Google

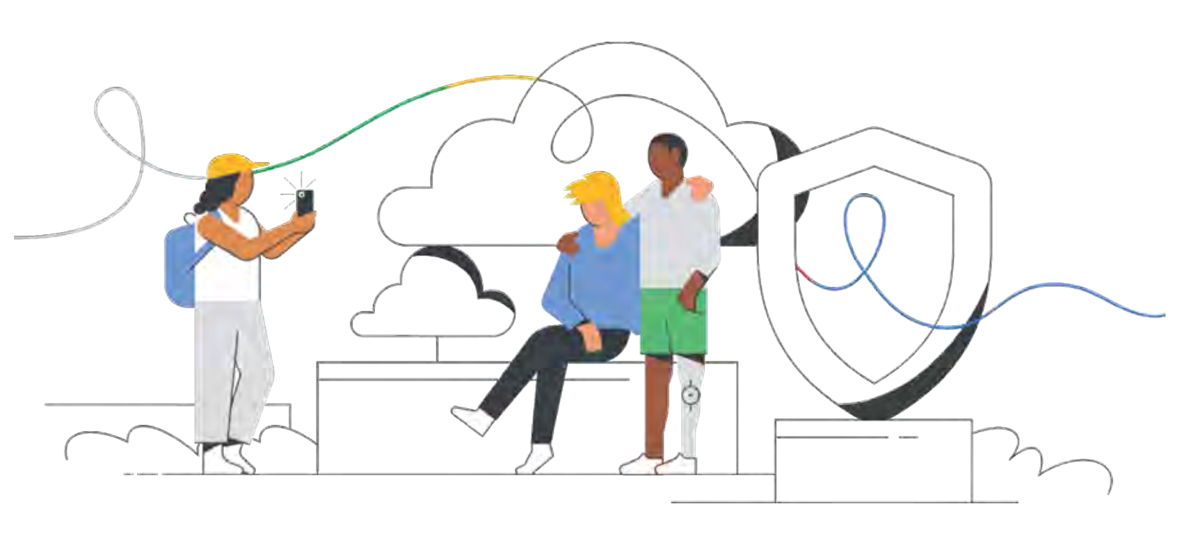
Nasza historia cyberbezpieczeństwa

Bezpieczniej z Google

Zapewniamy bezpieczeństwo większej liczbie internautów niż ktokolwiek inny na świecie.

W obliczu drastycznego nasilenia się cyberataków sponsorowanych przez władze państwowe i przestępczości internetowej jesteśmy przekonani, że nasze produkty i usługi mogą być przydatne tylko wtedy, gdy będą bezpieczne.

Google jeszcze bardziej niż dotychczas skupia się na ochronie ludzi, organizacji i władz państwowych. Dzielimy się swoją specjalistyczną wiedzą, motywujemy społeczeństwo do reagowania na nieustannie zmieniające się czynniki ryzyka w cyberprzestrzeni i stale pracujemy nad poprawą stanu wiedzy w zakresie cyberbezpieczeństwa, by uczynić świat bezpieczniejszym dla wszystkich.



Lata nieustannych innowacji

Od uruchomienia Gmaila w 2004 r. aż po wprowadzenie Protected Computing w 2022 r., Google pozostaje pionierem technologii cyberbezpieczeństwa i nieustannie wdraża innowacje w swoich produktach, platformach i partnerstwach, aby eliminować kolejne klasy zagrożeń i zapewniać lepszą przyszłość ludziom, organizacjom i społeczeństwu poprzez:

- ✓ Opracowywanie bezpiecznych platform i produktów
- ✓ Wspieranie różnych programów i partnerstw
- ✓ Budowanie zwinnych zespołów ds. bezpieczeństwa
- ✓ Udostępnianie niezbędnych środków finansowych na innowacje i szkolenia pracownicze

Podczas gdy ludzkie potrzeby i internet ewoluują, my nieodmiennie przodujemy w obszarze nowych technologii, które pozwalają zwalczać nieustannie zmieniające się cyberzagrożenia i dbać o to, by każdy dzień z Google był bezpieczniejszy.

2004
Ochrona przed spamem w Gmailu

Jako jedni z pierwszych wprowadziliśmy ochronę poczty elektronicznej opartą na sztucznej inteligencji.

Gmail blokuje 99.9% niebezpiecznych i podejrzanych e-maili

2007
Bezpieczne przeglądanie

Pomagamy aktywnie chronić urządzenia na całym świecie, ostrzegając użytkowników, którzy wchodzą na niebezpieczne strony. W 2020 r. wprowadziliśmy Ulepszone Bezpieczne przeglądanie.

Bezpieczne przeglądanie chroni 5 miliardów urządzeń

2009
reCAPTCHA

Kupiliśmy rozwiązanie przeznaczone do walki z oszustwami i botami, by wyeliminować ataki typu credential stuffing i przejmowanie kont oraz uniemożliwić szkodliwe działanie złośliwego oprogramowania lub fałszywych użytkowników.

Chronimy 5 milionów witryn internetowych

2008
Menedżer haseł Google

Wprowadzenie Menedżera haseł ułatwiło logowanie i zwiększyło jego bezpieczeństwo, ponieważ wyeliminowało konieczność zapamiętywania lub wpisywania haseł. Obecnie jest on stosowany do 50% wszystkich logowań w Chrome na wszystkich platformach.

1 miliard haseł jest codziennie sprawdzanych pod kątem naruszeń

2010
Zero Trust

Przetrwawszy Operację Aurora, serię skoordynowanych cyberataków, zrewolucjonizowaliśmy swoje podejście i opracowaliśmy architekturę zapewniającą bezpieczeństwo w standardzie, znaną obecnie jako „Zero Trust”. Architektura ta ogranicza liczbę wektorów ataku i możliwości utraty danych oraz daje użytkownikom więcej kontroli nad ważnymi systemami. Wspieramy działania Białego Domu mające na celu wprowadzenie modelu „Zero Trust” w rządzie federalnym. Dołączyliśmy go także do pakietu BeyondCorp Enterprise, dzięki czemu mogą z niego korzystać wszystkie przedsiębiorstwa.

2010
Threat Analysis Group (TAG)

Po Operacji Aurora powołaliśmy specjalny zespół ekspertów, który odpowiada za wykrywanie, analizowanie i przerywanie poważnych cyberzagrożeń ze strony grup przestępczych lub sponsorowanych przez władze państwowe. To właśnie zespół TAG wyśledził, że Wanna Cry, czyli największy atak typu ransomware w historii, pochodził z Korei Północnej. Ostatnio ujawnił także przykłady środowisk hakerów do wynajęcia z Indii, Rosji i Zjednoczonych Emiratów Arabskich.

2010
Google Bug Hunters

Nasz program nagród za wykrywanie luk w zabezpieczeniach Vulnerability Rewards przyciąga licealistów, prawników, informatyków i hobbystów, którzy tropią błędy w produktach Google w zamian za nagrody pieniężne. Kierują się przy tym różnymi motywami, ale przyświeca im ta sama misja: znaleźć nieznane dotąd luki w trosce o bezpieczeństwo usług internetowych.

Od 2010 r. wypłacono miliony dolarów nagród

2010
Red Team

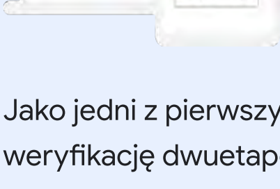
Zadaniem tego zespołu jest prowadzenie ofensywnych działań i hakowanie Google w celu wzmocnienia naszych mechanizmów ochronnych i wykrywania luk. Jego członkowie z różnych części świata nieustannie śledzą aktualne zagrożenia, doskonalą mechanizmy zabezpieczeń, wykrywają ataki i im zapobiegają, a także eliminują całe klasy luk, kształtując nowe, lepsze ramy bezpieczeństwa.

2013
Project Shield

Project Shield pomaga chronić media, organizacje broniące praw człowieka, portale wyborcze, organizacje polityczne i kampanie przed atakami typu DDoS w ponad 100 krajach. Rozpoznaje zagrożenia i umożliwia reagowanie podmiotom odpowiedzialnym za bezpieczeństwo i organom ścigania.

Obecnie chronimy ponad 150 witryn internetowych w Ukrainie

2011
Weryfikacja dwuetapowa



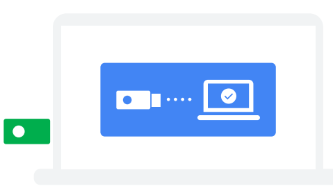
Jako jedni z pierwszych zaoferowaliśmy weryfikację dwuetapową w standardzie i jako pierwsi automatycznie włączyliśmy ją dla ponad 150 milionów osób w 2021 r., umożliwiając bezpieczne i proste logowanie. Twoje konto jest chronione, nawet jeśli ktoś wykradnie Twoje hasło.

Spadek liczby włamań na konta o 50% od czasu wprowadzenia weryfikacji dwuetapowej

2014
Project Zero

Specjalny zespół zajmujący się polowaniem na zero day exploits w całym internecie – w oprogramowaniu, sprzęcie, produktach Google oraz w innych miejscach – w trosce o bezpieczny i otwarty internet. Jego członkowie jako pierwsi opisali „Meltdown” i „Specter”, co umożliwiło programistom szybkie usunięcie luk bezpieczeństwa w procesorach i podjęcie działań w całym łańcuchu dostaw oprogramowania.

2017
Program ochrony zaawansowanej (APP)



Wzmocnione mechanizmy ochronne, w tym Klucz bezpieczeństwa, dla użytkowników zajmujących eksponowane stanowiska i szczególnie zagrożonych atakami, takich jak dziennikarze czy urzędnicy państwowi.

Zabezpieczyliśmy ponad 300 kampanii federalnych

2018
Klucz bezpieczeństwa Titan

Klucz bezpieczeństwa Titan powstał z myślą o użytkownikach potrzebujących kompleksowego rozwiązania Google. Klucze te są zgodne ze standardami FIDO i można ich używać wszędzie, nie tylko w Google.

2019
Ponowne uwierzytelnianie bez podawania hasła

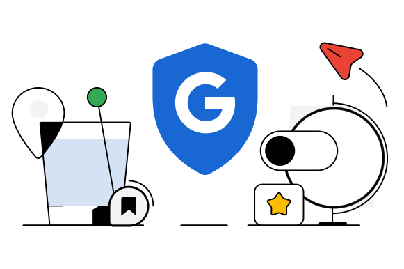
Rozszerzyliśmy obsługę FIDO w systemie Android, aby umożliwiać użytkownikom bezproblemowe logowanie się w portalach internetowych wyłącznie za pomocą kodu PIN lub biometrii, bez konieczności podawania hasła.

2017
Google Play Protect

Google Play Protect to najpopularniejsza na świecie usługa chroniąca przed zagrożeniami mobilnymi, stale modyfikowana i doskonalona dzięki uczeniu maszynowemu Google. Usługa ta skanuje aplikacje w poszukiwaniu złośliwego oprogramowania i szyfruje płatności dokonywane telefonami z systemem Android.

Codziennie skanujemy ponad 100 miliardów aplikacji pod kątem złośliwego oprogramowania

Codziennie szyfrujemy 150 milionów płatności dokonywanych przez użytkowników



2019
Chronicle

Chronicle to wyspecjalizowana warstwa naszej podstawowej infrastruktury, zapewniająca zabezpieczenia dla przedsiębiorstw w oparciu o technologię chmury w celu prywatnego przechowywania, analizowania i przeszukiwania ogromnych ilości danych dotyczących bezpieczeństwa i sieci.

2021
Inwestycje w rozwój cyberbezpieczeństwa

Zależy nam na wzmacnianiu cyberbezpieczeństwa, rozszerzaniu zakresu programów „zero trust”, pomocy w zabezpieczaniu łańcucha dostaw oprogramowania oraz poprawie bezpieczeństwa oprogramowania open source. Zobowiązaliśmy się do przeszkolenia 100 tys. Amerykanów w takich dziedzinach, jak wsparcie IT czy analiza danych, w ramach programu Google Career Certificate.

Przeznaczenie 10 miliardów dolarów na przedsięwzięcia związane z cyberbezpieczeństwem

2021
Confidential Computing

Z myślą o bezpieczeństwie i prywatności w zastosowaniach krytycznych wprowadziliśmy Google Cloud Confidential Computing, przełomową technologię, dzięki której dane pozostają zaszyfrowane podczas przetwarzania. Dzięki temu są bezpieczne przez cały cykl życia, również w spoczynku oraz podczas ich przesyłania. Teraz nawet najbardziej wrażliwe dane można spokojnie przenieść do chmury.

2021
Google Open Source Security Team (GOSST)

Zespół GOSST pracuje nad poprawą bezpieczeństwa oprogramowania open source, z którego korzysta cały świat. Nawiązaliśmy współpracę z Open Source Security Foundation (OpenSSF), aby opracować i opublikować Supply-Chain Levels for Software Artifacts (SLSA), czyli ramy służące zabezpieczaniu łańcucha dostaw oprogramowania i zapewniające długoterminowe bezpieczeństwo całego ekosystemu oprogramowania.

Przeznaczenie 100 milionów dolarów na zewnętrzne inicjatywy związane z bezpieczeństwem oprogramowania open source w celu wspierania usuwania luk bezpieczeństwa

2022
Standaryzacja kryptografii postkwantowej

Myśląc o przyszłości, kontynuujemy prace nad systemami kryptograficznymi nowej generacji, które chronią kryptosystemy z kluczem publicznym przed złamaniem oraz komunikację cyfrową przed przechwytywaniem. Narodowy Instytut Standaryzacji i Technologii wybrał na potrzeby standaryzacji propozycję opracowaną przy udziale Google (SPHINCS+).

2022
Protected Computing

Ogłosiliśmy wprowadzenie Protected Computing, stale powiększającego się zestawu narzędzi technologicznych, które zmieniają sposób, czas i miejsce przetwarzania danych, aby zapewniać poufność i bezpieczeństwo danych użytkownika. W tym celu zmniejszamy ilość gromadzonych danych, poddajemy je anonimizacji i ograniczamy dostęp do danych wrażliwych. Dzięki temu system Android może podpowiadać kolejne frazy tekstu i jednocześnie zapewniać całkowitą poufność rozmowy.

2023
Klucz: przyszłość bez haseł

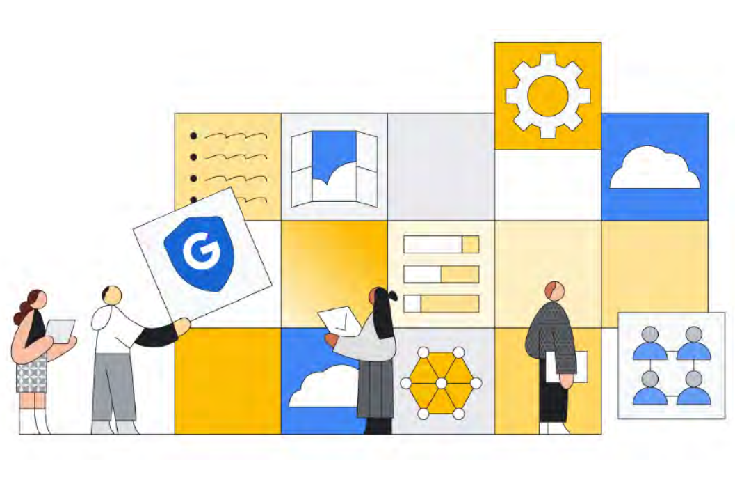
Od ponad dziesięciu lat przygotowujemy się do rezygnacji z haseł. W 2013 r. dołączyliśmy do organizacji FIDO Alliance, aby współtworzyć otwarte standardy dla świata bez haseł. Obecnie, dzięki rozszerzeniu w 2023 r. obsługi standardów logowania FIDO z zastosowaniem technologii klucza na system Android i Chrome, w końcu powstaną solidne podstawy dla przyszłości bez haseł.

2022
Mandiant i Google Cloud

Mandiant dostarcza w czasie rzeczywistym szeroki zakres informacji o cyberzagrożeniach nadsyłanych przez największe organizacje na świecie. W połączeniu z funkcjami bezpieczeństwa wbudowanymi w Google Cloud pomagamy przedsiębiorstwom i podmiotom sektora publicznego utrzymać ochronę w całym cyklu życia.

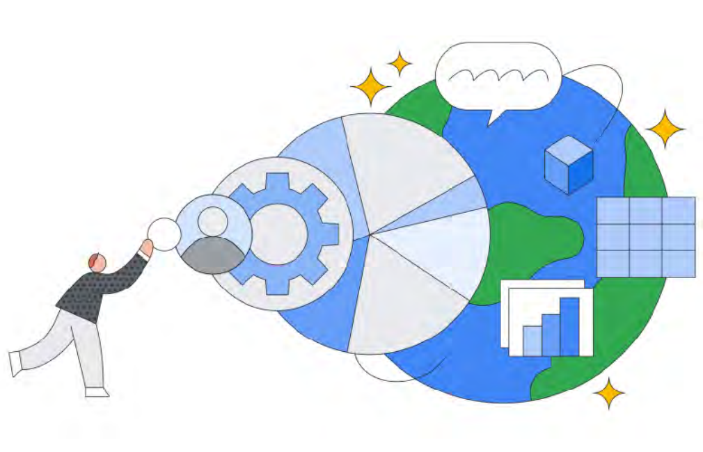
W epoce ciągłego rozwoju technologicznego zaufanie do technologii stanowi klucz do uwolnienia pełnego potencjału tkwiącego w społeczeństwie.

Dlatego też będziemy wykorzystywać naszą wiedzę o bezpieczeństwie i kontynuować współpracę z ludźmi, przedsiębiorstwami i władzami państwowymi, aby ich chronić oraz przyczynić się do nastania nowej ery cyberbezpieczeństwa.



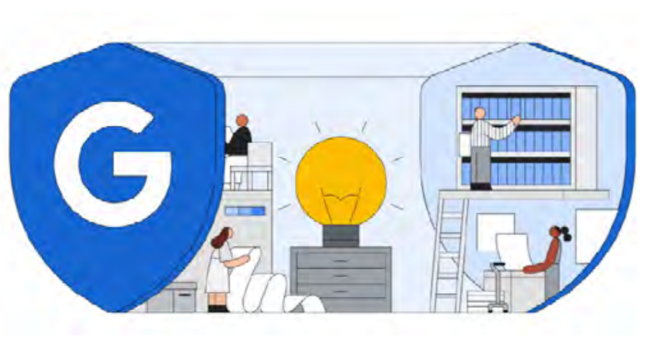
Ochrona dla ludzi, przedsiębiorstw i władz państwowych

Bezpieczeństwo stanowi podstawowy element naszej strategii produktowej. Dlatego wszystkie nasze produkty mają wbudowane zabezpieczenia, które gwarantują bezpieczeństwo w standardzie.



Ułatwiamy społeczeństwu reagowanie na zmieniające się zagrożenia w cyberprzestrzeni

Zachęcamy ludzi do pełnego wykorzystywania możliwości oprogramowania open source oraz w przejrzysty sposób dzielimy się swoją wiedzą i doświadczeniem w branży, aby zwiększyć bezpieczeństwo ekosystemów.



Rozwijamy technologie przyszłości

Chcemy chronić społeczeństwo przed kolejną generacją cyberzagrożeń. Wykorzystując swoje doświadczenie w dziedzinie sztucznej inteligencji, projektujemy nową generację architektury, która przesunie granice innowacji w obszarze bezpieczeństwa.

Google dba o Twoje bezpieczeństwo każdego dnia

Odwiedź stronę
g.co/safety/cyber

Google