पासकी: हम टेक्नोलॉजी को बिना पासवर्ड के इस्तेमाल करने के और करीब आ गए हैं

सरकार की ओर से निशाना बनाकर किए जाने वाले साइबर हमलों और ऑनलाइन नुकसान पहुंचाने वाले लोगों में नाटकीय ढंग से बढ़ोतरी हुई है. इससे निपटने के लिए, हम साइबर सुरक्षा में ऐडवांस टेक्नोलॉजी को और भी बेहतर बनाने के लिए लगातार काम कर रहे हैं. साथ ही, हम अपनी विशेषज्ञता शेयर करके लोगों, कारोबारों और सरकारों की सुरक्षा करने, समाज को सशक्त बनाने और सभी के लिए एक सुरक्षित दुनिया बनाने में मदद करने पर पहले से कहीं ज़्यादा ध्यान दे रहे हैं.

आज ऑनलाइन सुरक्षा के लिए पासवर्ड बेहद ज़रूरी हैं, लेकिन फ़िशिंग जैसे खतरे लगातार बढ़ रहे हैं. Google ने काफ़ी समय पहले इन समस्याओं को पहचान लिया था और इनका समाधान करने के लिए दो चरणों में पुष्टि (2SV) की सुविधा चालू करने, Google Password Manager, सिक्योरिटी की और अब पासकी जैसे पुष्टि करने की सुविधा देने वाले टूल के इस्तेमाल को बढ़ावा दे रहा है.

चुनौती

कंप्यूटर में पासवर्ड का इस्तेमाल 60 साल से ज़्यादा समय से किया जा रहा है. हालांकि, आज यूज़र्स और संगठनों के डेटा को सुरक्षित रखने के लिए पासवर्ड काफ़ी नहीं हैं. पासवर्ड में सुरक्षा से जुड़ी कमियों का फ़ायदा उठाकर पहचान में न आने वाले फ़िशिंग हमले बढ़ते जा रहे हैं. उदाहरण के लिए:

- 2021 में, **60% से ज़्यादा डेटा ब्रीच** में चोरी किए गए क्रेडेंशियल या फ़िशिंग हमले शामिल थे.[1]
- फ़िशिंग की वजह से हुए डेटा ब्रीच से संगठनों को 2022 में **औसतन $4.91 मिलियन** का नुकसान हुआ.[2]
- 2022 में, फ़िशिंग हमलों में **61%** की बढ़ोतरी हुई, जो छह महीने में 255 मिलियन तक पहुंच गई.[3]

दो चरणों में पुष्टि/दो तरीकों से पुष्टि की सुविधा (2SV/2FA) सुरक्षा में मदद करती है, लेकिन यह यूज़र के लिए थोड़ी असुविधाजनक हो सकती हैं. साथ ही, यह फ़ीचर अभी भी फ़िशिंग हमलों और SMS वेरिफ़िकेशन के लिए "सिम की अदला-बदली करके की जाने वाली हैकिंग" जैसे निशाना बनाकर किए जाने वाले हमलों से पूरी तरह से सुरक्षा नहीं करती है.

समाधान

FIDO Alliance के साथ मिलकर, हमने पासकी को ज़्यादा मज़बूत बनाया है - इसके तहत, हमने पासवर्ड का एक आसान और सुरक्षित विकल्प खोज निकाला, जो दुनिया भर के अरबों लोगों को फ़िशिंग हमलों से रोकथाम की नई टेक्नोलॉजी देता है. ज़्यादा आसान और सुरक्षित तरीके से साइन इन करने के लिए पासवर्ड के बजाय पासकी, फ़िंगरप्रिंट, फ़ेस स्कैन या स्क्रीन लॉक सुविधा का इस्तेमाल किया जा सकता है.

2023 की शुरुआत में, प्राइवेट Google खातों के साथ-साथ 9 मिलियन से ज़्यादा Google Workspace के यूज़र्स के लिए पासकी उपलब्ध हो गईं. साथ ही, Chrome और Android पर तीसरे पक्ष की साइट और ऐप्लिकेशन पर भी पासकी उपलब्ध हैं.

साइन-इन करने का आसान और तेज़ तरीका

पासकी का इस्तेमाल करना **4 गुना आसान** है, क्योंकि इन्हें याद रखने या टाइप करने की ज़रूरत नहीं होती. आप अपने सभी डिवाइस में साइन इन करने के लिए सिर्फ़ अपने फ़िंगरप्रिंट, फ़ेस स्कैन या स्क्रीन लॉक का इस्तेमाल कर सकते हैं.[4]

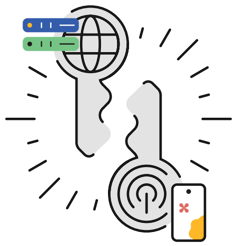
खाते की सुरक्षा के लिए अगली पीढ़ी की टेक्नोलॉजी

पासकी, फ़िशिंग जैसे खतरों के ख़िलाफ़ सबसे मज़बूत सुरक्षा देती हैं. ये आपके लोकल डिवाइस पर पहले से ही स्टोर होती हैं, इसलिए हमलावर इनका अनुमान नहीं लगा सकते और न ही इन्हें दोबारा इस्तेमाल किया जा सकता है. इस वजह से आपकी जानकारी पूरी तरह से सुरक्षित रहती है.

आपकी प्राइवेसी आपके सुरक्षित हाथों में

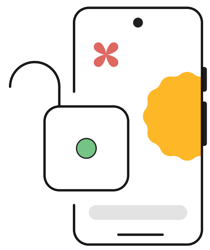
आपकी पासकी, आपके प्राइवेट डिवाइस पर सुरक्षित रहती है और इसे कभी भी Google या किसी थर्ड पार्टी पार्टनर के साथ शेयर नहीं किया जाता. आप अपनी प्राइवेट की ऐक्सेस करते समय खुद को वेरिफ़ाई करने के लिए बस अपने फ़िंगरप्रिंट, फ़ेस स्कैन या स्क्रीन लॉक का इस्तेमाल कर सकते हैं.

निजी तौर पर काम करना



पासकी के दो हिस्से होते हैं: जिस वेबसाइट पर आप साइन इन कर रहे हैं उसके लिए सर्वर पर एक पब्लिक की होती है और आपके डिवाइस पर एक प्राइवेट की होती है.

जब साइन इन किया जाता है, तो वेबसाइट यह चेक करती है कि आपकी पब्लिक की, आपकी प्राइवेट की से मेल खाती है या नहीं.



यह वेरिफ़ाई करने के लिए, आपसे सिर्फ़ अपने डिवाइस को अनलॉक करने के लिए कहा जाता है.

आपको खाते में साइन इन रखा जाएगा, आपकी प्राइवेट की और आपके बायोमेट्रिक्स आपके डिवाइस पर सुरक्षित रहेंगे और इन्हें कभी भी शेयर नहीं किया जाएगा.

सुरक्षित इकोसिस्टम बनाना

कारोबारों और सरकारों के लिए पासकी उपलब्ध कराना

पासकी की मदद से यूज़र्स को सुरक्षा और इस्तेमाल से जुड़े फ़ायदे मिलते हैं. साथ ही, हमें खुशी है कि हम इस टेक्नोलॉजी को अपने ग्राहकों - छोटे बिज़नेस और बड़े एंटरप्राइज़ से लेकर स्कूलों और सरकारों तक पहुंचा रहे हैं और हम ऐसा करने वाले पहले प्रमुख पब्लिक क्लाउड प्रोवाइडर हैं.

इंटरनेट पर बिना पासवर्ड के टेक्नोलॉजी का इस्तेमाल और सुरक्षित साइन-इन के लिए पार्टनरशिप करना

हम Chrome और Android प्लैटफ़ॉर्म पर पासकी उपलब्ध कराने के लिए ब्रैंड के साथ पार्टनरशिप करते हैं. इससे उनके यूज़र्स ज़्यादा सुरक्षित तरीके और आसानी से साइन-इन कर पाते हैं. ई-कॉमर्स, वित्तीय काम के लिए टेक्नोलॉजी, यात्रा और दूसरी इंडस्ट्री से जुड़े कई पार्टनर पहले से ही हमारे साथ बिना पासवर्ड के टेक्नोलॉजी का इस्तेमाल करने के इस सफ़र में शामिल हो चुके हैं. इन कंपनी में, 1Password, Adobe, Dashlane, DocuSign, Kayak, Mercari, PayPal और Yahoo! Japan शामिल हैं.

बिना पासवर्ड के टेक्नोलॉजी बनाने से जुड़ा हमारा सफ़र

पासकी की मदद से हम भविष्य में बिना पासवर्ड की टेक्नोलॉजी इस्तेमाल करने के बेहद करीब आ गए हैं. इसका ब्लूप्रिंट हम एक दशक से भी ज़्यादा समय से बना रहे हैं.

2008	2011	2012	2013	2014	2017	2019	2023
आसान और सुरक्षित साइन-इन के लिए Google Password Manager लॉन्च किया गया.	Google खातों के लिए 2-चरणों में पुष्टि (2SV) का फ़ीचर शुरू किया गया.	Google के कर्मचारियों को फ़िशिंग हमलों से सुरक्षा के लिए की उपलब्ध कराई गई.	बिना पासवर्ड की टेक्नोलॉजी इस्तेमाल करने वाली दुनिया के लिए खुले स्टैंडर्ड को आगे बढ़ाया और FIDO Alliance में शामिल हुए.	सभी को फ़िशिंग हमलों से बचाने के लिए, सिक्योरिटी की उपलब्ध कराईं.	ज़्यादा जोखिम वाले यूज़र्स के लिए Advanced Protection Program (APP) शुरू किया.	सभी वेबसाइट पर बिना पासवर्ड के दोबारा पुष्टि करने की सुविधा के लिए Android पर अपना FIDO सपोर्ट बढ़ाया.	Google खातों, Workspace के ग्राहकों और Chrome और Android पर थर्ड पार्टी पार्टनर के लिए पासकी उपलब्ध कराईं.

पासकी के हमारे शुरुआती सफ़र में पासवर्ड हमारे जीवन का हिस्सा बने रहेंगे. हम लोगों और इंडस्ट्री की दूसरी इकाइयों की मदद करने के लिए प्रतिबद्ध हैं. Google के साथ साइन इन को आसान और सुरक्षित बनाने के लिए हमारे साथ अगला कदम बढ़ाएं.

सोर्स: 1 - वेरिज़न डेटा ब्रीच इंवेस्टिगेशन रिपोर्ट 2022 | 2 - IBM कोस्ट ऑफ़ डेटा ब्रीच रिपोर्ट 2023
3 - CNBC की साइबर रिपोर्ट | 4 - Google का सुरक्षा ब्लॉग, मई 2023