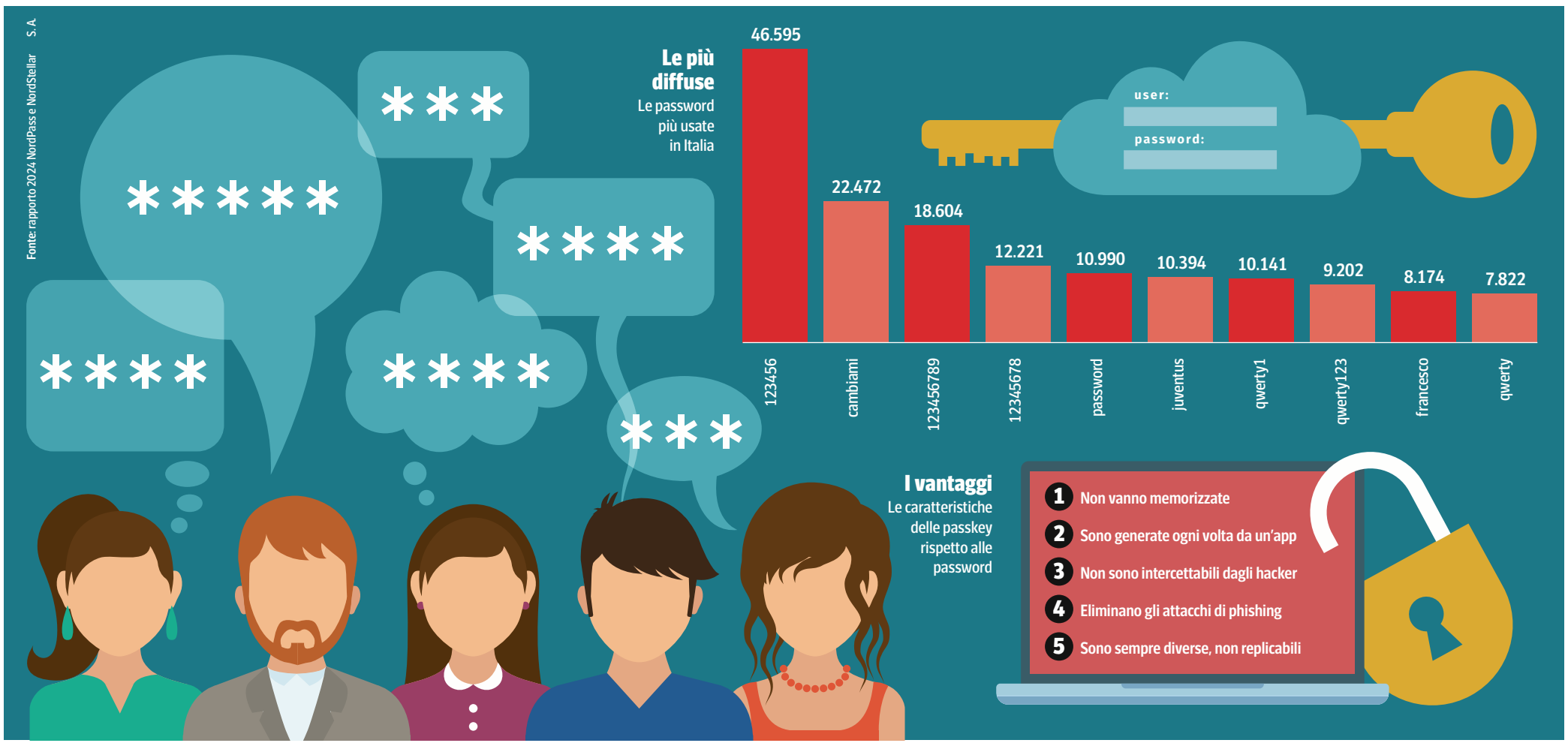
LE BIG TECH CAMBIANO I CODICI INTERNET, SE C'È LA PASSKEY IL PIRATA NON PASSA



Password tradizionali addio: Microsoft, Google, Apple e Amazon le sostituiscono con Pin, impronte digitali e riconoscimento facciale Diventa più difficile per gli hacker sottrarre i dati personali Mentre tre milioni di persone usano ancora lo schema «123456»...

di **UMBERTO TORELLI**

Tempo scaduto per le classiche password: presto verranno sostituite dalle «passkey». È una nuova procedura per accedere agli account dei servizi informatici usando un Pin, le impronte digitali e il riconoscimento facciale. Così aumenta la sicurezza i dati personali sono più protetti. Le big tech vi puntano. Microsoft, da inizio maggio 2025, ha esteso l'uso delle passkey al momento di creare nuovi account personali. Così l'accesso ai servizi come 365 e Copilot ora avviene tramite la scansione del viso e le impronte digitali, senza digitare alcuna password. La multinazionale di Redmond, guidata dal 2014 dall'amministratore delegato Satya Nadella, prevede di toccare il miliardo di utenti. Google ha introdotto le passkey l'anno scorso e oggi oltre 400 milioni di persone nel mondo le stanno usando.

Apple integra le passkey nei dispositivi dotati di sistemi iOs, iPadOs, macOs, con accesso tramite Face Id e Touch Id. Seguendo una tradizione consolidata, non rivela numeri.

Amazon, infine, ha annunciato l'uso della nuova modalità di identificazione sia su browser che nelle app, offrendo ai clienti la possibilità di autenticarsi in modo diretto.

Combinazioni deboli

Sembra incredibile, ma ancora oggi tanti cybernauti usano password deboli e scontate. NordPass, azienda lituana di sicurezza informatica, rivela che la combinazione «123456» continua a essere la più utilizzata al mondo. Nel 2024 erano oltre tre milioni gli utenti a farne uso (più di 46 mila in Italia): credono di tenere al sicuro i propri archivi digitali, ma non sanno che un hacker, con l'aiuto dei nuovi software d'intelligenza artificiale, impiega meno di un secondo a violarla.

L'anno scorso la gran parte delle intrusioni informatiche è avvenuta per l'assenza di caratteri speciali nella parola chiave

Lo scorso anno l'80% delle intrusioni informatiche, secondo i dati dell'americana IdDataweb, è avvenuto per la presenza di password prive di caratteri speciali. Un grave errore secondo Clusit, l'associazione italiana per la sicurezza informatica.

Spiega a proposito Alessio Pennasilico, del comitato scientifico di Clusit: «Questa leggerezza, abbinata all'utilizzo della stessa password per diversi servizi e al mancato aggiornamento del software dei dispositivi, mette a rischio tutta la sfera digitale personale». Spalancando le porte di dati e informazioni ai pirati informatici.

Con il rapido aumento degli account online, però, cresce anche la necessità di creare e ricordare innumerevoli password uniche, e la conseguente difficoltà di gestirle. Le app password manager, cioè le applicazioni per memorizzare le formule di accesso sul cloud, sono un passo importante per evitare confusione e avere le password disponibili in tempo reale.

«Tuttavia gli utenti possono rafforzare la sicurezza attivando l'autenticazione multi fattore con l'aggiunta di dati biometrici — spiega Luca Nilo Levrieri di CrowdStrike — . Questo assicura un livello di protezione extra». Ma va evitato il riutilizzo della stessa password su più siti, perché la violazione di un account può propagarsi agli altri.

La svolta

Con le passkey cambia tutto. Il riconoscimento personale per accedere agli account online (come email, banca, social) avviene senza che sia necessario scrivere password. Di fatto, invece di digitare «parole segrete», si usano un Pin e un'impronta, proprio come si fa per sbloccare i telefonini di nuova generazione.

Le passkey, però, esistono soltanto sui dispositivi in uso: computer, smartphone e tablet. Con molti vantaggi. Primo, non è più necessario ricordare parole complesse, eliminando il rischio di dimenticarle e annotarle.

Inoltre le passkey sono legate al sito web e all'applicazione per cui vengono create: significa che non possono essere riutilizzate in modo fraudolento, perché sono immuni agli attacchi di phishing.

Sono gli stessi utenti, infatti, a inserirle su pagine false. Ognuna viene trasmessa in modo crittografato, dunque le eventuali credenziali rubate da un servizio non possono essere utilizzate per accedere ad altri. Ad accrescerne l'efficacia esiste poi l'autenticazione « a fattori integrati». L'utilizzo di una passkey, infatti, spesso implica un'autenticazione a due livelli, in quanto richiede sia il possesso del dispositivo sia lo sblocco tramite Pin e sistemi biometrici.

Conferma Filipe Teixeira, amministratore di altermAInd, società nata da uno spin-off di Illimity, la banca fondata da Corrado Passera: «Adesso nuove tecnologie come le biometrie comportamentali permettono di verificare gli utenti, analizzando parametri come la velocità nel digitare caratteri sulla tastiera e i movimenti del mouse, rendendo così l'accesso al web più sicuro e personalizzato».

Le passkey, basate su dati biometrici , sono un ulteriore passo avanti: «Il livello di sicurezza è praticamente impenetrabile — dice Teixera — se sono supportate da sistemi di intelligenza artificiale».

46.000

Navigatori

Glu utenti dei servizi online che in Italia adoperano la password «123456» (fonte: NordPass)