

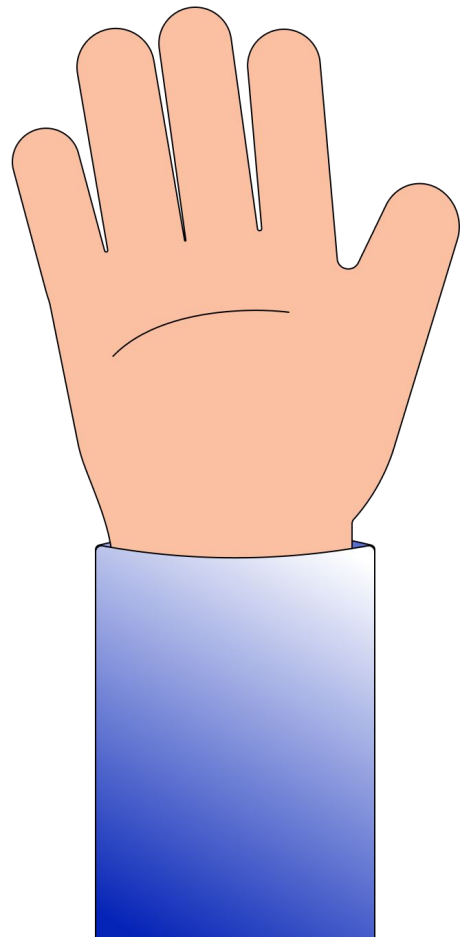
Практичні поради для забезпечення кібербезпеки



Привіт, майбутні кіберзахисники!

Команда GoIT підготувала для вас корисні поради, що допоможуть уникнути або пом'якшити можливі кіберзагрози та забезпечити кібербезпеку свого цифрового середовища.

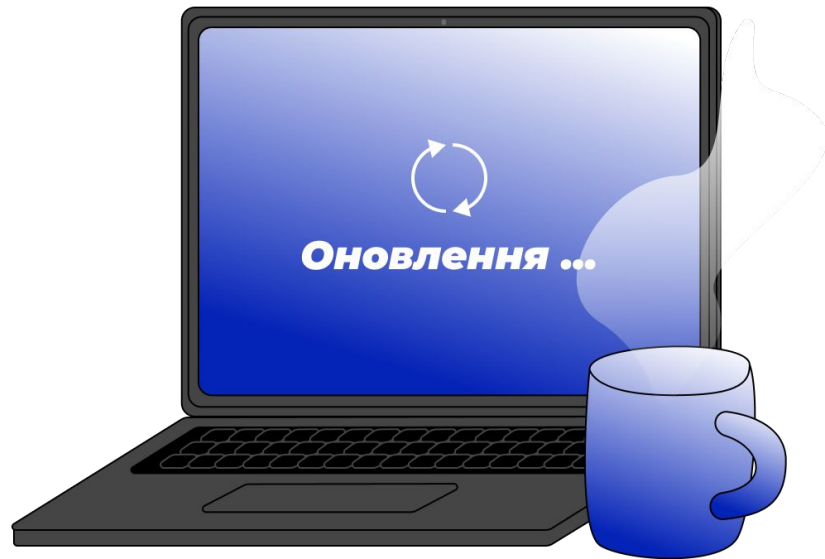
У цих правилах зібрані прості, але ефективні методи зменшення ризиків втрати даних або потенційних атак.



1. Оновлення програм та операційних систем

Завжди слід мати найновіші версії програм і операційних систем.

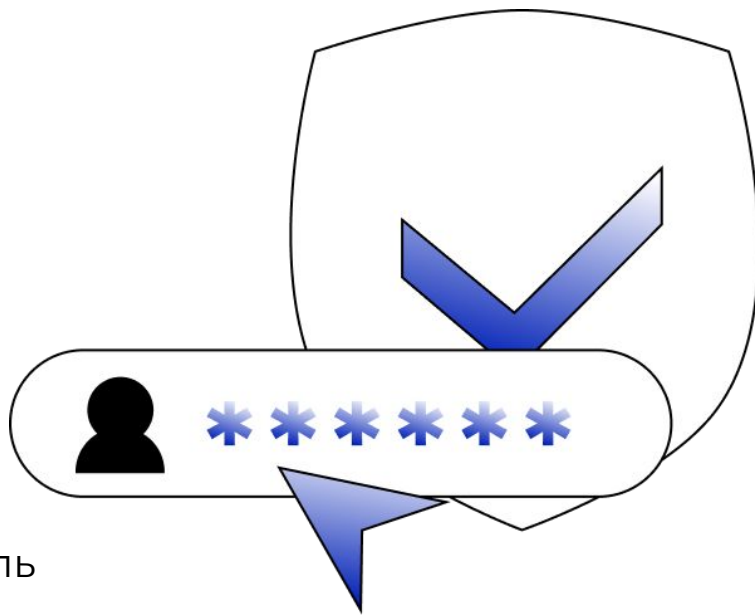
Регулярно оновлюйте всі програми та операційні системи, адже важливі оновлення часто містять покращення безпеки.



2. Створення складних паролів та їх регулярна зміна

Міцний пароль - це перша лінія захисту від кібератак.

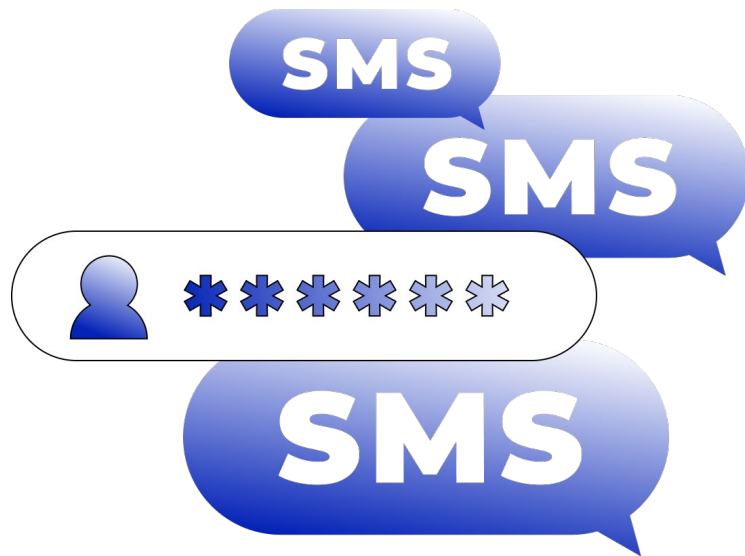
Рекомендуємо використовувати комбінацію букв, цифр і символів. А також регулярно змінювати паролі для різних облікових записів та не використовувати один і той самий пароль для всіх облікових записів.



3. Використання двофакторної автентифікації (2FA)

Увімкніть двоетапну автентифікацію для своїх онлайн-акаунтів, де це можливо.

Це додасть додатковий шар захисту, оскільки вона, окрім пароля, вимагає підтвердження ідентичності через додатковий пристрій або метод.



4. Уважність під час відкриття посилань та вкладень

Необхідно бути обережними при відкритті посилань в електронних листах або завантаженні файлів з невідомих джерел, оскільки це може бути джерелом шкідливого програмного забезпечення.

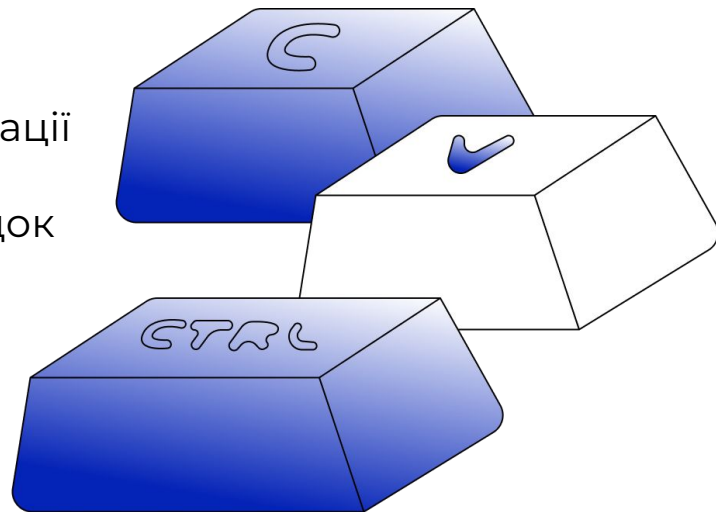
Уникайте натискання на посилання або завантаження вкладень від ненадійних джерел.



5. Резервне копіювання даних

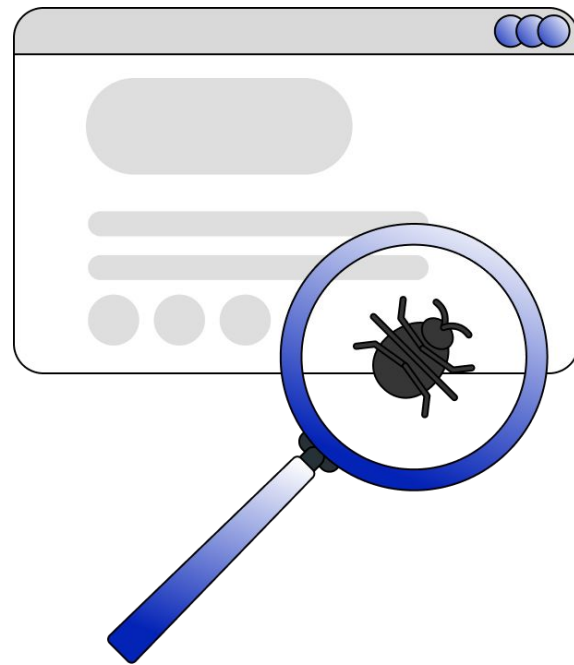
Створення резервних копій важливої інформації допомагає у відновленні даних у випадку їх втрати або пошкодження внаслідок кібератаки або помилки.

Радимо регулярно робити резервні копії важливих даних. Таким чином, у разі атаки або втрати ви зможете відновити необхідну інформацію.



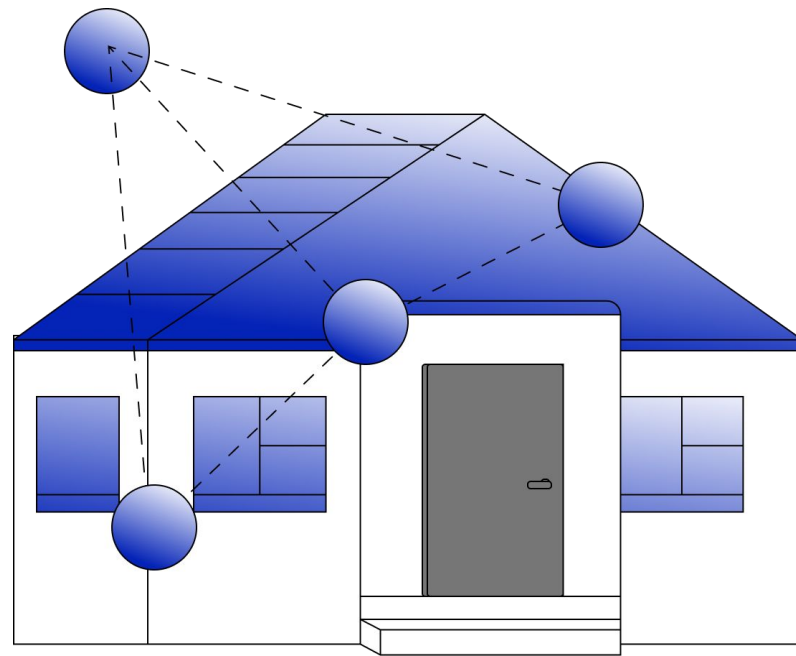
6. Антивірусне програмне забезпечення

Встановлюйте та оновлюйте антивірусне програмне забезпечення для захисту від вірусів і шкідливих програм.



7. Захист домашньої мережевої системи

Захищайте свою домашню мережу за допомогою сильного пароля для Wi-Fi та обмежте доступ до підключених пристроїв.



Ці правила допоможуть вам:

- уникнути атак, вірусів та інших кіберзагроз, що можуть шкодити вашій інформації та пристроям
- захистити конфіденційні дані та особисту інформацію
- уникнути крадіжки грошей, викупів даних та інших фінансових атак
- уникнути ситуацій, які можуть пошкодити вашу репутацію, як-от втрати даних або кібератаки
- зберегти доступ до ваших онлайн-активностей

**Успіхів у ваших
починаннях!**

