Дрогобицький державний педагогічний університет
імені Івана Франка

ДМИТРО КАРПИН, РОМАН ЛЕШКО,АННА КАРПИН,
ХРИСТИНА ВОЙТОВИЧ, НАТАЛІЯ ГОЙВАНОВИЧ

КІБЕРБЕЗПЕКА:
збірник практичних завдань, кейсів і ситуаційних вправ

Навчально-методичний посібник

Дрогобич, 2026

УДК: 004.056:37.091.3
К (КБК): 32.973.26-018.2я73

Рекомендовано до друку вченою радою
Дрогобицького державного педагогічного університету
імені Івана Франка

Протокол вченої ради №3 від 26.02.26.
Рецензенти:
І. Нищак – доктор педагогічних наук, професор, професор кафедри технологічної та професійної освіти Дрогобицького державного педагогічного університету імені Івана.
А. Шілінг – кандидат технічних наук, доцент, доцент кафедри соціальних комунікацій та інформаційної діяльності Національного університету “Львівська політехніка”.
Відповідальний за випуск: Карпин Д. С. – кандидат фізико-математичних наук, доцент кафедри фізики та інформаційних систем Дрогобицького державного педагогічного університету імені Івана Франка.
Карпин Дмитро, Лешко Роман, Карпин Анна, Лешко Ольга, Войтович Христина, Гойванович Наталія. “Кібербезпека: практикум”: Навчальний посібник – Дрогобич: ДДПУ ім. І. Франка, 2026. – 60 с.
Практикум є важливим інструментом, розробленим для переходу від теоретичного осмислення кіберзагроз до формування прикладних, практично орієнтованих навичок управління ризиками в будь-якій організації, чи то освітня установа, чи громадська організація. Його мета — забезпечити систематичну здатність ідентифікувати, класифікувати та захищати інформаційні активи від інцидентів. Через виконання практичних завдань та аналіз кейсів, посібник акцентує увагу на критичній ролі людського фактора. Успішне проходження практикуму гарантує формування стійких цифрових звичок, необхідних для самостійної оцінки рівня захищеності та підвищення професійної конкурентоспроможності фахівців на ринку праці. Бібліографія 22 назви.

ЗМІСТ

ВСТУП

В умовах стрімкої діджиталізації всіх сфер суспільної та професійної діяльності, забезпечення кібербезпеки організацій стає однією з ключових вимог до сучасного фахівця. Цей практикум розроблений для того, щоб перевести теоретичні знання про цифрові загрози у площину прикладних навичок управління ризиками. Актуальність набуття таких компетенцій є беззаперечною, оскільки, як показує статистика, переважна більшість (понад 90%) інцидентів пов'язана не зі складними зовнішніми кібератаками, а з внутрішніми факторами: людською помилкою, недостатньою обізнаністю персоналу та нехтуванням базовими правилами захисту. Таким чином, ефективний кіберзахист починається з відповідального підходу кожного суб'єкта.

Мета практикуму полягає у формуванні систематичної здатності ідентифікувати, класифікувати та захищати інформаційні активи організації, незалежно від її типу чи розміру. Навчальний процес структурований так, щоб користувачі, через виконання практичних завдань та аналіз реальних кейсів, змогли усвідомити критичну роль людського фактора як найбільш вразливої ланки. Особлива увага приділяється практичному аналізу типових загроз, таких як фішинг, соціальна інженерія та несанкціонований доступ, а також засвоєнню механізмів колективної відповідальності за безпеку, яка має бути чітко розподілена між усіма ролями в установі.

Успішне проходження практикуму забезпечує формування стійких цифрових звичок, необхідних для роботи в будь-якому сучасному колективі. Набуті практичні знання дозволяють фахівцям не лише розуміти, але й ефективно імплементувати сім принципів здорового цифрового середовища — від застосування багатофакторної автентифікації та створення надійних паролів до регулярного резервного копіювання та управління правами доступу. Результатом роботи є підготовка висококваліфікованих кадрів, здатних самостійно оцінювати базовий рівень

захищеності організації за допомогою контрольних чек-листів та оперативно реагувати на потенційні цифрові інциденти, що значно підвищує їхню професійну конкурентоспроможність.

Практикум укладений відповідно до програми дисципліни "Кібербезпека" спеціальності F3 Комп'ютерні науки і забезпечує такі компетентності як:

Загальні компетентності:
ЗК 2. Здатність застосовувати знання у практичних ситуаціях.
ЗК 3. Знання та розуміння предметної області та розуміння професійної діяльності.
ЗК 6. Здатність вчитися й оволодівати сучасними знаннями.
ЗК 9. Здатність працювати в команді.
ЗК 11. Здатність приймати обґрунтовані рішення.
ЗК 13. Здатність діяти на основі етичних міркувань.

Фахові компетентності:
СК 12. Здатність забезпечити організацію обчислювальних процесів в інформаційних системах різного призначення з урахуванням архітектури, конфігурування, показників результативності функціонування операційних систем і системного програмного забезпечення.

СК 13. Здатність до розробки мережевого програмного забезпечення, що функціонує на основі різних топологій структурованих кабельних систем, використовує комп'ютерні системи і мережі передачі даних та аналізує якість роботи комп'ютерних мереж.

СК 14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

Програмні результати навчання:
ПРН 13. Володіти мовами системного програмування

та методами розробки програм, що взаємодіють з компонентами комп’ютерних систем, знати мережні технології, архітектури комп’ютерних мереж, мати практичні навички технології адміністрування комп’ютерних мереж та їх програмного забезпечення.

ПРН 15. Розуміти концепцію інформаційної безпеки, принципи безпечного проєктування програмного забезпечення, забезпечувати безпеку комп’ютерних мереж в умовах неповноти та невизначеності вихідних даних.

1. ДЕСЯТЬ ПРАВИЛ БЕЗПЕЧНОГО ВИКОРИСТАННЯ ІНТЕРНЕТУ

1. Використовуйте надійні паролі.
Ваш пароль має бути довгим (не менше 12 символів) і унікальним.
Використовуйте комбінації великих і малих літер, цифр та символів.
Керуйте паролями через спеціальні програми, наприклад, менеджери паролів.

2. Не натискайте на підозрілі посилання.
Завжди перевіряйте джерело перед переходом за лінком.
Якщо отримали посилання від незнайомця або навіть друга, але воно виглядає підозріло — запитайте у відправника.
Пам'ятайте: офіційні організації ніколи не просять ввести ваші паролі чи дані через електронні листи.

3. Регулярно оновлюйте пристрої.
Сучасні програми оновлюються не лише для нових функцій, а й для закриття вразливостей у системі.
Активуйте автоматичне оновлення для операційної системи, браузера та антивірусу.

4. Установіть надійний антивірус.
Антивірус допомагає захистити ваш пристрій від вірусів, троянів, шпигунського ПЗ.
Регулярно скануйте систему, щоб виявляти потенційні загрози.
Використовуйте програми з функцією захисту в реальному часі.

5. Обережно користуйтеся публічними Wi-Fi мережами.
У кафе, готелях або аеропортах Wi-Fi не завжди захищений.
Якщо потрібно користуватися такими мережами, використовуйте VPN, щоб шифрувати ваші дані.

6. Перевірте налаштування конфіденційності у соцмережах.
Переконайтеся, що ваші профілі не доступні для сторонніх.
Видаліть старі пости, які можуть вас скомпрометувати.
Обмежте коло осіб, які бачать ваші фото та інформацію.

7. Подумайте перед публікацією.
Пам'ятайте, що те, що потрапило в Інтернет, може залишитися там назавжди.
Не публікуйте дані, які можуть бути використані проти вас.

8. Уникайте сумнівних файлів.
Завантажуйте програми лише з офіційних магазинів (наприклад, Google Play або App Store).
Перевіряйте файли на віруси перед відкриттям.

9. Активуйте двофакторну автентифікацію.
Це другий рівень захисту ваших акаунтів.
Наприклад, навіть якщо ваш пароль буде зламаний, зловмисник не зможе увійти без додаткового коду, надісланого на ваш телефон.

10. Бережіть свої особисті дані.
Ніколи не передавайте паролі, номер телефону чи банківські дані стороннім особам.
Залишайте мінімум інформації на сумнівних вебсайтах.

Порада:
Налаштуйте свій пристрій так, щоб він не підключався автоматично до відкритих Wi-Fi мереж.
Підказка:
Не поспішайте виконувати незвичні дії в Інтернеті. Спершу подумайте: це безпечно?

Правила створення надійного пароля

1. Довжина має значення.
Пароль повинен бути не менше 12 символів, але краще — 16 і більше.

2. Комбінуйте символи.
Використовуйте:
Великі та малі літери.
Цифри.
Спеціальні символи, як-от @, #, $, %.
Наприклад: Tru$tMe2024!

3. Не використовуйте особисту інформацію.
Дата народження, ім'я чи телефонний номер — це погані варіанти. Зловмисники легко знайдуть ці дані.

4. Уникайте простих послідовностей.
Паролі на кшталт 12345678 або qwerty можна зламати за кілька секунд.

5. Кожен обліковий запис — свій пароль.
Не використовуйте один пароль для всіх сайтів і сервісів. Якщо його зламають, зловмисник отримає доступ до всього.

Підказка!
Спробуйте створити пароль на основі улюбленої фрази. Наприклад:
Фраза: "Мій кіт любить рибу".
Пароль: MyK1tLyb1tRybu!

6. Використовуйте менеджери паролів.
Це програми, які створюють і зберігають складні паролі замість вас.
Рекомендовані програми:
LastPass.
1Password.
Bitwarden.

7. Двофакторна автентифікація — ваш друг.
Увімкніть підтвердження входу за допомогою SMS або додатка (наприклад, Google Authenticator).

8. Перевіряйте паролі на злом.
Сайти типу Have I Been Pwned допоможуть дізнатися, чи не став ваш пароль відомим після витоків даних.

9. Оновлюйте паролі регулярно.
Змінюйте ключі доступу хоча б раз на 6 місяців. Особливо, якщо підозрюєте, що ваш пароль могли зламати.

10. Не зберігайте паролі на папері чи в браузері.
Замість цього використовуйте надійні інструменти для зберігання даних.

Підсумок:
Ваш пароль — це ваш ключ до цифрового світу. Подбайте про його безпеку вже сьогодні!

3. 10 РЕКОМЕНДАЦІЙ ІЗ БЕЗПЕЧНОГО ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ

Соціальні мережі — це простір для спілкування, роботи та розваг. Але вони можуть стати джерелом загроз: виток даних, шахрайство чи навіть кібербулінг.

1. Налаштуйте конфіденційність профілю.
Перевірте, хто може бачити ваші публікації.
Обмежте видимість особистої інформації лише для друзів.
Вимкніть можливість перегляду профілю сторонніми.

2. Використовуйте складні паролі.
Не використовуйте один пароль для різних акаунтів.
Додайте двофакторну автентифікацію для посилення захисту.

3. Будьте обережні зі сторонніми запитами дружби.
Не приймайте запити від незнайомців, навіть якщо вони здаються «спільними знайомими».

4. Не публікуйте зайву інформацію.
Уникайте публікації контактів, адрес чи інформації про свої плани.
Пам'ятайте: злочинці можуть використовувати ваші публікації для підготовки атак.

5. Перевіряйте посилання перед натисканням.
Шахраї часто надсилають фішингові посилання через повідомлення.
Перевіряйте URL-адресу перед тим, як переходити за посиланням.

Підказка:
Ви можете налаштувати отримання сповіщень про нові входи у ваш акаунт. Це допоможе миттєво виявляти підозрілу активність.

6. Будьте обережні з фото та відео.
Не публікуйте знімки з конфіденційними даними, наприклад, квитки чи документи.
Уникайте фото, які можуть використати для шантажу.

7. Обережно встановлюйте додатки.
Не надавайте додаткам доступ до всіх даних вашого профілю.
Вимкніть доступ до непотрібної інформації у вже встановлених додатках.

8. Захистіть свої повідомлення.
Використовуйте функцію шифрування, якщо вона доступна у вашій соціальній мережі.
Не пересилайте конфіденційну інформацію через месенджери.

9. Слідкуйте за активністю на вашій сторінці.
Регулярно перевіряйте, чи не додано до вашого профілю підозрілі дописи чи посилання.
Переглядайте історію входів до акаунта.

10. Звертайте увагу на спам і шахрайство.
Не довіряйте повідомленням про «легкий заробіток» або «виграш у лотереї».
Якщо сумніваєтесь у достовірності повідомлення, не реагуйте.

Підсумок:
Дотримуючись цих простих правил, ви зможете спокійно користуватися соціальними мережами без ризику втрати конфіденційної інформації чи шахрайства.

Соціальна інженерія — це метод маніпуляції, який використовують зловмисники для отримання доступу до конфіденційної інформації. Вони експлуатують людську довіру та емоції, а не технічні вразливості.

1. Уникайте поспішних рішень.
Зловмисники часто створюють відчуття терміновості ("Ваш акаунт буде заблоковано через 24 години!").
Завжди аналізуйте ситуацію спокійно перед тим, як діяти.

2. Перевіряйте справжність запитів.
Якщо хтось просить ваші дані або доступ до акаунтів, перевірте, чи цей запит є офіційним.
Зателефонуйте в організацію або перевірте інформацію на офіційному сайті.

3. Не діліться конфіденційною інформацією.
Не розголошуйте паролі, PIN-коди, номер паспорта або банківської картки.
Справжні компанії ніколи не запитують цю інформацію через email, телефон чи месенджери.

4. Уникайте завантаження підозрілих файлів.
Зловмисники можуть надсилати файли, які виглядають офіційно, але містять віруси.
Перевіряйте відправника та завантажуйте файли лише з офіційних джерел.

5. Розпізнавайте маніпуляції довірою.
Шахраї можуть видавати себе за ваших колег, друзів або представників організацій.
Перевіряйте особу відправника, навіть якщо повідомлення здається легітимним.

6. Пильнуйте за фішингом.
Фішинг — це тип соціальної інженерії, коли вас обманом спонукають ввести дані на підробленому сайті.
Завжди перевіряйте URL-адресу сайту перед входом.

7. Уникайте спілкування з незнайомцями онлайн.
Не відповідайте на запити від невідомих користувачів у соцмережах чи месенджерах.
Використовуйте функції блокування, якщо хтось здається підозрілим.

8. Відмовляйтесь від підозрілих дзвінків.
Зловмисники можуть телефонувати, представляючись представниками банку чи служби підтримки.
Завжди перевіряйте номер та ініціюйте дзвінок самостійно на офіційний контакт.

9. Навчайтесь розпізнавати техніки соціальної інженерії.
Найпоширеніші методи:
Примус: "Вам потрібно діяти негайно!"
Лестощі: "Тільки ви можете нам допомогти".
Використання авторитету: "Я представляю банк/поліцію".

10. Підтримуйте здоровий рівень недовіри.
Навіть якщо повідомлення чи дзвінок здаються справжніми, перевірте всі деталі.
Ніколи не дійте під тиском чи з почуття провини.

Часті запитання (FAQ)
Питання: Як навчитися розпізнавати шахрайство?
Відповідь: Регулярно читайте матеріали про кібербезпеку та діліться досвідом із близькими.

5. ШВИДКИЙ ГІД ІЗ ВИКОРИСТАННЯ МЕНЕДЖЕРІВ ПАРОЛІВ

Менеджери паролів дозволяють зберігати складні та унікальні паролі для кожного вашого акаунта. Вони допомагають уникнути повторного використання паролів і захищають вас від хакерських атак.

1. Оберіть надійний менеджер паролів.
Виберіть відомі сервіси, такі як:
LastPass, 1Password, Bitwarden, Dashlane.
Переконайтеся, що менеджер використовує наскрізне шифрування для захисту даних.

2. Встановіть додаток на всі пристрої.
Менеджери паролів доступні як:
Мобільні додатки.
Розширення для браузера.
Десктопні програми.

3. Створіть надійний майстер-пароль.
Це єдиний пароль, який ви повинні пам'ятати.
Він має бути складним, довгим і унікальним, наприклад: М@йМайстерПар0ль2024!.

4. Додайте всі свої акаунти.
Внесіть облікові записи в менеджер паролів, включаючи логіни, паролі та додаткові дані (наприклад, резервні коди для 2FA).
Сервіс автоматично заповнюватиме ці дані при вході.

5. Використовуйте генератор паролів.
Менеджери паролів можуть створювати надійні паролі для ваших акаунтів.
Встановіть довжину пароля щонайменше 16 символів.

6. Налаштуйте двофакторну автентифікацію (2FA).
Для додаткового захисту активуйте 2FA для свого менеджера паролів.
Використовуйте автентифікаційний додаток, наприклад Google Authenticator або Authy.

7. Зберігайте резервну копію.
Збережіть резервний файл із паролями в зашифрованому вигляді.
Не зберігайте резервну копію на пристроях, підключених до Інтернету.

8. Уникайте автозбереження паролів у браузерах.
Браузери менш безпечні, ніж менеджери паролів.
Використовуйте менеджер для автозаповнення полів входу.

9. Перевіряйте наявність зламаних акаунтів.
Деякі менеджери паролів перевіряють, чи ваші дані потрапили у витоки.
Використовуйте функцію безпеки для заміни вразливих паролів.

10. Дотримуйтеся обережності з майстер-паролем.
Ніколи не записуйте майстер-пароль у відкритому доступі.
Не повідомляйте його стороннім особам.

Часті запитання (FAQ)
Питання: Чи безпечно використовувати безкоштовні менеджери паролів?
Відповідь: Так, якщо це надійні сервіси (наприклад, Bitwarden). Перевіряйте політику конфіденційності перед використанням.

Питання: Чи можуть хакери зламати мій менеджер паролів?
Відповідь: Зламати захищений менеджер практично неможливо, якщо ви використовуєте надійний майстер-пароль і 2FA.

6. ЯК НАЛАШТУВАТИ БРАНДМАУЕР ДЛЯ ЗАХИСТУ ТРАФІКУ?

Брандмауер — це перший бар'єр між вашим пристроєм і потенційними загрозами з Інтернету. Він блокує небезпечний трафік, захищає від хакерів і запобігає несанкціонованому доступу до вашої мережі.

Кроки для налаштування брандмауера на вашому пристрої
1. Перевірте, чи активований брандмауер.
На Windows: Відкрийте Панель управління.
Перейдіть до розділу Брандмауер Windows.
Увімкніть, якщо він вимкнений.
На macOS: Відкрийте Системні налаштування → Безпека та конфіденційність.
Перейдіть до вкладки Брандмауер.
Натисніть Увімкнути брандмауер.

2. Налаштуйте правила доступу для програм.
Перевірте, які програми мають доступ до мережі.
Дозволяйте тільки ті, яким ви довіряєте.
Наприклад, блокуйте невідомі або підозрілі програми.

3. Додайте виключення для довірених сервісів.
Якщо ви використовуєте спеціальне програмне забезпечення (VPN або корпоративні додатки), додайте їх до виключень, щоб уникнути блокувань.

Порада!
Регулярно перевіряйте налаштування брандмауера, особливо після встановлення нових програм.

Додаткові функції брандмауера
4. Увімкніть сповіщення про підозрілу активність.
Більшість брандмауерів можуть надсилати попередження, якщо програма намагається підключитися до мережі без вашого дозволу.

5. Налаштуйте фільтрацію вихідного трафіку.
Заблокуйте передачу даних від невідомих або шкідливих програм.
Це особливо важливо для запобігання витоку даних.

6. Увімкніть брандмауер на роутері.
Веб-інтерфейс роутера дозволяє керувати брандмауером для всієї мережі.
Зазвичай налаштування доступні у розділі Security (Безпека) або Firewall Settings.

Часті запитання (FAQ)
Питання: Чи потрібен брандмауер, якщо я маю антивірус?
Відповідь: Так, антивірус захищає ваш пристрій від вірусів, а брандмауер — від загроз у мережі. Вони працюють у парі.

Питання: Як дізнатися, чи працює брандмауер?
Відповідь: Ви можете перевірити це в налаштуваннях операційної системи. Якщо брандмауер увімкнений, зазвичай відображається статус Активний.

Питання: Чи потрібно оновлювати брандмауер?
Відповідь: Так, особливо якщо це стороння програма. Оновлення забезпечують актуальний захист від нових загроз.

Підсумок:
Брандмауер — це основа вашої цифрової безпеки. Налаштувавши його правильно, ви захистите свій пристрій і мережу від багатьох кіберзагроз.

7. АЛГОРИТМ НАЛАШТУВАННЯ WPA3 ДЛЯ WI-FI

WPA3 — це найсучасніший протокол безпеки для Wi-Fi. Він забезпечує захист вашої мережі від зломів і покращує конфіденційність даних. Налаштування WPA3 допоможе уникнути ризиків, пов'язаних із використанням застарілих протоколів, таких як WPA2 чи WEP.

Кроки для налаштування WPA3 на роутері
1. Увійдіть до налаштувань роутера.
Введіть IP-адресу роутера (зазвичай це 192.168.0.1 або 192.168.1.1) у браузері.
Увійдіть за допомогою облікових даних адміністратора (зазвичай вказані на нижній частині роутера).

2. Знайдіть налаштування безпеки Wi-Fi.
У меню налаштувань знайдіть розділ Wireless Settings або Wi-Fi Security.
Виберіть частотний діапазон (2.4 ГГц або 5 ГГц), якщо це потрібно.

3. Установіть тип захисту WPA3.
У полі Security Mode виберіть WPA3-Personal.
Якщо є можливість, увімкніть WPA3/WPA2 Mixed Mode для сумісності зі старими пристроями.

4. Задайте надійний пароль.
Створіть пароль із 12–16 символів, використовуючи великі та малі літери, цифри й спеціальні символи.
Приклад: Str0ngP@ssWiFi!2024.

Порада!
Якщо ваш роутер не підтримує WPA3, перевірте оновлення прошивки. Інструкції щодо оновлення зазвичай доступні на сайті виробника.

Додаткові налаштування для безпеки
5. Оновіть прошивку роутера.
У розділі Firmware Update перевірте, чи доступні оновлення.
Завантажте й установіть останню версію програмного забезпечення.

6. Вимкніть WPS (Wi-Fi Protected Setup).
Ця функція може бути вразливою до атак.
У налаштуваннях безпеки знайдіть параметр WPS і вимкніть його.

7. Вимкніть трансляцію SSID (якщо не потрібна).
Це допоможе приховати назву вашої мережі від сторонніх.
Пам'ятайте: це додатковий захід безпеки, але не заміна WPA3.

8. Увімкніть функцію блокування MAC-адрес.
Додайте до списку дозволених лише ті пристрої, які ви використовуєте.
Це створює додатковий бар'єр для несанкціонованого доступу.

Часті запитання (FAQ)
Питання: Як дізнатися, чи підтримує мій роутер WPA3?
Відповідь: Зазвичай ця інформація вказана в технічних характеристиках роутера або на сайті виробника.

Питання: Чи достатньо WPA3 для безпеки мережі?
Відповідь: WPA3 — це важливий крок, але додаткові заходи, як-от оновлення прошивки та надійні паролі, також необхідні.

Підсумок:
WPA3 забезпечує найкращий захист вашої мережі. Налаштуйте його правильно, і ваші дані будуть у безпеці навіть у сучасному кіберпросторі.

8. ЯК ЗАХИСТИТИ ДОМАШНІЙ РОУТЕР?

Ваш домашній роутер — це основа безпеки всієї вашої мережі. Якщо зловмисники отримають до нього доступ, вони можуть перехоплювати ваші дані або навіть використовувати вашу мережу для атак.

1. Змініть стандартний пароль адміністратора.
Після першого налаштування роутера обов'язково змініть пароль адміністратора.
Пароль має бути довгим і складним (наприклад, Adm1n@H0me2024).

2. Оновіть прошивку роутера.
Регулярно перевіряйте оновлення на сайті виробника вашого роутера.
Оновлення виправляють вразливості та додають нові функції безпеки.

3. Увімкніть WPA3 для Wi-Fi.
Перейдіть у налаштування безпеки Wi-Fi та виберіть протокол WPA3.
Якщо пристрій не підтримує WPA3, використовуйте WPA2, але оберіть довгий пароль.

4. Змініть ім'я мережі (SSID).
Уникайте стандартних назв, як-от TP-Link123 або HomeWiFi.
Створіть унікальне ім'я, яке не розкриває вашу особисту інформацію.

5. Вимкніть WPS (Wi-Fi Protected Setup).
Ця функція може бути вразливою до атак методом підбору PIN-коду.
У налаштуваннях роутера знайдіть WPS і вимкніть її.

Додаткові заходи для захисту
6. Вимкніть віддалений доступ до роутера.
Якщо ця функція увімкнена, її можуть використати зловмисники.
У налаштуваннях знайдіть розділ Remote Access або Remote Management і вимкніть його.

7. Увімкніть брандмауер роутера.
Більшість сучасних роутерів мають вбудований брандмауер.
Переконайтеся, що ця функція активна.

8. Використовуйте списки доступу за MAC-адресами.
Додайте до списку дозволених лише пристрої, яким ви довіряєте.
Це створить додатковий бар'єр для сторонніх.

9. Приховайте SSID.
Якщо ви не очікуєте, що хтось новий підключатиметься до вашої мережі, вимкніть трансляцію назви Wi-Fi.

10. Відслідковуйте активність мережі.
У налаштуваннях роутера переглядайте список підключених пристроїв.
Якщо ви помітили невідомі пристрої, змініть пароль і відключіть їх.

Часті запитання (FAQ)

Питання: Як часто потрібно оновлювати прошивку?
Відповідь: Рекомендується перевіряти оновлення щонайменше раз на три місяці.

Питання: Чи впливають ці заходи на швидкість Інтернету?
Відповідь: Ні, ці налаштування лише підвищують безпеку, не знижуючи продуктивність.

9. РЕКОМЕНДАЦІЇ З ВИКОРИСТАННЯ ГРОМАДСЬКИХ WI-FI

Безкоштовний Wi-Fi у кафе, аеропортах чи готелях здається зручним. Але ці мережі часто незахищені, і зловмисники можуть використовувати їх для перехоплення ваших даних.

1. Уникайте важливих дій у публічних мережах.
Не вводьте паролі, банківські дані чи іншу конфіденційну інформацію.
Відкладіть онлайн-покупки чи банківські операції на потім.

2. Використовуйте VPN.
VPN (Virtual Private Network) шифрує ваш трафік, захищаючи його від перехоплення.
Встановіть надійний VPN-додаток, як-от NordVPN, ExpressVPN чи ProtonVPN.

3. Перевіряйте назву мережі.
Уточнюйте у персоналу правильну назву мережі.
Уникайте підключення до мереж із назвами на кшталт «Free Wi-Fi» або «Open Network».

4. Вимкніть автоматичне підключення до Wi-Fi.
Ваш пристрій може автоматично підключатися до незахищених мереж.
У налаштуваннях вимкніть цю опцію для кращого контролю.

5. Вимкніть спільний доступ до даних.
Перевірте налаштування мережі на вашому пристрої та вимкніть функції, як-от File Sharing або Network Discovery.

Підказка!
Завжди використовуйте мобільний Інтернет, якщо у вас є така можливість.
Це набагато безпечніше.

6. Використовуйте HTTPS.
Перевіряйте, чи вебсайт використовує HTTPS (замок у адресному рядку).
Для додаткового захисту встановіть розширення браузера, як-от HTTPS Everywhere.

7. Не залишайте пристрій без нагляду.
Не залишайте ноутбук чи телефон без нагляду у публічних місцях.
Увімкніть блокування екрана паролем або біометрією.

8. Перевіряйте підключені пристрої.
У налаштуваннях мережі вашого пристрою перевірте, чи немає підозрілих підключень.

9. Вимикайте Wi-Fi після використання.
Завершивши роботу в громадській мережі, вимкніть Wi-Fi на пристрої.
Це запобігатиме автоматичному підключенню до інших незахищених мереж.

10. Переконайтеся у безпеці через налаштування.
Використовуйте оновлене програмне забезпечення на пристроях.
Переконайтеся, що ваш брандмауер і антивірус активні.

Часті запитання (FAQ)
Питання: Чи безпечно вводити паролі у громадських мережах?
Відповідь: Ні, зловмисники можуть перехопити ваші дані. Використовуйте VPN.

Питання: Як дізнатися, чи мережа захищена?
Відповідь: Захищені мережі запитують пароль і використовують шифрування WPA2 або WPA3.

10. РЕКОМЕНДАЦІЇ З БЕЗПЕЧНОГО ВИКОРИСТАННЯ BLUETOOTH

Bluetooth зручний для передачі даних і підключення пристроїв, але зловмисники можуть використовувати його для перехоплення інформації, чи отримання доступу до ваших пристроїв.

1. Увімкніть Bluetooth лише за потреби.
Тримайте Bluetooth вимкненим, якщо ви його не використовуєте.
Постійно ввімкнений Bluetooth збільшує ризик атак.

2. Використовуйте видимість лише для довірених пристроїв.
У налаштуваннях встановіть видимість для «відомих пристроїв» або вимкніть видимість повністю.
Не дозволяйте вашому пристрою бути видимим для всіх.

3. Не приймайте запити з невідомих пристроїв.
Якщо ви отримали запит на підключення від незнайомого пристрою, відхиліть його.
Зловмисники можуть використовувати підключення для викрадення ваших даних.

4. Використовуйте захищені паролем з'єднання.
Уникайте паролів за замовчуванням на пристроях Bluetooth.
Створіть свій власний, складний пароль для з'єднань.

5. Оновлюйте прошивку пристроїв.
Сучасні оновлення закривають вразливості, які можуть використовувати зловмисники.
Регулярно перевіряйте, чи доступні оновлення для ваших пристроїв.

Порада!
Користуйтеся функцією автоматичного вимкнення Bluetooth, якщо ваш пристрій підтримує її.

6. Уникайте використання Bluetooth у громадських місцях.
У людних місцях, таких як кафе чи аеропорти, Bluetooth-з'єднання може стати ціллю для атак.
Використовуйте дротові пристрої або функції Wi-Fi для передачі даних.

7. Стирайте старі підключення.
Видаляйте пристрої, якими ви більше не користуєтесь.
Це знижує ризик несанкціонованого доступу до вашого пристрою.

8. Використовуйте функцію шифрування.
У налаштуваннях Bluetooth переконайтеся, що шифрування увімкнене.
Це захищає дані, які передаються через з'єднання.

9. Уникайте передачі конфіденційної інформації.
Не передавайте паролі, фінансові дані чи особисту інформацію через Bluetooth.
Використовуйте захищені канали, як-от шифровані месенджери або VPN.

10. Перевіряйте журнали підключень.
Деякі пристрої дозволяють переглядати історію підключень.
Якщо ви помітили підозрілі з'єднання, скасуйте їх і змініть паролі.

Часті запитання (FAQ)
Питання: Як дізнатися, чи мій Bluetooth зламано?
Відповідь: Якщо ви помічаєте невідомі з'єднання або пристрій працює нестабільно, можливо, ваш Bluetooth під загрозою.

11. ШВИДКИЙ ГІД ІЗ НАЛАШТУВАННЯ БЕЗПЕКИ НА MACOS

macOS має репутацію безпечної операційної системи, але навіть вона не захищена від сучасних кіберзагроз. Дотримуйтесь цих кроків, щоб підвищити захист вашого Mac.

1. Оновлюйте macOS регулярно.
Перейдіть у Системні налаштування → Оновлення програмного забезпечення.
Увімкніть автоматичні оновлення, щоб завжди використовувати останню версію.

2. Увімкніть брандмауер.
Зайдіть у Системні налаштування → Безпека та конфіденційність → Брандмауер.
Натисніть Увімкнути брандмауер.
Налаштуйте опцію Блокувати всі вхідні з'єднання для додаткового захисту.

3. Налаштуйте FileVault для шифрування даних.
Відкрийте Системні налаштування → Безпека та конфіденційність → FileVault.
Увімкніть FileVault, щоб шифрувати всі дані на вашому диску.

4. Створіть складний пароль для вашого облікового запису.
Зайдіть у Системні налаштування → Користувачі та групи.
Виберіть свій обліковий запис і натисніть Змінити пароль.
Використовуйте унікальний пароль із великих і малих літер, цифр і символів.

5. Увімкніть двофакторну автентифікацію для Apple ID.
Відкрийте Системні налаштування → Apple ID → Пароль і безпека.
Увімкніть опцію Двофакторна автентифікація.

6. Увімкніть блокування екрана.
Перейдіть у Системні налаштування → Робочий стіл та економія енергії → Екранна заставка.
Встановіть короткий час для блокування (1–5 хвилин).
Увімкніть опцію Запитувати пароль після сну або заставки.

7. Контролюйте доступ додатків.
Зайдіть у Системні налаштування → Безпека та конфіденційність → Конфіденційність.
Перевірте, які програми мають доступ до вашої камери, мікрофона та місцезнаходження.
Вимкніть доступ для додатків, які ви не використовуєте.

8. Використовуйте Safari з підвищеною конфіденційністю.
У Safari зайдіть у Налаштування → Конфіденційність.
Увімкніть опції Блокувати файли cookie від сторонніх сторін та Запобігання відстеженню через сайти.

9. Уникайте завантаження програм поза App Store.
Зайдіть у Системні налаштування → Безпека та конфіденційність → Основні.
Виберіть опцію Дозволяти завантаження програм тільки з App Store.

10. Активуйте функцію "Знайти Mac".
Відкрийте Системні налаштування → Apple ID → Локатор (Find My).
Увімкніть Знайти Mac, щоб відстежувати пристрій у разі втрати чи крадіжки.

Підсумок:
Правильне налаштування безпеки macOS забезпечить вам захист від більшості загроз.
Виділіть трохи часу сьогодні — і ваш Mac буде в безпеці!

iOS відома своєю безпекою, але ризики завжди існують. Неправильні налаштування або легковажне використання можуть зробити ваш iPhone чи iPad вразливим.

1. Оновлюйте iOS регулярно.
Відкрийте Налаштування → Основні → Оновлення ПЗ.
Увімкніть Автоматичне оновлення, щоб завжди мати останню версію системи.

2. Увімкніть Face ID або Touch ID.
Перейдіть у Налаштування → Face ID/Touch ID та пароль.
Увімкніть функцію для розблокування пристрою та додатків.

3. Використовуйте складний пароль.
У налаштуваннях Face ID/Touch ID та пароль створіть пароль із 6 або більше символів.
Увімкніть Розширений цифровий код для більшої складності.

4. Увімкніть "Знайти iPhone".
Відкрийте Налаштування → Apple ID → Локатор (Find My).
Активуйте Знайти iPhone і Мережу Локатора для відстеження пристрою навіть офлайн.

5. Увімкніть двофакторну автентифікацію.
У розділі Apple ID → Пароль і безпека увімкніть Двофакторну автентифікацію.
Це захистить ваш обліковий запис навіть у разі витоку пароля.

Порада!
Якщо ваш пристрій підтримує eSIM, налаштуйте її з пін-кодом для додаткового захисту мобільної мережі.

6. Контролюйте доступ додатків.
Перейдіть у Налаштування → Конфіденційність і безпека.
Перевірте, які додатки мають доступ до камери, мікрофона, контактів і місцезнаходження.
Вимкніть доступ для додатків, які вам більше не потрібні.

7. Захистіть свої повідомлення.
У Налаштування → Повідомлення → Збереження повідомлень оберіть короткий термін зберігання (30 днів).
Увімкніть Повідомлення з перевіркою на екрані блокування.

8. Уникайте підозрілих Wi-Fi мереж.
Увімкніть функцію Попереджати про небезпечні мережі у розділі Wi-Fi.
Використовуйте VPN для захисту даних у публічних мережах.

9. Використовуйте Safari із захистом.
У налаштуваннях Safari → Конфіденційність і безпека увімкніть:
Блокування всіх файлів cookie.
Попередження про шахрайські вебсайти.
Запобігання відстеженню через сайти.

10. Використовуйте резервне копіювання.
Переконайтеся, що iCloud Backup увімкнено:
Зайдіть у Налаштування → Apple ID → iCloud → iCloud Backup.
Регулярно створюйте резервні копії для збереження даних.

Підсумок:
Захистіть свій iPhone чи iPad за допомогою цих простих налаштувань, і ваші дані залишатимуться у безпеці навіть у разі кібератак.

13. ШВИДКИЙ ГІД ІЗ НАЛАШТУВАННЯ БЕЗПЕКИ В WINDOWS

Windows — найпопулярніша операційна система, але її популярність робить її привабливою мішенню для кіберзлочинців.

1. Регулярно оновлюйте Windows.
Перейдіть у Параметри → Оновлення та безпека → Центр оновлення Windows.
Встановіть останні оновлення, щоб закрити вразливості.
Увімкніть автоматичне оновлення.

2. Увімкніть брандмауер Windows.
Відкрийте Панель управління → Система і безпека → Брандмауер Windows.
Переконайтеся, що брандмауер активний для всіх мереж (приватних і публічних).

3. Використовуйте антивірус Windows Defender.
Переконайтеся, що Windows Defender увімкнено:
Перейдіть у Параметри → Оновлення та безпека → Захисник Windows.
Увімкніть захист у реальному часі.

4. Установіть складний пароль для входу.
Відкрийте Параметри → Облікові записи → Параметри входу.
Використовуйте складний пароль або PIN-код.
Якщо доступно, увімкніть Windows Hello для входу за допомогою обличчя чи відбитка пальця.

5. Увімкніть захист облікового запису Microsoft.
Зайдіть у свій обліковий запис Microsoft (account.microsoft.com).
Увімкніть двофакторну автентифікацію для додаткового рівня безпеки.

6. Використовуйте контроль програм.
Відкрийте Параметри → Програми → Додаткові параметри.
Дозволяйте встановлення додатків лише з Microsoft Store.

7. Увімкніть функцію BitLocker (якщо доступно).
Відкрийте Панель управління → Система і безпека → Шифрування пристрою BitLocker.
Увімкніть шифрування для захисту даних на жорсткому диску.

8. Налаштуйте контроль облікових записів (UAC).
Увімкніть оповіщення про зміну системних налаштувань:
Відкрийте Панель управління → Облікові записи користувачів → Змінити параметри контролю облікових записів.
Встановіть повзунок на Повідомляти завжди.

9. Захистіть браузер.
Використовуйте сучасний браузер (Microsoft Edge, Chrome або Firefox) з активованим захистом від фішингу та шкідливих вебсайтів.
Встановіть розширення, як-от Adblock чи HTTPS Everywhere.

10. Використовуйте резервне копіювання.
Налаштуйте Історію файлів у розділі Параметри → Оновлення та безпека → Резервне копіювання.
Підключіть зовнішній диск або налаштуйте резервування в хмарі через OneDrive.

Підсумок:
Windows надає багато інструментів для захисту ваших даних. Налаштуйте систему правильно, і ваш комп'ютер буде надійно захищений від більшості загроз.

Linux вважається безпечною системою, але без належного налаштування ви можете залишити свій пристрій вразливим до атак.

1. Регулярно оновлюйте систему.
Слідкуйте за повідомленнями про оновлення та встановлюйте їх вчасно.
Активуйте автоматичне оновлення для впевненості, що ваша система захищена від нових загроз.

2. Налаштуйте брандмауер.
Увімкніть і налаштуйте брандмауер, наприклад, UFW або інший, доступний для вашої дистрибуції.
Дозвольте лише необхідні з'єднання (наприклад, для вебсервера чи SSH).

3. Захистіть віддалені підключення (SSH).
Використовуйте безпечні паролі або ключі для автентифікації.
Обмежте доступ до віддаленого підключення лише для потрібних IP-адрес.

4. Установіть антивірус.
Використовуйте антивірусне програмне забезпечення для перевірки системи, особливо якщо ви працюєте у змішаних мережах (Linux та Windows).

5. Створіть надійний пароль для свого облікового запису.
Пароль має бути унікальним і складатися з букв, цифр та символів.
Регулярно змінюйте паролі для важливих облікових записів.

Підказка!
Періодично перевіряйте журнали системи для виявлення незвичної активності.

6. Обмежте доступ до адміністративних функцій.
Дозволяйте виконання системних змін лише для облікових записів із правами адміністратора.
Видаліть або деактивуйте невикористовувані облікові записи.

7. Захистіть ваш сервер від DoS-атак.
Використовуйте інструменти захисту, які обмежують кількість запитів із підозрілих джерел.

8. Увімкніть шифрування диска.
Під час встановлення Linux виберіть опцію шифрування для захисту ваших даних.
Це захистить інформацію навіть у разі крадіжки вашого пристрою.

9. Використовуйте додатковий захист, як-от SELinux або AppArmor.
Ці інструменти захищають систему від виконання несанкціонованих процесів.
Переконайтеся, що захист увімкнений у вашій системі.

10. Створіть резервні копії.
Регулярно зберігайте копії важливих даних на зовнішньому диску чи у хмарному сховищі.
Автоматизуйте процес резервування для зручності.

Підсумок:
Linux є потужною і безпечною системою, якщо її правильно налаштувати. Виконання цих простих кроків зробить ваш пристрій максимально захищеним.

15. ШВИДКИЙ ГІД ІЗ НАЛАШТУВАННЯ БЕЗПЕКИ В ANDROID

Android — одна з найпоширеніших операційних систем, що робить її мішенню для зловмисників. Правильне налаштування безпеки забезпечить захист ваших даних і пристрою від атак.

1. Оновлюйте систему.
Регулярно перевіряйте наявність оновлень у Налаштування → Система → Оновлення ПЗ.
Увімкніть автоматичне завантаження оновлень, якщо це доступно.

2. Використовуйте екран блокування.
Увімкніть PIN-код, графічний ключ, пароль або біометричну автентифікацію (сканер обличчя/відбитка пальця) в Налаштування → Безпека → Екран блокування.

3. Увімкніть шифрування даних.
Більшість сучасних пристроїв автоматично шифрують дані.
Перевірте статус у Налаштування → Безпека → Шифрування та облікові дані.

4. Обмежте доступ додатків до ваших даних.
Перейдіть у Налаштування → Програми → Дозволи.
Вимкніть доступ до мікрофона, камери чи геолокації для програм, які цього не потребують.

5. Встановлюйте додатки лише з офіційних джерел.
Завантажуйте програми лише з Google Play Store.
Увімкніть опцію блокування встановлення з невідомих джерел у Налаштування → Безпека → Невідомі джерела.

Підказка!
Видаляйте додатки, якими ви більше не користуєтесь, щоб зменшити ризик витоку даних.

6. Використовуйте антивірус.
Встановіть надійний антивірус, як-от Avast, Bitdefender або Malwarebytes.
Регулярно скануйте систему на наявність загроз.

7. Захистіть свій обліковий запис Google.
Переконайтеся, що двофакторна автентифікація ввімкнена:
Зайдіть у Google Account → Безпека → Двофакторна автентифікація.

8. Увімкніть функцію "Знайти мій пристрій".
Увійдіть у Налаштування → Безпека → Знайти мій пристрій.
Це дозволить відстежити, заблокувати або видалити дані в разі втрати пристрою.

9. Використовуйте VPN у публічних Wi-Fi мережах.
Встановіть додаток для VPN (наприклад, NordVPN або ProtonVPN), щоб захистити свої дані від перехоплення.

10. Налаштуйте резервне копіювання даних.
Увімкніть автоматичне резервне копіювання до Google Drive у Налаштування → Система → Резервне копіювання.

Часті запитання (FAQ)
Питання: Чи можна довіряти Google Play Store?
Відповідь: Більшість програм у Google Play безпечні, але завжди читайте відгуки перед завантаженням.

16. ЯК ШИФРУВАТИ ДАНІ ЗА ДОПОМОГОЮ ВБУДОВАНИХ ІНСТРУМЕНТІВ?

Шифрування захищає вашу інформацію, перетворюючи її у зашифрований формат, який може бути прочитаний лише за допомогою ключа доступу. Це допомагає уникнути витоків даних у разі втрати чи крадіжки пристрою.

1. Шифрування диска на Windows
Використовуйте BitLocker, доступний у Windows Pro та Enterprise.
Відкрийте Панель управління → Система і безпека → Шифрування диска BitLocker.
Увімкніть шифрування для бажаного диска, створивши ключ відновлення.

2. Шифрування диска на macOS
Використовуйте FileVault для захисту вашого жорсткого диска:
Перейдіть у Системні налаштування → Безпека та конфіденційність → FileVault.
Увімкніть FileVault і задайте пароль для відновлення.

3. Шифрування на Android
Більшість сучасних Android-пристроїв уже шифрують дані автоматично.
Щоб перевірити:
Відкрийте Налаштування → Безпека → Шифрування та облікові дані.
Переконайтеся, що шифрування увімкнено.

4. Шифрування на iOS
Усі пристрої iOS шифрують дані за замовчуванням, якщо встановлено пароль.
Увімкніть пароль у Налаштування → Face ID/Touch ID та пароль.

5. Шифрування окремих файлів
На Windows:
Натисніть правою кнопкою на файл → Властивості → Додатково → Шифрувати вміст для захисту даних.
На macOS:
Використовуйте Дискову утиліту для створення зашифрованого образу файлу.

6. Шифрування зовнішніх носіїв
USB-накопичувачі або зовнішні жорсткі диски можна шифрувати:
На Windows: використовуйте BitLocker To Go.
На macOS: форматування через Disk Utility із вибором опції шифрування.

7. Використовуйте паролі для архівів
Для збереження конфіденційності файлів у ZIP або RAR використовуйте функцію встановлення пароля в архіваторах (наприклад, WinRAR чи 7-Zip).

8. Додаткові інструменти для шифрування
Використовуйте сторонні програми для універсального шифрування, наприклад:
VeraCrypt для створення зашифрованих сховищ.
AxCrypt для шифрування окремих файлів.

Часті запитання (FAQ)
Питання: Що станеться, якщо я забуду ключ відновлення?
Відповідь: Ви не зможете отримати доступ до зашифрованих даних, тому завжди зберігайте ключ у безпечному місці.

Питання: Чи потрібно шифрувати вже захищені хмарні дані?
Відповідь: Так, це додатковий рівень захисту, особливо для чутливої інформації.

17. 10 СПОСОБІВ ЗАБЕЗПЕЧИТИ КОНФІДЕНЦІЙНІСТЬ ДАНИХ

Ваші дані — це ключ до вашої ідентичності. Втрата конфіденційності може призвести до шахрайства, викрадення особистої інформації чи фінансових втрат. Дотримуйтесь цих порад, щоб захистити свої дані.

1. Використовуйте складні паролі.
Створюйте унікальні паролі для кожного облікового запису.
Використовуйте менеджери паролів для зручного керування.

2. Активуйте двофакторну автентифікацію (2FA).
Увімкніть додатковий рівень захисту для всіх важливих акаунтів.
Використовуйте додатки для 2FA, наприклад, Google Authenticator.

3. Шифруйте свої дані.
Увімкніть шифрування для жорстких дисків, смартфонів і резервних копій.
Використовуйте інструменти шифрування для конфіденційних файлів.

4. Захищайте публікації в соцмережах.
Обмежте видимість ваших публікацій лише для друзів.
Не публікуйте особисту інформацію, як-от адресу чи телефон.

5. Використовуйте VPN у публічних Wi-Fi мережах.
VPN шифрує ваш інтернет-трафік, захищаючи від перехоплення.
Це особливо важливо при використанні відкритих мереж у кафе чи готелях.

Підказка!
Завжди перевіряйте дозволи, які надаєте додаткам, особливо доступ до камери, мікрофона та контактів.

6. Уникайте підозрілих посилань і вкладень.
Не натискайте на посилання з невідомих джерел.
Перевіряйте адреси відправників електронних листів.

7. Видаляйте дані безпечно.
Використовуйте інструменти для безпечного видалення файлів.
Очищуйте накопичувачі перед продажем чи утилізацією пристроїв.

8. Налаштуйте резервне копіювання.
Створюйте регулярні резервні копії у зашифрованому вигляді.
Використовуйте хмарні сервіси з високим рівнем безпеки.

9. Контролюйте доступ до пристроїв.
Увімкніть екран блокування за допомогою пароля, Touch ID чи Face ID.
Не залишайте пристрої без нагляду у громадських місцях.

10. Слідкуйте за оновленнями.
Завжди встановлюйте останні оновлення операційної системи та програм.
Оновлення закривають вразливості, які можуть використовувати зловмисники.

Часті запитання (FAQ)
Питання: Чи безпечно використовувати хмарні сервіси для конфіденційних даних?
Відповідь: Так, за умови, що сервіс має функцію шифрування даних та багатофакторну автентифікацію.

Питання: Як дізнатися, чи моя інформація потрапила у витік даних?
Відповідь: Використовуйте сервіси на кшталт Have I Been Pwned, щоб перевірити свої акаунти.

18. ШВИДКИЙ ГІД ІЗ ПЕРЕВІРКИ КОМП'ЮТЕРА НА ВІРУСИ

Шкідливе програмне забезпечення може завдати шкоди вашим даним, сповільнити роботу пристрою чи викрасти конфіденційну інформацію. Регулярна перевірка допоможе вчасно виявити та усунути загрози.

1. Установіть антивірусне програмне забезпечення.
Оберіть надійний антивірус, наприклад, Windows Defender, Avast, Bitdefender.
Переконайтеся, що антивірус оновлюється автоматично.

2. Виконайте швидку перевірку.
Запустіть антивірус і виберіть опцію швидкого сканування.
Це дозволить швидко перевірити найвразливіші ділянки системи.

3. Заплануйте повне сканування.
Виберіть опцію повного сканування системи, щоб перевірити всі файли, диски та процеси.
Виконуйте цю перевірку хоча б раз на місяць.

4. Видаляйте або карантинуйте виявлені загрози.
Якщо антивірус знайде шкідливі файли, перемістіть їх до карантину або видаліть.
Переконайтеся, що важливі файли не видаляються помилково.

5. Перевірте завантаження.
У браузері перевіряйте всі завантажені файли перед відкриттям.
Використовуйте функцію перевірки файлів у вашому антивірусі.

6. Використовуйте онлайн-сканери.
Для додаткової перевірки використовуйте безкоштовні онлайн-сканери, наприклад:
VirusTotal для аналізу файлів.
ESET Online Scanner для перевірки системи.

7. Оновлюйте програми та операційну систему.
Застарілі програми можуть містити вразливості, які використовують зловмисники.
Увімкніть автоматичне оновлення для ОС і програм.

8. Очистіть тимчасові файли.
Використовуйте вбудовані інструменти або програми, як-от CCleaner, для видалення тимчасових файлів і кешу.
Це зменшить шанси прихованих загроз.

9. Перевірте автозавантаження.
Вимкніть підозрілі програми в автозавантаженні через диспетчер задач.
Це допоможе уникнути запуску шкідливих програм разом із системою.

10. Уникайте піратського ПЗ.
Не завантажуйте програми з ненадійних джерел.
Використовуйте лише офіційні сайти чи магазини програм.

Часті запитання (FAQ)
Питання: Чи можуть віруси зберігатися у файлах із архівів?
Відповідь: Так, архіви можуть містити шкідливі файли. Завжди перевіряйте їх перед розпакуванням.

Питання: Як зрозуміти, що комп'ютер заражений?
Відповідь: Основні ознаки — зниження швидкості роботи, поява незнайомих програм чи вікон, зміна домашньої сторінки в браузері.

19. ЯК СТВОРИТИ РЕЗЕРВНУ КОПІЮ В ХМАРНОМУ СХОВИЩІ?

Хмарні сховища дозволяють зберігати ваші дані на віддалених серверах, забезпечуючи доступ до них у будь-який час і з будь-якого пристрою. Це також захищає вас від втрати даних через несправність обладнання чи віруси.

1. Оберіть хмарний сервіс.
Найпопулярніші сервіси:
Google Drive (15 ГБ безкоштовно).
iCloud (5 ГБ безкоштовно).
OneDrive (5 ГБ безкоштовно).
Dropbox (2 ГБ безкоштовно).

2. Створіть обліковий запис.
Зайдіть на сайт або завантажте додаток обраного сервісу.
Зареєструйтесь, вказавши електронну пошту та створивши надійний пароль.

3. Налаштуйте синхронізацію.
Завантажте клієнт хмарного сховища на ваш пристрій (комп'ютер, смартфон чи планшет).
Увійдіть у свій обліковий запис.
Оберіть папки чи файли для автоматичної синхронізації.

4. Виберіть дані для резервування.
Створіть окрему папку для важливих файлів, які потрібно регулярно зберігати.
Додайте туди документи, фото, відео чи будь-які важливі дані.

5. Увімкніть автоматичне резервування.
У налаштуваннях клієнта оберіть опцію автоматичного збереження файлів у хмару.
Для смартфонів увімкніть автоматичне завантаження фото та відео.
6. Як створити резервну копію в Google Drive?
Відкрийте Google Диск на комп'ютері або смартфоні.
Натисніть Створити → Завантажити файли/папки.
Виберіть файли, які хочете зберегти, і дочекайтеся завершення завантаження.

7. Як створити резервну копію в iCloud?
Для iPhone/iPad:
Перейдіть у Налаштування → Apple ID → iCloud → Резервна копія iCloud.
Увімкніть автоматичне резервування.
Для Mac:
Відкрийте Системні налаштування → Apple ID → iCloud.
Переконайтеся, що вибрані потрібні дані для синхронізації.

8. Як створити резервну копію в OneDrive?
Відкрийте OneDrive на комп'ютері чи смартфоні.
Перемістіть файли в папку OneDrive для автоматичної синхронізації.
Перевірте, чи включено резервування робочого столу, документів та зображень.

9. Як створити резервну копію в Dropbox?
Створіть обліковий запис на dropbox.com.
Завантажте додаток і налаштуйте синхронізацію.
Перетягніть файли до папки Dropbox на вашому пристрої.

10. Перевіряйте резервні копії.
Регулярно переконуйтесь, що файли зберігаються у хмарному сховищі.
Перевіряйте, чи є доступ до файлів з інших пристроїв.

20. ШВИДКИЙ ГІД ІЗ НАЛАШТУВАННЯ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ В GOOGLE

Двофакторна автентифікація (2FA) додає додатковий рівень захисту до вашого облікового запису. Навіть якщо пароль буде зламано, зловмисники не зможуть отримати доступ без додаткового підтвердження.

1. Увійдіть у свій обліковий запис Google.
Перейдіть на сайт https://myaccount.google.com/.
Введіть свої логін і пароль для входу.

2. Відкрийте розділ "Безпека".
На головній сторінці облікового запису знайдіть вкладку Безпека.
У розділі Увійти в Google натисніть Двоетапна перевірка.

3. Почніть налаштування.
Натисніть Почати і введіть пароль ще раз для підтвердження.
Дотримуйтесь інструкцій на екрані.

4. Виберіть основний метод підтвердження.
Оберіть, як ви хочете отримувати код підтвердження:
Через SMS або дзвінок: Введіть номер телефону.
Через Google Authenticator: Встановіть додаток на смартфон.

5. Завершіть налаштування.
Введіть код, отриманий через вибраний метод.
Натисніть Увімкнути, щоб активувати 2FA.

Підказка!
Рекомендується використовувати додаток Google Authenticator або Authy, адже вони більш безпечні, ніж SMS.

6. Налаштуйте резервні методи підтвердження.
Після активації 2FA оберіть резервні варіанти на випадок, якщо ви втратите доступ до основного методу:
Резервні коди: Збережіть 10 унікальних кодів, які можна використовувати для входу.
Резервний номер телефону: Додайте ще один номер, якщо доступ до основного буде втрачено.

7. Увімкніть сповіщення на пристрої.
Ви можете увімкнути підтвердження через сповіщення Google:
Коли ви входите, Google надішле запит на ваш смартфон для підтвердження.

8. Використовуйте фізичний ключ безпеки (опційно).
Придбайте ключ безпеки (наприклад, YubiKey).
Підключіть його до облікового запису через USB або Bluetooth.

9. Регулярно перевіряйте підключені пристрої.
Перейдіть у розділ Безпека → Ваші пристрої.
Перевірте, які пристрої підключені до облікового запису, і видаліть зайві.

10. Перевірте налаштування.
Переконайтеся, що 2FA працює коректно:
Вийдіть із облікового запису та увійдіть знову, щоб перевірити процес підтвердження.

21. ШВИДКИЙ ГІД ІЗ НАЛАШТУВАННЯ КОНФІДЕНЦІЙНОСТІ В INSTAGRAM

Instagram — одна з найбільших соцмереж, де публікуються фото, відео та особиста інформація. Налаштування конфіденційності допоможе уникнути небажаного доступу до ваших даних та публікацій.

1. Переключіть акаунт у приватний режим.
Відкрийте Налаштування → Конфіденційність → Приватність акаунта.
Увімкніть опцію Приватний акаунт, щоб лише підписники бачили ваші дописи.

2. Контролюйте, хто може бачити ваші історії.
У Налаштування → Конфіденційність → Історії:
Виберіть Приховати історію від, щоб обмежити доступ для певних людей.
Дозвольте відповідати на історії лише друзям або вимкніть відповіді взагалі.

3. Обмежте коментарі.
У Налаштування → Конфіденційність → Коментарі:
Увімкніть фільтр образливих слів.
Додайте облікові записи до списку, які не можуть залишати коментарі.

4. Перевірте, хто може надсилати вам повідомлення.
У Налаштування → Конфіденційність → Повідомлення:
Обмежте можливість надсилати повідомлення лише друзям або підписникам.

5. Приховайте свою активність.
У Налаштування → Конфіденційність → Статус активності:
Вимкніть опцію, щоб інші не бачили, коли ви онлайн.

6. Управляйте тегами.
У Налаштування → Конфіденційність → Теги:
Увімкніть опцію, щоб теги з'являлися лише після вашого схвалення.

7. Обмежте доступ до геолокації.
Увімкніть геолокацію лише для потрібних постів.
У налаштуваннях телефону обмежте доступ Instagram до вашого місцезнаходження.

8. Контролюйте взаємодії з незнайомцями.
У Налаштування → Конфіденційність → Облікові записи, які ви обмежили:
Додайте облікові записи, взаємодія з якими буде обмежена.

9. Вимкніть показ персоналізованих оголошень.
У Налаштування → Конфіденційність → Оголошення:
Вимкніть персоналізацію реклами, щоб зменшити використання ваших даних.

10. Регулярно перевіряйте свій акаунт.
Відвідуйте розділ Доступ до ваших даних у налаштуваннях, щоб переглянути, яка інформація збирається про вас.
Видаляйте підозрілі або непотрібні програми, що мають доступ до вашого акаунта.

Часті запитання (FAQ)
Питання: Як обмежити коментарі без блокування користувача?
Відповідь: Ви можете додати користувача до списку обмежених у налаштуваннях конфіденційності.

Питання: Що робити, якщо мій акаунт зламано?
Відповідь: Змініть пароль, відкличте доступ підозрілих додатків і зверніться до служби підтримки Instagram.

22. ШВИДКИЙ ГІД ІЗ НАЛАШТУВАННЯ КОНФІДЕНЦІЙНОСТІ У FACEBOOK

Facebook містить багато особистої інформації, яка може бути використана шахраями чи зловмисниками. Налаштування конфіденційності допомагає захистити ваші дані та контролювати, хто їх бачить.

1. Перевірте налаштування конфіденційності.
Перейдіть у Налаштування → Конфіденційність.
Використовуйте інструмент Перевірка конфіденційності, щоб швидко оцінити та оновити ваші налаштування.

2. Обмежте видимість ваших публікацій.
У розділі Конфіденційність → Хто може бачити ваші публікації? виберіть Лише друзі або Лише я.
Налаштуйте видимість старих публікацій через опцію Обмежити аудиторію старих публікацій.

3. Контролюйте, хто може вас знаходити.
У розділі Конфіденційність → Як люди можуть знайти вас? обмежте можливість пошуку за номером телефону чи електронною поштою.
Вимкніть можливість індексації вашого профілю в пошукових системах.

4. Управляйте тегами.
У Налаштування → Профіль і позначки виберіть опцію Переглядати позначки перед їх появою у вашому профілі.
Це дозволить вам контролювати, які теги будуть видимі для інших.

5. Перевірте підключені додатки.
У Налаштування → Додатки та сайти перевірте список підключених програм.
Видаліть ті, якими ви більше не користуєтесь.

6. Налаштуйте конфіденційність історій.
У розділі Конфіденційність → Історії виберіть, хто може бачити ваші історії: Лише друзі або конкретні люди.
Вимкніть можливість відповідати на історії, якщо це не потрібно.

7. Захистіть вашу активність у групах.
Обмежте видимість груп, до яких ви приєдналися, у налаштуваннях Публічність груп.
Використовуйте опцію Закриті або приватні групи для додаткового захисту.

8. Налаштуйте сповіщення про входи.
У розділі Безпека та вхід → Сповіщення про невідомі входи увімкніть сповіщення на електронну пошту чи телефон.

9. Захистіть ваші публікації.
Використовуйте Хронологію та позначки, щоб перевіряти публікації, у яких вас відмітили.

10. Використовуйте двофакторну автентифікацію.
Увімкніть 2FA у Налаштування → Безпека та вхід → Двофакторна автентифікація.
Оберіть основний метод підтвердження (SMS, додаток або ключ безпеки).

Часті запитання (FAQ)
Питання: Як перевірити, як виглядає мій профіль для інших?
Відповідь: Використовуйте функцію Переглянути як у вашому профілі, щоб побачити, як ваш профіль виглядає для інших користувачів.

23. ШВИДКИЙ ГІД ІЗ НАЛАШТУВАННЯ TELEGRAM ДЛЯ БЕЗПЕКИ

Telegram — один із найбільш популярних месенджерів, але його правильне налаштування допоможе захистити ваші особисті дані.

1. Увімкніть двофакторну автентифікацію.
Перейдіть у Налаштування → Конфіденційність і безпека → Двофакторна автентифікація.
Установіть додатковий пароль для входу в акаунт.
Вкажіть резервний email для відновлення доступу.

2. Обмежте, хто може бачити ваш номер телефону.
У Налаштування → Конфіденційність і безпека → Номер телефону виберіть:
Хто може бачити мій номер: Ніхто або Мої контакти.
Хто може знайти мене за номером: оберіть Мої контакти.

3. Захистіть фото профілю.
У Налаштування → Конфіденційність і безпека → Фото та відео профілю виберіть, хто може бачити ваші зображення:
Виберіть Мої контакти або конкретних осіб.
Заблокуйте доступ для сторонніх.

4. Увімкніть блокування чату.
Увімкніть блокування доступу до Telegram за допомогою пароля або біометричних даних:
Налаштування → Конфіденційність і безпека → Код-пароль.
Установіть PIN-код або використовуйте сканер відбитка пальця.

5. Перевірте активні сесії.
У Налаштування → Пристрої перегляньте всі пристрої, де ви увійшли в Telegram.
Завершіть сесії на незнайомих або непотрібних пристроях.

6. Увімкніть самознищення акаунта.
У Налаштування → Конфіденційність і безпека → Автоматичне видалення акаунта оберіть час, після якого акаунт буде видалено за неактивності (наприклад, 6 місяців).

7. Використовуйте секретні чати.
Для конфіденційного спілкування створюйте Секретні чати:
Вони мають наскрізне шифрування.
Повідомлення можна налаштувати на автоматичне видалення через певний час.

8. Перевіряйте файли перед відкриттям.
Уникайте завантаження підозрілих файлів, навіть якщо вони отримані від знайомих.
Використовуйте антивірус для сканування файлів, отриманих у чатах.

9. Контролюйте доступ до груп і каналів.
У Налаштування → Конфіденційність і безпека → Групи та канали обмежте, хто може додавати вас до груп:
Оберіть Мої контакти або вкажіть конкретних людей.

10. Використовуйте функцію антиспам.
Якщо ви отримуєте підозрілі повідомлення, заблокуйте відправника та повідомте про нього через функцію Скарга.

24. ШВИДКИЙ ГІД ІЗ НАЛАШТУВАННЯ КОНФІДЕНЦІЙНОСТІ В TIKTOK

TikTok дозволяє ділитися відео з мільйонами користувачів. Без належного налаштування конфіденційності ваші дані, відео та особиста інформація можуть стати доступними для небажаних осіб.

1. Увімкніть приватний акаунт.
Перейдіть у Налаштування → Конфіденційність.
Увімкніть опцію Приватний акаунт, щоб ваші відео могли переглядати лише підтверджені підписники.

2. Обмежте, хто може знаходити ваш акаунт.
У Налаштування → Конфіденційність → Рекомендації акаунта вимкніть опцію Дозволити іншим знаходити мене.

3. Контролюйте коментарі.
У Налаштування → Конфіденційність → Коментарі оберіть:
Хто може коментувати ваші відео: Лише друзі або Ніхто.
Увімкніть Фільтр образливих слів.

4. Захистіть ваші повідомлення.
У Налаштування → Конфіденційність → Прямі повідомлення оберіть:
Хто може надсилати вам повідомлення: Друзі або Ніхто.
Вимкніть повідомлення від незнайомців.

5. Контролюйте завантаження ваших відео.
У Налаштування → Конфіденційність → Дозволи вимкніть опцію Дозволити завантаження відео, щоб інші не могли завантажувати ваші публікації.

Підказка!
Регулярно оновлюйте налаштування конфіденційності, оскільки TikTok часто додає нові функції або змінює наявні.

6. Приховайте взаємодії.
У Налаштування → Конфіденційність → Подобається виберіть, хто може бачити ваші вподобання: Лише я.

7. Перевірте доступ до ваших даних.
У Налаштування → Конфіденційність → Дозволи програми перевірте, які додатки мають доступ до вашого облікового запису.
Видаліть доступ для підозрілих додатків.

8. Вимкніть персоналізовану рекламу.
У Налаштування → Конфіденційність → Реклама вимкніть опцію Персоналізація реклами, щоб зменшити використання ваших даних для таргетингу.

9. Перевіряйте сповіщення про вхід.
У Налаштування → Безпека → Входи в акаунт перевіряйте всі активні сесії.
Завершіть підозрілі входи.

10. Використовуйте двофакторну автентифікацію (2FA).
У Налаштування → Безпека → Керування автентифікацією увімкніть додатковий захист через SMS або автентифікаційний додаток.

Часті запитання (FAQ)
Питання: Чи можна зробити профіль повністю приватним?
Відповідь: Так, увімкнення приватного акаунта приховує ваші відео від усіх, окрім підтверджених підписників.

25. ШВИДКИЙ ГІД ІЗ НАЛАШТУВАННЯ БЕЗПЕКИ У VIBER

Viber — популярний месенджер із великою кількістю користувачів. Ваша конфіденційність і безпека залежать від правильного налаштування, яке допоможе захистити особисті повідомлення.

1. Увімкніть перевірку контактів.
Увімкніть Довірені контакти:
Перейдіть у Налаштування → Конфіденційність → Перевірка контактів.
Ви отримаєте повідомлення, якщо хтось змінить свій номер або дані.

2. Увімкніть екран блокування.
Встановіть блокування доступу до додатка:
У Налаштування → Конфіденційність → Захист за PIN-кодом задайте PIN або використовуйте біометрію.

3. Використовуйте "Секретні чати".
Для чутливих розмов створюйте Секретні чати, які автоматично видаляють повідомлення після заданого часу.
Ці чати мають додатковий рівень шифрування.

4. Увімкніть двофакторну автентифікацію.
Увімкніть 2FA для захисту облікового запису:
Перейдіть у Налаштування → Безпека → Двофакторна автентифікація.
Додайте додатковий пароль або код підтвердження.

5. Обмежте доступ до вашої активності.
У Налаштування → Конфіденційність → Показувати мій статус в мережі вимкніть опцію, якщо не хочете, щоб інші бачили ваш статус.

Підказка!
Не переходьте за підозрілими посиланнями, навіть якщо вони надіслані від знайомих, адже їхній акаунт може бути зламано.

6. Обмежте доступ до фото профілю.
У Налаштування → Конфіденційність → Хто бачить моє фото профілю виберіть:
Мої контакти або конкретних людей.

7. Контролюйте, хто може додавати вас до груп.
У Налаштування → Конфіденційність → Групи обмежте, хто може додавати вас до груп.
Виберіть опцію Мої контакти або вкажіть конкретних людей.

8. Видаляйте важливі повідомлення.
Використовуйте функцію Видалити для всіх, щоб повністю видалити повідомлення з чату.
Це доступно протягом обмеженого часу після відправки.

9. Перевірте список підключених пристроїв.
У Налаштування → Пристрої перегляньте всі активні сесії.
Завершіть сесії на пристроях, якими більше не користуєтесь.

10. Уникайте відкритих мереж Wi-Fi.
Для захисту даних у публічних Wi-Fi використовуйте VPN.
Це допоможе уникнути перехоплення ваших повідомлень.

26. ШВИДКИЙ ГІД ІЗ НАЛАШТУВАННЯ БЕЗПЕКИ У WHATSAPP

WhatsApp є одним із найпоширеніших месенджерів у світі, але без належного налаштування ваші дані можуть стати вразливими для атак або небажаного доступу.

1. Увімкніть двоетапну перевірку.
Перейдіть у Налаштування → Обліковий запис → Двоетапна перевірка.
Увімкніть її та створіть PIN-код.
Вкажіть резервний email для відновлення доступу.

2. Перевіряйте налаштування конфіденційності.
У Налаштування → Конфіденційність налаштуйте:
Останній раз у мережі: оберіть Ніхто або Мої контакти.
Фото профілю: обмежте доступ, вибравши Мої контакти.
Інформація про себе: зробіть доступною лише для друзів або приховайте.

3. Увімкніть сповіщення про безпеку.
У Налаштування → Обліковий запис → Безпека увімкніть опцію Показувати сповіщення про безпеку.
Це дозволить дізнатися, якщо шифрування чату було змінено.

4. Заблокуйте небажані контакти.
Якщо ви отримуєте спам або небажані повідомлення, відкрийте чат із цим контактом, натисніть на ім'я контакту, а потім виберіть Заблокувати.

5. Захистіть доступ до WhatsApp.
Увімкніть блокування додатка за допомогою PIN-коду, пароля або біометрії:
Налаштування → Конфіденційність → Блокування екрана.
Виберіть час, після якого додаток автоматично заблокується.

6. Обмежте доступ до груп.
У Налаштування → Конфіденційність → Групи оберіть, хто може додавати вас до груп:
Мої контакти або Мої контакти, окрім...

7. Використовуйте функцію "Зникаючі повідомлення".
Для конфіденційного спілкування увімкніть автоматичне видалення повідомлень через певний час:
У чаті натисніть на ім'я контакту → Зникаючі повідомлення → виберіть час.

8. Уникайте підозрілих посилань.
WhatsApp автоматично позначає підозрілі посилання, але завжди перевіряйте URL перед натисканням.
Не відкривайте файли від незнайомців.

9. Перевіряйте активні пристрої.
У Налаштування → Пристрої перегляньте всі сесії, де ваш акаунт використовується.
Завершіть непотрібні сесії, натиснувши Вийти.

10. Оновлюйте додаток.
Переконайтеся, що WhatsApp завжди оновлений до останньої версії, адже оновлення включають виправлення вразливостей.

Часті запитання (FAQ)
Питання: Що робити, якщо хтось увійшов у мій акаунт без дозволу?
Відповідь: Завершіть усі сесії через Налаштування → Пристрої та змініть PIN-код.

27. ШВИДКИЙ ГІД ІЗ РЕЗЕРВНОГО КОПІЮВАННЯ ДАНИХ

Резервне копіювання — це ваша страховка від втрати важливих даних через помилки, віруси або технічні несправності. Правильне налаштування резервного копіювання збереже ваші документи, фото та інші файли.

1. Визначте, що потрібно зберегти.
Виділіть важливі файли: робочі документи, фотографії, контакти та інше.
Уникайте резервування тимчасових чи великих непотрібних файлів.

2. Виберіть спосіб резервного копіювання.
Локальне: використовуйте зовнішній жорсткий диск, USB-накопичувач або мережеве сховище (NAS).
Хмарне: виберіть хмарний сервіс, як-от Google Drive, iCloud, OneDrive чи Dropbox.

3. Налаштуйте регулярне резервування.
Переконайтеся, що резервне копіювання виконується автоматично.
Для Windows: використовуйте Історію файлів.
Для macOS: увімкніть Time Machine.

4. Використовуйте шифрування.
Для захисту конфіденційних даних увімкніть шифрування.
Більшість хмарних сервісів і локальних інструментів пропонують цю функцію.

5. Перевіряйте резервні копії.
Періодично переконуйтеся, що резервні копії зберігаються правильно і доступні для відновлення.

6. Резервне копіювання в Windows.
Відкрийте Параметри → Оновлення та безпека → Резервне копіювання.
Підключіть зовнішній диск і налаштуйте автоматичне збереження файлів.

7. Резервне копіювання в macOS.
Підключіть зовнішній диск.
Увімкніть Time Machine в Системних налаштуваннях → Time Machine.
Налаштуйте інтервал збереження резервних копій.

8. Резервне копіювання на Android.
Увійдіть у свій обліковий запис Google.
Увімкніть резервування в Налаштування → Система → Резервне копіювання.
Виберіть, що саме потрібно копіювати (додатки, контакти, фото).

9. Резервне копіювання на iOS.
Перейдіть у Налаштування → Apple ID → iCloud → Резервна копія iCloud.
Увімкніть автоматичне резервування.

10. Використовуйте додаткові інструменти.
Для локального резервування: Acronis True Image, EaseUS Todo Backup.
Для хмарного резервування: Backblaze, Carbonite.

Часті запитання (FAQ)
Питання: Як часто потрібно робити резервні копії?
Відповідь: Оптимально щодня для робочих даних і раз на тиждень для великих архівів.

28. ПАМ'ЯТКА: ЯК УНИКНУТИ ВІРУСІВ ЧЕРЕЗ USB-НАКОПИЧУВАЧІ

USB-накопичувачі можуть стати джерелом вірусів, які заражають ваш комп'ютер або викрадають дані. Дотримання простих правил допоможе уникнути ризиків і захистити ваші пристрої.

1. Використовуйте лише надійні накопичувачі.
Не підключайте USB-пристрої, отримані від незнайомих людей.
Уникайте використання знайдених USB-накопичувачів — вони можуть бути заражені вірусами.

2. Завжди перевіряйте накопичувач на віруси.
Відразу після підключення USB до комп'ютера виконайте перевірку за допомогою антивірусу.
Використовуйте функцію автоматичного сканування, доступну в більшості антивірусів.

3. Вимкніть функцію автозапуску.
Автозапуск може автоматично запускати шкідливі програми з USB.
Перевірте налаштування вашої операційної системи та вимкніть цю функцію.

4. Створіть резервну копію важливих даних.
Перед використанням USB-накопичувача збережіть резервну копію своїх файлів.
Це допоможе уникнути втрати даних у разі зараження пристрою.

5. Форматуйте підозрілі накопичувачі.
Якщо USB-накопичувач виглядає підозріло (незрозумілі файли, невідомий вміст), відформатуйте його перед використанням.

6. Уникайте підключення до незахищених пристроїв.
Не підключайте USB до чужих комп'ютерів чи пристроїв із низьким рівнем захисту.
Використовуйте лише ті пристрої, яким ви довіряєте.

7. Використовуйте USB із функцією захисту від запису.
Виберіть накопичувачі з перемикачем для захисту від запису.
Це унеможливить копіювання шкідливих файлів на пристрій.

8. Шифруйте дані на USB.
Для важливих даних використовуйте шифрування.
Це захистить ваші файли навіть у разі втрати накопичувача.

9. Видаляйте зайві файли.
Регулярно очищуйте накопичувач від файлів, які більше не потрібні.
Це зменшить ризик зараження під час роботи з різними пристроями.

10. Постійно оновлюйте антивірус.
Переконайтеся, що ваше антивірусне програмне забезпечення завжди актуальне.
Оновлення допоможуть вчасно виявляти нові види загроз.

Часті запитання (FAQ)
Питання: Як дізнатися, чи USB-накопичувач заражений?
Відповідь: Виконайте перевірку антивірусом. Якщо на накопичувачі з'являються невідомі файли чи папки, це може бути ознакою зараження.

Підсумок:
Дотримуючись цих рекомендацій, ви зможете безпечно користуватися USB-накопичувачами і захистити свої дані від вірусів та інших загроз.

29. ЯК ЗАХИСТИТИ СВОЇ ФОТО В ІНТЕРНЕТІ?

Фотографії, завантажені в Інтернет, можуть стати доступними для сторонніх осіб і використовуватися без вашого дозволу. Захист ваших зображень — це перший крок до збереження вашої конфіденційності.

1. Використовуйте приватність у соцмережах.
Перевірте налаштування конфіденційності у ваших акаунтах.
Зробіть свої фото видимими лише для друзів.

2. Не публікуйте надмірно особисті фото.
Уникайте завантаження фото, які містять конфіденційну інформацію (адреси, документи, особисті дані).
Пам'ятайте, що те, що потрапило в Інтернет, може залишитися там назавжди.

3. Використовуйте водяні знаки.
Наносьте на фото водяні знаки, щоб захистити їх від несанкціонованого використання.
Використовуйте сервіси на кшталт Canva або Photoshop для створення водяних знаків.

4. Завантажуйте фото в захищені сервіси.
Використовуйте платформи, які підтримують високий рівень безпеки, наприклад, Google Photos, iCloud чи Dropbox.
Переконайтеся, що ваш обліковий запис захищено двофакторною автентифікацією.

5. Видаляйте метадані із зображень.
Метадані (EXIF) можуть містити інформацію про місце, де зроблено фото.
Використовуйте програми, щоб видалити ці дані перед завантаженням фото в Інтернет.

6. Захистіть фото в хмарних сховищах.
Використовуйте хмарні сервіси, які підтримують шифрування файлів.
Увімкніть функцію резервного копіювання, щоб не втратити важливі фото.

7. Уникайте пересилання фото через незахищені платформи.
Використовуйте месенджери із наскрізним шифруванням, наприклад, Signal чи Telegram.
Не надсилайте конфіденційні фото через загальнодоступні платформи.

8. Регулярно перевіряйте свої фото онлайн.
Використовуйте пошук зображень у Google або TinEye, щоб перевірити, чи ваші фото не використовуються без дозволу.

9. Захищайте свої пристрої.
Установіть пароль або біометричний захист для ваших телефонів і комп’ютерів.
Використовуйте антивірус для виявлення шкідливих програм, які можуть отримати доступ до ваших зображень.

10. Уникайте публічних Wi-Fi мереж.
Якщо потрібно передати фото через Інтернет, використовуйте VPN для захисту трафіку.
Це запобігає перехопленню ваших даних сторонніми особами.

Часті запитання (FAQ)
Питання: Як зрозуміти, чи мої фото використовуються без дозволу?
Відповідь: Використовуйте функцію зворотного пошуку зображень у Google, щоб знайти копії ваших фото в Інтернеті.

30. АЛГОРИТМ РЕАГУВАННЯ НА ФІШИНГ

Фішинг — це метод шахрайства, коли зловмисники намагаються отримати ваші особисті дані (паролі, банківську інформацію) через підроблені сайти, електронні листи або повідомлення. Швидке реагування допоможе уникнути втрати даних чи грошей.

1. Уникайте підозрілих посилань.
Якщо отримали лист чи повідомлення із запитом перейти за посиланням:
Перевірте, чи ви очікували це повідомлення.
Наведіть курсор на посилання, щоб перевірити справжність URL.
Не натискайте на посилання з незнайомих джерел.

2. Перевіряйте адреси відправників.
Офіційні організації не використовують безкоштовні поштові домени (наприклад, @gmail.com).
Шукайте помилки в адресі відправника (наприклад, @paypa1.com замість @paypal.com).

3. Ніколи не надавайте конфіденційну інформацію.
Банки, державні установи та великі сервіси не запитують паролі чи банківські дані через листи або повідомлення.

4. Використовуйте антивірус із функцією антифішингу.
Антивірусні програми можуть виявити фішингові атаки та попередити вас про небезпеку.
Увімкніть функцію захисту браузера від фішингу.

5. Не відкривайте підозрілі вкладення.
Вкладення у вигляді архівів, документів або програм можуть містити віруси чи шкідливі програми.
Перевіряйте файли антивірусом перед відкриттям.

6. Перевірте автентичність сайту.
Вводьте свої дані лише на захищених сайтах із протоколом HTTPS (замок у адресному рядку).
Уникайте введення даних на сайтах із підозрілим дизайном чи помилками у домені.

7. Зверніться до офіційного джерела.
Якщо вам надходить лист нібито від банку чи сервісу, зайдіть на офіційний сайт вручну, ввівши URL у браузері.
Не використовуйте посилання з листа чи повідомлення.

8. Зробіть скриншот або збережіть повідомлення.
Якщо підозрюєте фішинг, зробіть скриншот чи збережіть повідомлення для подальшого розслідування.
Це допоможе повідомити про шахрайство відповідні органи чи службу підтримки.

9. Повідомте про фішингову атаку.
Увійдіть у свій акаунт на сервісі (наприклад, Gmail чи банківському сайті) і знайдіть опцію Скарга на фішинг.
Повідомте роботодавцю чи колегам, якщо це стосується робочого листа.

10. Змініть паролі.
Якщо ви випадково ввели свої дані на підозрілому сайті, негайно змініть пароль.
Увімкніть двофакторну автентифікацію для захисту акаунта.

31. АЛГОРИТМ РЕАГУВАННЯ НА ВТРАТУ ОСОБИСТИХ ДАНИХ

Втрачена чи викрадена особиста інформація може бути використана зловмисниками для шахрайства, викрадення особистості або доступу до ваших фінансів. Швидке реагування допоможе мінімізувати ризики.

1. Визначте, які дані були втрачені.
Перевірте, які саме дані були викрадені або оприлюднені:
Паролі.
Банківські реквізити.
Особисті документи (паспорт, ідентифікаційний код тощо).

2. Змініть паролі.
Якщо викрадені паролі, негайно змініть їх для всіх акаунтів.
Використовуйте складні й унікальні паролі для кожного акаунта.
Увімкніть двофакторну автентифікацію (2FA).

3. Повідомте свій банк.
Якщо викрадені фінансові дані, негайно зверніться до вашого банку.
Заморозьте рахунки або заблокуйте картки, якщо це потрібно.
Перевірте останні транзакції на наявність підозрілої активності.

4. Перевірте активність своїх облікових записів.
Увійдіть у всі важливі акаунти (електронна пошта, соцмережі) та перевірте історію входів.
Завершіть сесії на пристроях, які вам не належать.

5. Використовуйте сервіси перевірки витоків даних.
Використовуйте сервіси, як-от Have I Been Pwned, щоб дізнатися, чи ваші дані потрапили у витік.

6. Зверніться до відповідних органів.
Якщо втрачені документи, зверніться до поліції чи відповідних органів для блокування чи перевипуску.
У разі витоку банківських даних повідомте службу безпеки вашого банку.

7. Відновіть доступ до акаунтів.
Використовуйте опцію відновлення паролів через електронну пошту або SMS.
Переконайтеся, що всі резервні контакти (номер телефону чи інша пошта) актуальні.

8. Видаліть підозрілі програми чи додатки.
Перевірте ваші пристрої на наявність підозрілих програм.
Використовуйте антивірус для сканування пристроїв.

9. Контролюйте свої фінанси.
Регулярно перевіряйте виписки з банківських рахунків.
Увімкніть сповіщення про всі транзакції, щоб швидко виявити підозрілу активність.

10. Повідомте про інцидент.
Якщо витік стався через компанію чи сервіс, повідомте їх про проблему.
Уточніть, які заходи вони вживають для мінімізації наслідків.

Часті запитання (FAQ)
Питання: Що робити, якщо викрали мій телефон із важливими даними?
Відповідь: Використовуйте функцію "Знайти пристрій" для блокування чи видалення даних. Негайно змініть паролі для важливих акаунтів.

32. АЛГОРИТМ БЕЗПЕЧНОГО ВИКОРИСТАННЯ ЕЛЕКТРОННОЇ ПОШТИ

Електронна пошта є ключем до багатьох ваших облікових записів. Зловмисники можуть використовувати її для доступу до ваших особистих даних або фінансової інформації. Виконуйте ці кроки, щоб убезпечити свій поштовий обліковий запис.

1. Використовуйте складний пароль.
Пароль має містити щонайменше 12 символів, включаючи цифри, великі та малі літери, а також спеціальні символи.
Не використовуйте один і той самий пароль для різних акаунтів.

2. Увімкніть двофакторну автентифікацію (2FA).
Налаштуйте додатковий рівень захисту через SMS або автентифікаційний додаток, наприклад, Google Authenticator.

3. Не відкривайте підозрілі листи.
Уникайте відкриття листів із незнайомих адрес.
Не завантажуйте вкладення чи не переходьте за посиланнями у таких листах.

4. Використовуйте фільтри для спаму.
Активуйте функцію автоматичного фільтрування спаму у налаштуваннях вашої поштової програми.
Регулярно перевіряйте папку "Спам" на випадок помилкової класифікації важливих листів.

5. Перевіряйте адресу відправника.
Зловмисники можуть імітувати офіційні адреси. Уважно перевіряйте домен відправника (наприклад, @gmail.com замість @gmial.com).

6. Уникайте використання загальнодоступних мереж Wi-Fi.
Якщо ви перевіряєте пошту через публічну Wi-Fi мережу, обов'язково використовуйте VPN.

7. Регулярно оновлюйте пароль.
Змінюйте пароль хоча б раз на 6 місяців.
Якщо є підозра на витік даних, змініть його негайно.

8. Відстежуйте активність вашого облікового запису.
У налаштуваннях поштової служби переглядайте список пристроїв і місць, звідки виконувались входи.
Завершуйте підозрілі сесії.

9. Використовуйте окремі акаунти для різних цілей.
Заведіть окрему електронну адресу для роботи, особистих справ та реєстрації на сайтах.
Це зменшить ризики витоку важливих даних.

10. Активуйте HTTPS.
Переконайтеся, що під час доступу до пошти у веббраузері використовується захищений протокол HTTPS.
У налаштуваннях пошти перевірте, чи увімкнено функцію Безпечне підключення.

Часті запитання (FAQ)
Питання: Як дізнатися, чи моя пошта потрапила у витік даних?
Відповідь: Використовуйте сервіси на кшталт Have I Been Pwned для перевірки.

33. АЛГОРИТМ ПЕРЕВІРКИ ПОСИЛАНЬ ПЕРЕД ПЕРЕХОДОМ

Підозрілі посилання можуть вести на фішингові сайти, завантажувати шкідливе програмне забезпечення чи викрадати ваші дані. Перевірка перед переходом допоможе уникнути цих ризиків.

1. Наведіть курсор на посилання.
На комп'ютері: наведіть курсор на посилання, щоб побачити URL-адресу в нижній частині браузера.
На телефоні: утримуйте посилання, щоб відобразити його адресу.

2. Перевірте URL.
Переконайтеся, що сайт використовує захищений протокол HTTPS (зображення замка в адресному рядку).
Уважно перевірте домен на наявність помилок чи незвичних символів (наприклад, paypa1.com замість paypal.com).

3. Зверніть увагу на скорочені посилання.
Якщо посилання скорочене (наприклад, через bit.ly), використовуйте сервіси для розшифрування, такі як CheckShortURL.
Це допоможе зрозуміти, куди веде посилання, не переходячи за ним.

4. Перевірте посилання через онлайн-інструменти.
Використовуйте сервіси для перевірки URL на безпеку:
VirusTotal.
Google Safe Browsing.

5. Оцініть контекст посилання.
Чи очікували ви отримати це посилання?
Чи виглядає текст повідомлення логічним і чи збігається з адресою відправника?

6. Не натискайте на посилання з підозрілих листів.
Уникайте посилань у повідомленнях, які вимагають термінових дій, наприклад, "Ваш акаунт буде заблоковано".
Перевіряйте справжність відправника.

7. Уникайте завантаження файлів із невідомих сайтів.
Якщо посилання веде на завантаження файлу, переконайтеся, що сайт є офіційним.
Завантажуйте програми лише з перевірених джерел.

8. Використовуйте розширення для браузера.
Встановіть розширення, які перевіряють посилання на безпеку в реальному часі, наприклад:
McAfee WebAdvisor.
Avast Online Security.

9. Не вводьте особисті дані без перевірки.
Переконайтеся, що сайт, де ви вводите логін чи пароль, є офіційним.
Уникайте входу через посилання з електронних листів — заходьте через офіційний сайт.

10. Навчайтеся розпізнавати шахрайські сайти.
Звертайте увагу на дизайн сайту: офіційні сайти мають чіткий та акуратний вигляд.
Якщо сайт містить багато орфографічних помилок або виглядає незавершеним, це може бути шахрайство.

34. ЯК РОЗПІЗНАТИ ШАХРАЙСЬКІ МОБІЛЬНІ SMS?

Шахраї використовують SMS для крадіжки даних, грошей або встановлення шкідливого ПЗ на ваш пристрій. Знання ознак шахрайських повідомлень допоможе уникнути небезпеки.

1. Звертайте увагу на текст повідомлення.
Підозрілий текст зазвичай містить:
Помилки в словах і граматиці.
Несподівані пропозиції (виграш, знижки, кредити).
Термінові прохання, наприклад: "Ваш акаунт буде заблоковано".

2. Перевірте номер відправника.
SMS від офіційних організацій зазвичай приходять з ідентифікаторами (наприклад, "Банк" замість номера).
Підозрілі повідомлення можуть надходити з незнайомих або коротких номерів.

3. Уникайте переходу за посиланнями.
Шахрайські посилання зазвичай:
Виглядають дивно або мають неправильний домен (наприклад, bank-login-secure.com замість bank.com).
Скеровують на сторінки, які імітують офіційні сайти.

4. Не завантажуйте файли з SMS.
Ніколи не відкривайте вкладення чи не завантажуйте файли з невідомих SMS. Вони можуть містити шкідливе ПЗ.

5. Думайте, чи ви очікували це повідомлення.
Якщо SMS стосується виграшу, доставки чи іншої події, якої ви не очікували, це може бути шахрайством.

Підказка!
Офіційні організації ніколи не просять надіслати PIN-код, паролі чи інші конфіденційні дані через SMS.

6. Перевірте інформацію у офіційних джерелах.
Якщо повідомлення нібито від банку чи компанії, зайдіть на їхній офіційний сайт або зателефонуйте до служби підтримки.
Не використовуйте номери чи посилання з повідомлення.

7. Використовуйте антивірус для мобільного.
Антивіруси, як-от Kaspersky Mobile Security чи Avast Mobile, можуть блокувати шкідливі посилання або SMS.

8. Не відповідайте на підозрілі SMS.
Відповідь на такі повідомлення може підтвердити шахраям, що ваш номер активний.
Це може спричинити подальше спамування чи шахрайство.

9. Блокуйте підозрілі номери.
У налаштуваннях телефону додайте номер до списку заблокованих контактів.
Використовуйте вбудовані функції телефону для фільтрації спаму.

10. Повідомте про шахрайське SMS.
Зверніться до свого оператора зв'язку або служби підтримки організації, від імені якої надійшло повідомлення.
Повідомте про спробу шахрайства до відповідних органів, якщо це можливо.

35. ЯК УНИКАТИ АТАК ЧЕРЕЗ ПОВІДОМЛЕННЯ В МЕСЕНДЖЕРАХ?

Месенджери є популярним інструментом для спілкування, але вони також використовуються зловмисниками для шахрайства, викрадення даних чи зараження пристроїв шкідливим ПЗ. Знання про захист допоможе уникнути ризиків.

1. Не відкривайте підозрілі посилання.
Перевіряйте URL-адресу перед переходом.
Навіть якщо посилання надіслане знайомим, будьте уважні — їхній акаунт може бути зламано.

2. Уникайте завантаження файлів із невідомих джерел.
Не відкривайте вкладення з підозрілих повідомлень.
Використовуйте антивірус для перевірки файлів перед їхнім відкриттям.

3. Не діліться конфіденційними даними.
Не надсилайте через месенджери паролі, банківські дані чи копії документів.
Використовуйте спеціалізовані захищені платформи для обміну важливими даними.

4. Увімкніть двофакторну автентифікацію.
Більшість месенджерів підтримують 2FA для додаткового захисту.
Це допоможе захистити ваш акаунт навіть у разі витоку пароля.

5. Заблокуйте підозрілих користувачів.
Якщо отримуєте спам чи дивні повідомлення, блокуйте таких відправників.
Використовуйте функцію "Скарга" для повідомлення про зловмисників.

6. Використовуйте секретні чати.
У месенджерах, як-от Telegram чи Signal, секретні чати забезпечують додатковий рівень шифрування та самознищення повідомлень.

7. Перевіряйте активні сесії.
У налаштуваннях месенджера переглядайте всі пристрої, де увійшли в акаунт.
Завершуйте сесії на пристроях, які вам більше не потрібні.

8. Не встановлюйте сторонні додатки з повідомлень.
Якщо вам пропонують завантажити додаток, переконайтеся, що це офіційний ресурс.
Використовуйте лише магазини Google Play чи App Store для встановлення програм.

9. Увімкніть функції блокування спаму.
Багато месенджерів мають автоматичний захист від спаму, який можна налаштувати в параметрах конфіденційності.

10. Регулярно оновлюйте месенджер.
Переконайтеся, що додаток завжди оновлений до останньої версії, адже оновлення закривають вразливості.

Часті запитання (FAQ)
Питання: Як дізнатися, чи мій акаунт у месенджері зламано?
Відповідь: Якщо ви бачите невідомі повідомлення у ваших чатах або нові активні сесії, ваш акаунт може бути зламано.

Питання: Що робити, якщо отримав підозріле повідомлення?
Відповідь: Не відкривайте вкладення та не переходьте за посиланням. Заблокуйте відправника й повідомте про це адміністрацію месенджера.

36. АЛГОРИТМ ПЕРЕВІРКИ ПІДОЗРІЛИХ ФАЙЛІВ ПЕРЕД ВІДКРИТТЯМ

Підозрілі файли можуть містити віруси, трояни або шпигунське ПЗ. Перевірка перед відкриттям допоможе уникнути зараження вашого пристрою та викрадення даних.

1. Зверніть увагу на джерело файлу.
Не відкривайте файли, отримані від незнайомих людей або невідомих джерел.
Якщо файл отриманий через email чи месенджер, переконайтеся, що відправник є надійним.

2. Перевірте розширення файлу.
Шкідливі файли часто маскуються під документи чи зображення.
Зверніть увагу на подвійні розширення (наприклад, invoice.pdf.exe).
Відомі розширення: .exe, .bat, .scr — часто використовуються для вірусів.

3. Використовуйте антивірус для сканування.
Перед відкриттям файлу перевірте його за допомогою встановленого антивіруса.
Увімкніть опцію захист у реальному часі, щоб виявити загрози під час завантаження.

4. Завантажте файл у "пісочницю".
Використовуйте інструменти для запуску підозрілих файлів у віртуальному середовищі (наприклад, Sandboxie).
Це дозволяє перевірити файл без ризику для основної системи.

5. Скористайтеся онлайн-сканером.
Завантажте файл у безкоштовний онлайн-сервіс для перевірки: VirusTotal, Hybrid Analysis, MetaDefender.

6. Перевірте цифровий підпис.
Для програм і документів перевірте цифровий підпис, щоб переконатися, що файл не було змінено.
У разі відсутності підпису — будьте обережними.

7. Уникайте автоматичного відкриття файлів.
Налаштуйте свій поштовий клієнт чи браузер, щоб файли не відкривалися автоматично після завантаження.

8. Перевірте файли архівів.
Якщо файл надіслано в архіві, розпакуйте його за допомогою надійного архіватора.
Переконайтеся, що в архіві немає прихованих файлів із підозрілими розширеннями.

9. Використовуйте попередній перегляд.
Якщо файл є документом чи зображенням, спробуйте попередній перегляд, щоб переконатися, що він не містить нічого підозрілого.
Не завантажуйте та не відкривайте файли, які вимагають встановлення додаткового ПЗ.

10. Видаліть файл, якщо сумніваєтеся.
Якщо файл неочікуваний або викликає підозру — краще його видалити, щоб уникнути ризиків.
Очистіть кошик після видалення.

Часті запитання (FAQ)
Питання: Як дізнатися, чи файл містить подвійне розширення?
Відповідь: Увімкніть відображення розширень у налаштуваннях файлового менеджера.

37. ПАМ'ЯТКА: ЯК ВИЯВИТИ ШАХРАЙСЬКІ ОГОЛОШЕННЯ В ІНТЕРНЕТІ?

Шахрайські оголошення часто використовують для викрадення даних, фінансового шахрайства або розповсюдження шкідливого ПЗ.

1. Перевіряйте ціну.
Якщо ціна надто низька або виглядає нереалістичною, це може бути шахрайством.
Порівняйте пропозицію з ринковими цінами на аналогічні товари чи послуги.

2. Оцініть інформацію про продавця.
Перевірте відгуки про продавця або компанію на сторонніх ресурсах.
Відсутність контактної інформації або розмиті дані — це підозрілий знак.

3. Звертайте увагу на текст оголошення.
Шахрайські оголошення часто мають орфографічні помилки чи переклад із іншої мови.
Текст може бути надто загальним або містити суперечливу інформацію.

4. Уникайте поспішних рішень.
Якщо продавець наполягає на терміновій оплаті чи швидкому прийнятті рішення, це може бути способом тиску.
Завжди перевіряйте умови перед покупкою.

5. Аналізуйте зображення.
Використовуйте зворотний пошук зображень через Google або TinEye, щоб дізнатися, чи це фото не було скопійоване з інших сайтів.
Шахраї часто використовують зображення з безкоштовних фотостоків.

6. Перевіряйте спосіб оплати.
Уникайте прямих переказів на банківські картки чи електронні гаманці.
Використовуйте платформи з функцією захисту платежів (наприклад, PayPal, OLX Delivery).

7. Будьте уважні з акціями та подарунками.
Якщо оголошення обіцяє неймовірні знижки чи безкоштовні товари, це може бути пасткою.
Перевіряйте умови акцій на офіційному сайті компанії.

8. Остерігайтеся запиту на особисті дані.
Шахраї можуть просити вказати зайву інформацію (паспортні дані, номери карток тощо).
Ніколи не передавайте конфіденційні дані через Інтернет.

9. Уникайте оголошень із незахищеними сайтами.
Перевіряйте, чи сайт використовує HTTPS (значок замка в адресному рядку).
Якщо сайт виглядає застарілим або має багато помилок, краще його уникати.

10. Повідомляйте про шахрайство.
Якщо ви виявили підозріле оголошення, повідомте про нього адміністрацію платформи.
Зверніться до відповідних органів, якщо ви стали жертвою шахрайства.

Часті запитання (FAQ)
Питання: Як визначити, що зображення в оголошенні підроблене?
Відповідь: Використовуйте зворотний пошук зображень, щоб дізнатися, чи це фото використовувалося в інших оголошеннях.

38. ПАМ'ЯТКА: ЯК УНИКАТИ АТАК ЧЕРЕЗ QR-КОДИ

QR-коди зручні, але зловмисники використовують їх для фішингових атак, перенаправлення на шкідливі сайти чи зараження пристроїв вірусами. Уникнення цих ризиків вимагає уважності.

1. Завжди перевіряйте джерело QR-коду.
Використовуйте лише QR-коди від довірених джерел (наприклад, офіційних компаній, організацій).
Не скануйте коди з підозрілих роздаткових матеріалів чи плакатів.

2. Перегляньте посилання перед переходом.
Після сканування перевірте URL-адресу, перш ніж відкривати її.
Уникайте посилань із незвичними або скороченими адресами (наприклад, bit.ly).

3. Використовуйте безпечні програми для сканування.
Використовуйте додатки, які показують посилання перед його відкриттям (наприклад, Kaspersky QR Scanner або Norton QR Scanner).

4. Уникайте QR-кодів у публічних місцях.
Шахраї можуть розміщувати підроблені коди поверх оригінальних (наприклад, на плакатах чи банкоматах).
Переконайтеся, що код не має ознак підробки чи пошкоджень.

5. Не вводьте особисті дані через посилання з QR-коду.
Уникайте введення паролів, PIN-кодів або банківських реквізитів на сайтах, відкритих через QR-код.

Підказка!
Якщо QR-код обіцяє миттєві виграші чи бонуси — це майже завжди шахрайство.

6. Уникайте завантаження файлів через QR-коди.
Шахраї можуть використовувати коди для завантаження шкідливих програм на ваш пристрій.
Завантажуйте програми лише з офіційних магазинів (Google Play, App Store).

7. Звертайте увагу на контекст.
Якщо QR-код з'явився у несподіваному місці (наприклад, наклейка на банкоматі), уникайте його сканування.
Завжди перевіряйте, чи код відповідає джерелу, яке його розмістило.

8. Використовуйте VPN у публічних мережах.
Якщо скануєте QR-код у публічному Wi-Fi, використовуйте VPN для шифрування даних.
Це захистить ваші особисті дані навіть у разі підозрілого посилання.

9. Перевіряйте цифровий сертифікат сайту.
Якщо QR-код веде на сайт, переконайтеся, що він використовує HTTPS (значок замка в адресному рядку).

10. Повідомляйте про підозрілі QR-коди.
Якщо ви помітили підозрілий QR-код у публічному місці, повідомте адміністрацію закладу чи відповідні органи.

Часті запитання (FAQ)
Питання: Чи можна використовувати QR-коди у рекламі?
Відповідь: Так, але завжди перевіряйте, чи рекламодавець є надійним.

39. ШВИДКИЙ ГІД ІЗ ВИДАЛЕННЯ СТАРИХ ОБЛІКОВИХ ЗАПИСІВ

Старі облікові записи, навіть якщо ви їх не використовуєте, можуть стати мішенню для зловмисників. Видалення невикористовуваних акаунтів знижує ризик викрадення даних і забезпечує вашу конфіденційність.

1. Знайдіть усі ваші облікові записи.
Шукайте облікові записи в своїй електронній пошті: перевірте старі листи з підтвердженням реєстрації.
Використовуйте сервіси на кшталт JustDelete.Me для пошуку акаунтів, які можуть бути пов'язані з вашою електронною поштою.

2. Перевірте активність облікового запису.
Увійдіть у старий обліковий запис і перевірте, чи він активний.
Видаліть конфіденційні дані, якщо вони зберігаються у профілі.

3. Знайдіть опцію видалення акаунта.
Увійдіть у налаштування акаунта. Зазвичай опція видалення знаходиться в розділі Конфіденційність або Обліковий запис.
Якщо опція видалення не доступна, зверніться до служби підтримки.

4. Підтвердьте видалення.
Після подачі запиту система може надіслати на вашу пошту код підтвердження або інструкції.
Дотримуйтесь кроків, щоб завершити процес.

5. Видаліть збережені паролі.
Перевірте, чи збережений пароль від цього акаунту в браузері або менеджері паролів.
Видаліть його, щоб уникнути випадкового використання.

6. Очистіть пов'язані додатки та пристрої.
Відключіть акаунт від сторонніх додатків, які можуть використовувати ваші дані.
Перевірте, чи не підключено пристрої до цього акаунта (наприклад, телефони чи планшети).

7. Видаліть акаунти у соцмережах.
У соцмережах, таких як Facebook чи Instagram, процес видалення може зайняти 30 днів.
Переконайтеся, що ви завершили усі кроки для деактивації або видалення.

8. Видаліть акаунти на торгових платформах.
Увійдіть в акаунти на сайтах, як-от Amazon, eBay чи OLX.
Зітріть збережені платіжні дані та видаліть акаунт.

9. Використовуйте інструменти для автоматизації.
Деякі сервіси, як-от AccountKiller, допомагають автоматизувати процес видалення акаунтів.

10. Перевірте результат.
Після завершення процесу видалення спробуйте увійти в акаунт.
Якщо доступ заблоковано, обліковий запис успішно видалено.

Часті запитання (FAQ)
Питання: Що робити, якщо я забув пароль до старого акаунту?
Відповідь: Використовуйте функцію відновлення пароля через електронну пошту або службу підтримки.

40. РЕКОМЕНДАЦІЇ ЩОДО КІБЕРГІГІЄНИ ДЛЯ ДІТЕЙ

Діти все більше часу проводять в Інтернеті, що створює ризики зіткнення з небажаним контентом, шахрайством або кібератаками. Правильні звички допоможуть захистити їх у цифровому світі.

1. Навчіть дітей створювати надійні паролі.
Поясніть, що пароль має бути довгим і складним (мінімум 12 символів).
Нехай не використовують свої імена, дати народження чи іншу легко вгадувану інформацію.

2. Контролюйте їхні дії в Інтернеті.
Використовуйте батьківський контроль на пристроях і в браузерах.
Встановіть обмеження часу на використання Інтернету.

3. Вчіть дітей бути обережними з особистою інформацією.
Поясніть, що не можна ділитися своїм адресою, телефоном чи шкільними даними з незнайомцями.
Розкажіть, як небезпечно публікувати фото з особистими деталями.

4. Перевіряйте, які програми вони встановлюють.
Дозволяйте завантаження додатків лише з офіційних магазинів (Google Play, App Store).
Разом перевіряйте дозволи, які вимагають програми.

5. Навчіть розпізнавати фейкові повідомлення та сайти.
Поясніть, як виглядають підозрілі посилання, шахрайські пропозиції чи фішингові сайти.
Використовуйте приклади, щоб показати, як уникнути таких пасток.

Підказка!
Завжди обговорюйте з дитиною її досвід в Інтернеті. Це допоможе швидко реагувати на можливі проблеми.

6. Установіть антивірус на пристрої дитини.
Використовуйте антивірусне програмне забезпечення з функціями захисту дітей, як-от Norton Family або Kaspersky Safe Kids.

7. Вчіть уникати небажаних контактів.
Поясніть, що не можна додавати до друзів у соцмережах чи месенджерах незнайомих людей.
Розкажіть про небезпеку спілкування з незнайомцями онлайн.

8. Розповідайте про важливість оновлень.
Навчіть дітей регулярно оновлювати додатки та пристрої, щоб уникнути використання вразливостей.

9. Встановіть чіткі правила користування Інтернетом.
Разом визначте, які сайти можна відвідувати, а які — ні.
Створіть список дозволених платформ для навчання, ігор та спілкування.

10. Заохочуйте говорити про незвичні ситуації.
Поясніть, що важливо одразу розповісти дорослим, якщо щось їх налякало або здалося підозрілим в Інтернеті.
Завжди підтримуйте відкритий діалог із дитиною.

41. РЕКОМЕНДАЦІЇ ДЛЯ ЛІТНІХ ЛЮДЕЙ: ЯК УНИКАТИ КІБЕРЗАГРОЗ

Літні люди стають ціллю кіберзлочинців через недостатню обізнаність у цифрових технологіях. Виконання простих рекомендацій допоможе захистити себе від шахрайства та втрати даних.

1. Використовуйте складні паролі.
Створюйте унікальні паролі для кожного облікового запису.
Використовуйте комбінації цифр, літер та символів

2. Уникайте підозрілих посилань.
Не переходьте за посиланнями в листах чи повідомленнях від незнайомців.
Навіть якщо лист виглядає офіційно, перевіряйте його справжність.

3. Не передавайте особисту інформацію.
Нікому не повідомляйте PIN-коди, паролі чи номери банківських карт.
Справжні організації ніколи не запитують ці дані через телефон чи електронну пошту.

4. Установіть антивірус.
Використовуйте антивірусне програмне забезпечення для захисту пристроїв від вірусів і шкідливих програм.
Переконайтеся, що антивірус регулярно оновлюється.

5. Використовуйте лише перевірені джерела.
Завантажуйте програми та файли тільки з офіційних сайтів.
Уникайте програм, які пропонують безкоштовні бонуси чи швидке збагачення.

6. Захистіть свою електронну пошту.
Увімкніть двофакторну автентифікацію.
Не відкривайте вкладення в листах від незнайомих людей.

7. Будьте обережними з соціальними мережами.
Не додавайте до друзів незнайомих людей.
Не публікуйте особисту інформацію (адресу, телефон, деталі подорожей).

8. Уникайте публічних Wi-Fi.
Не вводьте паролі чи банківські дані в публічних мережах.
Використовуйте VPN для захисту даних, якщо це необхідно.

9. Регулярно оновлюйте пристрої.
Оновлення програмного забезпечення містять виправлення вразливостей, які можуть використовувати зловмисники.
Увімкніть автоматичне оновлення, якщо це можливо.

10. Звертайтеся до перевірених осіб за допомогою.
Якщо ви не впевнені у справжності листа, повідомлення чи дзвінка, зверніться до знайомих або технічної підтримки.
Уникайте поспішних рішень, які вимагають термінових дій.

Часті запитання (FAQ)
Питання: Як дізнатися, що сайт є безпечним?
Відповідь: Перевірте, чи сайт використовує HTTPS (значок замка в адресному рядку).

Криптовалюти забезпечують анонімність і децентралізацію, але через це вони також стають ціллю для хакерів і шахраїв. Дотримання простих правил допоможе захистити ваші активи.

1. Використовуйте надійний гаманець.
Виберіть перевірений криптогаманець:
Холодний гаманець (апаратний) для довгострокового зберігання.
Гарячий гаманець (онлайн) для щоденних операцій.

2. Захистіть свій гаманець паролем.
Створіть складний і унікальний пароль.
Використовуйте менеджер паролів для зберігання ключів і паролів.

3. Увімкніть двофакторну автентифікацію (2FA).
Налаштуйте 2FA для входу в криптогаманець або біржу.
Використовуйте автентифікаційний додаток (Google Authenticator, Authy).

4. Зберігайте резервні копії.
Збережіть seed-фразу (12-24 слова) для відновлення гаманця.
Не зберігайте фразу в електронному вигляді. Напишіть її на папері та сховайте у безпечному місці.

5. Перевіряйте адреси транзакцій.
Завжди уважно перевіряйте адресу, на яку відправляєте кошти.
Використовуйте функцію копіювання-вставлення, але обов'язково перевірте адресу після вставлення.

Підказка!
Ніколи не діліться приватним ключем або seed-фразою з іншими людьми.

6. Використовуйте тільки перевірені біржі.
Реєструйтесь лише на надійних криптобіржах із високим рівнем безпеки, таких як Binance, Coinbase чи Kraken.
Перевіряйте відгуки про біржу перед використанням.

7. Уникайте публічних Wi-Fi мереж.
Не здійснюйте транзакції через загальнодоступні мережі.
Якщо це необхідно, використовуйте VPN для шифрування трафіку.

8. Будьте обережними з фішингом.
Уникайте переходу за посиланнями з email чи повідомлень, які запитують ваші дані для входу.
Завжди заходьте на сайт біржі вручну, вводячи URL-адресу в браузері.

9. Розподіляйте активи.
Не зберігайте всі кошти в одному гаманці чи на одній платформі.
Використовуйте різні гаманці для різних цілей.

10. Слідкуйте за оновленнями безпеки.
Завжди оновлюйте криптогаманці та програмне забезпечення для захисту від нових загроз.
Використовуйте останні версії антивірусу на пристроях, де ви працюєте з криптовалютами.

43. ГІД ІЗ ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ДЛЯ ЗАХИСТУ РОЗУМНИХ ПРИСТРОЇВ

Розумні пристрої (камери, термостати, голосові помічники) спрощують життя, але через недостатній захист можуть стати ціллю для хакерів. Дотримання цих рекомендацій допоможе уникнути ризиків.

1. Використовуйте надійний роутер.
Встановіть пароль для Wi-Fi, який складно зламати.
Увімкніть шифрування WPA3 (або WPA2, якщо WPA3 недоступне).
Вимкніть функцію WPS (Wi-Fi Protected Setup), щоб знизити ризик атаки.

2. Змініть стандартні паролі.
Після налаштування пристрою змініть стандартний логін і пароль.
Створіть складний пароль, який містить великі й малі літери, цифри та спеціальні символи.

3. Використовуйте окрему мережу для IoT.
Створіть гостьову мережу на роутері для всіх пристроїв IoT.
Це ізолює основну мережу, забезпечуючи додатковий захист.

4. Увімкніть автоматичне оновлення програмного забезпечення.
Переконайтеся, що всі пристрої IoT отримують оновлення прошивки автоматично.
Оновлення виправляють вразливості, які можуть використовувати хакери.

5. Перевіряйте доступ до пристроїв.
Обмежте доступ до пристроїв лише з довірених IP-адрес.
Використовуйте функції моніторингу трафіку, якщо вони доступні.

6. Використовуйте фаєрвол.
Активуйте фаєрвол на роутері, щоб блокувати небезпечний трафік.
Додатково можна налаштувати програмний фаєрвол для моніторингу підключень.

7. Вимкніть зайві функції.
Відключіть функції віддаленого доступу, якщо вони не використовуються.
Вимкніть мікрофон чи камеру пристрою, коли вони не потрібні.

8. Використовуйте VPN для домашньої мережі.
Налаштуйте VPN на роутері, щоб шифрувати весь трафік IoT-пристроїв.
Це особливо важливо для пристроїв, які не мають вбудованого захисту.

9. Створюйте резервні копії налаштувань.
Для складних систем, як-от розумні термостати чи камери спостереження, створюйте резервні копії налаштувань.
Це допоможе швидко відновити роботу пристрою у разі атаки.

10. Використовуйте спеціалізовані інструменти захисту IoT.
Сервіси, як-от Bitdefender Box чи Trend Micro Home Network Security, дозволяють моніторити активність пристроїв у реальному часі.
Ці рішення надають додатковий захист від кібератак.

Часті запитання (FAQ)
Питання: Чи потрібно відключати IoT-пристрої, якщо вони не використовуються?
Відповідь: Так, відключення пристроїв, які не використовуються, знижує ризик атак.

44. ШВИДКИЙ ГІД ІЗ БЕЗПЕЧНОГО ВИКОРИСТАННЯ ВІДЕОКОНФЕРЕНЦІЙ

Відеоконференції дозволяють працювати та спілкуватися дистанційно, але вони також є мішенню для зловмисників.

1. Використовуйте перевірені платформи.
Вибирайте популярні та надійні сервіси, такі як Zoom, Microsoft Teams, Google Meet.
Переконайтеся, що програма регулярно оновлюється.

2. Захищайте свої зустрічі паролем.
Увімкніть опцію створення пароля для доступу до кожної конференції.
Надавайте пароль лише запрошеним учасникам.

3. Використовуйте функцію очікування (Waiting Room).
Активуйте зал очікування, щоб вручну перевіряти і впускати учасників.
Це дозволить уникнути небажаних гостей.

4. Увімкніть шифрування.
Переконайтеся, що платформа підтримує наскрізне шифрування.
Перевірте налаштування шифрування в програмі перед початком зустрічі.

5. Контролюйте доступ учасників.
Вимикайте можливість змінювати налаштування зустрічі для всіх, окрім організатора.
Обмежте можливість демонстрації екрана лише для організатора.

Підказка!
Не публікуйте ідентифікатори зустрічей або посилання у відкритих джерелах, таких як соцмережі.

6. Використовуйте унікальні ідентифікатори зустрічей.
Уникайте використання одного й того ж ID для різних зустрічей.
Створюйте новий ідентифікатор для кожної події.

7. Контролюйте аудіо- та відеопотоки.
Вимикайте мікрофони та камери учасників, якщо вони не говорять.
Це зменшує ризик розповсюдження небажаного контенту.

8. Перевіряйте учасників.
Переконайтеся, що всі учасники є запрошеними.
Видаляйте незнайомих або підозрілих осіб із зустрічі.

9. Захищайте запис зустрічей.
Якщо ви записуєте зустріч, зберігайте файл у захищеному місці (зашифрований диск або хмарне сховище).
Не діліться записом без необхідності.

10. Оновлюйте платформу.
Регулярно оновлюйте програмне забезпечення для відеоконференцій.
Нові версії часто містять виправлення вразливостей.

Часті запитання (FAQ)
Питання: Чи потрібен пароль для кожної зустрічі?
Відповідь: Так, це знижує ризик несанкціонованого доступу.

Питання: Як дізнатися, чи платформа підтримує шифрування?
Відповідь: Перевірте інформацію на офіційному сайті або в налаштуваннях програми.

45. ПАМ'ЯТКА: ЯК ЗАХИСТИТИ СВОЮ ЕЛЕКТРОННУ ПОШТУ

Електронна пошта є центральним вузлом вашої цифрової діяльності. Втрата доступу до неї може призвести до викрадення акаунтів, витоку даних або фінансових втрат.

1. Використовуйте унікальний пароль.
Створюйте складний пароль щонайменше з 12 символів, включаючи літери, цифри та спеціальні символи.
Уникайте паролів, які легко вгадати (дата народження, ім'я тощо).

2. Увімкніть двофакторну автентифікацію (2FA).
Додайте другий рівень захисту через SMS, автентифікаційний додаток або фізичний ключ.
Це унеможливить доступ до пошти без додаткового підтвердження.

3. Оновлюйте пароль регулярно.
Змінюйте пароль щонайменше раз на 6 місяців.
Виконуйте зміну негайно, якщо є підозра на витік даних.

4. Уникайте використання публічних Wi-Fi мереж.
Якщо необхідно скористатися публічним Wi-Fi, увімкніть VPN для шифрування даних.
Не вводьте конфіденційні дані під час підключення до загальнодоступних мереж.

5. Перевіряйте підозрілі листи.
Уникайте відкриття листів із невідомих адрес.
Не натискайте на посилання та не завантажуйте вкладення з підозрілих повідомлень.

6. Перевіряйте активність облікового запису.
У налаштуваннях поштового сервісу переглядайте історію входів.
Завершуйте сесії на пристроях, які більше не використовуєте.

7. Використовуйте HTTPS.
Переконайтеся, що ваш поштовий сервіс працює через захищене з'єднання (значок замка в адресному рядку).
Завжди перевіряйте, що сайт є офіційним.

8. Увімкніть фільтрацію спаму.
Активуйте автоматичні фільтри для підозрілих листів.
Регулярно перевіряйте папку "Спам", щоб уникнути пропуску важливих повідомлень.

9. Використовуйте окремі акаунти.
Заведіть різні електронні адреси для роботи, особистих справ і реєстрації на сайтах.
Це зменшить ризики витоку даних із основного облікового запису.

10. Оновлюйте пристрої та програми.
Завжди використовуйте останню версію операційної системи та поштового клієнта.
Оновлення виправляють вразливості, які можуть використовувати зловмисники.

Часті запитання (FAQ)
Питання: Що робити, якщо я випадково відкрив підозрілий лист?
Відповідь: Не переходьте за посиланнями, не завантажуйте вкладення та перевірте акаунт на наявність підозрілої активності.

Питання: Чи потрібно змінювати пароль після витоку даних?
Відповідь: Так, негайно змініть пароль та увімкніть 2FA.

46. ІНСТРУКЦІЯ: ЯК ПЕРЕВІРИТИ БЕЗПЕКУ НАЛАШТУВАНЬ БРАУЗЕРА?

Браузер — це головний інструмент доступу до Інтернету, але неправильно налаштований браузер може стати джерелом загроз. Перевірка та налаштування допоможуть захистити ваші дані й пристрій.

1. Перевірте оновлення браузера.
Переконайтеся, що ваш браузер оновлено до останньої версії.
Включіть автоматичне оновлення у налаштуваннях.

2. Перевірте безпеку розширень.
Вимкніть і видаліть розширення, якими ви більше не користуєтесь.
Завантажуйте розширення лише з офіційного магазину браузера.

3. Увімкніть блокування файлів cookie третіх сторін.
Перейдіть у Налаштування → Конфіденційність та безпека → Файли cookie.
Увімкніть опцію "Блокувати файли cookie третіх сторін".

4. Увімкніть захист від фішингу та шкідливих сайтів.
У Налаштування → Безпека активуйте функцію "Захист від небезпечних сайтів".
Перевірте, чи браузер попереджає про підозрілі сторінки.

5. Перевірте дозволи сайтів.
У Налаштування → Конфіденційність та безпека → Дозволи сайтів перевірте, які сайти мають доступ до камери, мікрофона, місцезнаходження.
Вимкніть доступ для сайтів, яким ви не довіряєте.

6. Установіть розширення для блокування реклами.
Використовуйте перевірені розширення, як-от AdBlock або uBlock Origin.
Це допоможе уникнути небажаної реклами та зловмисних скриптів.

7. Перевірте налаштування HTTPS.
Увімкніть опцію "Завжди використовувати HTTPS" у налаштуваннях безпеки.
Це забезпечить шифрування вашого з'єднання із сайтами.

8. Очистіть кеш і файли cookie.
Регулярно видаляйте кеш і файли cookie, щоб уникнути накопичення зайвих даних.
У Налаштування → Конфіденційність → Очистити дані вебперегляду виберіть параметри для видалення.

9. Вимкніть автозаповнення.
У Налаштування → Паролі та автозаповнення вимкніть функцію автоматичного збереження паролів і даних карток.
Використовуйте менеджери паролів для збереження даних у зашифрованому вигляді.

10. Перевірте звіти безпеки.
У деяких браузерах, наприклад Google Chrome, є розділ Перевірка безпеки.
Використовуйте його для швидкого аналізу стану безпеки браузера.

Часті запитання (FAQ)
Питання: Чи достатньо стандартних налаштувань браузера для безпеки?
Відповідь: Базових налаштувань може бути недостатньо. Додаткові налаштування й розширення підвищують рівень захисту.

47. ШВИДКИЙ ГІД ІЗ БЛОКУВАННЯ ШКІДЛИВИХ РОЗШИРЕНЬ У БРАУЗЕРІ

Шкідливі розширення можуть збирати ваші дані, вповільнювати роботу браузера чи спричиняти витік інформації. Блокування таких розширень допоможе уникнути небезпек.

1. Перевірте встановлені розширення.
У браузері відкрийте розділ Розширення або Додатки:
Google Chrome: Налаштування → Розширення.
Firefox: Меню → Додатки та теми → Розширення.
Edge: Налаштування → Розширення.

2. Видаліть зайві розширення.
Видаліть усі розширення, якими ви не користуєтесь.
Особливо зверніть увагу на ті, які встановились без вашого відома.

3. Перевірте джерело розширень.
Завантажуйте розширення лише з офіційних магазинів:
Chrome Web Store.
Firefox Add-ons.
Edge Add-ons.
Уникайте встановлення розширень із ненадійних сайтів.

4. Перевіряйте дозволи.
Під час встановлення переглядайте, які дозволи запитує розширення:
Якщо розширення запитує доступ до всієї історії переглядів або особистих даних, подумайте, чи це виправдано.

5. Використовуйте захист браузера.
Деякі браузери автоматично перевіряють розширення на шкідливість.
У Google Chrome увімкніть функцію Розширений захист у розділі Безпека.

6. Установіть розширення для захисту.
Використовуйте спеціалізовані розширення для моніторингу безпеки, наприклад:
Malwarebytes Browser Guard.
uBlock Origin для блокування реклами й небезпечних сайтів.

7. Увімкніть сповіщення про підозрілі розширення.
У налаштуваннях браузера активуйте функцію, яка сповіщатиме вас про шкідливі або автоматично встановлені розширення.

8. Регулярно оновлюйте розширення.
Перевіряйте, чи всі встановлені розширення оновлені до останньої версії.
Більшість браузерів оновлюють їх автоматично, але краще перевіряти це вручну.

9. Заблокуйте встановлення розширень з неперевірених джерел.
У налаштуваннях браузера увімкніть опцію "Дозволити встановлення тільки з офіційних магазинів".

10. Скануйте розширення за допомогою антивірусу.
Використовуйте інструменти для аналізу підозрілих розширень, наприклад, VirusTotal.
Перевіряйте нові розширення на наявність шкідливого коду перед використанням.

Часті запитання (FAQ)
Питання: Як дізнатися, чи розширення шкідливе?
Відповідь: Якщо розширення викликає появу небажаних вікон, змінює налаштування браузера або збирає зайві дані, воно може бути шкідливим.

48. ШВИДКИЙ ГІД ІЗ НАЛАШТУВАННЯ VPN

VPN (Virtual Private Network) створює захищений тунель для передачі ваших даних, приховує вашу IP-адресу та забезпечує безпеку в Інтернеті. Це особливо важливо при використанні публічних Wi-Fi мереж або доступі до конфіденційної інформації.

1. Виберіть надійний VPN-сервіс.
Рекомендується використовувати перевірені сервіси, наприклад:
NordVPN.
ExpressVPN.
ProtonVPN.
Уникайте безкоштовних VPN, які можуть збирати ваші дані.

2. Завантажте додаток VPN.
Перейдіть на офіційний сайт VPN-сервісу.
Завантажте програму для вашого пристрою (Windows, macOS, Android, iOS).
Уникайте сторонніх джерел для завантаження.

3. Зареєструйтесь і ввійдіть.
Створіть обліковий запис на платформі VPN.
Введіть свої дані для входу в додаток після встановлення.

4. Виберіть сервер.
Виберіть сервер у потрібній країні, залежно від ваших потреб:
Для доступу до регіонального контенту оберіть сервер у відповідній країні.
Для максимальної швидкості оберіть сервер, який знаходиться ближче до вашого місця розташування.

5. Увімкніть VPN.
Натисніть кнопку Connect (або "Підключити") в додатку.
Переконайтеся, що підключення успішне, перевіривши зміну вашої IP-адреси.

6. Використовуйте функцію Kill Switch.
Активуйте Kill Switch у налаштуваннях VPN.
Це дозволить автоматично розірвати інтернет-з'єднання у разі відключення VPN, запобігаючи витоку даних.

7. Перевірте шифрування.
Переконайтеся, що VPN використовує сучасні протоколи безпеки:
OpenVPN.
WireGuard.
IKEv2/IPSec.

8. Налаштуйте автозапуск.
У налаштуваннях VPN увімкніть функцію автозапуску при увімкненні пристрою.
Це гарантує, що ви завжди будете захищені.

9. Уникайте витоку DNS.
Перевірте налаштування DNS у VPN-додатку.
Використовуйте інструменти для перевірки витоку DNS, наприклад dnsleaktest.com.

10. Використовуйте VPN для всіх пристроїв.
Налаштуйте VPN на:
Смартфонах і планшетах.
Комп'ютерах і ноутбуках.
Роутері — це дозволить захистити всі пристрої у вашій домашній мережі.

49. 10 ПОРАД ДЛЯ БЕЗПЕЧНОГО ОНЛАЙН-ШОПІНГУ

Онлайн-шопінг значно спрощує процес покупок, але також створює ризики: шахрайство, викрадення даних чи зловмисні сайти. Дотримуючись цих порад, ви захистите себе від неприємностей.

1. Використовуйте лише надійні сайти.
Купуйте товари на перевірених сайтах із хорошою репутацією.
Адреса сайту повинна починатися з HTTPS, а в адресному рядку має бути значок замка.

2. Обирайте надійні способи оплати.
Використовуйте безпечні платіжні системи, як-от PayPal, Apple Pay, Google Pay.
Уникайте передоплат на банківські картки або електронні гаманці незнайомих продавців.

3. Використовуйте одноразові платіжні картки.
Для покупок в Інтернеті заведіть окрему картку або використовуйте віртуальну.
Це дозволить обмежити доступ шахраїв до ваших основних рахунків.

4. Уникайте публічних Wi-Fi мереж.
Не вводьте платіжні дані в публічних мережах.
Якщо це необхідно, використовуйте VPN для шифрування трафіку.

5. Читайте відгуки про продавця.
Перевіряйте рейтинг та відгуки інших покупців.
Якщо сайт виглядає новим або має мало відгуків, будьте обережними.

Підказка!
Якщо пропозиція здається надто привабливою, це може бути шахрайство.
Перевірте ціну товару на інших сайтах.

6. Створюйте складні паролі для акаунтів.
Використовуйте унікальні паролі для кожного інтернет-магазину.
Увімкніть двофакторну автентифікацію, якщо це можливо.

7. Перевіряйте умови доставки та повернення.
Ознайомтеся з політикою повернення товарів і умовами доставки.
Надійні магазини завжди мають чітко прописані правила.

8. Перевіряйте електронні листи від продавців.
Уникайте переходу за посиланнями в листах із підозрілих адрес.
Замість цього вручну вводьте адресу сайту в браузері.

9. Обмежуйте персональні дані.
Вказуйте лише необхідну інформацію для покупки (наприклад, адресу доставки).
Не повідомляйте зайвих даних, як-от номер паспорта чи ідентифікаційний код.

10. Зберігайте підтвердження транзакцій.
Завантажуйте квитанції та підтвердження замовлень.
Це допоможе вирішити суперечки з продавцем, якщо виникнуть проблеми.

Часті запитання (FAQ)
Питання: Чи безпечно зберігати платіжні дані на сайтах?
Відповідь: Зберігайте дані лише на перевірених сайтах із високим рівнем захисту.
Для додаткової безпеки краще не зберігати їх узагалі.

50. ПАМ'ЯТКА: БЕЗПЕКА ПІДЛІТКІВ У СОЦІАЛЬНИХ МЕРЕЖАХ

Соціальні мережі допомагають підліткам спілкуватися, навчатися та розважатися, але також несуть ризики: кібербулінг, витік особистих даних, маніпуляції чи контакти з небезпечними людьми. Правильна підтримка та контроль допоможуть уникнути небезпек.

1. Навчіть основам приватності.
Поясніть, що публічні пости та фото можуть бути доступні будь-кому.
Встановіть приватність облікових записів (видимість тільки для друзів).

2. Перегляньте налаштування конфіденційності.
Допоможіть дитині налаштувати приватність у соцмережах:
Хто може бачити пости.
Хто може надсилати повідомлення.
Хто може коментувати.

3. Обмежте особисту інформацію.
Не дозволяйте публікувати номер телефону, адресу чи деталі про школу.
Поясніть, що особиста інформація може використовуватись зловмисниками.

4. Навчіть уникати незнайомців.
Підліток повинен додавати до друзів лише знайомих людей.
Розкажіть, як уникати спілкування з підозрілими акаунтами.

5. Говоріть про небезпеку кібербулінгу.
Поясніть, як діяти у разі отримання образливих повідомлень:
Не відповідати.
Блокувати кривдника.
Повідомити дорослих чи адміністрацію платформи.

6. Обмежте час у соцмережах.
Разом встановіть ліміт часу на користування соцмережами.
Використовуйте функції контролю часу на пристрої.

7. Уникайте небажаного контенту.
Використовуйте фільтри для блокування небезпечного чи неприйнятного контенту.
Поясніть, чому важливо уникати сумнівних груп і сторінок.

8. Перевіряйте контакти дитини.
Поясніть, що батьки можуть перевіряти список друзів або контакти за згодою дитини.
Це допоможе виявити підозрілих осіб.

9. Розповідайте про фішинг і шахрайство.
Поясніть, як розпізнавати шахрайські посилання чи підроблені акаунти.
Навчіть перевіряти URL перед переходом.

10. Встановіть довірливі стосунки.
Підліток має відчувати, що може звернутися до вас у разі небезпеки.
Не критикуйте, а допомагайте розв'язати проблеми.

Часті запитання (FAQ)
Питання: Як дізнатися, що підліток має проблеми у соцмережах?
Відповідь: Ознаки: уникання спілкування, роздратованість після використання телефону, різка зміна настрою.

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva : International Organization for Standardization, 2022.

2. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. Geneva : International Organization for Standardization, 2022.

3. NIST Cybersecurity Framework (CSF) 2.0. Framework for Improving Critical Infrastructure Cybersecurity. Gaithersburg : NIST, 2024. URL: https://www.nist.gov/cyberframework (дата звернення: 10.01.2026).

4. Information Security Continuous Monitoring (ISCM). Special Publication 800-137. Gaithersburg : NIST, 2023. URL: https://csrc.nist.gov (дата звернення: 10.01.2026).

5. Cybersecurity Awareness and Hygiene. Brussels : ENISA, 2023. URL: https://www.enisa.europa.eu (дата звернення: 10.01.2026).

6. Guidelines on Incident Handling. Brussels : ENISA, 2022. URL: https://www.enisa.europa.eu (дата звернення: 10.01.2026).

7. EU Cybersecurity Strategy for the Digital Decade. Brussels : European Union, 2021. URL: https://digital-strategy.ec.europa.eu (дата звернення: 10.01.2026).

8. Cross-Sector Cybersecurity Performance Goals (CPGs). Washington : CISA, 2023. URL: https://www.cisa.gov (дата звернення: 10.01.2026).

9. Small Organisation Cyber Security Guidance. London : NCSC, 2023. URL: https://www.ncsc.gov.uk (дата звернення: 10.01.2026).

10. Security Awareness Toolkit. Bethesda : SANS Institute, 2024. URL: https://www.sans.org (дата звернення: 10.01.2026).

11. Mitnick, K., Simon, W. The Art of Deception: Controlling the Human Element of Security. Indianapolis : Wiley Publishing, 2002. 368 p.

12. Social Engineering Threat Landscape. Brussels : ENISA, 2023. URL: https://www.enisa.europa.eu (дата звернення: 10.01.2026).

13. OWASP Top 10: Web Application Security Risks. OWASP, 2021. URL: https://owasp.org (дата звернення: 10.01.2026).

14. MITRE ATT&CK Framework. Bedford : MITRE, 2024. URL: https://attack.mitre.org (дата звернення: 10.01.2026).

15. Online Safety Fundamentals. Google Safety Center, 2024. URL: https://safety.google (дата звернення: 10.01.2026).
16. Digital Citizenship Curriculum. Common Sense Education, 2023. URL: https://www.commonsense.org/education (дата звернення: 10.01.2026).
17. Youth Online Safety Resources. Meta Safety, 2024. URL: https://about.meta.com/safety (дата звернення: 10.01.2026).
18. General Data Protection Regulation (GDPR). Regulation (EU) 2016/679 of the European Parliament and of the Council. Brussels : European Union, 2016.
19. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI (зі змінами). URL: https://zakon.rada.gov.ua (дата звернення: 10.01.2026).
20. OECD Privacy Guidelines. Paris : OECD, 2022. URL: https://www.oecd.org (дата звернення: 10.01.2026).
21. Google Workspace Security Whitepaper. Mountain View : Google LLC, 2024. URL: https://security.google (дата звернення: 10.01.2026).
22. Cloud Security Alliance Guidance. Cloud Security Alliance, 2023. URL: https://cloudsecurityalliance.org (дата звернення: 10.01.2026).