Ψηφιακές και προσβάσιμες εκδόσεις εδώ

Google

Κλειδιά πρόσβασης: Ένα βήμα πιο κοντά σε ένα μέλλον χωρίς κωδικούς πρόσβασης

Με τη δραματική αύξηση των κυβερνοεπιθέσεων με κρατική υποστήριξη και των κακόβουλων χρηστών στο διαδίκτυο, εστιάζουμε περισσότερο από ποτέ στην προστασία των ανθρώπων, των επιχειρήσεων και των κυβερνήσεων, με το να μοιραζόμαστε την τεχνογνωσία μας, να ενδυναμώνουμε την κοινωνία και να εργαζόμαστε συνεχώς για την εξέλιξη της τεχνολογίας στον τομέα της κυβερνοασφάλειας, ώστε να οικοδομήσουμε έναν ασφαλέστερο κόσμο για όλους.

Σήμερα οι κωδικοί πρόσβασης είναι απαραίτητοι για την ασφάλεια στο διαδίκτυο, αλλά οι απειλές όπως το ηλεκτρονικό ψάρεμα (phishing) εξακολουθούν να αυξάνονται. Η Google έχει από καιρό αντιληφθεί αυτά τα προβλήματα και συνιστά τη χρήση εργαλείων ελέγχου ταυτότητας, όπως η επαλήθευση σε 2 βήματα (2SV), ο Διαχειριστής κωδικών πρόσβασης Google, τα κλειδιά ασφαλείας και πλέον τα κλειδιά πρόσβασης (passkeys).

Πρόκληση

Οι κωδικοί πρόσβασης χρησιμοποιούνται στους υπολογιστές για πάνω από 60 χρόνια, αλλά σήμερα απλά δεν επαρκούν πια για να διατηρήσουν ασφαλή τα δεδομένα των χρηστών και των οργανισμών. Οι επιθέσεις ηλεκτρονικού ψαρέματος (phishing) εξακολουθούν να αυξάνονται σε κλίμακα και πολυπλοκότητα, καθώς εκμεταλλεύονται τις αδυναμίες ασφάλειας των κωδικών πρόσβασης. Για παράδειγμα:

- Το 2021, πάνω από το **60% των παραβιάσεων δεδομένων** αφορούσαν κλεμμένα διαπιστευτήρια σύνδεσης ή ηλεκτρονικό ψάρεμα (phishing).[1]
- Οι παραβιάσεις δεδομένων λόγω ηλεκτρονικού ψαρέματος (phishing) κόστισαν στους οργανισμούς **κατά μέσο όρο 4,91 εκατομμύρια δολάρια** το 2022.[2]
- Οι επιθέσεις ηλεκτρονικού ψαρέματος (phishing) αυξήθηκαν κατά **61%** το 2022, αγγίζοντας τα 255 εκατομμύρια σε ένα εξάμηνο.[3]

Η επαλήθευση σε 2 βήματα/ο έλεγχος ταυτότητας 2 παραγόντων (2SV/2FA) βοηθάει, αλλά μπορεί να δημιουργήσει επιπλέον τριβή για τον χρήστη και εξακολουθεί να μην προστατεύει πλήρως από επιθέσεις ηλεκτρονικού ψαρέματος (phishing) και στοχευμένες επιθέσεις όπως οι απάτες «ανταλλαγής κάρτας SIM» (SIM swapping) για επαλήθευση μέσω SMS.

Λύση

Συνεργαζόμενοι με τη Συμμαχία FIDO, ενεργοποιήσαμε την υποστήριξη για κλειδιά πρόσβασης — μια απλούστερη και ασφαλέστερη εναλλακτική λύση έναντι των κωδικών πρόσβασης που παρέχει σε δισεκατομμύρια χρήστες παγκοσμίως τεχνολογία προστασίας από το ηλεκτρονικό ψάρεμα (phishing). Με τα κλειδιά πρόσβασης, μπορείτε να παρακάμψετε τον κωδικό πρόσβασής σας για μια ευκολότερη και ασφαλέστερη εμπειρία σύνδεσης, χρησιμοποιώντας το δακτυλικό σας αποτύπωμα, τη σάρωση προσώπου ή το κλείδωμα οθόνης.

Από τις αρχές του 2023, τα κλειδιά πρόσβασης είναι διαθέσιμα για προσωπικούς λογαριασμούς Google, για περισσότερους από 9 εκατομμύρια πελάτες του Google Workspace, καθώς και για ιστοτόπους και εφαρμογές τρίτων στο Chrome και το Android.

Ο απλούστερος και ταχύτερος τρόπος σύνδεσης

Τα κλειδιά πρόσβασης είναι **4 φορές απλούστερα** στη χρήση, καθώς δε χρειάζεται να τα θυμάστε ή να τα πληκτρολογείτε. Απλά χρησιμοποιείτε το δακτυλικό σας αποτύπωμα, τη σάρωση προσώπου ή το κλείδωμα οθόνης για να συνδεθείτε σε όλες τις συσκευές και τις πλατφόρμες σας.[4]

Ασφάλεια λογαριασμού επόμενης γενιάς

Τα κλειδιά πρόσβασης παρέχουν την ισχυρότερη προστασία από απειλές όπως το ηλεκτρονικό ψάρεμα (phishing). Και εφόσον αποθηκεύονται τοπικά στη συσκευή σας, δεν μπορούν να παραβιαστούν ή να επαναχρησιμοποιηθούν, προστατεύοντας τις πληροφορίες σας από εισβολείς.

Απόρρητο που είναι αποκλειστικά δικό σας

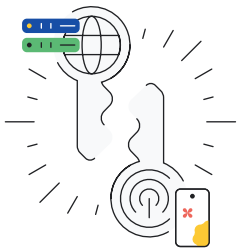
Το κλειδί πρόσβασής σας παραμένει ιδιωτικό στην προσωπική σας συσκευή και δεν κοινοποιείται ποτέ στην Google ή σε τρίτους συνεργάτες. Απλώς χρησιμοποιείτε το δακτυλικό σας αποτύπωμα, τη σάρωση προσώπου ή το κλείδωμα οθόνης για να επιβεβαιώσετε ότι είστε εσείς που χρειάζεστε πρόσβαση στο ιδιωτικό σας κλειδί.

Safer with Google

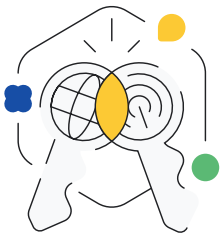
Ψηφιακές και προσβάσιμες εκδόσεις εδώ

Google

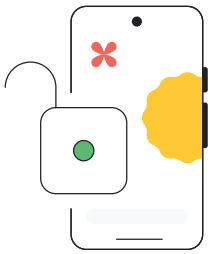
Σύνθετες επιλογές



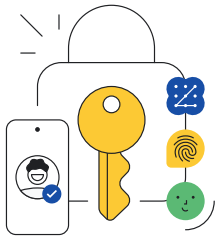
Ένα κλειδί πρόσβασης αποτελείται από δύο μέρη: ένα δημόσιο κλειδί στον διακομιστή του ιστοτόπου στον οποίο συνδέεστε και ένα αντίστοιχο ιδιωτικό κλειδί στις συσκευές σας.



Όταν συνδέεστε, ο ιστότοπος ελέγχει αν το δημόσιο κλειδί σας ταιριάζει με το ιδιωτικό.



Για να επαληθευτεί ότι ταιριάζει, σας ζητείται απλώς να ξεκλειδώσετε τη συσκευή σας.



Έτσι, συνδέεστε στον λογαριασμό σας και το ιδιωτικό σας κλειδί, καθώς και τα βιομετρικά σας στοιχεία παραμένουν ασφαλή στη συσκευή σας και δεν κοινοποιούνται ποτέ.

Ένα ασφαλέστερο οικοσύστημα

Εφαρμογή των κλειδιών πρόσβασης σε επιχειρήσεις και κυβερνήσεις

Τα κλειδιά πρόσβασης προσφέρουν σημαντικά πλεονεκτήματα ευχρηστίας και ασφάλειας στους χρήστες. Είμαστε ενθουσιασμένοι που είμαστε ο πρώτος μεγάλος πάροχος public cloud που εξασφαλίζει αυτήν την τεχνολογία στους πελάτες μας — από μικρές και μεγάλες επιχειρήσεις μέχρι εκπαιδευτικά ιδρύματα και κυβερνήσεις.

Συνεργασία για μια ασφαλέστερη σύνδεση χωρίς κωδικούς πρόσβασης σε όλο το Διαδίκτυο

Συνεργαζόμαστε με επωνυμίες για να ενεργοποιήσουμε τα κλειδιά πρόσβασης στις πλατφόρμες Chrome και Android, παρέχοντας ευκολότερη και ασφαλέστερη σύνδεση για τους χρήστες τους. Πολλοί συνεργάτες σε κλάδους όπως το ηλεκτρονικό εμπόριο, η χρηματοοικονομική τεχνολογία, ο τουρισμός κλπ. έχουν ήδη ξεκινήσει μαζί μας το ταξίδι για ένα μέλλον χωρίς κωδικούς πρόσβασης, συμπεριλαμβανομένων των 1Password, Adobe, Dashlane, DocuSign, Kayak, Mercari, PayPal και Yahoo! Japan.

Το ταξίδι μας για ένα μέλλον χωρίς κωδικούς πρόσβασης

Τα κλειδιά πρόσβασης μας φέρνουν πολύ πιο κοντά στο μέλλον χωρίς κωδικούς πρόσβασης που σχεδιάζουμε για πάνω από μια δεκαετία.

2008
Κυκλοφόρησε ο Διαχειριστής κωδικών πρόσβασης Google για ευκολότερες και ασφαλέστερες συνδέσεις.

2011
Ενεργοποιήσαμε την επαλήθευση σε 2 βήματα (2SV) για τους λογαριασμούς Google.

2012
Παρουσιάσαμε ένα κλειδί ασφαλείας για τους υπαλλήλους της Google που είναι ανθεκτικό στο ηλεκτρονικό ψάρεμα (phishing).

2013
Ενταχθήκαμε στη Συμμαχία FIDO για την προώθηση ανοικτών προτύπων για έναν κόσμο χωρίς κωδικούς πρόσβασης.

2014
Διαθέσαμε σε όλους τα ανθεκτικά στο ηλεκτρονικό ψάρεμα (phishing) κλειδιά ασφαλείας.

2017
Παρουσιάσαμε το Πρόγραμμα Προηγμένης Προστασίας (APP) για χρήστες υψηλού κινδύνου.

2019
Επεκτείναμε την υποστήριξή μας για το FIDO σε Android για εκ νέου εξουσιοδότηση χωρίς κωδικούς πρόσβασης σε όλους τους ιστοτόπους.

2023
Ενεργοποιήσαμε τα κλειδιά πρόσβασης για τους λογαριασμούς Google, τους πελάτες του Workspace και τους συνεργάτες τρίτων σε Chrome και Android.

Ενώ οι κωδικοί πρόσβασης θα συνεχίσουν να αποτελούν μέρος της ζωής μας καθώς κάνουμε τη μετάβαση στα passkeys (κλειδιά πρόσβασης), είμαστε αποφασισμένοι να βοηθήσουμε τους χρήστες και άλλους στον τομέα, να κάνουν το επόμενο βήμα, ώστε να συνδέονται ευκολότερα και ασφαλέστερα με την Google.

Πηγές: 1 - Verizon Data Breach Investigation report 2022 | 2 - IBM Cost of Data Breach report 2023
3 - CNBC's Cyber Report | 4 - Google Security Blog, May 2023

Safer with Google

Εξερευνήστε τους τρόπους με τους οποίους η Google συμβάλλει στη διατήρηση της ασφάλειας όλων των χρηστών στο διαδίκτυο στη διεύθυνση safety.google/intl/el_gr/