Ера Інтернету

Мрієш стати супергероєм? Ласкаво просимо в еру Інтернету. Володіння новими технологіями дозволяє відкрити цілий світ в усьому його розмаїтті. Ми впевнені, що ти вже випробував на собі «ефект присутності», коли за допомогою Інтернету миттєво зв’язувався з людьми по всьому світу і був у курсі будь-яких подій. Хіба це не дивно?! Кілька кліків — і в твоєму розпорядженні будь-яка інформація, музика або фільми з хмарного сховища даних. А за знаннями зовсім не обов’язково їхати до столиці — Інтернет дозволяє створити глобальне наукове середовище онлайн і здобувати освіту безкоштовно.

І постійно з’являється щось нове. У 2013 році компанія Google анонсувала окуляри з доповненою реальністю, які поєднують навколишнє середовище і зображення, згенероване комп’ютером. Інтернет — це надможливості! Чи використовуєш ти їх?

Що дає Інтернет

Як щодо того, щоб вирушити у навколосвітню подорож? Розпочни, наприклад, із дослідження віддалених вулканічних Галапагоських островів. Побувай в лабораторії живої природи Дарвіна! Любителі піших прогулянок можуть поблукати вуличками Барселони або пройти складним гірським маршрутом до Гранд-Каньйону. Колекція «Чудес світу» включає найвідоміші місця планети.
Це дивовижне зібрання об'єктів всесвітньої спадщини ЮНЕСКО.
Арт-проект Google розкрив для тебе двері більш ніж 200 музеїв із 40 країн світу. Із українських музеїв тут представлено Музей Івана Гончара (Національний центр народної культури).

Ти можеш роздивитися шедеври світового мистецтва в найдрібніших деталях, як не зміг би цього зробити навіть у музеї.

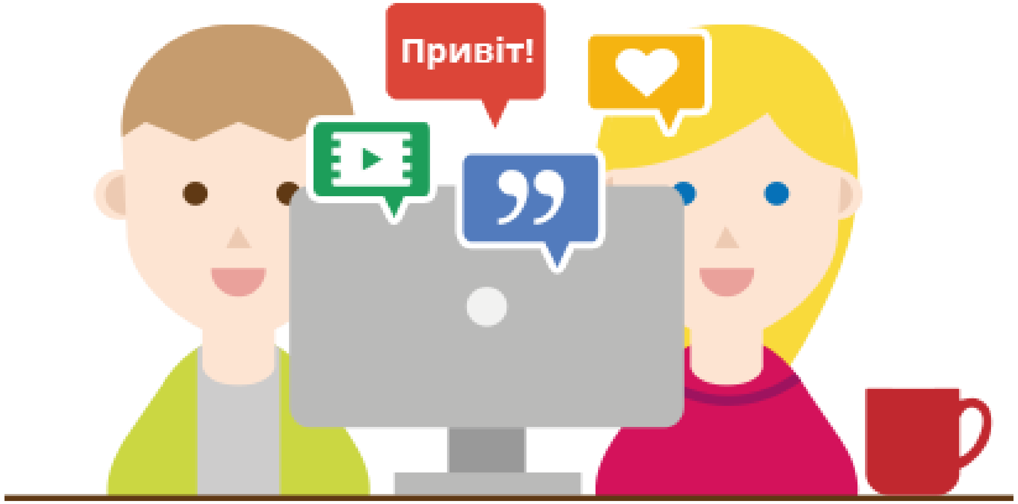
А хочеш досліджувати історичні архіви, які неможливо побачити в реальному житті? З Інтернетом ти маєш доступ практично до будь-якої інформації.
Читай книги, вивчай рідкісні мови, будь у курсі передових наукових публікацій — відкривай світ, межі якого стирає Інтернет. Тепер тобі доступні освітні програми будь-якого рівня — від школи та коледжу до кращого університету. А з проектом «Вікіпедія» ти, звісно, вже познайомився, коли готувався до уроків або писав реферат.
«А розваги?» — спитаєш ти. Звичайно! Телеконтент, колекції фільмів художнього та документального жанрів, мультфільми... А може, краще купити квиток онлайн і піти з друзями до кінотеатру?

Мультимовна освітня Академія Хана

Я в Інтернеті

Інтернет дає тобі новий ступінь свободи, який ні з чим не порівняти. Завдяки Інтернету ти можеш реалізувати себе в будь-якій галузі, заявити світові про свої захоплення, таланти та плани на майбутнє. Хіба не надихає приклад 16-річного експерта з безпеки Android Хіроми Якура та 17-річного Ора Саги — учасника космічної програми з власним проектом безпілотника на Місяць?! Або онлайн-кондитерська Аманди Лім, чи 15-річна Анна Дрованді — президент компанії з виробництва і продажу сирів та йогуртів? Чи підозрював Джастін Бібер, що ролик, викладений на YouTube, зробить його зіркою? Що заважає тобі досягти таких самих результатів? Почни свій проект, збери свою спільноту!

І пам’ятай: завжди можна безпосередньо звернутися за допомогою до професіоналів і навіть отримати фінансову підтримку. Адже ми вже казали, що в Інтернеті немає жодних бар’єрів і нічого неможливого!



Літературний проект Adora Svitak

Технічні аспекти

Інтернет став звичною частиною нашого повсякденного життя. Ми використовуємо його, не замислюючись, як телевізор або мікрохвильову піч. Клік-клік — усе дуже просто. Розробникам справді вдалося зробити складні й наукомісткі технології дружніми для користувача.

Однак іноді ця легкість оманлива, тому важливо засвоїти базові принципи безпечного використання Інтернету.

ЗМІСТ

Програмне забезпечення

Для перегляду веб-сайтів використовується спеціальне програмне забезпечення — браузер. Різні налаштування браузера покликані зробити користування Інтернетом простим та безпечним.

Наприклад, у браузері Google Chrome опція збереження паролів спрощує доступ до регулярно відвідуваних сайтів. Достатньо один раз ввести логін та пароль, застосувати функцію «запам'ятати пароль» — і надалі браузер вводитиме цю інформацію автоматично. Але використовувати таку функцію можна лише на персональному пристрої, до якого ніхто, крім тебе, не має доступу.

Функція автозаповнення дозволяє один раз ввести ім'я, адресу, номер телефону, адресу електронної пошти та іншу контактну інформацію, щоб програма її запам'ятала й автоматично пропонувала під час повторного введення облікових даних. Щоб збереженою інформацією не могли скористатися зловмисники, вмикай цю опцію браузера, лише коли вводиш неконфіденційну інформацію.

У Google Chrome історія відвіданих сторінок зберігається автоматично. Це зручно, якщо потрібно повернутися назад на сторінку або відновити події. Працюючи на громадському комп'ютері, краще використовувати режим анонімного перегляду, у якому історія не зберігається.

Спливаючі вікна найчастіше використовуються для розміщення в мережі рекламних повідомлень. Google Chrome автоматично блокує спливаючі вікна, щоб вони не заважали. При цьому в адресному рядку з'являється значок:

Браузери дозволяють зберігати файли з Інтернету на локальному диску комп'ютера. Під час завантаження файла (наприклад, із розширенням EXE, DLL або BAT) браузер зробить запит про підтвердження операції. Це дозволяє запобігти автоматичному завантаженню шкідливого програмного забезпечення на твій комп'ютер. Якщо URL файла, що завантажується є в актуальному списку шкідливих веб-сайтів — браузер видасть попередження.

Безпека підключення

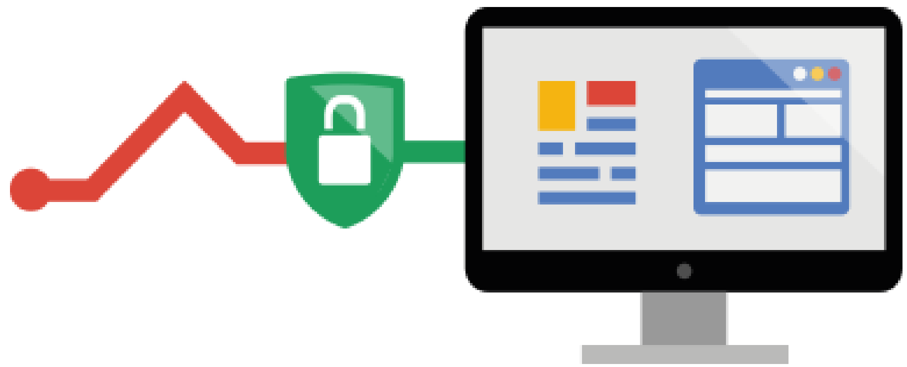
Способи доступу в Інтернет різняться за ступенем надійності. Найвразливішим вважається вихід в Інтернет через громадські комп'ютери або публічні Wi-Fi-мережі. Основний ризик — крадіжка пароля від акаунтів у соціальних мережах, від пошти або електронних гаманців. Тому намагайся не використовувати платіжні системи та інші важливі сервіси під час такого підключення.

Заходячи на сайт, стеж, щоб його адреса починалася з **https://**. Ще краще, якщо поряд буде стояти іконка замка:

Перше означає, що з'єднання з веб-сайтом зашифроване, друге — що воно захищене і безпечне.

Додаткова ступінь захисту — сертифікат надійності. Якщо сайт має такий сертифікат, то його індикатор з'явиться на зеленому тлі між значком замка та URL-адресою.

Встановивши домашній Wi-Fi, обов'язково захисти мережу паролем, використовуй власну комбінацію символів, а не ту, яка пропонується за замовчуванням. У налаштуваннях доступу обирай більш надійний протокол WPA2.



Паролі

Ідентифікатором користувача у віртуальному середовищі є ім’я (логін), вибране під час реєстрації. Логін використовується разом із паролем, який потрібен для аутентифікації користувача. Правильна пара «логін — пароль» забезпечує вхід до системи.

Багато сайтів (особливо це стосується платіжних веб-ресурсів та систем онлайн-банкінгу) застосовують ефективніший спосіб двоетапної аутентифікації з підтвердженням пароля через одноразовий код, який приходить по SMS або електронною поштою. Ця опція є й у поштовому сервісі Gmail. Крадіжка пароля від електронної пошти відкриває зловмисникам несанкціонований доступ до багатьох ресурсів від імені користувача, тому слід максимально захистити свій акаунт.

Але насамперед ти маєш знати, як самому підвищити надійність пароля:

1. **Ідеальний пароль — це комбінація з різних 8 та більше літер, цифр, а також знаків пунктуації та символів.**

2. **Використовуй різні паролі для кожного облікового запису.**

3. **Регулярно змінюй свої паролі.**

4. **Для генерації та зберігання паролів користуйся спеціальними програмами.**

Захист комп’ютера від вірусів

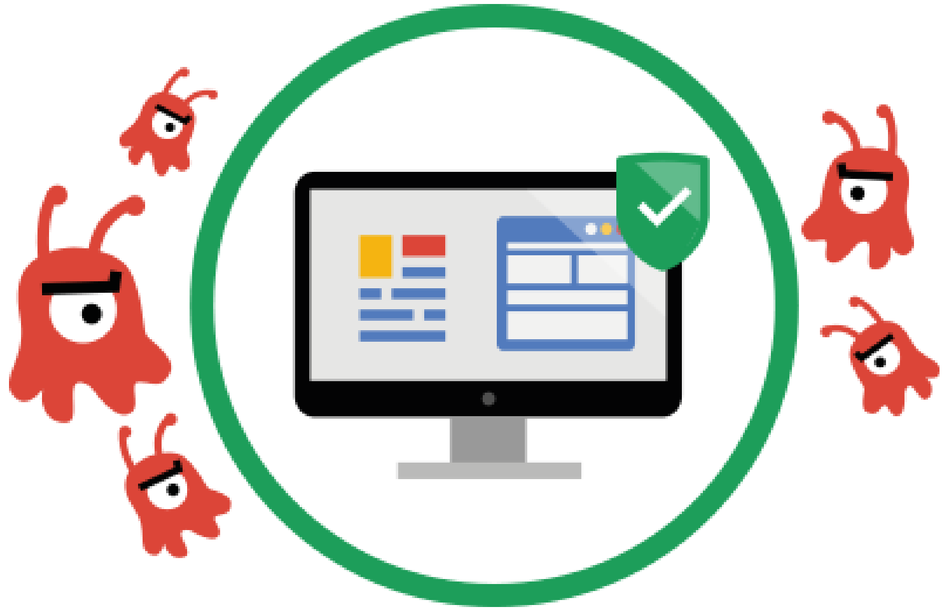
Робота в Інтернеті робить комп’ютер вразливим для шкідливих програм — вірусів. Щоб запобігти зараженню, дотримуйся таких правил:

1. **Регулярно оновлюй браузер**, операційну систему та антивірусну базу. Браузер Chrome автоматично оновлюється до останньої версії під час кожного запуску, забезпечуючи надійний захист без зусиль з боку користувача.
2. **Перевіряй адреси сайтів**, не завантажуй невідомі файли з розширенням .exe, .dll, .bat і не переходь за посиланнями зі спливаючих вікон.
3. Якщо твої дії призвели до **блокування екрана** підозрілим повідомленням, закрий браузер у диспетчері завдань або моніторі активності своєї операційної системи.
4. **Завантажуй ПЗ тільки з офіційних сайтів-розробників.**
5. **У разі неадекватної роботи ПЗ** (пристрій повільно працює, з’являються спливаючі вікна, виконуються незрозумілі платежі) відразу видали його за допомогою останньої версії антивірусної програми.
6. **Обирай антивірусні програми які добре зарекомендували себе** і встановлюй лише ліцензійні версії.

7. **Установи наступні налаштування антивірусної програми:**

— увімкни проактивний та поведінковий аналіз — ці режими дозволяють відловити шкідливі програми, яких ще немає в антивірусній базі;
— налаштуй перевірку поштових повідомлень та їх вкладень;
— проводь повне сканування комп’ютера і пристроїв, які підключаються, не рідше ніж 1 раз на тиждень.

8. **Не встановлюй на комп’ютер відразу кілька засобів захисту**. Програми розпізнають одна одну як шкідливе ПЗ і починають конкурувати або взагалі припиняють роботу.



[Як захистити комп’ютер від атак]

[Як захистити комп’ютер і мобільний пристрій від зловмисників]

Конфіденційність

В Інтернеті, як у будь-якій публічній сфері, розміщення персональних даних має обмежуватися з міркувань конфіденційності та особистої безпеки. Добре, коли батьки за твоїми чекінами можуть бачити, що з тобою все гаразд. Але якщо інформація про твоє місцеперебування є у відкритому доступі, нею можуть скористатися й зловмисники — наприклад, чек-ін на відпочинку підкаже, що сім'я виїхала з міста й залишила квартиру без нагляду. Тому, ділячись інформацією, не забудь правильно встановити налаштування доступу.

Центр безпеки Google+ разом з загальними налаштуваннями захисту даних запровадив спеціальні налаштування для підлітків.

Під час завантаження домашнього відео на YouTube, рекомендується обирати варіант «Приватне відео» або «Доступне тим, у кого є посилання».

Пам'ятай, що, спілкуючись у чаті Gmail або в додатку Google Hangouts, ти можеш вимкнути запис чату.

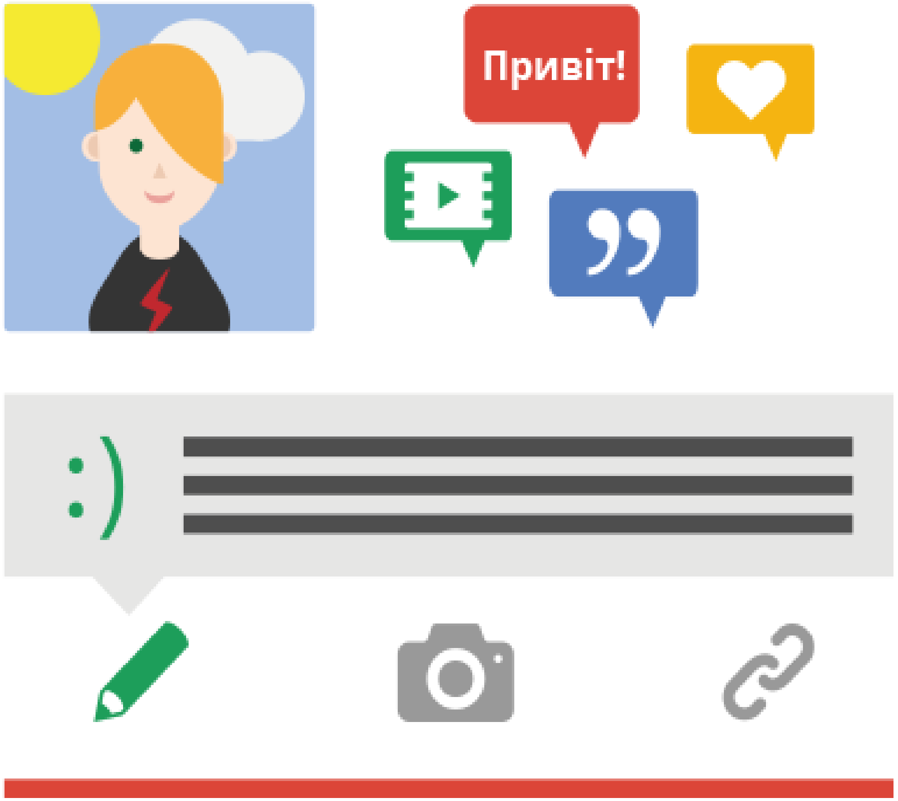
Технології безпеки Gmail включають перевірку на віруси, фільтрацію спаму, доступ по протоколу HTTPS та двоетапну аутентифікацію.

Якщо конфіденційні дані потрапили в панораму вулиць на картах Google (Street View), ти можеш надіслати запит на «розмиття» зображення.

Незважаючи на загальнодоступність, блоги в Blogger мають опцію обмеження доступу читачів.

Відправка геоданих: ви зможете в будь-яку мить увімкнути й вимкнути відправку геоданих, якщо захочете поділитися своїми координатами в Google+, зберегти історію місцезнаходжень або використовувати цю функцію з іншою метою.

Сервіс «Я в Інтернеті» від Google дозволяє відстежувати інформацію про тебе в мережі й керувати публікацією твоїх особистих даних іншими користувачами

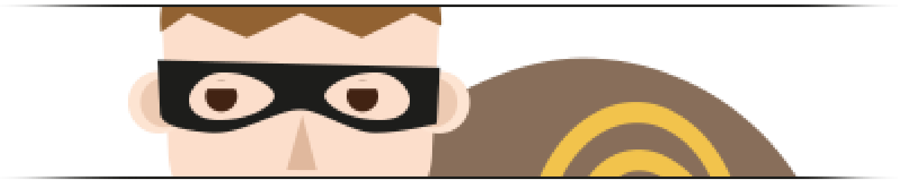


Інструменти безпеки та конфіденційності Google

Захист від розкрадання особистих даних

Кіберзловмисники крадуть особисті дані, щоб використовувати їх зі злочинною метою. Не дай шахраям обдурити тебе!

1. **Не передавай паролі, особисті та фінансові дані** електронною поштою, у повідомленнях чату або спливаючих вікнах сайту.
2. **Не переходь за оманливо знайомими посиланнями з підозрілих повідомлень** — введи URL самостійно або скористайся закладками.
3. **Нікому не передавай свій пароль** і пам'ятай, що офіційний сайт ніколи не вимагатиме таких даних
4. **Вводячи облікові дані, стеж, щоб URL сайту** починався з https://, а в адресній стрічці платіжної системи або банку обов'язково стояв значок замка.
5. **Завжди** повідомляй **про підозрілі** листи або спроби шахрайства.



Технології захисту особистої інформації в Інтернеті

Як не допустити викрадення особистих даних

Висновки

Інтернет — глобальне джерело інформації і знань. Це унікальна платформа для спілкування, творчості, створення власних проектів та самореалізації.

Максимально використовуючи можливості Інтернету, намагайся звести до мінімуму ризики, пов’язані з викраденням особистих даних і зараженням комп’ютера вірусами.

Для цього обирай безпечні способи підключення до мережі. Стеж за надійністю та секретністю свого пароля.

Встанови на комп’ютер ліцензійну антивірусну програму і грамотно встанови параметри захисту.

За допомогою налаштувань конфіденційності, які мають всі сервіси Google, обмеж доступ до своєї особистої інформації та будь уважним, із ким, як і чим ти ділишся.

Повідомляй про спроби шахрайства і пам’ятай, що батьки, вчителі та спеціалісти служби технічної підтримки завжди готові прийти тобі на допомогу.