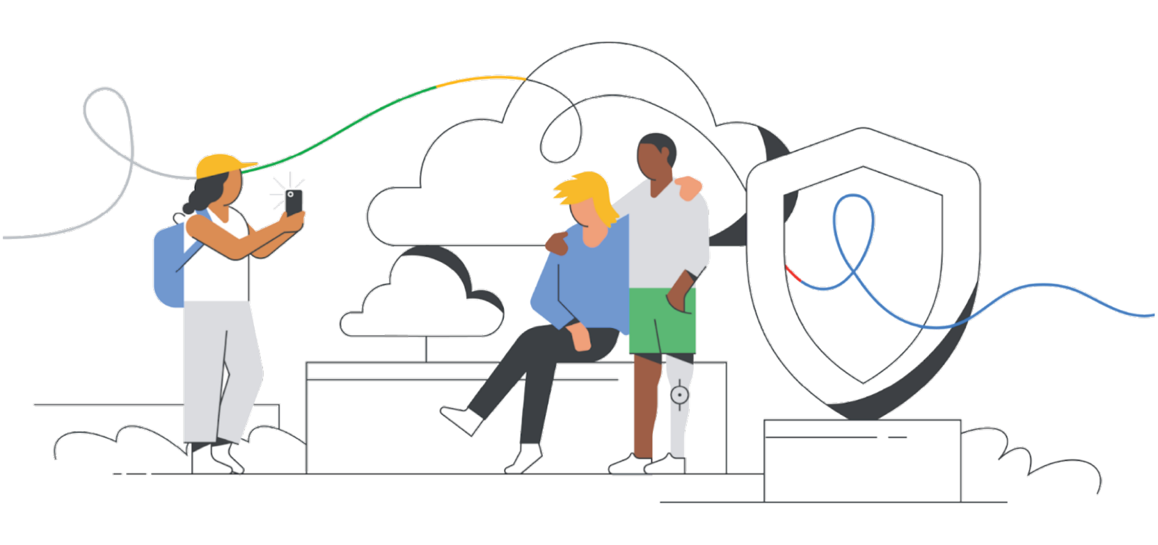
Наша подорож світом кібербезпеки крізь роки

Під захистом Google

Google щодня працює над тим, щоб зробити Інтернет безпечнішим для всіх

З різким зростанням кількості кібератак і зловмисників в Інтернеті ми вважаємо, що наші продукти й послуги корисні настільки, наскільки вони безпечні.

У Google ми як ніколи зосереджені на захисті людей, організацій і урядів. Ми ділимося нашим досвідом, розширюємо можливості суспільства протистояти кіберризикам, що постійно зростають, і працюємо над тим, щоб підняти сучасний рівень кібербезпеки й зробити світ безпечнішим для всіх.



Постійні інновації протягом багатьох років

З моменту запуску Gmail у 2004 році до впровадження Protected Computing у 2022 році, Google є першовідкривачем у сфері технологій кібербезпеки й постійно створює інноваційні продукти, платформи й партнерства, щоб усунути цілі класи загроз і створити безпечніше майбутнє для людей, організацій і суспільств такими методами:

- ✓ Розробляє безпечні продукти й платформи
- ✓ Створює гнучкі команди захисту безпеки
- ✓ Започатковує програми й партнерства
- ✓ Забезпечує критичне фінансування для інноваційних проектів і навчання персоналу

Оскільки потреби людей та Інтернет розвиваються, ми продовжуємо розробляти нові технології для зниження ризиків кіберзагроз, які постійно змінюються, гарантуючи, що з Google кожен день стає безпечнішим.

2004
рік – Захист від спаму в Gmail

Ми були одними з перших, хто створив засоби захисту електронної пошти на основі штучного інтелекту.

99,9% небезпечних і підозрілих електронних листів блокуються Gmail

2007
рік – Безпечний пошук

Ми допомагаємо захищати пристрої в усьому світі, сповіщаючи користувачів, коли вони відвідують небезпечні веб-сайти, а у 2020 році перетворюємо цей інструмент онлайн-захисту на Безпечний перегляд із розширеним захистом.

5 млрд пристроїв захищено за допомогою Безпечного перегляду

2009
рік – reCAPTCHA

Ми придбали рішення для протидії шахрайству й роботам, щоб зупинити передачу облікових даних і захоплення облікових записів, а також запобігти шахрайським діям із боку зловмисного програмного забезпечення/фальшивих користувачів.

5 млн веб-сайтів захищено

2008
рік – Менеджер паролів Google

Завдяки Менеджеру паролів вхід в облікові записи став простішим і безпечнішим, адже користувачам не потрібно запам'ятовувати або вводити паролі. Тепер Менеджер паролів використовується для 50% усіх входів у Chrome на різних платформах.

1 млрд паролів щоденно перевіряється на предмет злому

2010
рік – Zero Trust

Переживши скоординовану серію кібератак Operation Aurora, ми здійснили революцію у своєму підході до створення безпечної архітектури за умовчанням, яка тепер відома як Zero Trust. Це забезпечує менше векторів атак, менше можливостей втрати даних і більше контролю над системами, від яких залежать користувачі. Ми підтримуємо зусилля Білого дому щодо впровадження моделі Zero Trust у федеральному уряді, а також включили її в BeyondCorp Enterprise, щоб будь-яке підприємство могло використовувати цю функцію.

2010
рік – Threat Analysis Group (TAG)

Після Operation Aurora ми сформували спеціалізовану команду експертів, відповідальну за виявлення, аналіз і знищення серйозних кримінальних кіберзагроз. Група TAG відстежила Wanna Cry, найбільшу атаку програм-вимагачів в історії, до Північної Кореї і нещодавно поширила зразки хакерських екосистем з Індії, Росії і Об'єднаних Арабських Еміратів.

2010
рік – Мисливці за помилками Google

Наша програма винагород за виявлення вразливостей Vulnerability Rewards залучає старшокласників, юристів, IT-спеціалістів і любителів шукати помилки в продуктах Google і винагороджує їх грошовими призами. Учасники програми мають різні мотиви, але місія в них одна: знайти невиявлені вразливості, щоб забезпечити захист онлайн-сервісів.

Мільйони доларів виплачено як винагороди з 2010 року

2010
рік – The Red Team

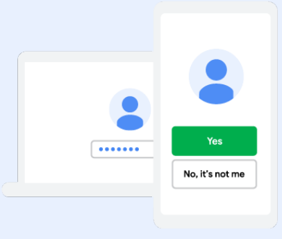
Ця команда створена, щоб протистояти зловмисним намірам і зламам систем Google, а також допомогти зміцнити наш захист і виявити недоліки. Вона працює в усьому світі й допомагає нам не відставати від поточних загроз, покращувати засоби контролю безпеки, виявляти атаки й запобігати їм, а також усувати цілі класи вразливостей завдяки створенню нових і кращих інфраструктур.

2013
рік – Project Shield

Проект Project Shield допоміг захистити новини, правозахисні організації, виборчі дільниці, політичні організації і кампанії від DDoS-атак (Distributed Denial of Service) у більш ніж 100 країнах, виявляючи загрози й дозволяючи спільноті підтримки безпеки й правоохоронним органам реагувати на них.

150+ веб-сайтів зараз захищено в Україні

2011
рік – Двохетапна перевірка



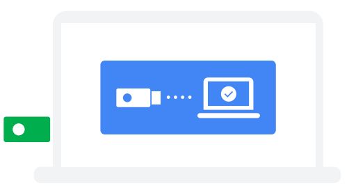
Ми були одними з перших, хто запропонував двохетапну перевірку (2SV) за умовчанням, і першими, хто автоматично ввімкнув її для понад 150 мільйонів користувачів у 2021 році, забезпечуючи безпечний і простий спосіб входу в облікові записи. Навіть якщо ваш пароль викрали, ваш обліковий запис залишається захищеним.

На 50% зменшилася кількість зламаних облікових записів після введення двохетапної перевірки

2014
рік – Project Zero

Це спеціалізована робоча група, яка займається пошуком вразливостей нульового дня в Інтернеті – у програмному забезпеченні, апаратному забезпеченні, продуктах Google тощо – щоб зробити Інтернет безпечним і відкритим. Вони були першими, хто детально описав уразливості Meltdow і Spectre, дозволяючи розробникам швидко виправляти вразливості ЦП і застосовувати засоби мінімізації ризиків у всьому ланцюжку постачання програмного забезпечення.

2017
рік – Програма додаткового захисту



Додатковий надійний захист, зокрема ключ безпеки, для користувачів із високою видимістю і високим ризиком атаки, таких як журналісти й урядовці.

300+ федеральних кампаній захищено

2018
рік – Ключ безпеки Titan

Ми створили Ключ безпеки Titan для користувачів, яким потрібне наскрізне рішення Google. Ці ключі сумісні зі специфікацією для афтентифікації FIDO й можуть використовуватися не лише в продуктах Google.

2019
рік – Повторна автентифікація без пароля

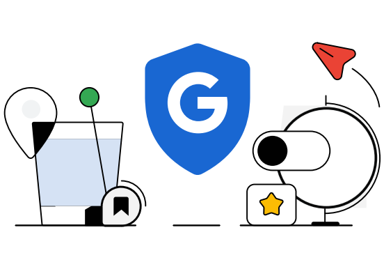
В Android було розширено підтримку FIDO, щоб користувачі могли легко входити на веб-сайти лише за допомогою PIN-коду або біометричних даних, без пароля.

2017
рік – Google Play Захист

Ц найпоширеніший сервіс захисту від мобільних загроз у світі, який постійно адаптується і вдосконалюється за допомогою машинного навчання Google. Google Play Захист автоматично сканує додатки на наявність зловмисного програмного забезпечення і шифрує платежі користувачів на телефонах Android.

100+ млрд додатків сканується на наявність зловмисного програмного забезпечення щодня

150 млн платежів користувачів шифрується щодня



2019
рік – Chronicle

Створений як спеціалізований рівень захисту на основі нашої основної інфраструктури, Chronicle забезпечував хмарний захист і був розроблений для підприємств, щоб анонімно зберігати, аналізувати й шукати величезні обсяги даних безпеки й мережеві дані.

2021
рік – Інвестиції в розвиток кібербезпеки

Ми прагнемо посилити кібербезпеку, розширити програми нульової довіри, допомогти захистити ланцюжок постачання програмного забезпечення та підвищити безпеку відкритого коду. Ми взяли на себе зобов'язання допомогти здобути 100 000 американцям навички в таких галузях, як IT-підтримка й аналітика даних, завдяки програмі Професійної сертифікації Google.

10 млрд доларів виділено на ініціативи з кібербезпеки

2021
рік – Confidential Computing

Для захисту, безпеки й конфіденційності критично важливих даних ми запровадили Google Cloud Confidential Computing – революційну технологію, яка зберігає дані в зашифрованому вигляді під час їх обробки, дозволяючи їм залишатися в безпеці протягом усього життєвого циклу, зокрема під час збереження чи передавання. Тепер навіть найбільш конфіденційні дані можна впевнено перенести в хмару.

2021
рік – Google Open Source Security Team (GOSST)

Команду безпеки GOSST було створено для підвищення безпеки програмного забезпечення з відкритим кодом, на яке покладається світ. Ми співпрацюємо з Open Source Security Foundation (OpenSSF), щоб розробити й випустити Supply-Chain Levels for Software Artifacts (SLSA), структуру для захисту ланцюжка постачання програмного забезпечення, а також надати довгострокову підтримку безпеки для всієї екосистеми програмного забезпечення.

100 млн доларів виділено на сторонні програми з підвищення безпеки відкритого коду, щоб допомогти усунути вразливості

2022
рік – Post-Quantum Cryptography Standardization

Орієнтуючись на майбутнє, ми продовжуємо розробляти криптографічні системи нового покоління, які захищають криптосистеми з відкритим ключем від зламу й запобігають компрометації цифрових комунікацій. Національний інститут стандартів і технологій вибрав для стандартизації заявку за участю Google (SPHINCS+).

2022
рік – Protected Computing

Ми анонсували Protected Computing – набір технологій, що постійно розширюється і змінює підхід до того, як, де й коли обробляються дані, щоб технічно забезпечити конфіденційність і безпеку користувачів. Ми робимо це шляхом мінімізації обсягу даних, деідентифікації даних і обмеження доступу до конфіденційних даних. Це означає, що Android може запропонувати вам наступну фразу, коли ви вводите текст, зберігаючи розмову повністю приватною.

2023
рік – Ключ безпеки: майбутнє без паролів

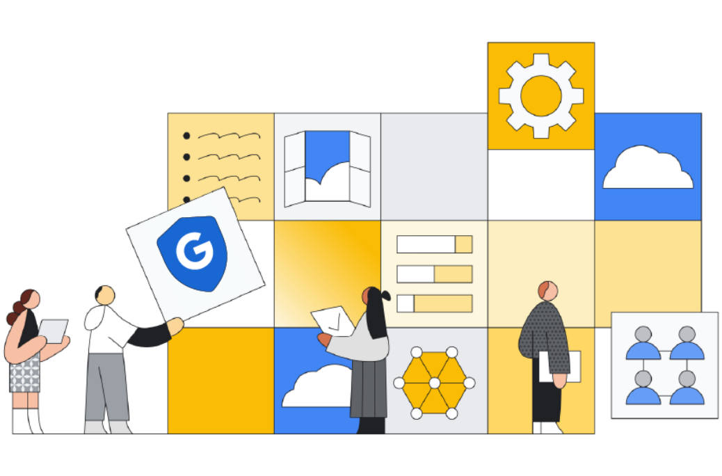
Ми готуємося до майбутнього без паролів уже більше ніж десять років. Ми приєдналися до Альянсу FIDO у 2013 році, щоб просувати відкриті стандарти для світу без паролів, і тепер, розширивши нашу підтримку стандартів авторизації FIDO на Android і Chrome через технологію ключа доступу у 2023 році, ми нарешті отримаємо платформу для дійсно безпарольного майбутнього.

2022
рік – Mandiant і Google Cloud

Компанія Mandiant – лідер ринку аналізу загроз кібербезпеці в реальному часі. У поєднанні з хмарними рішеннями безпеки Google Cloud ми допомагаємо підприємствам і державним установам залишатися захищеними протягом життєвого циклу безпеки, ділячись своїми знаннями і досвідом з іншим організаціями світу.

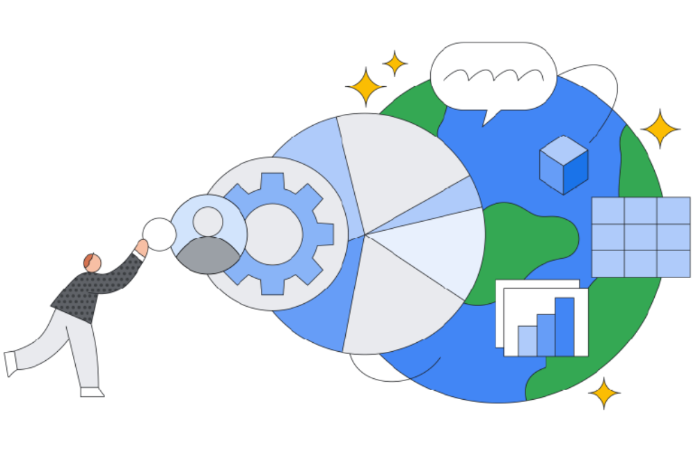
В епоху постійного розширення технологічного охоплення довіра до технологій є ключем до розкриття справжнього потенціалу суспільства.

Застосовуючи наші знання з безпеки на практиці, ми продовжуватимемо співпрацювати з людьми, компаніями й урядами, щоб захистити їх безпеку й розпочати нову еру кібербезпеки.



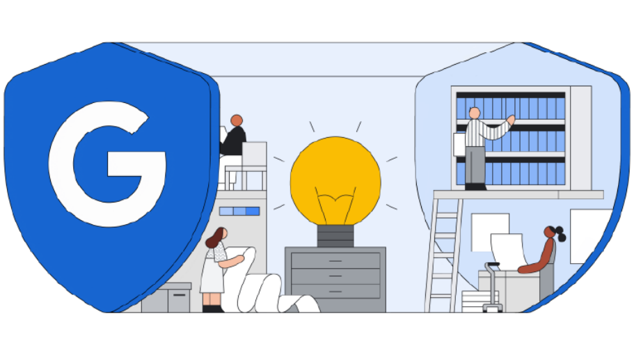
Захист людей, компаній і урядів

Безпека є наріжним каменем нашої продуктової стратегії. Ось чому всі наші продукти мають вбудовані засоби захисту, які роблять їх безпечними за умовчанням.



Розширення можливостей суспільства для подолання зростаючих ризиків кібербезпеки

Ми надаємо суспільству можливість розкрити потенціал відкритого коду й прозоро ділимося нашими знаннями та досвідом із галуззю, щоб зробити екосистеми безпечнішими.



Розвиток технологій майбутнього

Ми хочемо захистити суспільства від наступного покоління кіберзагроз. Спираючись на наш досвід штучного інтелекту, ми розробляємо наступну хвилю архітектур, щоб розширити межі інновацій у сфері безпеки.

З Google кожен день безпечніший

Відвідайте g.co/safety/cyber