Кібербезпека у сучасному світі

Захист особистих даних

Використання складних паролів

Паролі повинні містити великі та малі літери, цифри й спеціальні символи.

Рекомендується змінювати паролі кожні 2–3 місяці.

Конфіденційність інформації

Не передавайте свої паролі іншим людям.

Уникайте збереження паролів у відкритих документах.

Двофакторна аутентифікація

Використовуйте додаткові коди підтвердження.

Підключайте автентифікацію через мобільні додатки.

Безпечна робота в Інтернеті

Перевірка електронних листів

Звертайте увагу на адресу відправника.

Не відкривайте підозрілі вкладення.

Захист від фішингу

Не переходьте за сумнівними посиланнями.

Використовуйте браузери з вбудованим захистом.

Соціальні мережі

Обмежуйте доступ до особистої інформації.

Використовуйте налаштування приватності.

Технічні засоби захисту

Антивірусні програми

Регулярно оновлюйте бази даних антивірусу.

Виконуйте повне сканування комп’ютера.

Резервне копіювання

Створюйте копії важливих файлів.

Використовуйте хмарні сховища для зберігання даних.

Оновлення програмного забезпечення

Встановлюйте офіційні оновлення системи.

Не використовуйте піратські програми.

Кібербезпека — це сукупність практик, процесів і технологічних рішень, призначених для захисту комп'ютерів, серверів, мобільних пристроїв, мереж і даних від цифрових атак, пошкоджень чи несанкціонованого доступу.

Основні цілі (триада безпеки)

- **Конфіденційність:** доступ до інформації мають лише уповноважені особи.
- **Цілісність:** захист даних від випадкової або навмисної зміни чи підробки.
- **Доступність:** гарантія того, що системи та файли працюють і доступні тоді, коли вони потрібні.

Головні кіберзагрози

- **Фішинг та соціальна інженерія:** спроби обманом виманити паролі чи особисті дані через підроблені листи чи сайти.
- **Програми-вимагачі (Ransomware):** шкідливе ПЗ, що блокує або шифрує дані та вимагає викуп за їхнє повернення.
- **Шкідливе програмне забезпечення:** віруси, трояни та шпигунські програми.
- **DDoS-атаки:**