Google

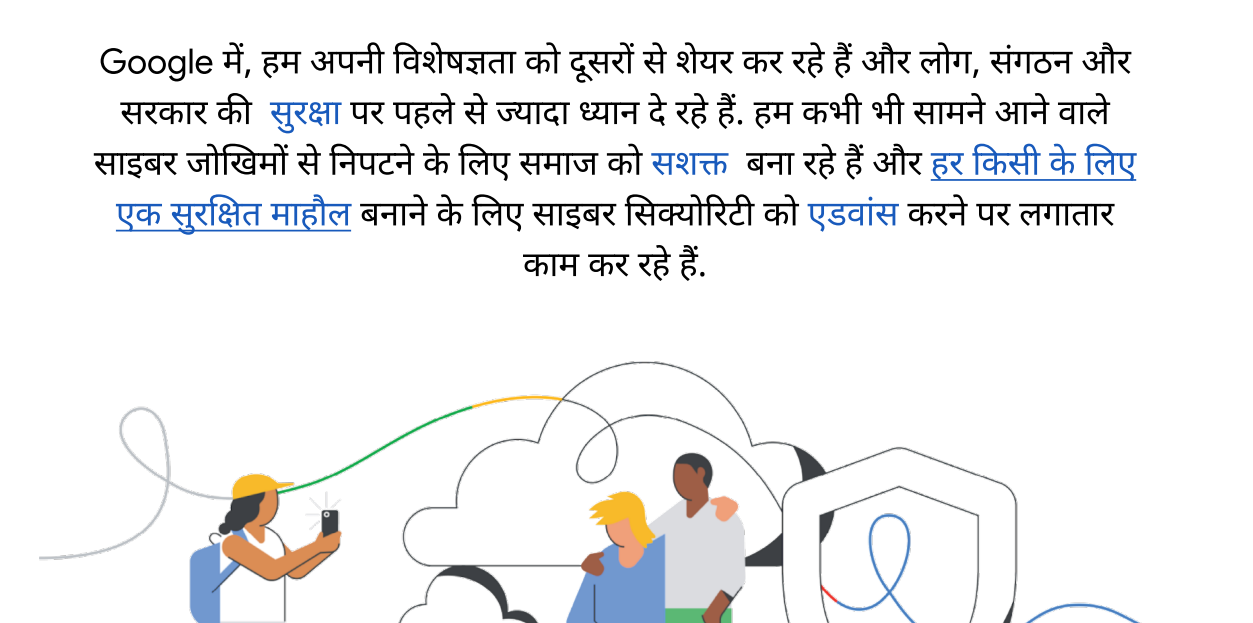
हमारी सालों की साइबर सिक्योरिटी यात्रा

Safer with Google

Google सभी के लिए इंटरनेट को सुरक्षित बनाने को लेकर हर दिन काम करता है

स्टेट-स्पॉन्सर्ड साइबर हमलों और नुकसान पहुंचाने वालों की ऑनलाइन बढ़ोतरी को देखते हुए, हम मानते हैं कि हमारी प्रोडक्ट और सर्विस ही सहायक हैं क्योंकि उन्हें बेहद सिक्योर बनाया गया है.

Google में, हम अपनी विशेषज्ञता को दूसरों से शेयर कर रहे हैं और लोग, संगठन और सरकार की सुरक्षा पर पहले से ज्यादा ध्यान दे रहे हैं. हम कभी भी सामने आने वाले साइबर जोखिमों से निपटने के लिए समाज को सशक्त बना रहे हैं और हर किसी के लिए एक सुरक्षित माहौल बनाने के लिए साइबर सिक्योरिटी को एडवांस करने पर लगातार काम कर रहे हैं.



वर्षों से लगातार नई खोज करना

2004 में Gmail के लॉन्च से लेकर 2022 में प्रोटेक्टेड कंप्यूटिंग की शुरुआत तक, Google साइबर सिक्योरिटी तकनीक में अग्रणी रहा है और इनके ज़रिए लोगों, संगठनों और समाज के लिए एक सुरक्षित भविष्य बनाने के लिए खतरों के पूरे हिस्से को खत्म करने के लिए प्रोडक्ट, प्लेटफ़ॉर्म और साझेदारी पर लगातार नई कोशिशें कर रहा है:

- सिक्योर प्रोडक्ट और प्लेटफ़ॉर्म डेवलप करना
- प्रोग्राम और साझेदारी को बढ़ावा देना
- चुस्त सिक्योरिटी टीम बनाना
- इनोवेशन और वर्कफ़ोर्स ट्रेनिंग के लिए ज़रूरी फ़ंडिंग देना

जैसे-जैसे लोगों की ज़रूरतें और इंटरनेट विकसित होते जा रहे हैं, वैसे-वैसे हम लगातार बदलते साइबर खतरों को कम करने के लिए नई तकनीकों में सबसे आगे बने हुए हैं, यह सुनिश्चित करते हुए कि Google के साथ हर दिन सुरक्षित हो.

2004
2004 Gmail Spam Protection

हम AI-संचालित ईमेल प्रोटेक्शन बनाने वाली पहली कंपनियों में से एक थे.

99.9% खतरनाक और संदेहास्पद ईमेल Gmail द्वारा ब्लॉक कर दिए जाते हैं

2007
सुरक्षित ब्राउज़िंग का

हम खतरनाक वेबसाइट पर जाने वाले उपयोगकर्ता को सतर्क करके दुनिया भर में डिवाइस को सक्रिय रूप से प्रोटेक्ट करने में मदद करते हैं, इन ऑनलाइन प्रोटेक्शन को 2020 में Enhanced सुरक्षित ब्राउज़िंग का में विकसित किया है.

सुरक्षित ब्राउज़िंग का से5 अरब डिवाइस प्रोटेक्ट किए गए

2008
Google Password Manager

Password Manager की शुरुआत ने आपके पासवर्ड को याद रखने या टाइप करने की ज़रूरत के बिना साइन-इन को आसान और सुरक्षित बना दिया है और अब Chrome में सभी प्लेटफ़ॉर्म पर 50% लॉगिन के लिए इस्तेमाल किया जाता है.

हर दिन उल्लंघनों के लिए1 अरब पासवर्ड चेक किए जाते हैं

2009
reCAPTCHA

हमने क्रेडेंशियल स्टफ़िंग और अकाउंट टेकओवर को रोकने, और मैलीशियस सॉफ़्टवेयर/नकली उपयोगकर्ता की अपमानजनक गतिविधियों को रोकने के लिए फ़्रॉड और बॉट मैनेजमेंट सॉल्युशन हासिल किया.

5 लाख वेबसाइट का रक्षित्र

2010
Threat Analysis Group (TAG)

Operation Aurora के बाद, हमने सरकार का नुकसान रोकने और गंभीर आपराधिक साइबर खतरों का पता लगाने, उनका विश्लेषण करने और उन्हें रोकने के लिए जिम्मेदार विशेषज्ञों की एक विशेष टीम बनाई. TAG ने उत्तर कोरिया में इतिहास के सबसे बड़े रैंसमवेयर हमले Wanna Cry का पता लगाया और हाल ही में भारत, रूस और संयुक्त अरब अमीरात से हैक-फ़ॉर-हायर इकोसिस्टम के उदाहरण साझा किए.

2010
Zero Trust

Operation Aurora, साइबर हमलों की एक सोची-समझी सीरीज़, से बचे रहने के बाद हमने एक सिक्योर-बाय-डिफ़ॉल्ट आर्किटेक्चर बनाने के लिए अपने दृष्टिकोण में क्रांति ला दी, जिसे अब "Zero Trust" के रूप में जाना जाता है. यह कम हमलावर वेक्टर, डेटा खोने के कम अवसर और उन सिस्टम पर ज़्यादा नियंत्रण पक्का करता है जिन पर उपयोगकर्ता निर्भर करते हैं.

2010
Google Bug Hunters

हमारा इनाम प्रोग्राम में हाई स्कूल में जाने वालों, वकीलों, IT पेशेवरों और शौकीनों को Google प्रोडक्ट में बग खोजने पर नकद पुरस्कार मिलता है और इससे वे इसको लेकर आकर्षित होते हैं. उनके मकसद अलग-अलग हैं, लेकिन उनका मिशन एक ही है: ऑनलाइन सर्विस को सुरक्षित और सिक्योर रखने के लिए अनदेखी खामियों का पता लगाना.

2010 के बाद से रिवॉर्ड में कईमिलियन डॉलर का भुगतान किया गया

2010
The Red Team

मुकाबला करने वाली सोच से लड़ने और हमारे बचाव को मजबूत करने व खामियों को दूर करने में मदद के लिए Google को हैक करने के लिए लॉन्च किया गया. वे मौजूदा खतरों से निपटने, सिक्योरिटी कंट्रोल में सुधार करने, हमले का पता लगाने/रोकथाम करने और नए और बेहतर ढांचे को चलाकर कमजोरियों के पूरे हिस्से को खत्म करने के लिए दुनिया भर में काम करते हैं.

2011
2-चरणों में पुष्टि

हम डिफ़ॉल्ट रूप से 2-चरणों में पुष्टि (2SV) की पेशकश करने वाली पहली कंपनियों में से एक थे, और 2021 में 15 करोड़ से ज़्यादा लोगों के लिए 2SV को ऑटो-एनेबल करने वाली भी पहली कंपनी थे, जिससे हमने लॉग इन करने का एक सुरक्षित और आसान तरीका दिया. भले ही आपका पासवर्ड चोरी हो जाए, आपका अकाउंट प्रोटेक्टेड है.

2SV के बाद से असुरक्षित अकाउंट में 50% की कमी आई

2013
Project Shield

Project Shield ने खतरों की पहचान करके और सिक्योरिटी कम्युनिटी और एनफ़ोर्समेंट एजेंसियों की प्रतिक्रिया को चालू करके समाचार, मानवाधिकार संगठनों, चुनाव स्थलों, राजनीतिक संगठनों और कैंपेन को Distributed Denial of Service (DDoS) हमलों से 100 से ज़्यादा देशों में साइबर हमलों से बचाने में मदद की है.

वर्तमान में यूक्रेन में 150+ वेब साइट प्रोटेक्टेड हैं

2014
Project Zero

पूरे इंटरनेट में ज़ीरो डे की हन्टिंग पर काम करने वाली एक विशेष टास्क फ़ोर्स - सॉफ़्टवेयर, हार्डवेयर, Google प्रोडक्ट में और उससे भी आगे एक सुरक्षित और ओपन इंटरनेट को सुनिश्चित करने के लिए. उन्होंने सबसे पहले "मेल्टडाउन" और "स्पेक्टर" की जानकारी दी, जिस वजह से डेवलपर CPU खामियों को जल्दी से दूर कर सके और सॉफ़्टवेयर सप्लाई चेन को आसान बना सके.

2017
(APP)

पत्रकारों और सरकारी अधिकारियों जैसे हाई-विज़िबिलिटी और उच्च-जोखिम वाले उपयोगकर्ता के लिए सुरक्षा कुंजी सहित और भी सिक्योर प्रोटेक्शन.

300+ संघीय कैंपेन प्रोटेक्टेड

2017
Google Play Protect

मोबाइल खतरे के लिए दुनिया में सबसे बड़े पैमाने पर काम कर रही प्रोटेक्शन सर्विस, Google की मशीन लर्निंग को लगातार अपना रही है और सुधार भी कर रही है, Google Play Protect ऑटोमैटिकली मैलवेयर के लिए ऐप स्कैन करता है और Android फ़ोन पर उपयोगकर्ता भुगतान को एन्क्रिप्ट करता है.

100+ अरब ऐप हर दिन मैलवेयर के लिए स्कैन किए जाते हैं

150 करोड़ उपयोगकर्ता भुगतान हर दिन एन्क्रिप्ट किए जाते हैं

2018
Titan

हमने Titan सुरक्षा कुंजी ऐसे उपयोगकर्ता के लिए बनाई है जो एंड-टू-एंड Google समाधान चाहते हैं. कुंजियां FIDO के मुताबिक हैं और Google के अलावा, दूसरी जगह भी इनका इस्तेमाल किया जा सकता है.

2019
पासवर्ड रहित री-ऑथेंटिकेशन

हमने Titan सुरक्षा कुंजी ऐसे उपयोगकर्ता के लिए बनाई है जो एंड-टू-एंड Google समाधान चाहते हैं. कुंजियां FIDO के मुताबिक हैं और Google के अलावा, दूसरी जगह भी इनका इस्तेमाल किया जा सकता है.

2021
साइबर सिक्योरिटी को एडवांस करने के लिए निवेश

हम साइबर सिक्योरिटी को मज़बूत करने, zero-trust प्रोग्राम का विस्तार करने, सॉफ़्टवेयर सप्लाई चेन को सिक्योर करने में मदद करने और ओपन-सोर्स सिक्योरिटी को बढ़ाने के लिए प्रतिबद्ध हैं. हमने 100,000 स्कॉलरशिप शुरू करने का संकल्प लिया है, ताकि ज़्यादा से ज़्यादा लोग नई डिजिटल स्किल्स सीख सकें. GCC प्रोग्राम के ज़रिए, हम 2 साल में 10 लाख भारतीयों तक पहुंचेंगे.

साइबर सिक्योरिटी पहल के लिए $10 बिलियन की प्रतिबद्धता

2019
Chronicle

हमारे मुख्य बुनियादी ढांचे के टॉप पर एक खास परत के तौर पर निर्मित, Chronicle को क्लाउड-आधारित सिक्योरिटी देने के लिए पेश किया गया था, जो एंटरप्राइस को भारी मात्रा में सिक्योरिटी और नेटवर्क डेटा को निजी तौर पर बनाए रखने, विश्लेषण करने और खोजने के लिए डिज़ाइन किया गया था.

2021
Google Open Source Security Team (GOSST)

GOSST को ओपन सोर्स सॉफ़्टवेयर की सिक्योरिटी में सुधार के लिए बनाया गया था, जिस पर दुनिया निर्भर है. हमने Supply-Chain Levels for Software Artifacts (SLSA), सॉफ़्टवेयर सप्लाई चेन को सुरक्षित करने और पूरे सॉफ़्टवेयर इकोसिस्टम के लिए लंबे वक्त तक सुरक्षा का ढांचा विकसित करने और जारी रखने के लिए Open Source Security Foundation (OpenSSF) के साथ भागीदारी की.

कमजोरियों को ठीक करने में मदद के लिए थर्ड पार्टी के ओपन सोर्स सिक्योरिटी ऑपरेशन के लिए $100 मिलियन की प्रतिबद्धता

2021
कॉन्फिडेंशियल कंप्यूटिंग

क्रिटिकल सिक्योरिटी, बचाव और निजता के लिए, हमने Google Cloud कॉन्फिडेंशियल कम्प्यूटिंग की शुरुआत की, जो एक सफल तकनीक है जो डेटा को प्रोसेस किए जाने के दौरान इसे एन्क्रिप्टेड रखती है, जिससे यह रेस्ट या ट्रांज़िट सहित अपने पूरे जीवन चक्र में सिक्योर रहता है. अब यहां तक कि सबसे संवेदनशील डेटा को भी भरोसे के साथ क्लाउड पर माइग्रेट किया जा सकता है.

2022
प्रोटेक्टेड कंप्यूटिंग

हमने प्रोटेक्टेड कंप्यूटिंग की घोषणा की, जो तकनीकों का एक बढ़ता हुआ टूलकिट है. यह यूज़र की गोपनीयता और सुरक्षा को तकनीकी रूप से सुनिश्चित करने के लिए डेटा को कैसे, कब और कहां प्रोसेस किया जाता है, इसे ट्रांसफ़ॉर्म करता है. हम डेटा फ़ुटप्रिंट को कम करके, डेटा की पहचान को कम करके और संवेदनशील डेटा तक एक्सेस को प्रतिबंधित करके ऐसा करते हैं. इसका मतलब है कि संचार को पूरी तरह से निजी रखते हुए, Android टेक्स्ट में अगले हिस्से का सुझाव दे सकता है.

2022
पोस्ट-क्वांटम क्रिप्टोग्राफ़ी मानकीकरण

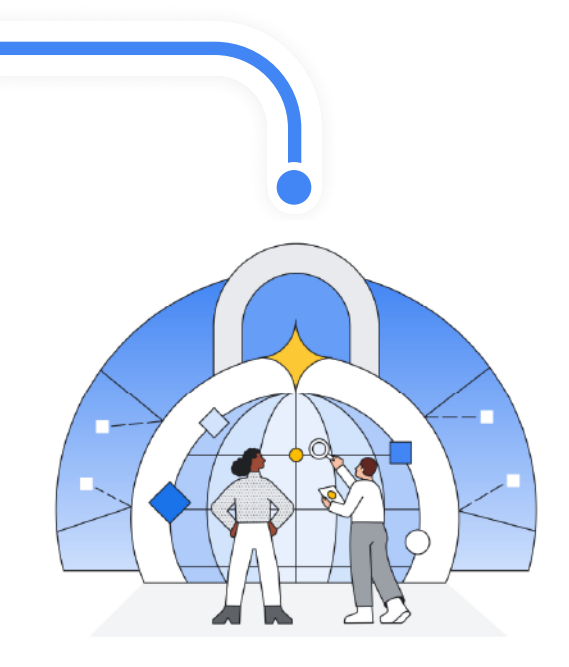
भविष्य पर केंद्रित, हम अगली पीढ़ी के क्रिप्टोग्राफ़िक सिस्टम विकसित करना जारी रखे हुए हैं, जो सार्वजनिक-कुंजी क्रिप्टोसिस्टम में खामी होने और डिजिटल संचार को असुरक्षित होने से बचाते हैं. राष्ट्रीय मानक और प्रौद्योगिकी संस्थान ने मानकीकरण के लिए Google की भागीदारी के साथ एक सबमिशन (SPHINCS+) का चुनाव किया.

2022
Mandiant Google

Mandiant, साइबर सिक्योरिटी की फ़्रंटलाइन पर दुनिया के सबसे बड़े संगठनों के साथ खतरे की रियल टाइम, गहरी खुफिया जानकारी देता है. Google Cloud की क्लाउड-नेटिव सिक्योरिटी पेशकशों के साथ मिलकर, हम एंटरप्राइस और सार्वजनिक क्षेत्र की एजेंसियों को पूरे सिक्योरिटी जीवनचक्र में प्रोटेक्टेड रहने में मदद करते हैं.

2023
पासकी: पासवर्ड रहित भविष्य

हम एक दशक से ज़्यादा समय से पासवर्ड रहित भविष्य के लिए चरण निर्धारित कर रहे हैं हम पासवर्ड रहित दुनिया के लिए खुले मानकों को चलाने के लिए 2013 में FIDO Alliance में शामिल हुए और अब 2023 में पासकी तकनीक के ज़रिए Android और Chrome के लिए FIDO साइन-इन मानकों के लिए अपने सपोर्ट का विस्तार करके, हमारे पास वास्तव में पासवर्ड रहित भविष्य के लिए प्लेटफ़ॉर्म होगा.

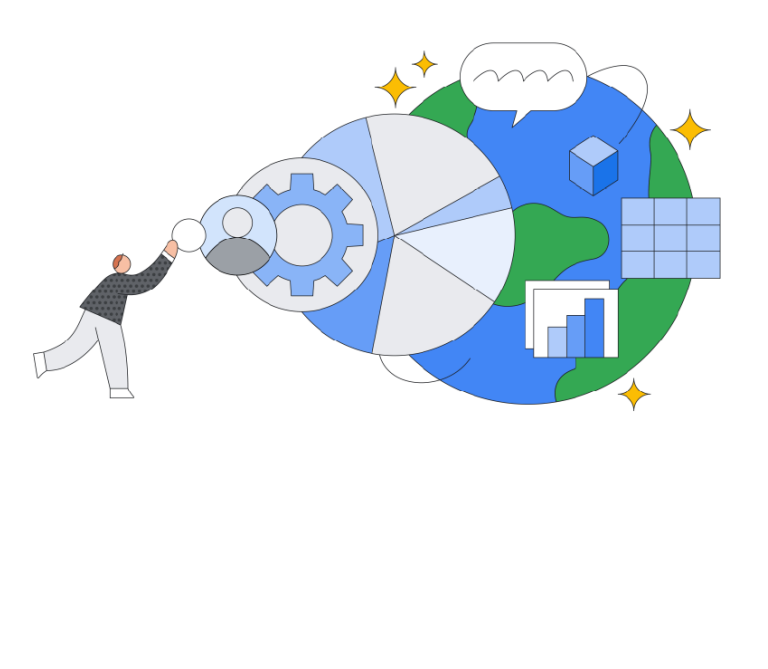


लगातार बढ़ते हुए तकनीकी एक्सेस के युग में, तकनीक में विश्वास समाज की वास्तविक क्षमता को अनलॉक करने की कुंजी है.

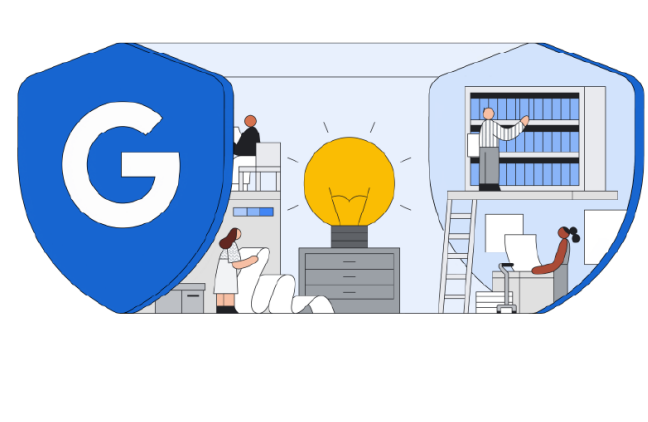
जैसा कि हम अपने सुरक्षा ज्ञान को व्यवहार में लाते हैं, हम लोगों, कारोबार और सरकारों के साथ उनकी सिक्योरिटी की रक्षा करने और साइबर सिक्योरिटी में एक नए युग की शुरुआत करने के लिए साझेदारी करना जारी रखेंगे.

लोग, कारोबार और सरकारों की रक्षा करना

सिक्योरिटी हमारी प्रोडक्ट रणनीति का आधार है. यही कारण है कि हमारे सभी प्रोडक्ट में बिल्ट-इन प्रोटेक्शन होती है जो उन्हें डिफ़ॉल्ट रूप से सिक्योर बनाती है.



हम ओपन सोर्स की क्षमता को अनलॉक करने के लिए समाजों को सशक्त बनाते हैं, और इकोसिस्टम को सुरक्षित रखने के लिए इंडस्ट्री के साथ अपने ज्ञान और विशेषज्ञता को पारदर्शी रूप से शेयर करते हैं.



हम समाज को अगली पीढ़ी के साइबर खतरों से बचाना चाहते हैं. अपनी AI विशेषज्ञता के आधार पर, हम सिक्योरिटी इनोवेशन की सीमाओं को आगे बढ़ाने के लिए ढांचे का अगला स्तर डिजाइन कर रहे हैं.

Google के साथ आप हर दिन ज़्यादा सुरक्षित होते हैं

Visit g.co/safety/cyber

Google