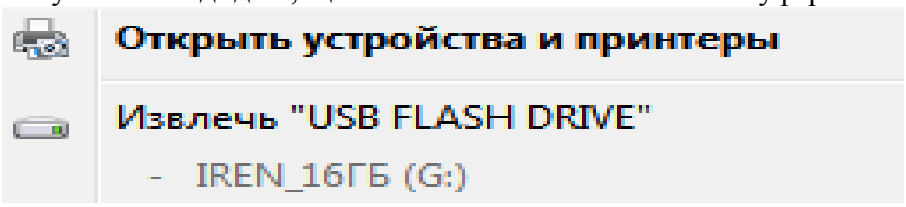
Встановіть антивірус одразу після встановлення операційної системи і постійно його оновлюйте.

Користуйтеся ліцензійними або з вільною ліцензією програмним забезпеченням, вчасно їх оновлюйте.

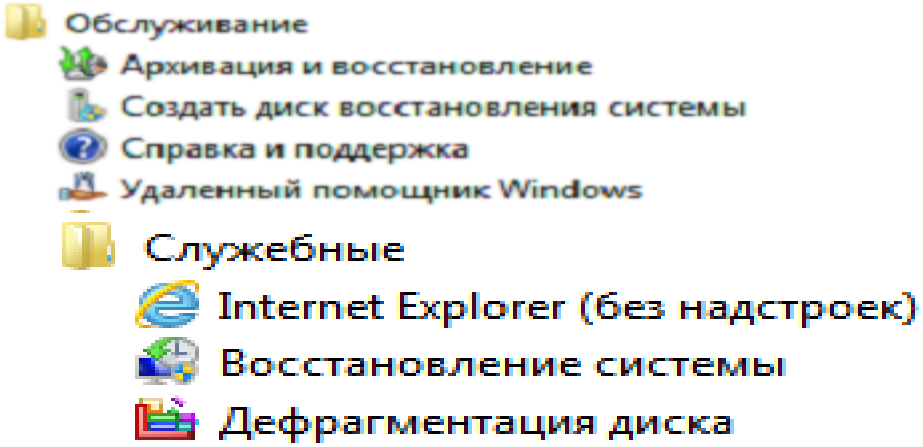
Захист даних на дисках

Наведемо деякі рекомендації щодо запобігання втраті даних.

- ✓ Не зберігайте важливі дані на системному диску, робочому столі, у папках власної Бібліотеки (Моя музика, Мої документи т ощо), бо системний диск найчастіше підпадає під вплив шкідливих програм.
- ✓ Періодично робіть резервне копіювання важливої інформації. Для бекапу використовуйте зовнішні накопичувачі (оптичні CD- і DVD-диски, окремі жорсткі диски тощо) та зовнішні хмарні диски.
- ✓ Після збереження даних на флеш-носії слід дотримуватися правил його безпечного вилучення. Тоді дані, що не встигли скопіюватися із буфера запису, не втратяться.



- ✓ Для резервного копіювання файлів і можливості відновлення операційної системи користуйтесь утилітами ОС Windows.



Безпечне видалення даних

Пам’ятайте, що у разі випадкового видалення інформації є можливість її відновити. Для видалення файлів і папок із можливістю їх відновлення використовують, як вам відомо, папку ***Кошик.*** Не копіюйте нову інформацію на жорсткий диск. Вимкніть комп’ютер, зверніться у сервісний центр.

Зберігайте робочі файли не на системному диску.

Не транспортуйте увімкнений ноутбук. Якщо увімкнений ноутбук впаде на підлогу, то із вірогідністю 70% Ви ВТРАТИТЕ ІНФОРМАЦІЮ.

А що робити, коли конфіденційну інформацію потрібно видалити без жодної можливості її відновлення, наприклад у разі передавання жорсткого диску в користування іншій особі? Очищення ***Кошика*** проблеми не розв’язує, бо в більшості випадків видалені файли можна відновити спеціальними програмами. У такому випадку навіть форматування диска не завжди гарантує остаточне видалення файлів. Для повного стирання даних доцільно використовувати спеціальні програми, наприклад, ***Eraser, CCleaner***, які на місце видалених даних записують нові.

Захист даних в Інтернеті

Для забезпечення інформаційної безпеки в Інтернеті недостатньо захистити дані на комп’ютері-клієнті або комп’ютері-сервері. Зловмисник може перехопити дані під час обміну ними через канали зв’язку. Захист даних забезпечується спеціальним криптографічним протоколом шифрування даних під час їхнього передавання.

Захищений сайт - це сайт, який використовує для обміну даними протоколи захищеного зв'язку. Щоб визначити, що сайти **захищені**, слід звернути увагу на їхню ***URL-адресу*** — вона починається з *https://.* Це — протокол зашифрованого підключення, що забезпечує більш ефективний захист даних. У деяких браузерах поруч із назвою протоколу відображається значок замка 

— це означає, що з'єднання захищене й більш безпечне.

Для захисту даних під час роботи в Інтернеті доцільно також використовувати підключення, захищене шифруванням. Наприклад, за замовчуванням *Google* шифрує з'єднання з *Gmail*, а також при виборі інших сервісів *Google*, наприклад *Google Диск*, активується ***протокол шифрування SSL***, який використовується до завершення сеансу роботи.

Брандмауери

Для запобігання інтернет-загрозам між комп'ютером і мережею встановлюють перешкоди — міжмережеві екрани (нім. *Brandmauer*, англ. *Firewall* — вогнестійка стіна»). Брандмауер - це технічний пристрій (маршрутизатор, роутер тощо) або програмний засіб для контролю даних, що надходять до комп'ютера через мережу. Брандмауери захищають комп'ютер від зловмисного проникнення або потрапляння шкідливих програм. Але не запобігають витоку конфіденційної інформації користувача та завантаже-нню вірусів. ОС Windows має вбудований персональний брандмауер. Щоб увімкнути і налаштувати його, слід виконати команди:

Пуск → Панель керування → брандмауер Windows

Засоби браузера, призначені для гарантування безпеки

Браузери Mozilla Firefox, Safari, Opera, Google Chrome мають багато вбудованих засобів захисту. Одним із найпопулярніших браузерів для комп'ютерів, телефонів і планшетів є Google Chrome, який:

- ✓ попереджає про відкриття сайта із загрозою фішингу або шкідливих програм;
- ✓ ізольовано відкриває веб-сторінки, що в разі загрози приводить до закриття лише однієї шкідливої веб-сторінки;
- ✓ дозволяє вимкнути збереження конфіденційних даних;
- ✓ надає можливість налаштувати показ спливних вікон.

Браузер Google Chrome

Для налаштування засобів безпеки в браузері необхідно відкрити меню браузера за допомогою інструмента  в правій частині вікна та обрати вказівку *Налаштування*. У вікні, що відкриється, слід перемістити в нижню частину сторінки та обрати посилання *Показати розширені налаштування.* Додаткові параметри захисту можна встановити, якщо в розділі *Конфіденційність* натиснути кнопку *Налаштування вмісту*

Для уникнення ризиків, пов'язаних з роботою в Інтернеті, варто дотримуватися таких порад:

Не розміщуйте в Інтернеті:

- ✓ домашню адресу, номер телефона (як домашнього так і мобільного);
- ✓ розпорядок дня (свій або рідних);
- ✓ повідомлення про можливі тривалі подорожі або виїзд на дачу;
- ✓ фото, що можуть скомпрометувати вас або ваших знайомих тощо;

Не надавайте незнайомим людям та не надсилайте через відкриті мережі персональні дані, дані про паролі доступу до поштових скриньок, екаунтів у соціальних мережах;

Нікому і ніколи не повідомляйте особисту фінансову інформацію.

Суворо конфіденційні дані:

- Термін дії картки
- CVV-2 код
- PIN-код

Для переказу коштів достатньо:

- Імені власника картки
- Номеру картки
- Уважно поводьтеся з паролями.

Для створення паролів використовуйте:

- Складне слово чи вислів
- Великі і маленькі літери
- цифри

Змінюйте паролі:

- Для нових акаунтів
- Періодично (раз на 3-6 міс.)
- У разі підозрілих ситуацій

Привяжіть номер мобільного телефону до важливих акаунтів (двохфакторна авторизація)

Не відкривайте вкладень до листів від незнайомих осіб;

Уважно ставтесь до посилань в повідомленях у соц. мережах та інших месенджерах;

Не надсилайте СМС-повідомлення для отримання будь-яких послуг в Інтернеті;

Використовуйте **окрему картку** для інтернет оплат;

Користуйтеся лише знайомими банкоматами, огляньте банкомат перед використанням;

Уважність – практично єдиний спосіб захисту від скімінгу.

Всі вищезгадані поради стосуються і мобільних пристроїв (смартфонів, планшетів).

- ✓ Встановлюйте мобільні додатки лише з офіційних магазинів.

- ✓ *Періодично перевіряйте ваші мобільні пристрої на предмет незнайомих додатків на головному екрані та в меню.*
- ✓ *При встановленні та оновленні додатків уважно стежте за тим, які* ***дозволи вони вимагають.***

Отож, визначимо основні правила безпечної роботи в Інтернеті:

- Використовуйте тільки ліцензійне програмне забезпечення. Установлюйте програми тільки з офіційних джерел. Перед установленням читайте відгуки інших користувачів, якщо вони доступні.
- Установлюйте та оновлюйте антивірусне програмне забезпечення як на стаціонарні, так і на мобільні комп'ютери. Бажано, щоб оновлення антивірусних баз здійснювалося регулярно та автоматично.
- Завжди встановлюйте оновлення операційної системи та іншого програмного забезпечення.
- Використовуйте надійні паролі. Не використовуйте на різних інтернет-ресурсах один і той самий пароль, змінюйте його регулярно.
- Приєднуйтеся тільки до перевірених Wi-Fi-мереж. Не відправляйте важливі дані (дані кредитних карток, онлайн-банкінгу тощо) через публічні та незахищені Wi-Fi-мережі.
- Установіть фільтр спливаючих вікон у браузері.
- Перевіряйте сертифікат безпеки сайтів у вигляді замка в адресному рядку браузер.
- Не відкривайте повідомлення електронної пошти від невідомих вам осіб і прикріплені до них файли, яких ви не очікуєте.
- Подумайте про можливі ризики для вас перед тим, як викласти щось у мережу Інтернет. Дуже легко розмістити дані в мережі Інтернет, але дуже складно їх видалити з неї.
- Створюйте резервні копії важливих для вас даних, зберігайте їх на носіях даних, відключених від мережі Інтернет**.**