

Le grandi aziende della Silicon Valley studiano metodi di sicurezza alternativi: hanno codici sempre diversi che non devono essere memorizzati e sono a prova di hacker

# Password

Dalle impronte all'anello magico così finisce l'era della parola chiave

## I METODI

ALBERTO FLORES D'ARCAIS

**NEW YORK**  
I più raffinati usano uno *smart ring*, un anello "magico" (negli Stati Uniti è in vendita a 27,99 dollari) che inserisce automaticamente una password sempre diversa. Aziende e università si affidano a un codice numerico di cinque cifre inviato via sms. I maghi informatici di Google stanno lavorando da un anno a un protocollo che permette di connettersi con i propri account online autenticandosi attraverso lo smartphone. La vecchia password ha i giorni (mesi, anni?) contati, e per i ladri d'identità diventerà più difficile carpire i nostri segreti.

Il concetto di password è vecchio di secoli (erano usate dai militari romani) ma per l'uso che ne facciamo noi la data di nascita è il 1961, quando venne varata dagli ingegneri del

### ALFANUMERICA

La maggior parte dei sistemi attuali usa password composte da lettere e numeri ma sono facilmente decriptabili

### SMART RING

È un anello "intelligente" diffuso negli Stati Uniti: ogni volta genera automaticamente password diverse

### IRIDE

Allo studio anche la lettura dell'iride come sistema di sicurezza che sostituirà la password su tablet, pc e cellulari



### SMARTPHONE

Google lavora a un protocollo che permetta di autenticarsi ai propri account online grazie al cellulare

### IMPRONTA DIGITALE

Negli smartphone più all'avanguardia il Pin può essere sostituito dall'impronta digitale del proprietario



REPTV-LAEFFE  
Alle 13.45 su RNews  
(canale 50 del Dte e 139 di Sky) il servizio sulla fine delle password



Lo *smart ring* — un anello in lega di acciaio e titanio — funziona grazie al Nfc (Near Field Communication) e ai suoi due chip incorporati. Il primo è una sorta di biglietto da visita virtuale, basta avvicinare l'anello ad uno smartphone (dotato di modulo Nfc) per trasferire al suo interno i nostri dati personali quali nome, indirizzo, email ed eventuale sito web. Il secondo permette di sbloccare alcune applicazioni, accedere

al telefono o inserire automaticamente delle password. L'autenticazione attraverso un messaggio di testo (o una *app* particolare, che ha il vantaggio di funzionare anche quando non c'è segnale per il cellulare) è semplice, veloce e permette nel caso di intrusioni di bloccare tutto rapidamente. Per mandare al macero la vecchia password sono al lavoro un po' tutti nella Silicon Valley e nei prossimi mesi oltre a Google si

avranno le proposte di aziende specializzate come Telesign (che lo ha anticipato al *Wall Street Journal*) e Authy.

Può sembrare assurdo rimpiazzare un codice di autenticazione che uno (in teoria) può conservare solo nella propria memoria (la password alfanumerica) con uno che si deve tenere in tasca o nella borsa (come lo smartphone) e che può essere facilmente rubato. Chi vuole abolire la password la spiega così: nel primo caso ci sarà sempre in giro un hacker che può penetrare nell'account, nel secondo basta bloccare l'iPhone (o il Samsung Android). In più negli smartphone c'è anche un Pin, che nei modelli più recenti può essere la propria impronta digitale. Lo smartphone diventerà dunque sempre più indispensabile, anche per chi ne vorrebbe fare a meno.

© RIPRODUZIONE RISERVATA

Tra gli altri c'è anche l'autenticazione attraverso un sms che arriva sullo smartphone

Mit di Boston. Oggi è parte integrante della nostra vita con un paio di regole molto semplici: più è complicata e più è difficile da ricordare, più ne abbiamo e più ce le dobbiamo scrivere da qualche parte, che sia la vecchia agenda o il post-it virtuale sul computer.

La gente è piuttosto prevedibile, uno studio ha dimostrato che negli Stati Uniti per la maggioranza delle password vengono usati codici banali come "password" (che fantasia!), "123456", "daddy", "hamburger". Banali e facili da rubare per i criminali che imperversano nella rete e che — in numero sempre maggiore — riescono ad impadronirsi della nostra privacy, siano documenti, foto o conti bancari. L'uso sfrenato del web e dei social network, le password dei sistemi pubblici in balia degli hacker, lo spionaggio della Nsa (e di tanti altri) stanno provocando una crisi di rigetto verso il vecchio metodo di sicurezza ed ecco allora la necessità di sostituirlo con qualcosa di più sicuro.

