

Per proteggere la nostra vita digitale, una semplice password non basta più.
Per fortuna sono sempre più numerosi i servizi che offrono una forma di autenticazione più robusta.

AUTENTIC A DUE



AZIONE FATTORI

● Di Marco Schiaffino

Il cloud permette di accedere ai propri documenti e a tanti servizi utili da qualsiasi luogo e in qualsiasi momento. Ma qual è il livello di sicurezza? Nella maggior parte dei casi, l'accesso è protetto da una semplice password. Un approccio che ha molti limiti e che, soprattutto se utilizzato con leggerezza, espone al rischio di subire il furto dei dati. Eppure esiste una forma di protezione molto più efficace: la cosiddetta autenticazione a due fattori, che oggi molti servizi online permettono di implementare con grande facilità. In questo articolo esamineremo i punti deboli della tradizionale autenticazione tramite password, poi vi spiegheremo come funziona l'autenticazione a due fattori e vi mostreremo come attivarla per blindare la vostra identità digitale e proteggere meglio i vostri dati nel cloud.

Nell'estate del 2012, il giornalista americano Mat Honan è stato vittima di un attacco da parte di un gruppo di hacker il cui obiettivo, come ha raccontato nel suo blog, era impadronirsi del suo account Twitter. L'attacco ha avuto successo, ma non si è fermato a Twitter: nel giro di un'ora la vita digitale di Honan si è disintegrata. Oltre a sottrargli l'account Twitter, gli hacker hanno eliminato anche il suo account Gmail e hanno cancellato da remoto tutti i dati che conservava sull'iPhone, sull'iPad e sul MacBook, compresi anni di fotografie familiari (di cui colpevolmente non aveva mai fatto il backup). Un vero incubo, ma fa ben comprendere l'importanza che oggi ha la nostra identità digitale.

Nell'era del cloud, il "patrimonio digitale" di una persona può comprendere documenti, contatti, musica, foto, video e libri, ma anche informazioni riservate, comunicazioni personali, accrediti per i servizi di home banking e persino documenti relativi alle comunicazioni con la pubblica amministrazione. Beni intangibili, che tuttavia possono avere un valore anche superiore a quelli fisici. L'aspetto della loro protezione, però, è ancora sottovalutato ed è grave, perché la sempre maggiore decentralizzazione degli ecosistemi digitali in cui si muoviamo ha assottigliato il livello di controllo che abbiamo sulla loro gestione. Come insegna la disavventura di Honan, la disponibilità della nostra vita digitale dipende dalla nostra identità e, in definitiva, dall'efficacia con cui può essere verificata attraverso l'autenticazione, ovvero il processo che permette di associare un'identità a una persona.



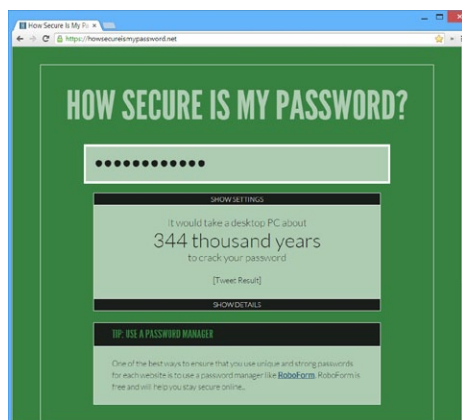
Nell'estate del 2012 un attacco hacker ha distrutto la "vita digitale" del giornalista americano Matt Honan. La sua storia insegna quanto sia importante oggi la nostra identità digitale.

C'ERA UNA VOLTA LA PASSWORD

Il metodo di autenticazione più semplice e diffuso è la password, ovvero qualcosa che conosciamo e che ci permette di confermare la nostra identità in maniera

relativamente semplice. Uno dei rischi legati all'utilizzo della password è quello di sottovalutarne la fragilità: come vedremo, questa dipende da numerosi aspetti, che incidono in misura maggiore o minore sul livello di sicurezza di tutti gli account. Il primo è più ovvio riguarda la robustezza della password. Qui la minaccia è rappresentata dagli attacchi di *brute forcing*, ovvero da quei software che cercano di violare una password utilizzando il metodo più semplice: provare tutte le possibili combinazioni nella speranza di identificare quella giusta. A prima vista può sembrare un'operazione disperata, ma non è così.

Utilizzando un normale PC desktop per la verifica di tutte le combinazioni possibili, il tempo necessario per individuare una password composta da 8 lettere minuscole digitate a caso, infatti, richiede meno di un minuto secondo le stime del sito www.howsecureismypassword.net. Usando però per i calcoli i potentissimi processori grafici (Gpu) delle moderne schede video, i tempi si riducono drasticamente. Un prototipo di questo tipo, realizzato un paio di anni dallo Strictur Consulting Group, usava un cluster di 5 server con in tutto 25 Gpu e si era rivelato un "mostro" in grado di provare 348 miliardi di combinazioni al secondo. Teoricamente i servizi online dovrebbero essere protetti dagli attacchi basati sul brute forcing attraverso l'imposizione di un limite massimo di tentativi di accesso in un dato periodo di tempo. Le eccezioni, però, ci sono. Lo scorso marzo, per esempio, il ricercatore Ibrahim Balic ha individuato nel sistema



Il sito **www.howsecureismypassword.net** permette di stimare il tempo necessario per violare una password utilizzando un normale Pc desktop e la tecnica del brute forcing.

di autenticazione iCloud di Apple una falla che permetteva di eseguire "pacchetti" di 20.000 tentativi di accesso alla volta, aprendo la strada all'uso del brute forcing per violare gli account del servizio. Una falla che, secondo quanto riportato lo stesso Balic, è stata chiusa solo dopo sei lunghi mesi dalla sua scoperta.

DALLA PASSWORD ALLA PASSPHRASE

Se l'ipotesi di un attacco basato sul brute forcing rimane un rischio concreto anche per i servizi online, l'unica contromisura è rappresentata dall'uso di una password "robusta" che sia molto difficile o virtualmente impossibile da individuare. Gli elementi che determinano la robustezza di una password sono essenzialmente la lunghezza e i caratteri utilizzati; normalmente si

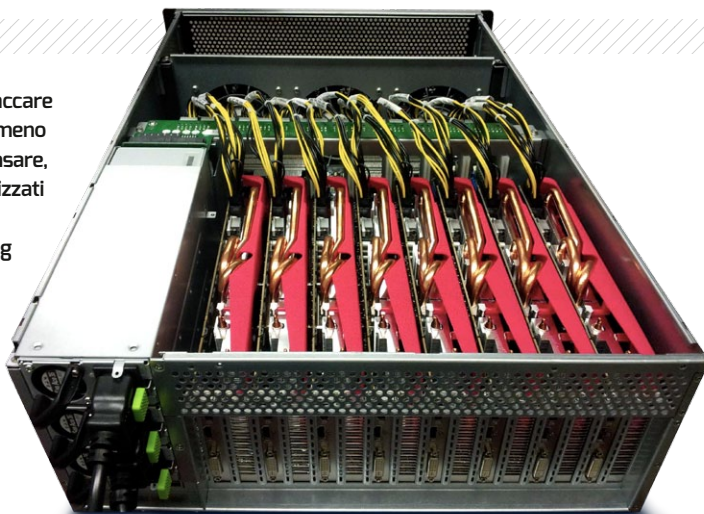
sconsiglia di utilizzare password che abbiano come minimo 8 caratteri, anche se per servizi particolarmente critici (come un sistema di home banking) è opportuno non scendere sotto i 12 caratteri. È bene tenere presente che non solo l'aumento del numero di caratteri migliora esponenzialmente la robustezza della password, ma l'utilizzo di numeri, lettere maiuscole e simboli speciali in aggiunta ai normali caratteri dell'alfabeto incide in maniera ancora maggiore. Nell'esempio citato in precedenza, abbiamo sostituito le prime tre lettere rispettivamente con una maiuscola, un numero e un carattere non alfanumerico: il tempo stimato per individuare la password è salito a circa tre giorni. Aggiungendo quattro lettere minuscole casuali, per arrivare a 12 caratteri, la stima è passata a oltre 347.000 anni! Lavorando su entrambi i gli aspetti (numero di caratteri e presenza di caratteri non alfabetici), si può quindi arrivare a una password ragionevolmente robusta. In questo caso spesso non si parla più di "password", ma di "passphrase".

Se sotto il profilo della sicurezza la passphrase è un sensibile passo in avanti, il suo utilizzo pratico può creare qualche problema. Una passphrase molto lunga e complessa, infatti, diventa molto difficile da ricordare. L'utilizzo di parole di senso compiuto, poi, rappresenta un'arma a doppio taglio. Lo sforzo richiesto per la memorizzazione scende, ma scende anche il tempo necessario per il brute forcing. Molti dei software specializzati nell'individuazione delle password, infatti, sfruttano per il brute forcing un dizionario che combina i termini di uso comune (compresi i nomi

Facile o robusta?

Le password lunghe e complesse sono robuste ma difficili da ricordare

Quanto ci vuole per craccare una password? Molto meno di quello che si può pensare, usando sistemi specializzati come quello realizzato dallo Strictur Consulting Group: un cluster dotato di 25 Gpu (in foto uno dei server) capace di verificare 384 miliardi di combinazioni al secondo.



CHI CONOSCE LA MIA PASSWORD?

In un mondo perfetto i gestori di un servizio Internet non vengono mai a conoscenza della password di un loro utente. Dispongono invece di un codice unico, calcolato a partire dalla password stessa, con il quale possono accertarsi che la parola chiave fornita al momento dell'accesso sia effettivamente quella giusta. Nel mondo reale invece non sono ancora rari i casi di servizi che mantengono le password in chiaro nel loro database degli utenti: un rischio enorme sotto il profilo della sicurezza. Ma anche quando il database in questione non contiene direttamente le password ma solo i codici associati (chiamati *hash*), non è detto che gli utenti possano stare tranquilli. In teoria non è possibile ricostruire la password a partire dall'hash, sempreché l'hash stesso sia stato generato in modo corretto. Nella pratica, invece, errori – a volte incredibilmente stupidi – nella procedura di generazione dell'hash possono rendere fattibile il recupero della password associata. Società anche di enormi dimensioni a volte si sono rese colpevoli di questa inaccettabile superficialità nella gestione delle password dei loro utenti.



GESTIRE LE **PASSWORD** CON UN SOFTWARE AD HOC

A avete individuato una password robusta e per giunta facile da memorizzare? Perfetto. Ora dovrete trovarne almeno un'altra decina, o anche di più. Sfruttare la stessa parola chiave per tutti i servizi che usare, infatti, è una pessima idea. Per informazioni chiedete ad Aaron Barr, Ceo della società di sicurezza informatica HBGary Federal. Nel 2011 Barr si lasciò andare ad alcune dichiarazioni un po' troppo "ottimistiche" relativamente alle sue indagini su Anonymous, il gruppo di cyber-attivisti che in quei mesi stava strapazzando gli uffici dell'Fbi. Aveva addirittura annunciato l'imminente smantellamento di Anonymous, che sosteneva di essere riuscito a infiltrare. Anonymous non l'ha presa bene e ha reagito con un attacco ai server email di HBGary, di cui Aaron Barr stesso era amministratore. Purtroppo per lui, Barr aveva commesso l'errore di usare la stessa password per tutti i suoi servizi online. Oltre a pubblicare sul Web oltre 50.000 email di HBGary, gli hacker di Anonymous si sono divertiti a cancellare circa 1 TByte di dati di backup dello stesso Barr, estromettendolo anche dai suoi account su Twitter e Facebook. Come ciliegina sulla torta, hanno utilizzato il suo Apple ID



per cancellare da remoto tutti i dati del suo iPad. Per non fare la fine di Aaron Barr quindi, è essenziale non riutilizzare una password: il rischio è quello di essere travolti da un "effetto valanga" che potrebbe avere conseguenze disastrose.

Come fare a creare e tenere a mente passphrase distinte e abbastanza complesse da garantire un buon livello di sicurezza? La soluzione è quella di rivolgersi a un password manager come il popolarissimo LastPass (<https://lastpass.com>), disponibile in una versione gratuita, già molto versatile, e in una più potente ma a pagamento. Compatibile con Windows, Linux, OS X, oltre che con tutte le principali piattaforme mobili e i browser più diffusi, LastPass consente di memorizzare le credenziali di accesso di qualsiasi servizio Web e di ottenerne l'inserimento automatico alla digitazione di una "password master", l'unica che è necessario tenere a mente. Il ricorso a un password manager rende quindi molto più semplice, utilizzare passphrase "robuste" e diverse per ogni servizio; la maggioranza dei programmi di questo tipo possono anche generare automaticamente passphrase casuali, utilizzabili al momento della registrazione a nuovi servizi o per sostituire quelle

propri) e le loro varianti, in modo da ridurre il tempo necessario all'elaborazione. Per quanto riguarda i numeri, è poi consigliabile evitare quelli troppo ovvi, come la propria data di nascita: si tratta di informazioni che oggi, con l'uso sempre più diffuso dei siti di social networking, sono fin troppo facili da rintracciare. Uno dei metodi per irrobustire una passphrase basata su parole di senso compiuto è quello di sostituire alcune lettere con numeri che, per il loro aspetto, le ricordino. Il termine "password", per esempio, può essere trasformato in "p455w0rd". Si tratta però di un sistema ormai inflazionato, al punto che gli stessi dizionari utilizzati per il brute forcing prevedono generalmente anche le varianti di questo tipo. Meglio quindi adottare un metodo personalizzato che consenta di ricordare le passphrase e le varianti (maiuscole, numeri e caratteri speciali) con una certa facilità.

UNA PASSWORD ROBUSTA NON BASTA

Pensare che una password (o una passphrase) a prova di brute forcing risolva tutti i problemi può essere rischioso. Un'ottima dimostrazione è il caso delle foto osé di molte celebrità finite lo scorso settembre sul sito di immagini

4chan. La vicenda, oltre ad aver creato qualche imbarazzo ad Apple e alle altre aziende coinvolte, ha acceso i riflettori sulla scarsa consapevolezza degli utenti riguardo la protezione dei dati personali conservati nel cloud.

A farne le spese sono state in particolare alcune famose attrici statunitensi, tra cui la protagonista di Hunger Games Jennifer Lawrence, che hanno visto comparire sul sito appena citato numerose fotografie private trafugate dai loro account iCloud. Si trattava principalmente di selfie inviate a fidanzati e mariti e che erano anche state memorizzate nel

cloud. Nonostante in un primo momento si fosse fatta largo l'ipotesi di un hacking di iCloud attraverso una tecnica di brute forcing, le successive indagini condotte da Apple in collaborazione con l'Fbi hanno permesso di ricostruire le modalità del furto. Il responsabile, che aveva poi pubblicato parte delle foto su un forum online chiedendo donazioni in bitcoin per proseguire la pubblicazione, era riuscito a ottenere le credenziali di accesso degli account violati partendo dai rispettivi indirizzi di posta elettronica (che corrispondono al nome utente) e utilizzando il sistema di recupero della password. Nel caso di iCloud, la

il Fatto Quotidiano SEZIONI BLOG FATTO TV ABBONATI FQ SHOP

Foto di Jennifer Lawrence e altre star nude sul web. Hacker violano account iCloud

Cronaca

Jennifer Lawrence è una delle numerose attrici a cui lo scorso anno è stato violato l'account iCloud: pochi giorni dopo le sue foto private scattate col telefonino e memorizzate su iCloud sono finite su un sito pubblico.



LastPass, disponibile sia in una versione gratuita sia in una versione più potente ma a pagamento, è uno dei password manager più diffusi.

“deboli” già esistenti. Prima di mettere nelle mani di LastPass o di qualsiasi altro password manager le proprie password (un'ottima alternativa open source è KeePass, <http://keepass.info>), occorre però fare qualche considerazione. L'utilizzo di un software del genere è certamente pratico fino a quando si utilizza un singolo computer (o più sistemi, dispositivi mobili compresi, con sincronizzato il database delle password). Ma quando il password manager non è disponibile si rischia di incappare in qualche difficoltà: usare un password manager significa poter usare parole chiave davvero robuste e quindi praticamente impossibili da ricordare. LastPass tenta di risolvere il problema rendendo accessibile l'archivio delle password anche tramite una versione Web. Naturalmente l'accesso ad un servizio online effettuato su un computer non sicuro – come quello di un cybercafé – è rischioso: potrebbe essere presente un keylogger capace di memorizzare i tasti premuti, credenziali di accesso comprese. Il rischio è poi enorme per un servizio come LastPass, che fornisce le chiavi accesso all'intera vita digitale dei suoi utenti. Di conseguenza in questi casi bisogna fare molta attenzione a digitare le credenziali non dalla tastiera fisica ma da quella virtuale, a prova di keylogger, richiamabile dalla stessa pagina Web di LastPass. Come vedremo in seguito, però, è possibile blindare ulteriormente LastPass per prevenire accessi indesiderati anche in caso di furto della password grazie proprio all'autenticazione a due fattori.

procedura richiede una verifica attraverso la risposta alle classiche domande segrete che vengono impostate al momento della creazione dell'account. Un sistema piuttosto comune e in grado di fornire un discreto livello di sicurezza alle persone normali.

Ma per chi è costretto a rilasciare di continuo interviste che inevitabilmente coinvolgono anche aspetti della vita privata, ha una pagina pubblica di Facebook, una dettagliata biografia su Wikipedia e qualche decina di fan club che pubblicano a ritmo continuo curiosità e informazioni, le cose cambiano. Non è un caso che Apple, poche ore dopo lo scoppio del

caso, abbia invitato gli utenti di iCloud ad attivare un sistema di autenticazione più sofisticato, disponibile già da tempo ma poco pubblicizzato, per l'accesso ai propri account.

Tra le debolezze della semplice password come metodo di autenticazione c'è anche la necessità che sia in qualche modo conosciuta non solo dall'utente ma anche dal gestore del servizio (vedete il riquadro “Chi conosce la mia password?”): questo apre alla possibilità che possa essere sottratta non solo dal computer del legittimo proprietario o attraverso un'azione di hacking mirata sul suo account, ma direttamente dalla

banca dati di chi gestisce il servizio. La cronaca recente riporta numerosi casi di questo genere. A rimanere vittima di furti in massa dei dati di accesso dei loro clienti è stato anche un gigante come Sony, mentre tentativi di questo genere hanno interessato un po' tutti i fornitori di servizi online, da Twitter a Microsoft, passando per Blizzard. Nel caso di aziende di grosso calibro come quelle citate, gli episodi di furti di credenziali di accesso sono relativamente rare, ma le aziende più piccole o semplicemente meno attente alla sicurezza, rischiano di essere vittime di azioni di hacking con grande facilità.

Molti servizi permettono di recuperare l'accesso all'account rispondendo a una serie di domande estremamente personali. Ma, specie per i personaggi pubblici, le risposte potrebbero non essere così difficili da trovare.

Una delle tendenze in atto è l'interconnessione sempre più spinta tra i servizi online, che dialogano tra loro per offrire funzioni aggiuntive. Ne offre un esempio l'integrazione introdotta nelle settimane scorse di Office con Dropbox, che consente l'accesso diretto ai documenti memorizzati nel cloud dal programma Microsoft. Una funzione senza dubbio utile sotto il profilo pratico, ma con implicazioni da non trascurare sotto quello della sicurezza. Moltiplicando i luoghi in cui vengono conservate e utilizzate le credenziali per l'autenticazione, infatti, si moltiplica anche il rischio di un loro furto. A farne le spese, recentemente, sono

stati proprio gli utenti di Dropbox. Quando nell'ottobre scorso è stato annunciato il furto di 7 milioni di account del popolare servizio di storage online, la credibilità di Dropbox ha vacillato pericolosamente. Gli accertamenti seguenti, però, hanno chiarito come gli account fossero stati rubati attraverso un attacco a servizi di terze parti, alle quali gli utenti avevano spontaneamente fornito le credenziali di accesso per rendere più rapido l'accesso ai propri file. Per capire in che modo la condivisione

di informazioni finisca per indebolire il livello di sicurezza di un servizio, possiamo tornare al caso di Mat Honan citato in apertura. La ricostruzione dell'attacco subito dal giornalista statunitense, infatti, disegna un panorama sconsolante e chiarisce perché le policy di sicurezza dei servizi cloud non possano essere lasciate nella splendida anarchia in cui si sono sviluppate fino a oggi. Gli hacker che si sono impadroniti dell'identità digitale di Honan, infatti, hanno potuto ottenere l'accesso al suo ID Apple semplicemente chiamando il servizio di assistenza e sostenendo di essere lui.

Per verificarne l'identità, gli addetti Apple hanno chiesto alcune informazioni che, in teoria, avrebbero dovuto rappresentare una forma di autenticazione: l'indirizzo di fatturazione fornito ad Apple e le ultime quattro cifre della sua carta di credito. Non un granché, per la verità. L'indirizzo, infatti, può essere facilmente recuperato usando un elenco telefonico.

Diverso il discorso per il numero di carta di credito, che sembrerebbe più ostico da rintracciare. Sbagliato: tutto quello che i pirati informatici hanno dovuto fare è stato rivolgersi al servizio clienti di Amazon, inscenando una piccola



recita che ha permesso loro di avere accesso ad alcune informazioni sui dati di pagamento. Non tutti, ovviamente: anche se si ha accesso all'account Amazon, infatti, una parte delle informazioni "sensibili" rimangono invisibili, tra cui il numero di carta di credito. Per consentire agli utenti di distinguere una carta dall'altra, però, il sito lascia in chiaro le ultime quattro cifre: proprio ciò che serviva agli hacker. In pratica, la violazione degli account di Honan è stata possibile solo a causa del fatto che

un'azienda considera "riservate" delle informazioni che per un'altra azienda non lo sono. Da qui è partito l'effetto valanga: una volta ottenuto l'accesso all'ID Apple, gli hacker hanno usato l'account @me.com di Honan, che il giornalista aveva impostato come email di recupero, per richiedere il reset della password del suo account Gmail: a questo punto hanno avuto accesso a tutto il resto.

L'ELEMENTO UMANO

Ai rischi intrinseci della password si aggiunge l'attitudine degli utenti a commettere con estrema facilità harakiri in termini di sicurezza. È successo recentemente anche con Snapchat, il servizio di messaggistica con "auto-distruzione" che deve il suo successo proprio all'attenzione per la privacy. Nell'ottobre di quest'anno gli utenti Snapchat hanno subito un furto di dati piuttosto consistente: sul Web sono comparse circa 100.000 tra video e fotografie per un totale di 13 GByte. Il caso ha sollevato immediatamente un vero polverone e, come prevedibile, molti media hanno frettolosamente messo alla gogna il servizio di chat. Salvo scoprire, poi, che il materiale



ATTENZIONE ALL'EMAIL!

Tutti i servizi online sono importanti, ma alcuni lo sono più di altri. Sotto il profilo della sicurezza, la posta elettronica ha un'importanza particolare. Non solo perché l'accesso a una casella di posta elettronica permette di rintracciare più informazioni di qualsiasi altro servizio sulla sfera digitale di un individuo, ma anche per il ruolo che svolge in molti processi di autenticazione. Nei sistemi di registrazione, l'email personale è al vertice di una piramide che consente, a cascata, di accedere a tutti gli altri account. Una volta in possesso delle credenziali per la casella di posta, ottenere l'accesso a qualsiasi altro servizio diventa fin troppo facile: basta fare clic sul proverbiale "hai dimenticato la password" e affrontare, male che vada, lo scoglio di qualche domanda segreta. Senza contare che molti servizi di registrazione inviano tramite email una conferma che contiene tutti i dati (username e password). Queste conferme sono facilmente rintracciabili attraverso una semplice ricerca per parola chiave all'interno dei messaggi memorizzati.

TIPS

→ AUTENTICAZIONE A DUE FATTORI (2FA)

L'autenticazione a due fattori, a volte indicata con la sigla 2FA (dall'inglese *Two-Factor Authentication*) è un processo di autenticazione che prevede l'utilizzo congiunto di due elementi di identificazione: di solito "qualcosa che si conosce", come una password memorizzata, e "qualcosa che si possiede", ad esempio un dispositivo hardware in grado di generare sul momento un codice usa-e-getta". Un altro elemento di autenticazione possibile è "qualcosa che si è", ovvero una caratteristica unica del corpo (come l'impronta digitale, l'iride o il timbro vocale aspetto fisico) che viene rilevata da un sensore biometrico.

non era stato trafugato dai server di Snapchat: gli ignoti hacker avevano preso di mira invece Savedsnap.com, un sito Internet piuttosto frequentato che si interfacciava con Snapchat e permetteva agli utenti di memorizzare in maniera permanente i messaggi altrimenti destinati all'autodistruzione. La conferma è arrivata a stretto giro dallo stesso fondatore del sito ("bucato" a causa di una configurazione errata dei server). Insomma: oltre a ricorrere a un servizio in netto contrasto con la ragione di esistere di Snapchat e in palese violazione dei suoi termini d'uso, le vittime del furto avevano affidato dati estremamente riservati a un sito che non osservava i criteri minimi di sicurezza. A seguito del furto, il proprietario e fondatore di Savedsnap ha deciso di chiudere i battenti del servizio, cancellando tutto il materiale conservato sui suoi server.

L'AUTENTICAZIONE A DUE FATTORI

Come abbiamo visto, l'uso di una password espone a un elevato rischio di furto d'identità. Non importa che la violazione sia fatta tramite un attacco basato sul brute forcing, l'azione di un malware o sfruttando una falla di sicurezza nella gestione del servizio. La debolezza è intrinseca. L'uso di unico strumento di autenticazione, infatti, rappresenta una barriera troppo sottile e permeabile. Rispetto alla semplice password, i sistemi di **autenticazione a due fattori** aggiungono un elemento all'equazione, aumentando il livello di sicurezza e riducendo drasticamente il rischio che un estraneo possa accedere in maniera fraudolenta a un servizio. Oltre a "qualcosa che si conosce", la password, per l'accesso è richiesto qualche cosa d'altro. Può trattarsi, come nel caso dei sistemi biometrici, di "qualcosa che si è", oppure di "qualcosa che si possiede", come una chiavetta con la quale generare sul momento un codice usa-e-getta. Quale che sia il metodo utilizzato, l'idea è quella di arrivare a rendere virtualmente impossibile un'autenticazione fraudolenta.

Non si tratta certamente di una novità: un esempio di autenticazione a due fattori implementata da tempo e utilizzata da un gran numero di persone è il bancomat, che sfrutta qualcosa che si possiede (il tesserino) e qualcosa che si conosce (il codice Pin) per verificare l'identità del titolare del conto.

Due è meglio di uno

L'autenticazione a due fattori migliora drasticamente la sicurezza

codice Pin) per verificare l'identità del titolare. Il sistema è efficace, ovviamente fino al momento in cui non si commette l'errore di conservare nel portafogli il Pin scritto su un foglietto insieme al tesserino. Come vedremo, però, anche l'autenticazione a due fattori per i servizi Internet solleva numerosi problemi e richiede qualche accorgimento per essere utilizzata in maniera efficace.

I SISTEMI BIOMETRICI

Almeno in teoria, il sistema più efficace di identificazione è quello che fa riferimento a "qualcosa che si è". Scansione dell'iride, riconoscimento facciale o vocale e rilevazione delle impronte digitali si basano su elementi di riconoscimento virtualmente unici e irriproducibili, che dovrebbero garantire la massima certezza nell'identificazione. Nella pratica, però, la biometria mostra qualche limite. I sistemi di riconoscimento facciale e la scansione dell'iride, per esempio, sono a volte aggirabili attraverso l'uso di immagini digitali.

Lo stesso vale per le impronte digitali: la possibilità – per ora teorica – di riprodurle usando una stampante 3D rende l'ipotesi del loro furto per lo meno un'ipotesi da considerare. Sistemi come la lettura delle linee delle vene della mano offrono una maggiore sicurezza, ma comportano costi proibitivi per un loro utilizzo su larga scala. Oltre al costo e al livello di sicurezza effettivo, i sistemi biometrici pongono però anche dei problemi di carattere



Il bancomat è un ottimo esempio di autenticazione a due fattori: sfrutta qualcosa che si possiede (il tesserino) e qualcosa che si conosce (il codice Pin) per verificare l'identità del titolare del conto.



Le caratteristiche del corpo, come l'impronta digitale (in foto un lettore di impronte), sono utilizzate di rado in ambito consumer e quasi mai come fattore aggiuntivo di autenticazione: di solito sono semplicemente un'alternativa alla password.



Un secondo fattore di autenticazione molto comune è un token hardware, come quello della foto, che genera sul momento un codice numerico usa-e-getta che prova l'effettivo possesso del dispositivo

pratico. Vincolare l'autenticazione a un parametro unico, prima di tutto, impedisce qualsiasi forma di delega. Ci troviamo in un luogo in cui non è possibile una connessione alla rete o non abbiamo a disposizione il dispositivo che consente di verificare la nostra identità? Se il servizio che vogliamo usare dipende esclusivamente dall'uso di un sistema di autenticazione biometrico, ci si può scordare di chiedere a qualcun altro di accedere al nostro posto, anche se si tratta di una persona in cui riponiamo la massima fiducia. L'alternativa è quella di abilitare più soggetti all'accesso, ma un simile escamotage si tradurrebbe in un'inevitabile riduzione del livello di sicurezza.

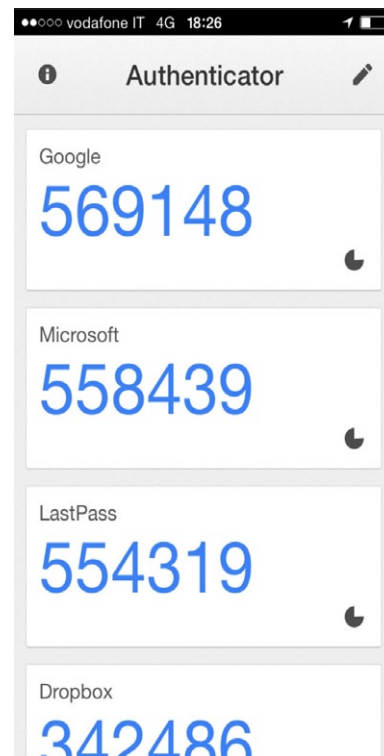
Insomma, la biometria è perfetta per i film di fantascienza, ma nel prosaico presente rappresenta al massimo una comoda alternativa all'uso della password, e non un vero "secondo fattore". Un po' come succede con il Touch ID introdotto da Apple in iPhone e iPad, o da Samsung sui suoi dispositivi. L'uso dell'impronta digitale, in questi casi, si affianca all'uso della password senza sostituirla: le operazioni possono essere eseguite sia con la biometria sia con la password (o il codice Pin). È lo stesso meccanismo adottato da alcuni produttori di computer, che sui portatili di fascia professionale spesso offrono un

lettore di impronte digitali per l'accesso all'account di Windows. Anche in questo caso, però, l'impronta digitale è solo un'alternativa più pratica da inserire alla password, e non un vero secondo fattore di autenticazione.

LA VIA PIÙ FACILE

A conti fatti, la via più praticabile è quella di utilizzare come secondo fattore per l'identificazione qualcosa che si possiede. Per i servizi Internet di tipo consumer si usa generalmente come secondo fattore un token hardware, come le classiche "chiavette" fornite da molti servizi di home banking.

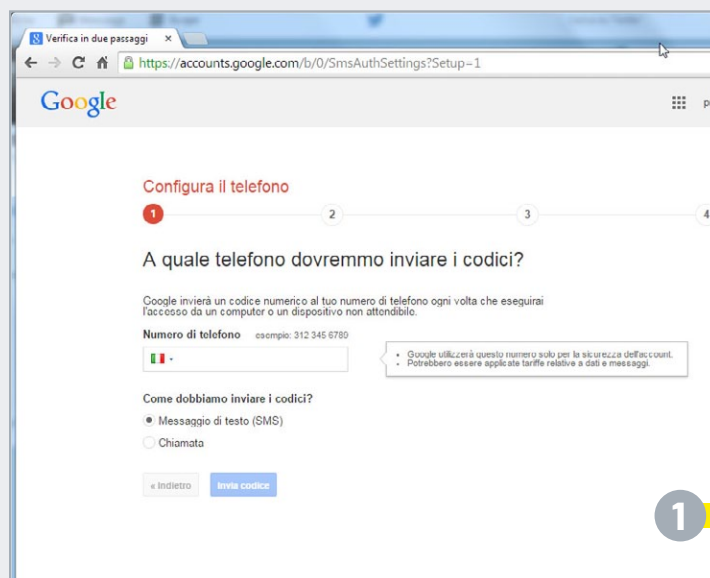
Queste chiavette, come già accennato, permettono di generare sul momento un codice numerico la cui digitazione permette di provare l'effettivo possesso del dispositivo. Il codice è legato all'orario:

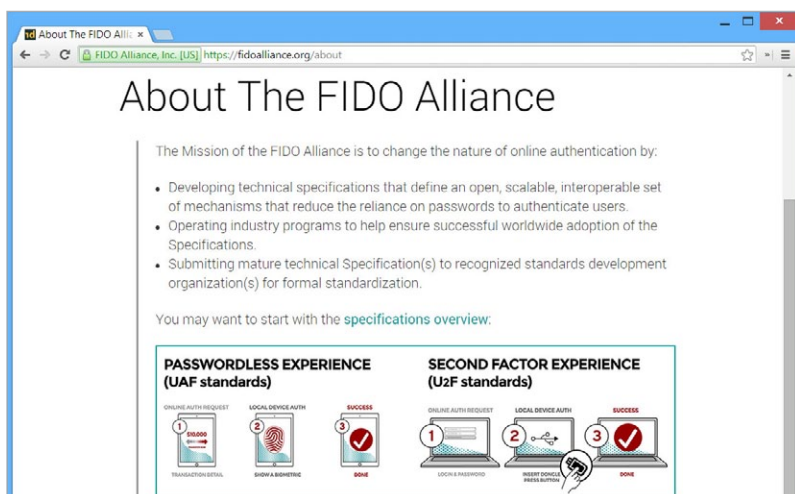


Al posto di un token hardware, per generare i codici usa-e-getta di un sistema 2FA spesso è possibile utilizzare un'App da installare sullo smartphone. In figura, Google Authenticator.

ATTIVARE LA VERIFICA IN DUE PASSAGGI DI GOOGLE

L'attivazione del sistema di autenticazione a due fattori di Google richiede pochi passaggi. Una volta eseguito l'accesso a Google Account, è necessario individuare nella sezione delle impostazioni la voce *Verifica in due passaggi*: se l'opzione non è stata ancora attivata, accanto alla voce comparirà la scritta Off. Fate clic su quest'ultima per avviare la procedura guidata che abilita il sistema di autenticazione a due fattori (Google vi chiederà di inserire nuovamente la password per proseguire). Il primo passaggio prevede l'indicazione del numero di cellulare associato all'account: se non è già presente, dovrete inserire il vostro numero di telefono (figura 1) e scegliere come ricevere i codici di autenticazione. Oltre alla classica opzione *Messaggio di testo (SMS)*, è disponibile anche *Chiamata telefonica*: in questo caso sarà un sintetizzatore vocale a leggersi il codice di sicurezza. La prima opzione però, è sicuramente quella più pratica. Una volta inserito il numero, fate clic su *Invia codice* per procedere alla verifica. Google vi invierà un messaggio (figura 2) con un codice a 6 cifre che dovrete inserire subito in modo che il sistema possa essere certo del buon funzionamento del sistema appena attivato: inseritelo nel campo corrispondente e fate clic





La FIDO Alliance è un'organizzazione che si propone di fissare gli standard per l'utilizzo delle tecnologie di autenticazione a due fattori.

il token ha infatti un orologio interno che al momento dell'attivazione viene sincronizzato con quello del server di autenticazione usato dal servizio Web. Questa sincronizzazione iniziale assicura che i codici generati (la cui validità è limitata a un minuto o anche meno) possano essere riconosciuti e accettati. Oggi sempre più servizi permettono di usare un token virtuale, che prende la forma di un'App per smartphone. Un altro metodo che sfrutta come token un telefono cellulare (di qualunque tipo, non necessariamente smart) è quello basato sugli Sms. In questo caso il codice usa-e-getta non viene generato sul telefono: è il servizio stesso che, quando rileva una richiesta di accesso, lo spedisce via Sms al numero di telefono

registrato in precedenza dall'utente. Un token hardware offre indubbi vantaggi: si tratta di dispositivi facili da portare con sé e spesso (dipende dalle politiche del gestore del servizio) è possibile averne più esemplari, in modo che due persone possano utilizzare indipendentemente l'autenticazione a due fattori nel caso in cui abbiano, per esempio, un conto corrente cointestato. Esistono però anche token il cui utilizzo non prevede la generazione di codici: la loro semplice presenza è il fattore di autenticazione. Le chiavette di questo tipo si collegano alla porta Usb e hanno,

Token virtuale

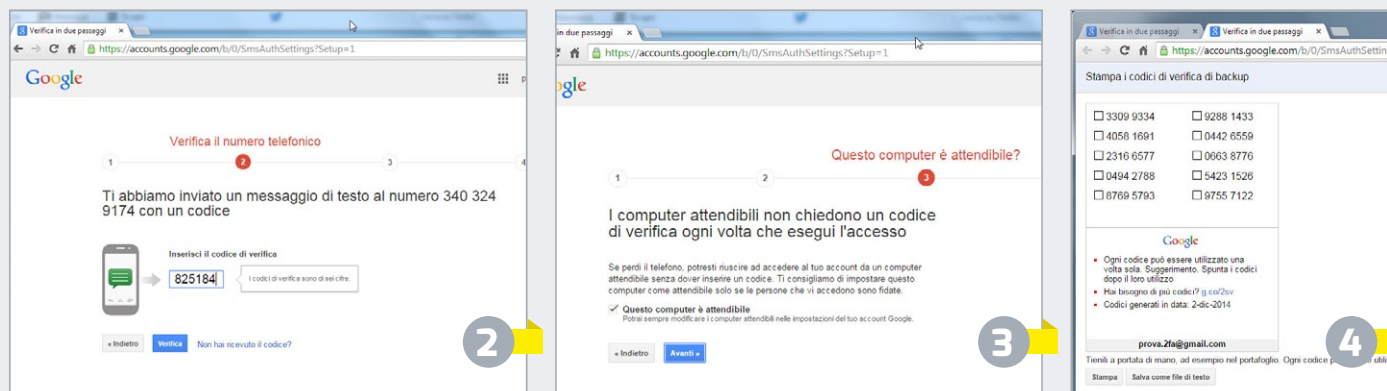
Al posto di un token hardware spesso è possibile usare una pratica App

di conseguenza, il limite di non poter essere utilizzate con dispositivi privi di una porta di questo tipo.

E gli svantaggi? Il principale è la possibilità che il token venga rubato o perso. Nella maggior parte dei casi, però, la conseguenza è una semplice scoccatura, dato che il token da solo non serve a nulla: per ottenere l'accesso al servizio occorrono anche il nome utente e la password corretti. Tutti i sistemi che utilizzano token hardware prevedono la possibilità di revocare rapidamente l'autorizzazione al dispositivo smarrito o rubato, sia facendo riferimento a pagine Web dedicate o, male che vada, al servizio di assistenza.

E, tipicamente, prevedono anche un meccanismo di autenticazione di emergenza per consentire l'accesso al servizio durante il periodo di indisponibilità del token. Alcuni usano gli Sms come secondo fattore alternativo, mentre altri all'attivazione del servizio forniscono un "codice di emergenza" che permette di disattivare temporaneamente la richiesta del secondo fattore:

La FIDO Alliance è un'organizzazione che si propone di fissare gli standard per l'utilizzo delle tecnologie di autenticazione a due fattori.



su Verifica. Il passaggio seguente (figura 3) permette di identificare come "attendibile" il computer che si sta usando, in modo che non richieda l'inserimento del secondo fattore ogni volta che si tenta di accedere ai servizi Google: sul computer personale sarebbe piuttosto fastidioso. L'ultimo passaggio prevede la conferma dell'attivazione della verifica in due passaggi: Fate clic su Conferma per terminare la procedura. Da questo momento il vostro account Google potrà essere utilizzato solo dai computer attendibili o con l'uso di un codice usa e getta. Verrete quindi reindirizzati alla pagina principale

relativa all'autenticazione a due fattori di Google. Prima di chiudere la pagina, però, è consigliabile creare dei codici di backup che vi consentano l'accesso quando non avete a disposizione il cellulare. Scorrete la pagina e individuate la sezione Codici di backup. Fate clic su Stampa o scarica per generare i codici. Il sistema permette di stampare immediatamente i codici o salvarli su un file di testo (figura 4) per conservarli in formato digitale. La prima opzione è quella migliore. Memorizzarli sul computer, infatti, li esporrebbe al rischio di furto in caso di un attacco da parte di un malware.



si tratta com'è ovvio, di un codice da conservare con grande cura e in un luogo sicuro.

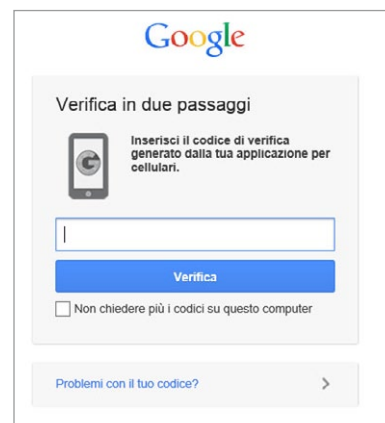
ALLA RICERCA DI UNO STANDARD

Come ogni evoluzione tecnica che interessa il Web, anche quella dell'autenticazione multifattore richiede standard tecnici a cui tutti i soggetti possano fare riferimento. Anche se siamo ancora lontani dalla definizione di un vero standard, qualcosa si sta muovendo. Uno delle organizzazioni più attive in questo ambito è la FIDO (*Fast IDentity Online*) Alliance, un progetto che vede la collaborazione di aziende del calibro di BlackBerry, Google, Lenovo, MasterCard, Microsoft, PayPal, Synaptics e Visa. Fido, nata nell'estate del 2012, è un'organizzazione che si propone di fissare gli standard per l'utilizzo di tecnologie di *strong authentication* (ovvero di un'autenticazione più robusta

di quella basata sulla sola password, com'è appunto l'autenticazione a due fattori). L'obiettivo dichiarato è quello di consentire l'interoperabilità tra i vari sistemi di autenticazione 2FA e di arrivare a superare del tutto l'uso della password. L'attività di FIDO Alliance ha portato, per esempio, alla definizione dello standard **U2F** (*Universal 2nd Factor*), oggi largamente adottato per i token Usb.

L'AUTENTICAZIONE A DUE FATTORI DI GOOGLE

Tra i provider di servizi online *mainstream*, Google è quello che ha dedicato maggiori energie per mettere in campo un sistema di autenticazione a due fattori realmente efficace. Questa attenzione alla sicurezza non sorprende: già soltanto l'enorme popolarità del suo servizio di posta elettronica giustificherebbe lo sforzo compiuto. Dal 26 giugno 2012, quando ha raggiunto



Attivata la verifica a due passaggi, per accedere a un account Google è necessario fornire anche un codice di sei cifre generato al momento. Spuntando la casella visibile in figura si possono evitare successive richieste del codice.

i 425 milioni di utenti attivi, Gmail è infatti il servizio di posta elettronica più usato. Ma le credenziali di un account Google danno accesso non solo a Gmail, ma a ecosistema sempre più ampio che comprende tanti altri serbatoi di informazioni personali: dai file ospitati su Google Documenti e Google Drive per arrivare ai dati memorizzati da Chrome per l'accesso a siti Internet e alle foto accessibili tramite Picasa Web

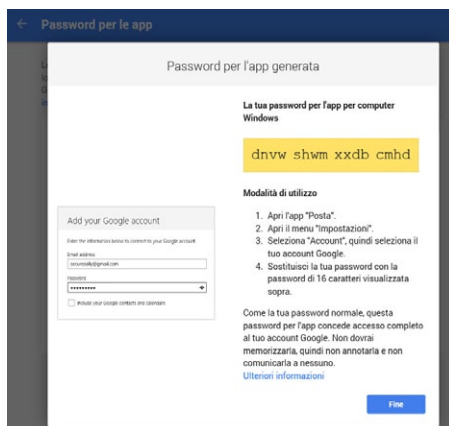
Ormai da quasi quattro anni (il lancio ufficiale è avvenuto nel febbraio del 2011) Google offre opzionalmente per i suoi account un sistema di autenticazione a due fattori, che chiama "verifica in due passaggi"; è possibile impostarlo con pochi clic nelle opzioni dell'account stesso (vedete il riquadro "Attivare la verifica in due passaggi di Google") e sfrutta come secondo fattore un codice numerico usa-e-getta di sei cifre, ottenibile in una varietà di modi. Per chi dispone di uno

→ U2F

U2F (*Universal 2nd Factor*, secondo fattore universale) è uno standard aperto di autenticazione progettato per rendere più semplice e robusta l'autenticazione a due fattori basata su token Usb o dispositivi Nfc (*Near Field Communication*). Sviluppato inizialmente da Google, ora è uno standard aperto gestito dalla Fido Alliance.



I token hardware U2F (nella foto la FIDO Security Key prodotta da Yubico) possono essere utilizzati per gestire l'autenticazione a qualsiasi servizio che supporta questo standard.



Non tutti i programmi che accedono ai servizi Google sono compatibili con l'autenticazione a due fattori: per consentirne il funzionamento è possibile usare password specifiche (estremamente robuste) generate ad hoc.

smartphone, il modo più semplice per riceverlo prevede l'uso dell'App Google Authenticator, disponibile per Android, iPhone e BlackBerry (gli utenti di Windows Phone possono rivolgersi a un'App compatibile, chiamata semplicemente Authenticator).

Chi non possiede uno smartphone può richiedere l'invio del codice, tramite un Sms, a un numero di telefono cellulare associato all'account. Non solo: è prevista la possibilità di ricevere il codice tramite una normale telefonata, anche a un numero fisso, durante la quale il codice verrà letto da un sintetizzatore vocale.

In alternativa alla digitazione del codice numerico, Google permette di utilizzare un token di sicurezza: una chiavetta Usb – conforme allo standard FIDO 2UF – da inserire in una porta Usb del computer. In Italia l'acquisto è possibile su Amazon: mentre scriviamo ne sono disponibili due, che costano, rispettivamente, meno di 6 e 18 euro.

“

Chi non possiede uno smartphone ma ha un normale telefono cellulare può ricevere il codice anche tramite un semplice Sms.

Bisogna in ogni caso tenere presente che l'uso di un token di sicurezza non solo richiede la presenza di una porta Usb, ma consente l'accesso all'account solo tramite il browser Chrome. Cosa succede nel caso in cui non si abbia temporaneamente accesso allo smartphone (o al token Usb)? Il sistema messo in piedi da Google prevede anche questa ipotesi e permette di creare dei codici di backup da utilizzare in caso di bisogno.

La procedura permette di generare un set di 10 codici, che avranno validità fino alla generazione di un nuovo set, stampabili o memorizzabili in un file di testo. La prima opzione ci sembra di gran lunga preferibile: nel caso in cui si dovesse rimanere vittima di un furto di dati in seguito all'infezione da parte di un malware, infatti, la presenza sul disco di un file di testo con i codici di backup diventerebbe un problema. Ovviamente, implementare l'autenticazione a due fattori in maniera rigida in una varietà di servizi come quelli offerti da Google (dall'email a Docs, passando per Google Drive) risulterebbe ben poco pratico. Il sistema, quindi, obbliga a inserire il secondo fattore solo al primo accesso effettuato da un determinato dispositivo: contestualmente si può definire il dispositivo "affidabile"

In caso di emergenza
Il sistema 2FA di Google permette di creare dei codici di backup

ed evitare richieste successive. Gli eventuali tentativi di accesso da altri dispositivi non ancora indicati come affidabili rimarranno naturalmente soggetti alla verifica 2FA.

L'accesso tramite browser, però, è solo uno dei livelli di interazione possibile con i servizi Google: molti programmi (e molte App per smartphone e tablet) vi si collegano, e non è detto che siano compatibili con il meccanismo di autenticazione a due fattori. Rimanendo solo a Gmail, per esempio, è probabile che l'accesso alla casella avvenga attraverso un software che prevede l'inserimento di un nome

utente e di una password ma non del codice aggiuntivo richiesto dal sistema di 2FA. L'ostacolo è superabile attraverso l'impostazione di password specifiche per i software incompatibili con l'autenticazione a due fattori: per ciascun programma (o App) di questo tipo si può infatti generare una password estremamente robusta (12 caratteri casuali) in grado di "scavalcare" il sistema di 2FA consentendo l'accesso completo all'account.

Ogni password specifica può essere revocata in qualsiasi momento dalla pagina Web del Google Account dedicata alla gestione della verifica in due passaggi; in caso ad esempio di furto dello smartphone o del portatile,

I SERVIZI WEB CHE SUPPORTANO LA 2FA

	CODICE OTTENIBILE TRAMITE:		
	SMS	TOKEN VIRTUALE	TOKEN HARDWARE
Apple ID	●	✗	✗
Blizzard	●	●	●
Dropbox	●	●	✗
Evernote	●	● ¹	●
Facebook	●	●	✗
Google Account	●	●	●
Hushmail	●	●	✗
LastPass	✗	●	✗
LinkedIn	●	●	✗
Microsoft Account	●	✗	✗
Paypal	● ²	● ²	● ²
TeamViewer	✗	●	✗
Twitter	●	●	✗
WordPress.com	●	●	✗
Yahoo! Mail	●	✗	✗

1) solo per gli utenti della versione Premium 2) non disponibile per gli utenti italiani

Si= ●
No= ✗

PAYPAL: NIENTE 2FA PER L'ITALIA

PayPal offre un servizio di autenticazione a due fattori che prevede l'invio di un codice usa-e-getta al telefono cellulare o, in alternativa, l'uso di un token che genera un codice temporaneo ogni 30 secondi. Il servizio è gratuito per il cellulare, mentre il token può essere acquistato per 29,95 dollari (in alternativa si può usare un token virtuale sotto forma di App per smartphone). Al momento, però, il servizio di autenticazione a due fattori di PayPal non è disponibile per i clienti italiani.

sarà sufficiente revocare subito le password assegnate ai programmi o alle App presenti sul dispositivo per impedire loro il collegamento all'account Google.

MICROSOFT, APPLE E GLI ALTRI

Il sistema di autenticazione a due fattori basato su un codice usa-e-getta inviato al cellulare o generato da un'App per smartphone non è un'esclusiva di Google. Anzi: sono moltissimi, ormai, i servizi che offrono questa forma di verifica aggiuntiva (vedete la tabella "I servizi Web che supportano la 2FA"). L'uso di un App per la generazione del codice, altamente consigliato, permette di gestire con la massima facilità la procedura. Non solo è possibile ottenere il codice anche quando non è disponibile una connessione internet o cellulare, ma una sola App permette di generare i codici per tutti i servizi utilizzati. L'aggiunta all'App di un nuovo servizio è molto semplice e a volte può essere fatta semplicemente leggendo un semplice QR Code, che viene mostrato durante la procedura di attivazione della 2FA. Dato che tutti i servizi citati in tabella sfruttano algoritmi standard, per generare il secondo fattore è possibile utilizzare sia Google Authenticator sia App analoghe come quelle di Duo Mobile o di Amazon AWS.

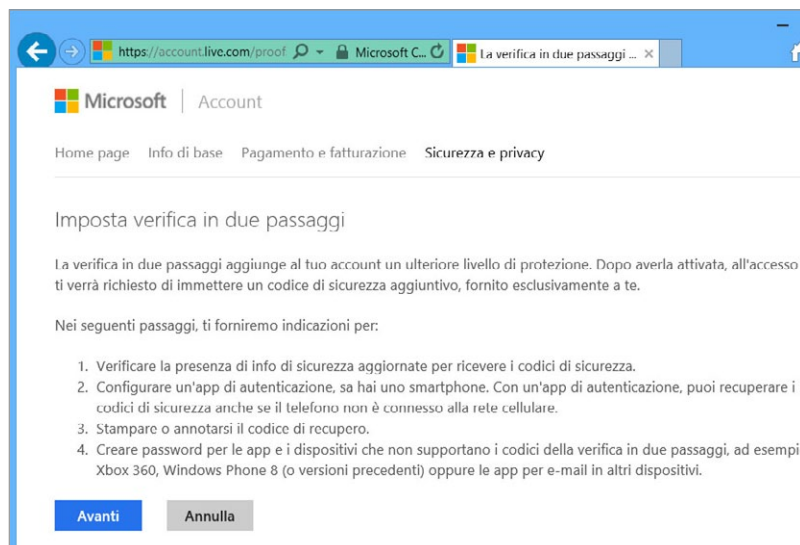
L'uso dell'autenticazione a due fattori è particolarmente importante quando si ha a che fare con account critici.

2FA ovunque
Tutti i principali servizi Web oggi offrono l'autenticazione a due fattori

Oltre a quello di Google, entrano di diritto nella categoria quelli di Microsoft e Apple: gli utenti dei sistemi Mac e Windows, infatti, sono ormai legati a doppio filo con il cloud.

Microsoft Account permette di usare la 2FA dal 2013. Una volta collegati a <https://login.live.com/it> ed eseguito l'accesso con l'account Microsoft, è possibile attivare l'autenticazione a due fattori in maniera abbastanza rapida attraverso la sezione *Sicurezza e privacy* / *Gestisci Sicurezza Avanzata*. Di default il sistema prevede il ricorso ad un'App per generare il codice, ma (nonostante a prima vista non sembri un'opzione disponibile) può inviarlo anche via Sms. In caso di impossibilità di accedere al cellulare o allo smartphone, è possibile usare un codice di recupero (composto da 25 caratteri, come quello per l'attivazione di Windows) fornito al termine della procedura di attivazione per disabilitare l'autenticazione a 2 fattori: a nostro avviso è una soluzione meno efficace rispetto ai codici di backup adottati da Google. Abbiamo apprezzato, invece, il fatto che la stessa pagina Web sconsigli di memorizzare il codice di recupero su un dispositivo. Purtroppo le informazioni sul sistema di autenticazione a due fattori di Microsoft, per lo meno nell'edizione italiana del sito, non brillano certo per chiarezza e completezza.

Anche Apple prevede un sistema di autenticazione a due fattori per il suo ID Apple ma, tanto per cambiare, è completamente interno al suo



Anche Microsoft, con un paio di anni di ritardo rispetto a Google, ha iniziato a offrire l'autenticazione a 2FA per proteggere più efficacemente l'accesso ai propri account.

ecosistema. Il meccanismo, però, è sostanzialmente lo stesso di quello usato da Microsoft e Google. L'unica differenza è che, oltre che su un telefono cellulare, è possibile ricevere i codici (di 4 cifre) direttamente sui dispositivi registrati: niente App, quindi.

Nel caso in cui non sia disponibile il dispositivo utilizzato per la ricezione del codice, è possibile ricorrere ad una chiave di recupero: si tratta di un codice lungo 14 caratteri, che viene generato al momento in cui si attiva l'autenticazione a due fattori e che deve essere stampato e conservato con cura. Esattamente come nel caso di Google, l'accesso al servizio di email di Apple attraverso applicazioni di terze parti che non supportano la 2FA richiede la generazione di password specifiche. Se ne possono usare un massimo di 25, che possono essere revocate in qualsiasi momento singolarmente o in blocco.

Praticamente tutti i servizi Web più popolari, tra cui Facebook, Dropbox, LinkedIn e LastPass, implementano l'autenticazione a due fattori. Purtroppo non sempre pubblicizzano in maniera adeguata questa possibilità; l'attivazione della verifica in due passaggi non di rado è nascosta tra le pieghe delle impostazioni di sicurezza e le informazioni riguardanti il suo funzionamento, complici anche traduzioni dall'inglese non sempre impeccabili, risultano piuttosto vaghe. È un vero peccato, perché la 2FA rende molto più sicuro l'uso di Internet e del cloud: vi consigliamo di attivarla senza indugio per tutti i servizi che usate e che la supportano.