SICUREZZA TOTALE
PER DATI E DISPOSITIVI

Di **Dario Orlandi**

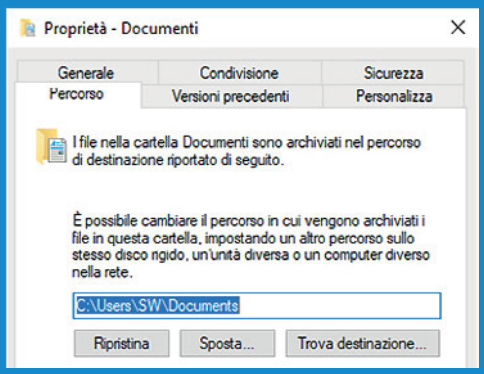
La proliferazione dei dispositivi portatili ha reso sempre più rilevante il problema della sicurezza dei dati: computer, smartphone e tablet memorizzano infatti informazioni sensibili, documenti privati e impostazioni che non devono cadere nelle mani sbagliate. Nelle prossime pagine analizzeremo le funzioni, le strategie e le tecnologie per evitare che lo smarrimento o il furto di un dispositivo personale possano avere conseguenze ben peggiori di un mero danno economico.

LO SCORSO ANNO IL NUMERO DI ACCESSI WEB GENERATI DAI DISPOSITIVI MOBILE HA SUPERATO PER LA PRIMA VOLTA QUELLI PROVENIENTI DAI COMPUTER. MA LA PORTABILITÀ HA ANCHE UN LATO OSCURO: È PIÙ FACILE SMARRIRE QUESTI OGGETTI, RUBARLI OPPURE DANNEGGIARLI IN MODO IRREPARABILE. PER QUESTO MOTIVO, NEL CORSO DEL TEMPO SONO STATE INTRODOTTE MOLTE FUNZIONI E TECNOLOGIE PENSATE PER PROTEGGERE I DATI CONTENUTI NEI DEVICE MOBILI. NON ESISTE, PERÒ, UNA SOLUZIONE TUTTO-IN-UNO: BISOGNA CONOSCERE LE OPPORTUNITÀ OFFERTE DA OGNI SISTEMA, SOFTWARE E SERVIZIO, PER IMPLEMENTARE UNA STRATEGIA DI SICUREZZA TOTALE PER DATI E DISPOSITIVI.

Ogni volta che usciamo di casa con uno smartphone in tasca, portiamo con noi una chiave capace di aprire molte porte: al suo interno, infatti, sono contenuti l'elenco completo dei contatti, immagini e video privati, le credenziali di login ai servizi online e altro ancora. Con un po' di fortuna, un malintenzionato può perfino raggiungere la intranet di un'azienda e scaricare documenti professionali di grande valore, oppure recuperare le credenziali di accesso all'home banking, raggiungere l'account di posta elettronica o inserirsi in un servizio di cloud storage, in cui spesso vengono memorizzati dati sensibili come ricette o esiti di esami medici, buste paga e dichiarazioni dei redditi, o addirittura copie digitali dei documenti di identità. Quando un dispositivo smart esce dall'abitazione, tutti questi dati sono potenzialmente a rischio; ma anche all'interno delle mura domestiche la sicurezza non è totale: tra le prede più ambite dai ladri d'appartamento ci sono proprio tablet, smartphone e notebook, oggetti piccoli, facili da trasportare e da rivendere. In molti casi i ladri sono interessati solo al valore del dispositivo fisico: eliminano al più presto i dati del legittimo proprietario, effettuando un reset totale che prepara il device a essere rivenduto. Ma esistono organizzazioni specializzate nell'estrazione dei dati dai device rubati, alla ricerca di informazioni personali che possano avere un valore economico. Per i proprietari, invece, il danno (o il timore del danno) va ben oltre il costo del device fisico: un po' come accade nel caso dei danni hardware al Pc, è più grave la potenziale perdita di dati (o, peggio ancora, la loro compromissione) rispetto al costo del dispositivo o del componente che viene rubato, perduto o danneggiato. Dover acquistare un nuovo smartphone o un nuovo computer portatile può essere sgradevole, ma trovarsi ad affrontare un furto di identità digitale o la perdita di dati irrecuperabili (che siano documenti importanti per il proprio lavoro oppure le foto di un momento irripetibile) ha implicazioni personali più gravi rispetto al semplice esborso di denaro.

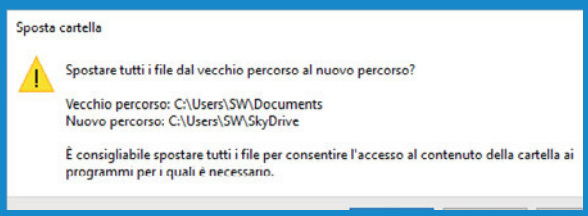
> Il danno causato dal furto di un dispositivo va ben oltre il costo del device stesso

Lo scenario che abbiamo dipinto è senza dubbio inquietante, ma non bisogna



Spostando la cartella Documenti in un percorso sincronizzato con il cloud, si può garantire la salvaguardia di molti file personali in modo completamente automatizzato.

Dopo aver modificato la posizione della cartella Documenti, Windows propone di spostarvi i file contenuti nel vecchio percorso, per continuare ad accedervi nello stesso modo.



disperare: esistono infatti soluzioni per proteggere i dati e i dispositivi in maniera tale da non farsi trovare impreparati neppure di fronte alle evenienze più traumatiche.

Purtroppo, non esiste una singola opzione capace di garantire una sicurezza completa: bisogna invece impostare una strategia globale che coinvolga tutti i dispositivi utilizzati e che preveda meccanismi di risposta rapida in caso di crisi. Si tratta di comportamenti utili nel caso degli utenti casalinghi, ma addirittura essenziali negli ambienti lavorativi: la perdita o la compromissione di informazioni importanti può causare danni economici ingenti, anche e soprattutto nelle aziende di dimensioni piccole e medie. Al contrario degli ambienti più grandi e strutturati, infatti, le realtà più piccole hanno spesso infrastrutture informatiche più deboli, e un singolo colpo può metterle in grave difficoltà. Basti pensare al danno che potrebbe causare la divulgazione dell'elenco dei clienti per un agente di commercio, oppure la pubblicazione anticipata di un'offerta per una azienda che voglia concorrere a un bando pubblico.

Bisogna quindi armarsi di un po' di buona volontà e ripensare in modo critico scelte, abitudini e flussi di lavoro, alla ricerca di eventuali punti deboli, per poi sfruttare le funzioni, le tecnologie e le applicazioni disponibili (e spesso addirittura integrate direttamente nel sistema operativo) per migliorare la sicurezza dei dati e dei dispositivi (computer, smartphone e tablet) utilizzati in mobilità.

SALVAGUARDARE I DATI PERSONALI

I dati personali hanno ormai da tempo superato il limite dei singoli dispositivi: la causa di questa tendenza è proprio nella proliferazione dei device, che ha reso sempre più scomodo e poco pratico legare le informazioni a una singola posizione fisica. Chi si ostina a mantenere i dati memorizzati su un solo dispositivo si espone al rischio che la sua sottrazione o smarrimento causi una perdita irreparabile. Inoltre si innesca una serie di complicanze, come la moltiplicazione delle versioni dei documenti, evitabili nella grande maggioranza dei casi.
La soluzione più comune per condividere le informazioni tra più device, specie se di tipo diverso, è un servizio di cloud storage. Esistono molte soluzioni, con pregi e difetti peculiari, che possono essere implementate con poca fatica e integrate anche nei flussi di lavoro aziendali. Il più semplice da utilizzare in ambiente Windows,

ONEDRIVE COME CARTELLA DOCUMENTI

Per semplificare ancor più il salvataggio nel cloud, si può impostare OneDrive come destinazione predefinita per la cartella Documenti: ogni volta che si salverà un file all'interno della cartella Documenti, questo sarà automaticamente sincronizzato anche nel cloud. Scopriamo come procedere. Per prima cosa, aprite Esplora file e raggiungete la sezione *Accesso rapido*; fate clic destro sull'icona *Documenti* (nella sezione *Cartelle frequenti*) e selezionate la voce *Proprietà*. Nella finestra di dialogo successiva aprite la scheda *Percorso* e fate clic sul pulsante *Sposta*; indicate la cartella principale di OneDrive (o una sua sottocartella) come nuova destinazione, e confermate con un clic su *Selezione cartella*. Tornati alla finestra precedente, fate clic su *Applica*; un'ulteriore finestra di dialogo chiederà conferma della volontà di spostare tutti i contenuti della vecchia cartella Documenti nella nuova posizione: confermate con un clic su *Sì* e attendete qualche istante. La procedura sarà finalmente conclusa. Se OneDrive non è il vostro cloud storage preferito, non temete: la stessa identica procedura può essere applicata a qualsiasi altro servizio basato su un client locale capace di sincronizzare lo storage remoto con il contenuto di una cartella locale.

anche se non il più ricco di funzioni, è OneDrive di Microsoft: il client, infatti, è installato e attivo per default in tutte le installazioni di Windows 10, ed è collegato all'account Microsoft, lo stesso che viene utilizzato ogni giorno per il login al sistema operativo. L'offerta gratuita non è particolarmente generosa: lo spazio di archiviazione è pari a soli 5 Gbyte, una quantità di spazio che può essere sufficiente per la memorizzazione dei documenti personali o lavorativi, ma che comincia presto a stare stretta se invece si vogliono salvare anche immagini o, peggio ancora, video ad alta risoluzione. Utilizzare OneDrive, dicevamo, è davvero banale: basta fare doppio clic sull'icona a forma di nuvola, nell'area di notifica della barra delle applicazioni, ed eventualmente inserire i dati di autenticazione che, come abbiamo già accennato, sono identici a quelli utilizzati per accedere a Windows. Si aprirà una finestra di Esplora file che elencherà i file sincronizzati con il server remoto. Per memorizzare i documenti nel cloud, e poi accedervi anche da tutti gli altri dispositivi collegati allo stesso account, basta salvarli in questa cartella.
Come abbiamo già accennato, gli account gratuiti di OneDrive offrono 5 Gbyte di spazio di memorizzazione remoto: una quantità discreta, ma facilmente esauribile se non si fa attenzione a quali tipi di file vi vengono salvati; per ampliare lo spazio si possono attivare abbonamenti a pagamento, che sono molto generosi.
OneDrive, infatti, rientra nell'offerta Office365 *(https://products.office.com/it-it/compare-all-microsoft-office-products)*: per 69 Euro all'anno (ma spesso si trovano online offerte ancor più vantaggiose) si può acquistare un abbonamento Personal, che oltre a uno spazio di spazio di memorizzazione online pari a ben 1 Tbyte offre anche l'intera suite delle applicazioni di Office (Word, Excel, PowerPoint e così via), installabile e utilizzabile su un computer (Pc oppure Mac), uno smartphone e un tablet, iOS, Android oppure Windows. OneDrive non è l'unico servizio di cloud storage sul mercato: al contrario, deve vedersela con concorrenti agguerriti, che offrono per molti versi un'esperienza d'uso superiore. Il punto di riferimento del settore continua a essere Dropbox *(www.dropbox.com)*, un servizio ricco e avanzato: gli account gratuiti hanno un limite iniziale di soli 2 Gbyte, che però può facilmente essere incrementato (fino a un massimo di 16 Gbyte) invitando amici e conoscenti a iscriversi al servizio. Rispetto a OneDrive, è necessario un passo in più per integrare le sue funzioni all'interno del computer: dopo aver completato l'iscrizione al servizio, creando nuove credenziali o sfruttando quelle di Google, bisogna infatti scaricare e installare il client che consente di ottenere un meccanismo di funzionamento del tutto analogo a quello di OneDrive.
Una terza opzione, sempre più competitiva, è Google Drive *(https://drive.google.com)*, il servizio di cloud storage di Google. Anche in questo caso le sue funzioni sono analoghe a quelle proposte da OneDrive e Dropbox, dopo aver installato il client di sincronizzazione locale. Google Drive offre 15 Gbyte di spazio gratuito, condiviso però tra tutti i servizi legati allo stesso account Google (tra cui Gmail e Google Foto), mentre gli abbonamenti a pagamento partono da 1,99 Euro al mese per 100 Gbyte. Uno dei vantaggi di Google Drive è l'integrazione stretta con gli altri servizi di Google, un aspetto che può risultare decisivo in particolare per i moltissimi utenti degli smartphone e dei tablet basati sul sistema operativo Android.

La soluzione più comune per condividere le informazioni tra più device, specie se di tipo diverso, è un servizio di cloud storage

GOOGLE FOTO

Se si accetta una leggera compressione delle immagini e dei video, Google Foto permette di salvare i contenuti senza limitazioni.

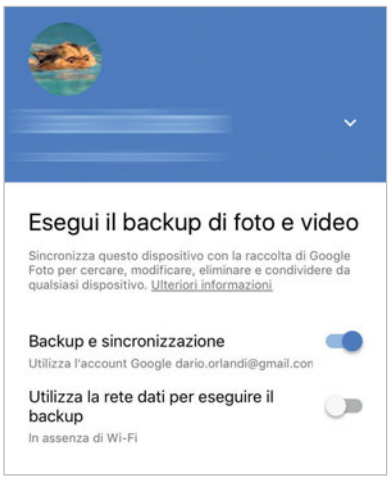
DOCUMENTI, IMMAGINI E VIDEO

Finora abbiamo concentrato l'attenzione in particolare sui computer, che siano desktop oppure notebook. Ma una vera strategia di salvaguardia dei dati deve includere anche i dispositivi mobile, come smartphone e tablet. L'accesso ai servizi di cloud storage da mobile è semplice: tutti i principali provider, infatti, offrono App native sia per iOS sia per Android, che possono essere utilizzate per accedere ai documenti memorizzati nel cloud o per salvare nuove informazioni.
Le App sono abbastanza simili nelle funzioni di base, e integrano tutte le principali opzioni di ciascun servizio. L'aspetto che può differenziarle è la maggiore o minore integrazione con gli altri componenti dell'offerta di servizi dei vari provider. Nel caso di Microsoft, per esempio, OneDrive è perfettamente integrato con l'ecosistema di Office, e semplifica la vita di chi crea, visualizza e modifica documenti con le applicazioni di questa suite.

Un discorso simile vale anche per Google: Drive è ben integrato con le applicazioni online di produttività Google Docs, e rappresenta la soluzione più naturale per gli utenti dei dispositivi Android o dei notebook basati su Chrome OS (i cosiddetti Chromebook, per la verità non troppo diffusi nel nostro Paese).
La scelta, quindi, dipende dalle specifiche esigenze di ciascuno, che deve valutare non soltanto l'offerta di storage in sé stessa, ma anche l'integrazione in un ecosistema hardware e software più ampio. Nulla, comunque, vieta di installare e utilizzare anche più di un servizio, magari con obiettivi differenti: per esempio Google Drive per la sincronizzazione con il mondo Android, e OneDrive per l'integrazione con Windows e Office, o ancora Dropbox per le sue funzioni di condivisione e collaborazione avanzate. Il semplice salvataggio dei documenti, però, non esaurisce le opzioni di sincronizzazione: ci sono, infatti, altri aspetti da considerare. Il primo è quello che riguarda le fotografie e i video, specialmente quelli scattati con un dispositivo mobile. In realtà tutti i principali servizi di cloud storage offrono funzioni di sincronizzazione automatica di questi contenuti, ma utilizzandole ci si scontra presto con le limitazioni imposte allo spazio di memorizzazione online per gli account gratuiti: le fotografie e, soprattutto, i filmati possono saturare lo spazio disponibile, ed è opportuno destinarlo al salvataggio di informazioni per cui non sia disponibile una soluzione alternativa. Nel caso dei file multimediali esistono infatti diversi servizi specializzati, che garantiscono una capienza superiore e funzioni di sincronizzazione, condivisione e visualizzazione ottimizzate.

La scelta del cloud storage dipende anche dall'ecosistema di servizi offerto

Google propone un Uploader per il servizio Foto dedicato anche ai sistemi operativi per computer, che permette di caricare nel cloud anche le immagini salvate nelle schede di memoria e nelle fotocamere digitali.



L'App di Google Foto per i dispositivi mobile è molto semplice da usare: la sua funzione principale è quella di sincronizzare con lo storage remoto le fotografie scattate sul device.

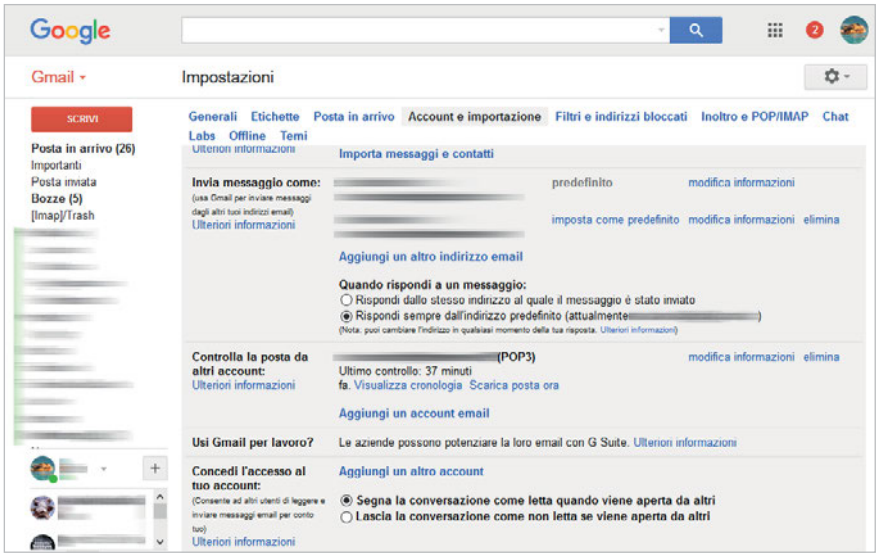
Una delle migliori è **Google Foto** *(https://photos.google.com/?hl=it)*, un servizio dedicato alla memorizzazione di contenuti multimediali che offre uno spazio di storage addirittura illimitato, se si accetta una leggera compressione delle immagini originali. Per mantenere i file nella qualità originale basta attivare l'opzione *Originale* nella pagina delle *Impostazioni*, ma in questo caso lo spazio occupato verrà scalato dal totale disponibile per l'account Google.
Sempre nella stessa pagina si trovano anche altre opzioni interessanti, come quella che rimuove le informazioni di geolocalizzazione per gli elementi condivisi, e quella che mostra gli elementi della libreria di Google Foto anche nel file system accessibile tramite Google Drive. Salvare immagini e filmati da mobile è semplice: basta scaricare l'App di Google Foto e impostare il backup automatico delle immagini memorizzate. Si può anche decidere se utilizzare la connessione cellulare per inviare e ricevere le informazioni, o se avviare la sincronizzazione soltanto quando il dispositivo è collegato a una rete Wi-Fi. Esiste anche un client per i

computer Windows e Mac (chiamato Uploader), che consente di caricare automaticamente le foto salvate nel sistema, oppure quelle memorizzate in una fotocamera o in una scheda di memoria collegate al computer.

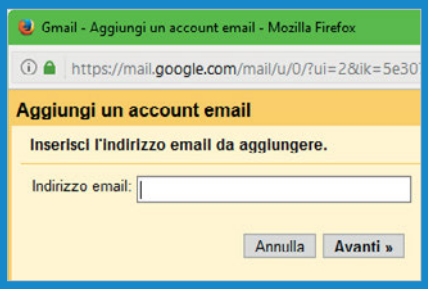
La soluzione offerta da Google è probabilmente la più semplice da attivare e utilizzare, ma di certo non l'unica. Da anni, per esempio, Flickr *(www.flickr.com)* di Yahoo offre funzioni simili e garantisce qualche vantaggio non trascurabile, come per esempio uno spazio di archiviazione gratuito di ben 1 Tbyte, senza ricompressione dei contenuti originali. I difetti principali di Flickr sono un'interfaccia di manipolazione un po' farraginosa (quella di consultazione, invece, è gradevole) e l'appartenenza all'ecosistema dei servizi online di Yahoo, che in passato ha mostrato qualche falla di troppo in tema di sicurezza. Un'altra soluzione potente ma poco nota è Amazon Prime Foto *(https://www.amazon.it/clouddrive/primefoto)*, un servizio offerto a tutti gli utenti Prime di Amazon (non si tratta, quindi, di un servizio del tutto gratuito). Prime Foto propone spazio di storage illimitato per le immagini (più 5 Gbyte per video e documenti), e alcune valide App di backup e sincronizzazione dedicate ad Android e iOS; esistono anche client per Windows e Mac OS, che hanno lo scopo principale di garantire il backup delle immagini dal cloud verso il sistema locale, per ottenere un duplice livello di sicurezza. Tutte le soluzioni citate offrono funzioni di riproduzione e condivisione con controllo degli accessi; possono essere utilizzate non soltanto per il backup personale delle immagini provenienti da smartphone, tablet e fotocamere digitali, ma anche per condividere album e singole fotografie con amici e parenti. Basterà decidere quali album o fotografie condividere e selezionare l'elenco degli utenti autorizzati all'accesso per rendere disponibili interi album, spesso anche con funzioni di riproduzione gradevoli (slide show con dissolvenze).

EMAIL E IMPOSTAZIONI

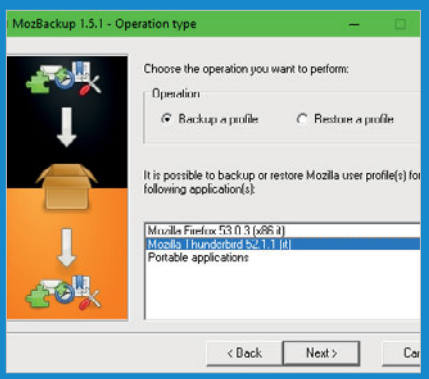
Fino a questo punto la sincronizzazione si è rivelata tutto sommato semplice, e quasi del tutto automatica; esistono però anche altre tipologie di dati e informazioni che si vorrebbe poter salvare, ma la difficoltà aumenta e non sempre si riesce ad ottenere il risultato cercato. Non mancano, comunque, alcune strategie interessanti, che è bene tenere in considerazione.
Alcune tipologie di informazioni sono intrinsecamente condivise nel cloud, e non c'è bisogno di preoccuparsi quasi di nulla: è il caso, per esempio, dell'archivio di posta elettronica (se si utilizza una casella Imap), oppure dei messaggi di Google+ e Hangout, che vengono sincronizzati in remoto e distribuiti a tutti i client collegati. Il caso dell'email è cruciale, e merita qualche altra considerazione. Come abbiamo già accennato, se si utilizza una casella di posta elettronica che offre l'accesso Imap tutti i messaggi rimarranno archiviati in remoto, e non sarà necessario fare nulla per salvarli e sincronizzarli. Se invece il provider propone



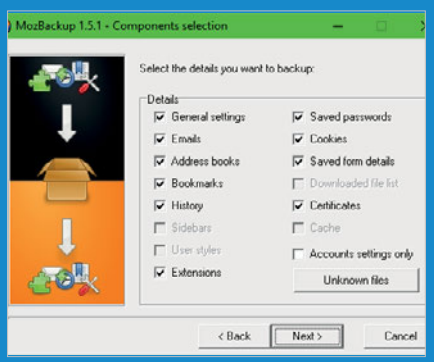
Se alcuni account non supportano il protocollo Imap, si può configurare lo scaricamento dei messaggi utilizzando la funzione di Gmail *Controlla la posta da altri account*.



Una semplice procedura guidata accompagna l'utente nella configurazione della funzione di scaricamento automatico della posta da account esterni a Gmail.



Il primo passaggio significativo per salvare le impostazioni di Thunderbird è selezionare l'applicazione nell'interfaccia guidata di MozBackup.



Per creare un backup delle impostazioni di Thunderbird basta togliere la spunta alla voce Email: le missive saranno scaricate automaticamente dai server remoti una volta completato il ripristino della configurazione.

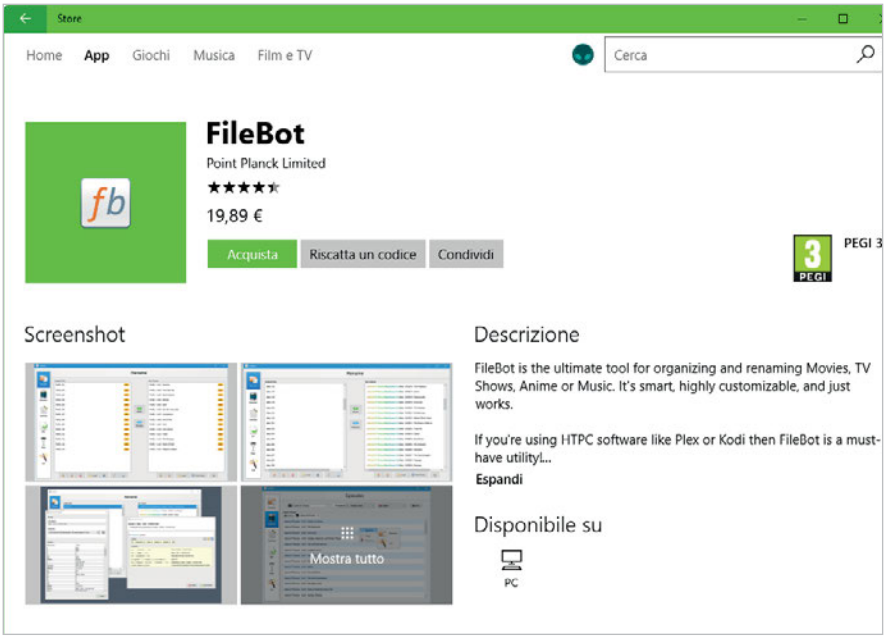
soltanto una casella Pop3 (spesso, tra l'altro, di dimensioni limitate), si può ovviare al problema configurando lo scaricamento automatico da parte di un servizio che invece possa garantire accesso Imap e ampio spazio di memorizzazione: è il caso, per esempio, di Gmail. Per raggiungere le opzioni cercate basta aprire l'interfaccia Web del servizio, all'indirizzo *https://mail.google.com*, fare clic sul pulsante a forma di ruota dentata, in alto a destra, e selezionare la voce *Impostazioni* nel menu a discesa. Nella pagina delle impostazioni fare clic sul collegamento *Account e importazione*, e poi su *Aggiungi un account email* nella sezione *Controlla la posta da altri account*. Si aprirà una procedura guidata che permetterà di impostare tutti i dati necessari per completare l'importazione dei messaggi. Chi volesse utilizzare l'account connesso anche per inviare nuovi messaggi, e non soltanto per riceverli, dovrà impostare una nuova voce anche nella sezione *Invia messaggio come*, facendo clic sul collegamento *Aggiungi un altro indirizzo email* e seguendo le istruzioni della procedura guidata.

La sincronizzazione dei messaggi è garantita dall'uso del protocollo Imap, ma la configurazione di un client di posta elettronica comprende anche altri elementi, come per esempio le credenziali d'accesso ai vari account, le specifiche impostazioni del software ed eventualmente le estensioni di terze parti installate. Salvare anche queste informazioni può essere utile per ripristinare velocemente la piena funzionalità del sistema in caso di problemi che costringano a passare a un nuovo computer, o comunque a reinstallare il sistema operativo da zero. Nel caso di Mozilla Thunderbird, il salvataggio di queste informazioni è semplice: basta scaricare l'utility gratuita MozBackup *(http://mozbackup.jasnapaka.com)*. Il tool non è più supportato, e lo sviluppatore segnala che potrebbero esserci problemi di compatibilità. Nei nostri test, anche con le ultime release dei software di Mozilla, non abbiamo però riscontrato alcun problema particolare. Il tool è semplice da utilizzare, ed è basato su una procedura guidata. Basta scegliere di effettuare un nuovo backup, selezionare Mozilla Thunderbird tra le applicazioni rilevate, decidere quale profilo salvare (di solito è presente soltanto quello di default) e specificare il percorso di destinazione. Il software permette di proteggere il backup con una password (è un suggerimento che vale la pena di seguire) e finalmente si raggiunge la pagina di selezione dei componenti: per evitare che MozBackup salvi l'intero archivio dei messaggi basta togliere il segno di spunta accanto alla voce *Emails*, mentre tutto il resto può essere mantenuto attivo. Il file di backup comprenderà tutte le impostazioni e le configurazioni del software, ma non l'archivio dei messaggi. Quando il backup sarà ripristinato su un altro computer o una nuova installazione di Windows (dopo aver installato un'altra copia di Thunderbird), la configurazione originale verrà applicata e i messaggi saranno scaricati da remoto.

> La sincronizzazione dei messaggi è garantita dall'uso del protocollo Imap

Sempre in tema email, un'altra precauzione utile è il backup dell'archivio Imap, che può proteggere i dati in caso di violazione dell'account, compromissione delle credenziali di accesso o nel malaugurato caso che un problema lato server porti alla perdita di informazioni. In questo caso si può utilizzare MailStore Home *(www.mailstore.com)*, un'utility gratuita per uso privato capace di salvare (e ripristinare) direttamente i contenuti delle caselle email remote, senza doversi appoggiare a client esterni. In caso di necessità, comunque, MailStore supporta anche l'accesso agli archivi di Outlook, Exchange Server, Office 365, Thunderbird, Windows Mail e altri client per Windows e Linux. MailStore permette anche il ripristino verso una destinazione diversa rispetto a quella di partenza, e garantisce quindi una notevole flessibilità.

Nel caso dei dispositivi mobile, invece, l'accesso alle email avviene di solito da remoto, tramite standard come Imap; il problema del backup semplicemente non sussiste, una volta configurati gli account per essere accessibili tramite caselle memorizzate sui server dei diversi provider.



Lo store di Windows ha iniziato a proporre anche una selezione di software Win32; le funzioni di sincronizzazione e aggiornamento automatico rendono vantaggioso il suo utilizzo rispetto all'installazione tradizionale.

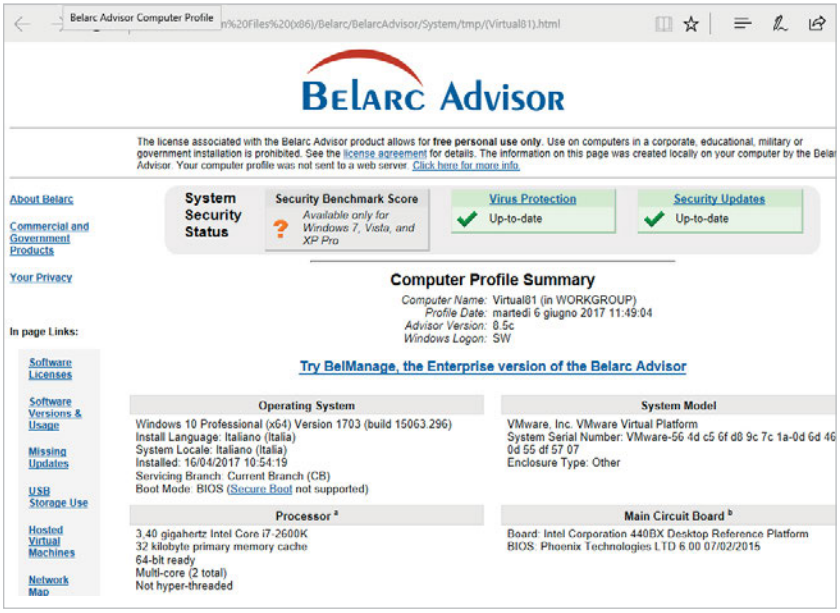
SOFTWARE E PASSWORD

Un altro scenario in cui i sistemi mobile garantiscono vantaggi significativi rispetto ai computer tradizionali è nella gestione del software: la stretta integrazione con i rispettivi App Store consente ai possessori di smartphone e tablet di ripristinare le applicazioni installate nel giro di pochi minuti, scegliendo di reinstallare automaticamente tutti i software scaricati in passato. Con qualche minuto in più si può anche consultare l'elenco delle applicazioni installate in precedenza e scegliere soltanto quelle realmente utili.

Questo non esaurisce la procedura di ripristino su un nuovo dispositivo oppure dopo il reset, ma rappresenta un primo passo da non sottovalutare; quello che manca sono i dati salvati da ciascuna applicazione, a meno che non siano stati in qualche modo memorizzati in remoto. Questo è il motivo per cui, dopo aver ripristinato le App su un dispositivo mobile, bisogna dedicare qualche decina di minuti (o qualche ora, a seconda del numero di elementi) a reinserire le credenziali di accesso alle varie App e a configurare le impostazioni degli strumenti software. Per evitare o limitare al minimo anche questo passaggio ci si può affidare agli strumenti e alle funzioni di backup, di cui parleremo più avanti.

Nel caso dei computer tradizionali, la situazione è in generale molto peggiore: se non si dispone di un backup, ogni singolo software dev'essere reinstallato e riconfigurato da zero; un impegno davvero oneroso, per un processo che non sempre è coronato da successo. Anche per questo motivo, Microsoft e Apple stanno spingendo l'utilizzo degli App Store anche nei sistemi operativi tradizionali. Nel caso di Windows, però, il numero di software disponibili tramite lo store è ridotto, e copre soltanto una minima percentuale dell'universo di strumenti, utility e applicazioni realizzate per questo sistema operativo. Vale comunque la pena di visitare di tanto in tanto lo Store di Windows, alla ricerca di nuove applicazioni tra quelle utilizzate più spesso: un po' come accade con i sistemi operativi mobile, le App scaricate e installate tramite lo Store rimangono legate all'account dell'utente, e possono essere ripristinate facilmente su altri dispositivi, oppure dopo aver reinstallato il sistema operativo.

Utile è anche mantenere un elenco aggiornato di tutto il software installato nel sistema. Esistono varie applicazioni dedicate a questo scopo; una delle più semplici è Belarc Advisor *(www.belarc.com/products_belarc_advisor)*, un tool

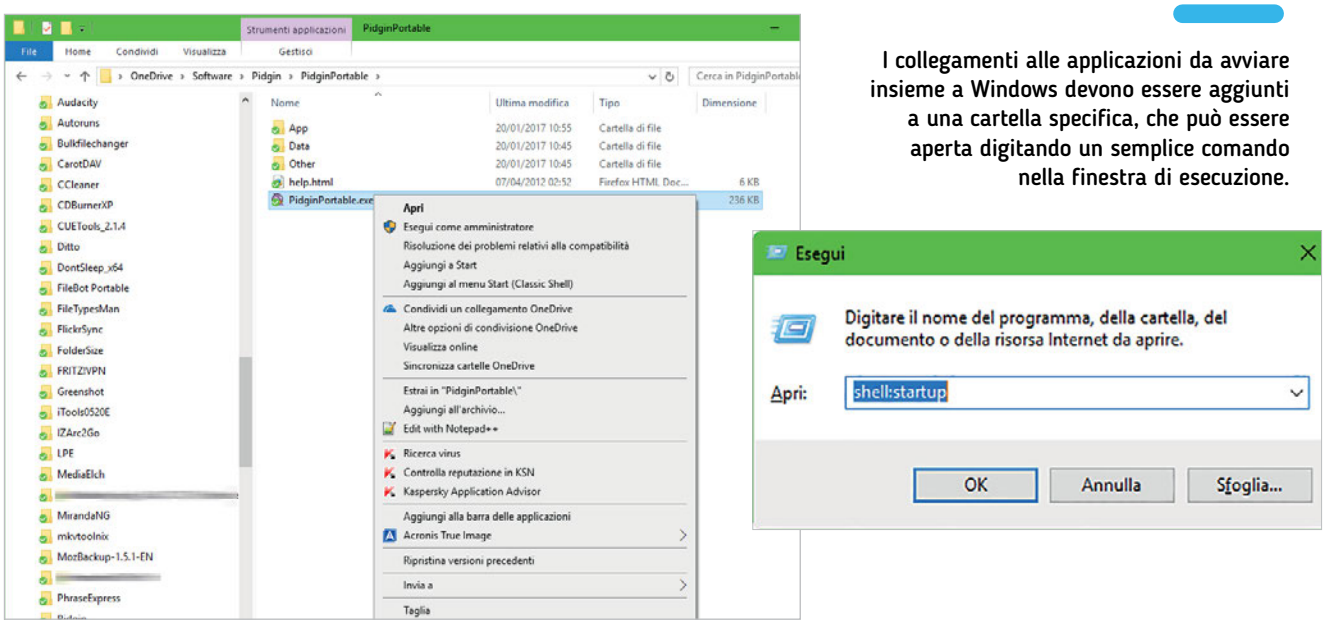


Belarc Advisor è un semplice tool che analizza la configurazione del sistema e produce un report dettagliatissimo, completo di numeri di versione per i principali software installati.

Una tipologia di dati essenziale, da preservare a ogni costo, è l'archivio delle credenziali di login

gratuito che analizza la configurazione del computer e genera un report dettagliato, in cui si trovano informazioni sulle applicazioni Win32 e Universal installate, la loro versione, gli aggiornamenti di Windows scaricati e applicati, e perfino le chiavi di licenza di molti software. Si tratta di informazioni preziose, e vale la pena di mantenerle sempre aggiornate. Un'altra strategia, semplice e parziale ma capace di ridurre i tempi di reinstallazione, è utilizzare software portable ovunque possibile; per chi non lo sapesse, si tratta di applicazioni e utility che possono essere avviate da qualsiasi cartella, senza bisogno di una precedente installazione. Tradizionalmente questi tool sono pensati per essere salvati su una chiavetta Usb oppure su un hard disk esterno, ma si prestano a essere memorizzati anche in uno spazio di cloud storage; in questo modo, tutti i computer collegati allo stesso account possono automaticamente accedere a una collezione di applicazioni e strumenti condivisa, sempre sincronizzata nelle funzioni e nelle impostazioni. Non tutti i software sono disponibili in questo formato, ma il loro numero cresce ogni giorno.

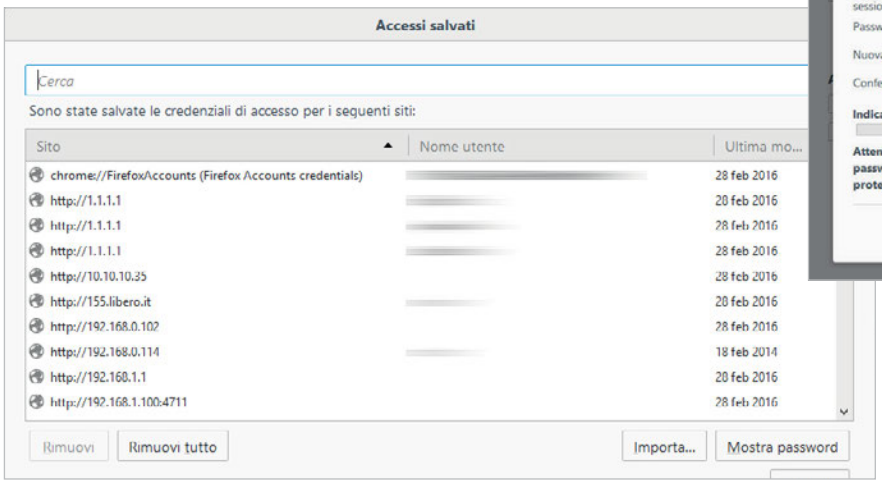
Oltre ai tool dedicati alla manutenzione del computer, ottimi candidati alla sincronizzazione tramite cloud storage sono i client di instant messaging; si può per esempio scaricare la versione portable di Pidgin *(https://portableapps.com/apps/Internet/pidgin_portable)*, oppure di Miranda NG *(http://www.miranda-ng.org/en/downloads)*. Entrambi possono essere configurati per connettersi a diverse reti di messaggistica istantanea, e condivideranno le impostazioni e l'archivio dei messaggi tra tutti i computer collegati allo stesso account di cloud storage. L'unica accortezza è quella di evitare l'esecuzione contemporanea su più sistemi, poiché i software portable in genere non sono progettati per condividere l'archivio e le impostazioni tra più istanze attive nello stesso istante. Con qualche accorgimento, dunque,

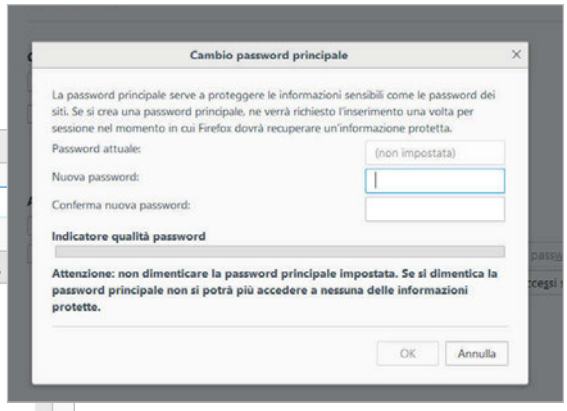


I collegamenti alle applicazioni da avviare insieme a Windows devono essere aggiunti a una cartella specifica, che può essere aperta digitando un semplice comando nella finestra di esecuzione.

Per eseguire automaticamente un programma portable all'avvio di Windows bisogna prima creare un collegamento, sfruttando la relativa funzione presente nel menu contestuale di Esplora file.

Le funzioni di memorizzazione delle credenziali di accesso integrate nei vari browser sono comode, ma non garantiscono la sicurezza dei dati: basta sapere dove cercare per scoprire tutte le password dell'utente.

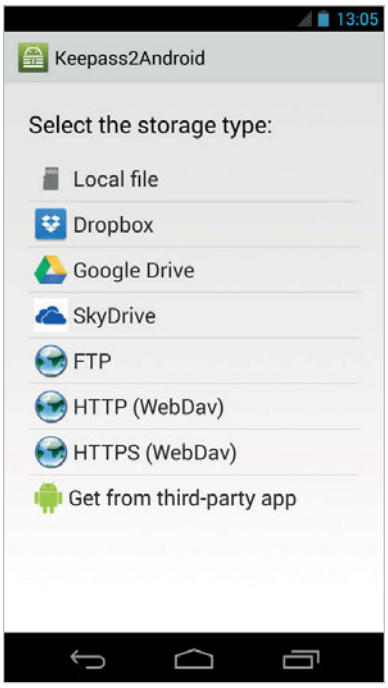




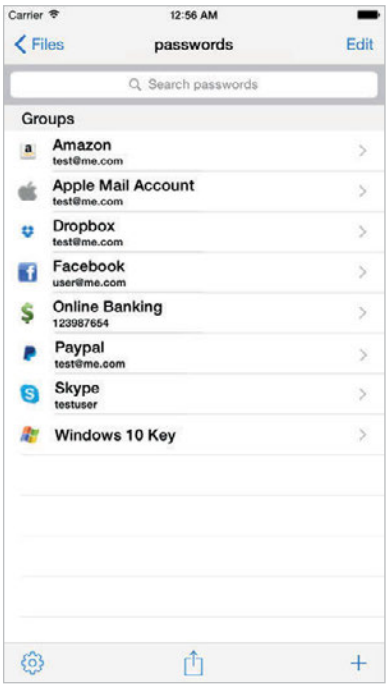
Un livello minimo di protezione dei dati di autenticazione è garantito dall'applicazione di una password principale, che dev'essere digitata prima di poter accedere ai dati.

si può ottenere un'esperienza d'uso del tutto analoga a quella disponibile tramite un'installazione di tipo tradizionale; scopriamo, per esempio, come forzare l'esecuzione del client di instant messaging all'avvio di Windows. Per prima cosa raggiungete la cartella che ne contiene l'eseguibile, fate clic destro sul file .Exe e selezionate la voce *Crea collegamento* nel menu contestuale. Richiamate poi la finestra di esecuzione, per esempio con la scorciatoia da tastiera *Windows+R*, e digitate la stringa di comando *shell:startup* per aprire una finestra di Esplora file che punta alla cartella dei collegamenti ai programmi da eseguire automaticamente all'avvio del sistema.
Spostate in questa cartella il collegamento all'eseguibile creato in precedenza, e chiudete le finestre aperte. Al prossimo avvio, l'instant messenger (o qualsiasi altro programma portable) verrà avviato insieme al sistema operativo.

Un'altra tipologia di dati essenziale, da preservare a ogni costo, è l'archivio delle credenziali di login: per garantire nello stesso tempo l'accesso alle informazioni e la loro sicurezza, è importante trovare un sistema di memorizzazione che sia nello stesso tempo flessibile e robusto. La soluzione più semplice e diffusa, ma anche meno sicura, è affidarsi alle funzioni di memorizzazione integrate direttamente nel browser: il salvataggio e il recupero delle credenziali sono quasi del tutto automatizzate, così come la sincronizzazione tra più dispositivi, a patto di utilizzare lo stesso browser su tutte le piattaforme. Il problema di queste funzioni è la loro scarsa sicurezza: se un dispositivo viene smarrito o rubato, c'è il rischio reale che l'archivio delle credenziali di accesso possa essere compromesso senza grandi difficoltà. Nel caso di Firefox, per esempio, basta aprire la pagina delle Opzioni *(Strumenti/Opzioni)*, raggiungere la sezione *Sicurezza* e fare clic sul pulsante *Accessi*



L'App Keepass2Android supporta la sincronizzazione con un gran numero di servizi di cloud storage, che garantiscono la massima flessibilità.



Nel mondo iOS il supporto per Keepass non è evoluto come in quello Android: un paio di App consentono di accedere agli archivi creati con il programma.

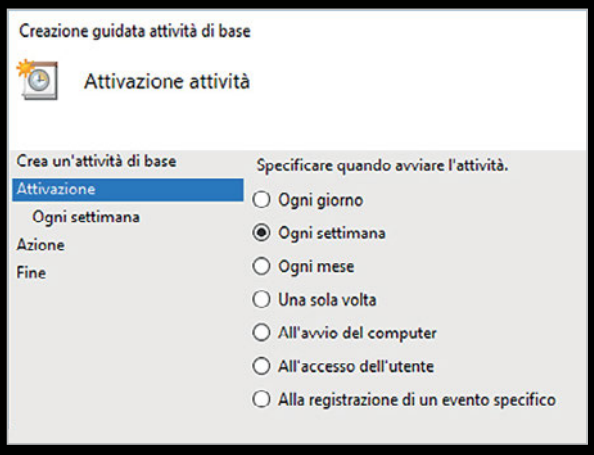
salvati per ottenere l'elenco di tutte le credenziali di accesso salvate. Un clic su *Mostra password* rende visibile anche questo campo, e garantisce un accesso completo a tutte le informazioni di autenticazione. Anche nel caso di Chrome il livello di protezione è analogo; l'unica differenza è la richiesta della password di sistema prima di rendere visibili le password memorizzate.

Chi non vuole rinunciare alla comodità delle funzioni di autenticazione integrate nel browser dovrebbe per lo meno aggiungere una master password per proteggere i dati: nel caso di Firefox, sempre nella sezione *Sicurezza* della finestra delle *Opzioni*, aggiungete un segno di spunta accanto alla voce *Utilizza una password principale* e scegliete una parola d'ordine robusta.
Per ottenere il livello di massimo protezione, però, bisogna affidarsi a un password manager esterno: questi software specializzati garantiscono un livello di protezione superiore, offrono funzioni avanzate e possono essere utilizzati con più browser. In molti casi, per esempio, permettono di implementare sistemi di autenticazione a più fattori, che possono scongiurare il rischio di una violazione della sicurezza anche se il malintenzionato dovesse venire in possesso del dispositivo e perfino scoprire la master password. Abbiamo parlato di questi tool in un articolo pubblicato sul numero 308 di *PC Professionale* (novembre 2016), ma in questa sede vorremmo suggerire un approccio più semplice. Alcuni password manager, come per esempio il freeware Keepass *(http://keepass.info)*, sono distribuiti anche come applicazioni portable, e possono essere memorizzati in una cartella sincronizzata nel cloud. Sia l'applicazione sia l'archivio delle credenziali di accesso saranno disponibili in tutti i dispositivi collegati allo stesso account.

La versione 2.x di Keepass integra un meccanismo di sincronizzazione che può gestire l'accesso concorrente e riconcilia automaticamente le modifiche effettuate da istanze diverse dell'applicazione. Per quanto riguarda il supporto ai sistemi operativi mobile, bisogna trovare la giusta combinazione di applicazioni e servizi per ottenere un sistema perfettamente funzionante. Keepass, infatti, pubblica le specifiche dei suoi file di archivio, ma si affida a

AUTOMATIZZARE IL REPORT DI BELARC ADVISOR

Non tutti i software integrano opzioni di esecuzione a intervalli regolari; Belarc Advisor, per esempio, è stato pensato soltanto per essere eseguito dall'utente. Ma Windows offre tutto il necessario per pianificare questo genere di attività. Scopriamo come procedere.
Dopo aver installato Belarc Advisor richiamate l'Utilità di pianificazione, fate clic su *Crea attività di base* nell'elenco *Azioni*, scegliete la frequenza di esecuzione (per esempio *Ogni settimana*) e poi indicate il percorso del programma. Nella finestra di riassunto aggiungete una spunta alla casella *Apri la finestra di dialogo Proprietà quando viene scelto Fine* e poi fate clic su *Fine*. Nella finestra delle *Proprietà* spuntate l'opzione *Esegui con i privilegi più elevati*, nella sezione *Opzioni di sicurezza* della scheda *Generale*, e poi passate alla scheda *Impostazioni*; qui aggiungete una spunta a *Avvia appena possibile se un avvio pianificato non viene eseguito*, per garantire l'esecuzione del processo. Confermate con un clic su *OK* per concludere la configurazione. Per rendere la procedura ancor più automatizzata si potrebbe poi pensare di creare un file batch che copi il report in una cartella sincronizzata, e che magari chiuda il programma alla fine dell'elaborazione.

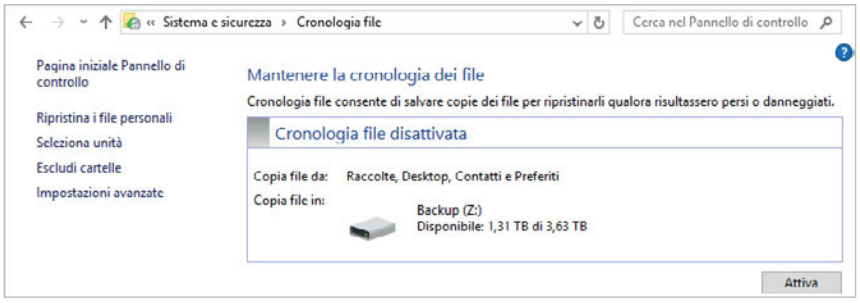


Se il software non lo prevede espressamente (come nel caso di Belarc Advisor) si può automatizzare l'esecuzione periodica creando una nuova attività pianificata tramite gli strumenti di Windows.

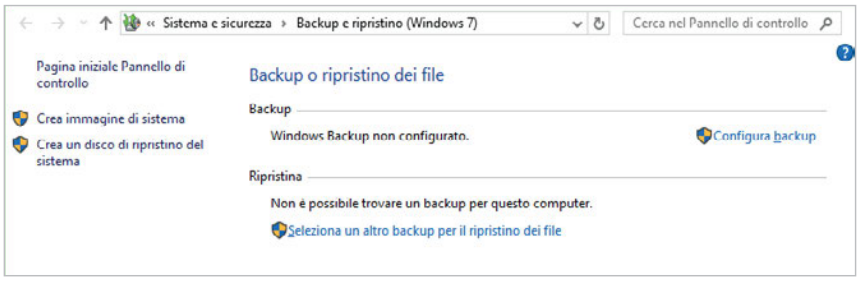
sviluppatori di terze parti per garantirne il supporto nei dispositivi mobile. Per Android si può scaricare Keepass2-Android, un tool open source che si segnala per il supporto a una grande varietà di servizi di cloud storage, tra cui Dropbox, Google Drive, OneDrive. Il panorama per iOS non è altrettanto ricco, ma si possono comunque trovare strumenti interessanti: segnaliamo in particolare KeePass Touch, che supporta la sincronizzazione con Dropbox, oltre che l'accesso ai file memorizzati su server Ftp. Molto interessante è la funzione di sblocco tramite lettore di impronte digitali, che rende l'uso del password manager veloce, pur garantendo la sicurezza dei dati.

BACKUP DEI DATI E DEL SISTEMA

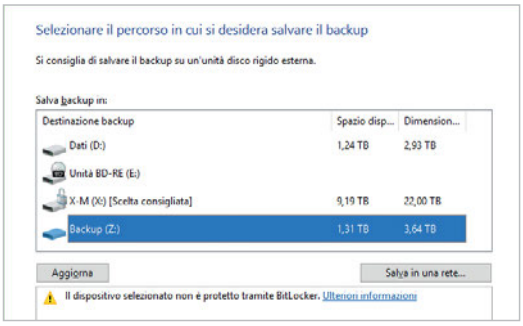
Appoggiarsi a un servizio di cloud storage può mettere al riparo da molti problemi, ma non sostituisce una strategia di backup di tipo tradizionale. Per garantire una protezione completa bisogna mettere in campo anche questo secondo livello di protezione. Esistono ottimi software gratuiti e commerciali dedicati al backup, e anche i sistemi operativi offrono alcune funzioni proprio per questo scopo. Un ottimo strumento, che offre gratuitamente gran parte delle sue funzioni, è Crashplan *(www.crashplan.com)*. Il software, dicevamo, è gratuito, mentre si paga per poter sfruttare le funzioni di memorizzazione remota dei backup (da 5 dollari Usa al mese per un computer). Il software è semplice da installare e utilizzare, e offre un ottimo compromesso tra funzioni e usabilità. Crashplan supporta Windows, Mac OS e Linux, e richiede la creazione di un account (basta inserire nome, indirizzo email e password); una volta completato questo passaggio, bisogna configurare il backup. L'unica impostazione davvero importante è la destinazione: si può salvare il backup in una cartella (meglio se in una condivisione di Rete, o su un hard disk esterno) o su un altro computer collegato allo stesso account, che dev'essere attivo e avere Crashplan installato. Per default, Crashplan salva il contenuto delle cartelle personali dell'utente. Per estendere il backup all'intero hard disk bisogna fare clic



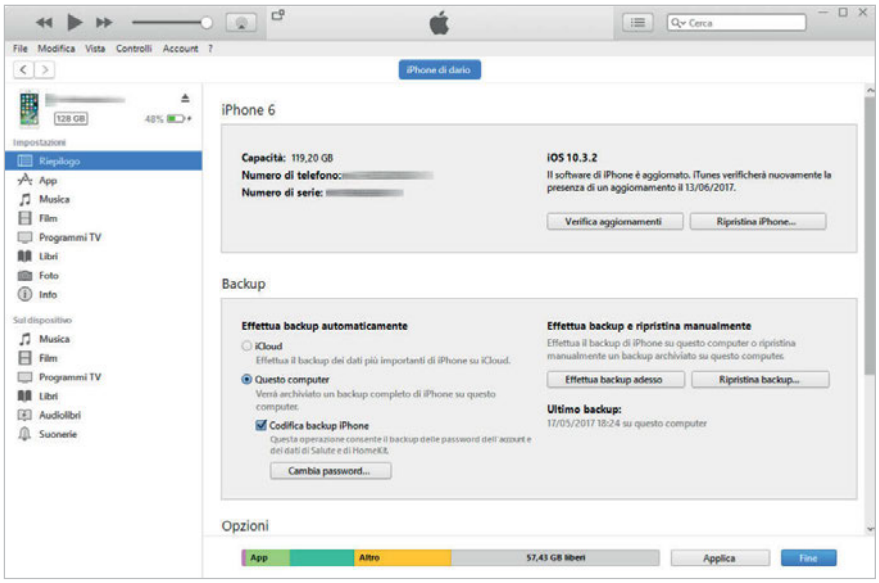
Cronologia File è una funzione di backup continuo dedicata ai file personali, integrata nel sistema operativo Microsoft dai tempi di Windows 8.



La funzione di creazione dei backup completi del sistema è inclusa in Windows da parecchie versioni, ma per richiamarla bisogna sapere dove cercare.



Le opzioni di salvataggio del tool di imaging di Windows non sono molto ricche: si può memorizzare il backup soltanto su un'unità collegata al sistema, su un supporto ottico oppure in una condivisione di rete.



Quando si satura lo spazio di memorizzazione remoto offerto da iCloud, l'unica soluzione per effettuare il backup dei dispositivi iOS è collegarli a un computer e utilizzare la tradizionale funzione integrata in iTunes.

sul pulsante *Cambia*, nella sezione *File* della scheda *Backup*, e spuntare tutti i dischi e le cartelle da mettere al sicuro. Non bisogna neppure sottovalutare le funzioni di backup integrate nel sistema operativo: Windows 10, per esempio, offre la Cronologia file, uno strumento di backup continuo piuttosto potente e semplice da usare. Per attivarlo basta collegare al sistema un hard disk esterno, aprire il Pannello di controllo e raggiungere la sezione *Sistema e sicurezza\Cronologia file*. Una configurazione predefinita sarà proposta automaticamente, ma si possono usare i collegamenti presenti nel pannello di sinistra per modificare l'unità di destinazione, le cartelle da includere ed escludere dal backup e le impostazioni avanzate, come per esempio la frequenza di salvataggio e il numero di versioni da mantenere. Windows integra anche una funzione di backup completo, che genera un file immagine con il contenuto dell'intero sistema operativo. Per richiamarla basta fare clic sul collegamento *Backup delle immagini di sistema*, in basso a sinistra nella finestra di Cronologia file, di cui abbiamo appena parlato.

Il backup dei dispositivi mobile è più semplice, anche se presenta comunque qualche criticità da non sottovalutare: nel caso di iOS, per esempio, il sistema stesso tenta un backup settimanale su iCloud di tutte le sue impostazioni, ma lo spazio disponibile gratis su questo servizio di storage è pari a soli 5 Gbyte, e basta scattare qualche fotografia di troppo o installare molte applicazioni per superare il limite. In questo caso le alternative non sono molte: si può acquistare altro spazio a pagamento (50 Gbyte costano 0,99 Euro al mese) oppure sfruttare la tradizionale funzione di backup locale, che prevede il collegamento del device a un computer, l'avvio di iTunes e l'utilizzo degli strumenti di salvataggio. Il mondo Android, come spesso accade, è ancor più frazionato: esistono ottimi tool di backup, ma non tutti sono disponibili per ogni dispositivo e per ogni versione del sistema operativo. Gli utenti di un device Samsung, per esempio, possono sfruttare SmartSwitch, ottimizzato per copiare le impostazioni e le applicazioni da un dispositivo all'altro, mentre chi ha effettuato il root del suo dispositivo può utilizzare applicazioni avanzate come Titanium Backup, che nella versione Pro (6,49 Euro sul Google Play Store) è capace di sincronizzare i backup anche con vari servizi di cloud storage, come Dropbox, Box e Google Drive.

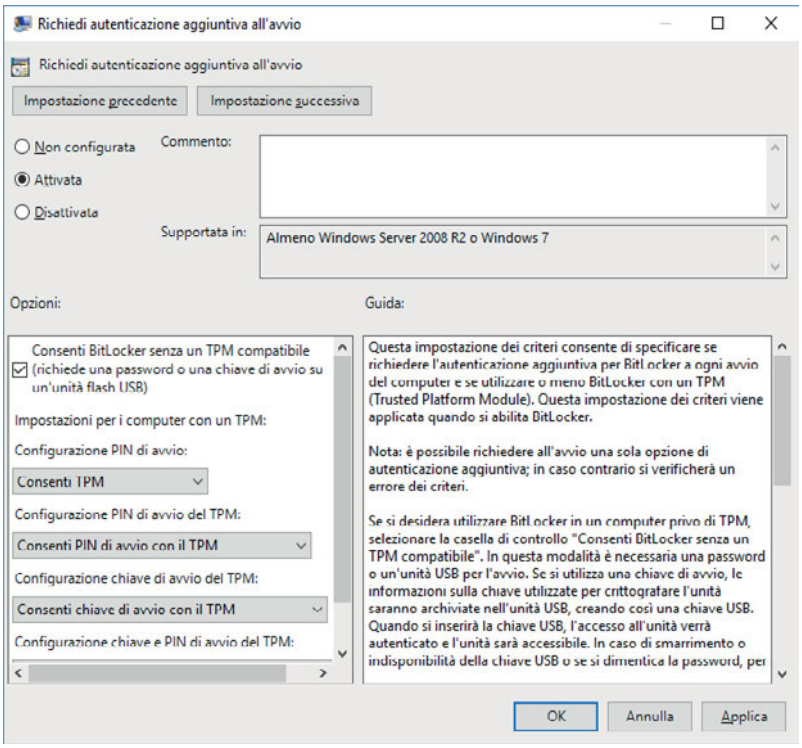
Cifrare i contenuti di tutti i device è una precauzione che può rivelarsi provvidenziale

PROTEGGERE DISPOSITIVI E DOCUMENTI

Dopo essersi assicurati che i dati personali non vengano perduti in caso di smarrimento o furto di un device, il passo successivo è proteggerli per evitare che cadano nelle mani sbagliate; se da un lato è vero che la maggior parte dei furti sono perpetrati da ladri di basso profilo, interessati solo al valore economico dell'oggetto sottratto, dall'altro esiste comunque la possibilità che le informazioni personali vengano estratte dal device per essere utilizzate o rivendute, specialmente se non si fa il possibile per salvaguardarle. Molti utenti, per esempio, ancora oggi non proteggono l'accesso allo smartphone e al tablet: è una misura di sicurezza minima, la cui assenza rappresenta una vulnerabilità davvero ingiustificabile. Nel corso del tempo le funzioni di protezione e sicurezza, sia per i computer tradizionali sia per i dispositivi mobile, sono cresciute moltissimo, e oggi si possono utilizzare varie tecnologie che garantiscono una protezione soddisfacente.

Nel caso dei Pc Windows, la prima misura di protezione dei dati è la cifratura del disco fisso: la tecnologia BitLocker è integrata nel sistema operativo Microsoft ormai da tempo, e si è dimostrata tanto affidabile quanto semplice da utilizzare. Cifrare la partizione di sistema permette di rendere inaccessibili tutti i suoi contenuti se non si conosce la password di accesso al sistema: anche smontando l'hard disk dal computer e collegandolo a un altro sistema, non si riuscirebbe comunque a estrarne nulla.

Il rovescio della medaglia è un leggero incremento dei tempi di lettura e scrittura, ma le prestazioni offerte dai computer moderni e le velocità di trasferimento raggiungibili dai dischi a stato solido riescono a garantire comunque un'ottima usabilità del sistema. Abilitare la cifratura BitLocker è semplice: scopriamo come procedere. Aprite Esplora file, raggiungete la vista *Questo PC* e fate clic destro sull'unità di sistema (normalmente C:); nel menu contestuale selezionate *Attiva BitLocker*. Se il vostro sistema non integra un chip Tpm (Trusted Platform Module), è necessario un passaggio ulteriore. Aprite l'Editor Criteri di gruppo



La chiave di cifratura del disco con BitLocker è normalmente basata su una password, ma si può anche scegliere di creare una chiave Usb di sblocco.

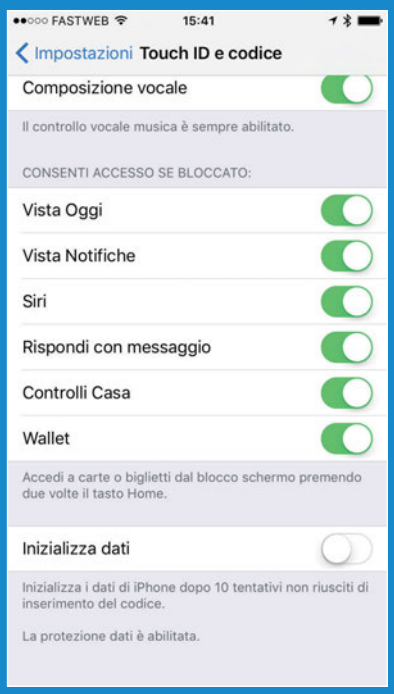
Per utilizzare la cifratura BitLocker nei sistemi che non integrano un chip Tpm, bisogna attivare la relativa opzione tramite l'editor dei Criteri di gruppo.

locali e raggiungete la sezione *Criteri Computer locale/Configurazione computer/Modelli amministrativi/Componenti di Windows/Crittografia unità BitLocker/Unità del sistema operativo*. Qui troverete il criterio *Richiedi autenticazione aggiuntiva all'avvio*; apritelo con un doppio clic e selezionate l'opzione *Attivata*, poi spuntate la voce *Consenti BitLocker senza un TPM compatibile* nel riquadro *Opzioni*, e confermate con *OK*. Il contenuto del chip Tpm viene utilizzato come chiave di decifratura; se non è disponibile, bisognerà invece scegliere se utilizzare una chiavetta Usb (che dovrà essere sempre inserita nel sistema per consentirne l'avvio), oppure digitare una password ogni volta. L'applicazione della cifratura BitLocker richiede un po' di tempo, ma viene completata automaticamente. È comunque meglio evitare di utilizzare intensamente il computer finché l'operazione non sarà conclusa. La cifratura del dispositivo è attiva per default in iOS, e ha dimostrato un ottimo livello di robustezza. Bisogna soltanto assicurarsi di attivare la protezione del device tramite Pin, codice alfanumerico o impronta digitale: tutte le relative opzioni si possono trovare in *Impostazioni/Touch ID e codice*. Nel caso di Android, invece, la cifratura non è sempre attiva, e funziona in modo diverso a seconda delle versioni del sistema operativo e delle personalizzazioni introdotte dai vari produttori. In generale, bisogna aprire le impostazioni, raggiungere la sezione *Generale/Sicurezza* e selezionare la voce *Crittografia dispositivo*. Dopo aver collegato il device a un caricabatterie fate clic sul pulsante *Crittografa dispositivo* e preparatevi a una lunga attesa: l'operazione, infatti, può richiedere anche oltre un'ora. Insieme a *Crittografa dispositivo*, spesso è presente anche la voce *Crittografa scheda SD*, che permette di proteggere i dati memorizzati su una scheda di memoria estraibile: è una precauzione utile (estrarre le informazioni da una scheda Sd è ancor più semplice che lavorare sulla memoria interna del dispositivo) ma bisogna considerare che, una volta cifrati, i dati saranno accessibili soltanto nel dispositivo. Non si potrà utilizzare più la scheda Sd per spostare informazioni dal device a un altro sistema.

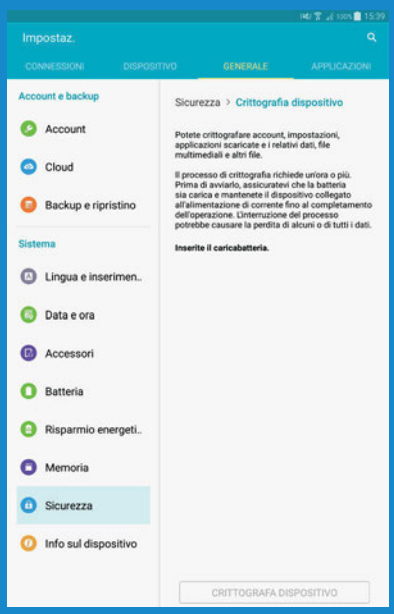
Nel caso di Android la cifratura non è sempre attiva e funziona in modo diverso a seconda delle versioni del sistema operativo

UTENTI E AUTENTICAZIONE

La cifratura dei dati si intreccia con un altro argomento cruciale per la sicurezza dei dispositivi informatici: l'autenticazione dell'utente. Per sbloccare l'accesso a un dispositivo protetto bisogna prima garantire l'identità dell'utente, un compito tradizionalmente demandato all'inserimento di username e password. Negli ultimi anni, specialmente nel settore mobile, questo sistema di autenticazione ha però lasciato il posto a soluzioni più rapide e intuitive, che meglio si sposano con i pattern di utilizzo tipici di questi device: non si può pensare di costringere l'utente a un login di tipo tradizionale ogni volta che deve leggere un Sms sul suo telefono. Perfino un semplice Pin numerico, però, sembra essere troppo oneroso per alcuni utenti, che rinunciano anche a questa primordiale forma di protezione in nome della comodità.
Per evitare l'enorme falla di sicurezza causato da questi comportamenti, sempre più produttori hanno inserito nei loro device (specialmente in quelli di livello medio/alto) meccanismi di

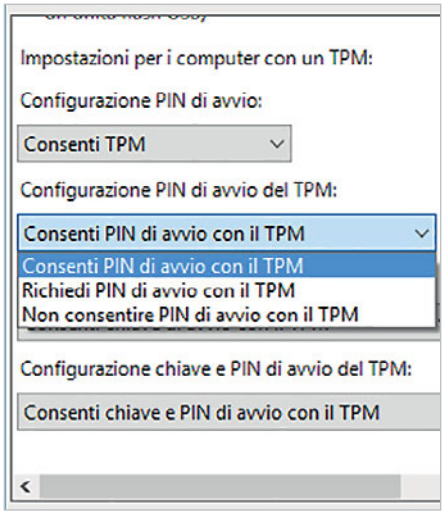


La protezione dei dati memorizzati sui dispositivi iOS è legata all'impostazione di un codice di sblocco numerico: una dicitura in fondo a questa pagina conferma che la protezione è effettivamente attiva.



Per attivare la cifratura di un dispositivo Android bisogna raggiungere la relativa sezione delle Impostazioni, collegare il device a un caricabatteria e avviare la procedura, che può richiedere tempi lunghi.

autenticazione alternativi, come lettori di impronte digitali, algoritmi di riconoscimento del volto o addirittura sistemi di scansione dell'iride. Se sono disponibili sul proprio device è opportuno attivare questi sistemi di sblocco, che migliorano il livello di protezione senza complicare la procedura di accesso; al contrario, in molti casi la semplificano: può bastare soltanto un clic sul pulsante home del telefono, oppure guardare lo schermo del dispositivo per essere riconosciuti e accedere al sistema.
Anche Windows 10 offre un sistema di login biometrico avanzato, che può sfruttare il riconoscimento del volto oppure la lettura delle impronte digitali al posto delle consuete password e Pin numerici. Il suo nome è Windows Hello, e richiede hardware compatibile per poter essere attivato: nel caso del riconoscimento facciale, in particolare, serve una camera con sensore 3D, compatibile con la tecnologia RealSense di Intel, come la Senz3D di Creative Labs, la Brio 4k Pro Webcam di Logitech o la Stargazer di Razer.



BitLocker può essere impostato per richiedere due diversi fattori di autenticazione, come la presenza di un chip Tpm e un codice Pin numerico.

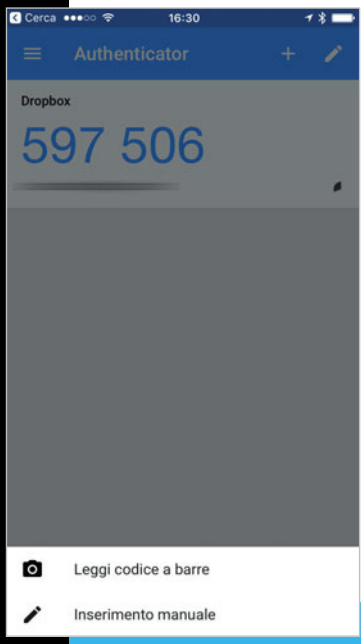
I sistemi di autenticazione possono anche essere combinati per garantire un livello di sicurezza più elevato: è la cosiddetta autenticazione a più fattori, che combina diversi metodi di riconoscimento per aumentare il livello di probabilità che la persona di fronte allo schermo sia veramente chi sostiene di essere.
Tradizionalmente, queste tecnologie combinano "qualcosa che si sa", ossia una password o un codice, con "qualcosa che si ha", cioè un dispositivo, una tessera o una chiave. Un terzo fattore di autenticazione può essere "qualcosa che si è", ossia una caratteristica fisica personale, come il volto, l'impronta digitale o l'iride. Anche se l'introduzione di questi sistemi di autenticazione nel mondo dell'informatica consumer è piuttosto recente, non è una novità in senso assoluto: per esempio, da decenni l'accesso ai terminali bancomat prevede l'associazione di un elemento fisico (la tessera) con un'informazione conosciuta (il Pin). L'autenticazione a più fattori può essere impostata anche per l'accesso a Windows: esistono infatti applicazioni specifiche, come KeyLock *(https://sourceforge.net/p/usbraptor/wiki/Home)* o USB Raptor *(https://sourceforge.net/p/usbraptor/wiki/Home)*, che consentono l'accesso al computer soltanto se è connessa al sistema una chiavetta Usb. In realtà, come abbiamo già visto, un risultato analogo può essere ottenuto anche tramite la cifratura con BitLocker del disco di sistema, utilizzando una chiavetta Usb come contenitore della chiave.

Il Criterio di sistema già visto in precedenza *(Criteri Computer locale/Configurazione computer/Modelli amministrativi/Componenti di Windows/Crittografia unità BitLocker/Unità del sistema operativo/Richiedi autenticazione aggiuntiva all'avvio)* permette anche di specificare un secondo fattore di autenticazione, in aggiunta al Tpm (che deve essere presente nel sistema). Il secondo fattore può essere un codice Pin con una lunghezza compresa tra 6 e 20 cifre, oppure una chiavetta Usb che contiene le chiavi di decifratura. Per rendere obbligatoria la presenza di uno di questi due elementi basta modificare la relativa casella a discesa da *Consenti* a *Richiedi*. Si può anche rendere obbligatoria la richiesta di entrambi i fattori di protezione, modificando l'opzione *Configurazione chiave e PIN di avvio del TPM*.

AUTENTICAZIONE A DUE FATTORI IN DROPBOX

L'associazione di più fattori di autenticazione è un ottimo modo per migliorare il livello di sicurezza complessivo dei dati e dei dispositivi, e dovrebbe essere attivato ovunque sia disponibile: è il caso, per esempio, di molti servizi basati sul Web, e in particolare dei sistemi di cloud storage. Vediamo, per esempio, come attivare l'autenticazione a due fattori in Dropbox. Questo servizio può sfruttare Google Authenticator, un semplice e ottimo sistema di autenticazione che genera codici alfanumerici con vita brevissima (qualche decina di secondi), in modo simile ai token utilizzati da vari istituti di credito per l'accesso ai loro servizi di home banking.
Come primo passo, quindi, scaricate l'App di Google Authenticator per il vostro dispositivo mobile. Poi raggiungete la pagina principale di Dropbox, all'indirizzo *www.dropbox.com*, e se necessario completate l'autenticazione. Fate clic sull'icona del profilo dell'utente (per default una faccina sorridente) collocata in alto a destra, accanto alla casella di ricerca. Selezionate *Impostazioni* nel menu a discesa, e poi passate alla scheda *Sicurezza* nella pagina successiva.

Individuate la sezione *Verifica in due passaggi* e selezionate il collegamento *Fai clic per riattivare* per aprire una procedura guidata. Fate clic su *Inizia*, inserite nuovamente la password del servizio, e poi selezionate *Utilizza un'applicazione per cellulari*. Aprite Google Authenticator sullo smartphone, fate tap su + per aggiungere un nuovo servizio e poi sulla voce *Leggi codice a barre*. Inquadrate con la fotocamera dello smartphone il codice QR visualizzato nella pagina di Dropbox per completare l'associazione. È opportuno indicare anche un metodo di autenticazione secondario, utile per esempio in caso di smarrimento del device.

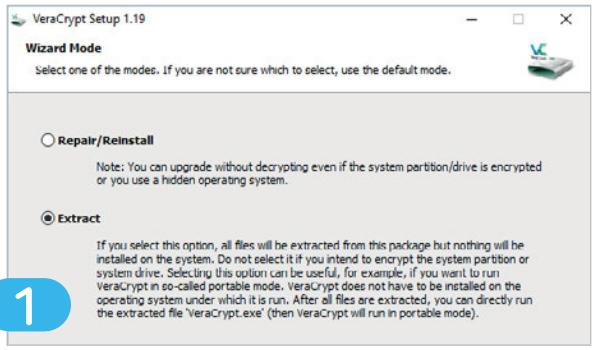


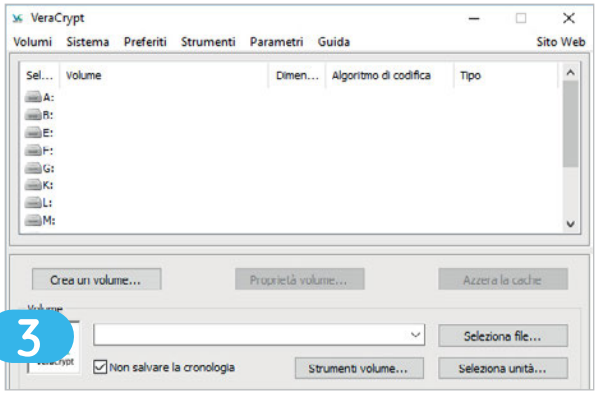
Google Authenticator è una semplice App per dispositivi mobile che consente di generare codici numerici utilizzabili come secondo fattore di autenticazione da numerosi servizi Web.

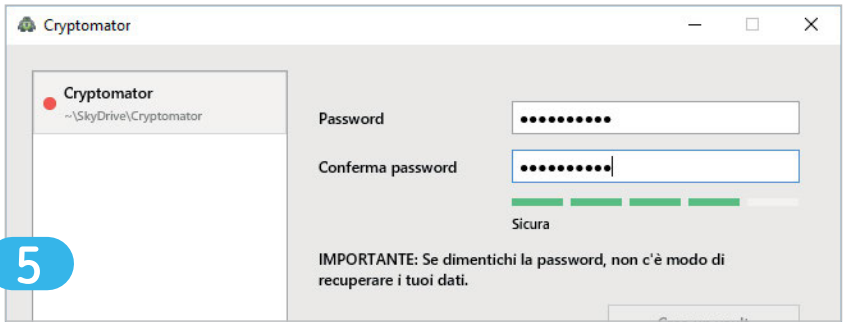
CIFRATURA DEI DATI

BitLocker ha permesso di familiarizzare con le opportunità di protezione offerte dalla cifratura dei dati, ma il mercato offre molti altri strumenti di crittografia. Il tool di Microsoft può essere applicato alle partizioni che contengono dati e perfino ai dischi esterni e alle chiavette Usb, ma esistono anche altri strumenti che sfruttano la cifratura per proteggere le informazioni più sensibili. Per esempio, si possono utilizzare strumenti come VeraCrypt *(https://veracrypt.codeplex.com)* per creare unità virtuali cifrate in cui salvare i dati più preziosi, proteggendoli con sistemi di cifratura robusti. Questo tool è basato sul noto progetto TrueCrypt, e ne ha raccolto l'eredità quando il suo sviluppo è stato interrotto nel 2014. Il funzionamento è analogo a quello del suo predecessore: scopriamo come creare e utilizzare un volume cifrato.

Per prima cosa, scaricate e installate il programma dal sito ufficiale: è disponibile in varie versioni, per tutti i principali sistemi operativi. Il file di Setup permette di installare il software in modo tradizionale, oppure di estrarre semplicemente tutti i dati in una cartella, per l'utilizzo portable: anche VeraCrypt è un ottimo candidato a essere ospitato in una cartella sincronizzata tramite un servizio di cloud storage. Aprite l'interfaccia principale del software e selezionate *Settings/Language;* evidenziate l'italiano nell'elenco e fate clic su *OK* per tornare alla finestra principale. Selezionate ora il pulsante *Crea un volume* per aprire la relativa procedura guidata: il primo passo permette di scegliere se creare un file contenitore, se criptare una partizione o un disco di dati, oppure se cifrare il disco di sistema (un po' come abbiamo illustrato in precedenza nel paragrafo dedicato a BitLocker). In questo caso selezionate la prima opzione e proseguite al passo successivo; scegliete di creare un *Volume standard* (i volumi nascosti sono un argomento interessante, ma vanno oltre lo scopo di questo articolo), e indicate il percorso di destinazione. Il passaggio successivo permetterà di scegliere l'algoritmo di cifratura tra molte opzioni diverse; le impostazioni di default (Aes, con hash SHA-512) rappresentano un ottimo compromesso tra sicurezza e prestazioni, e possono essere utilizzate







senza timore. La procedura guidata permetterà poi di decidere la dimensione del disco virtuale, e chiederà di inserire la password. Nella pagina successiva si possono specificare alcune opzioni relative al file system, mentre il sistema raccoglie dati pseudocasuali provenienti dai movimenti del cursore del mouse. Una volta che questa operazione sarà completata si potrà fare clic su *Formatta* per creare l'unità. Per accedere ai contenuti bisogna ritornare alla finestra principale di VeraCrypt, selezionare il file contenitore appena creato, indicare una delle lettere di unità libere e fare clic sul pulsante *Monta*. Il disco criptato sarà accessibile da Esplora file e da qualsiasi altra applicazione, tramite l'unità virtuale aggiunta al sistema. Come abbiamo potuto intuire durante questa procedura passo per passo, VeraCrypt offre anche altre opzioni: permette, per esempio, di creare intere partizioni cifrate, e di sfruttare fattori di autenticazione diversi, come per esempio file chiave.

VeraCrypt non offre applicazioni ufficiali per il mondo mobile, ma – un po' come accade per Keepass – pubblica tutte le informazioni sul formato dei suoi file, che possono essere utilizzate da sviluppatori terzi per fornire soluzioni compatibili. Per Android, ad esempio, si può scaricare Eds (Encrypted Data Store, 6,49 Euro sul Google Play Store), mentre per il mondo iOS si può scegliere tra Disk Decipher e Crypto Disks, entrambe disponibili al prezzo di 1,09 Euro. Un altro ambito in cui la cifratura dei dati può essere

1 Oltre all'installazione tradizionale, i file necessari a VeraCrypt possono anche essere semplicemente copiati in una cartella, realizzando una configurazione di tipo portable.

2 VeraCrypt permette di creare un file contenitore cifrato, di proteggere un'intera partizione e addirittura di codificare il disco di sistema.

3 L'interfaccia principale di VeraCrypt è semplice da utilizzare, pur offrendo funzioni interessanti, ed è derivata direttamente dall'impostazione del progetto TrueCrypt.

4 VeraCrypt offre una notevole selezione di algoritmi di cifratura e hash, che permettono di trovare il compromesso più efficiente tra prestazioni e sicurezza.

5 Cryptomator è un semplice strumento gratuito di cifratura dei file, ottimizzato per lavorare in combinazione con i client di cloud storage come OneDrive, Dropbox o Google Drive.

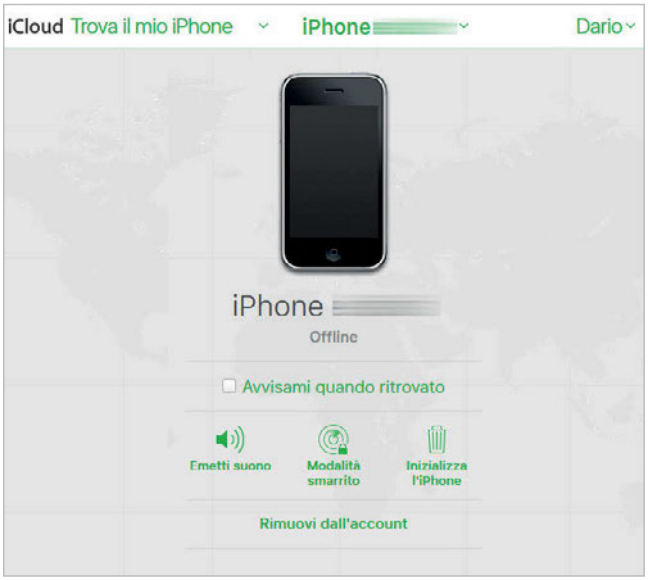
L'ultimo passaggio per assicurare la protezione dei dati è quello di forzarne l'eliminazione da un dispositivo rubato oppure smarrito

preziosa, è quello dei cloud storage: al loro interno capita di memorizzare informazioni delicate, che si vorrebbe proteggere con un ulteriore livello di sicurezza. In questo caso si possono utilizzare applicazioni specifiche, come BoxCryptor o Cryptomator. Quest'ultima, in particolare, è distribuita secondo il paradigma dell'open source ed è disponibile per tutti i principali sistemi operativi desktop: Windows, Mac OS e Linux, a 32 e 64 bit. Il suo funzionamento è semplice: una volta completata l'installazione basta aprire l'interfaccia del programma e creare un nuovo vault, ossia una cartella protetta all'interno di un albero di cartelle collegato a un servizio di cloud storage. Il vault viene montato e visualizzato come unità virtuale. Basta copiare i dati nell'unità virtuale per proteggerli: una volta smontato il vault, le informazioni saranno cifrate e illeggibili. Cryptomator funziona bene finché i documenti protetti devono essere aperti su un computer, ma l'assenza di applicazioni per il mondo mobile non lo rende una soluzione universale. Chi avesse bisogno di accedere ai dati cifrati anche da smartphone e tablet può rivolgersi a BoxCryptor, che funziona in modo analogo ma offre client anche per iOS, Android e Windows Phone. Non si tratta però di un programma gratuito: l'abbonamento che sblocca tutte le sue funzioni costa 36 Euro all'anno per gli utenti privati, e 72 Euro all'anno per i professionisti.

ELIMINARE LE INFORMAZIONI PRIVATE

L'ultimo passaggio per assicurare la protezione dei dati è quello di forzarne l'eliminazione da un dispositivo rubato oppure smarrito: nel caso di smartphone e tablet, sono molte le funzioni pensate per la gestione remota dei device. iOS, per esempio, integra ormai da tempo un'App chiamata Trova iPhone: mostra l'elenco dei dispositivi collegati all'Apple ID e ne indica l'ultima posizione rilevata (rimane memorizzata fino a 24 ore dopo lo spegnimento o l'esaurimento della batteria). Aprendo la pagina dei dettagli si accede ad alcune funzioni

L'App Trova iPhone permette di individuare facilmente i dispositivi smarriti, e offre anche alcune funzioni aggiuntive per bloccarne l'accesso o cancellarne i contenuti da remoto.

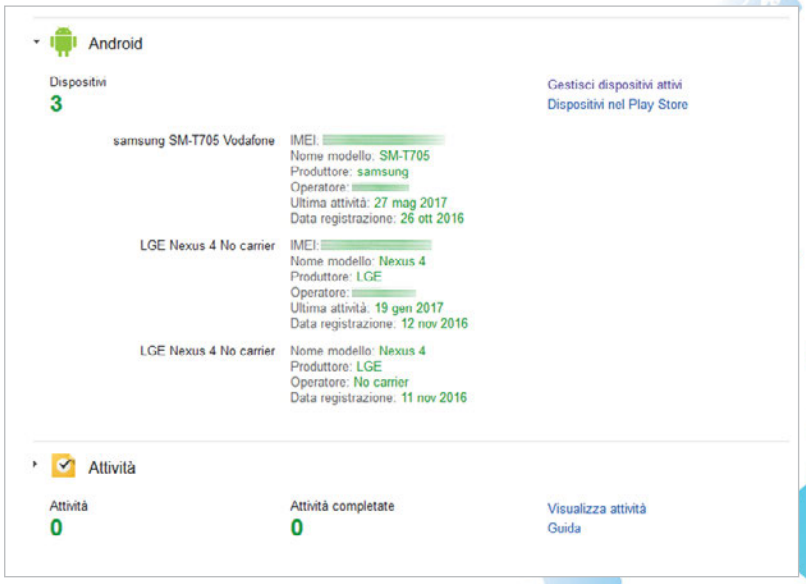


La funzione Trova iPhone è disponibile anche via Web: basta raggiungere il proprio account di iCloud e scegliere la relativa funzione per accedere alle stesse funzioni offerte dall'App per iOS.

aggiuntive: *Riproduci suono* attiva una suoneria che viene riprodotta anche se si è impostata la modalità silenziosa, in modo da facilitare l'individuazione del dispositivo (utile se non si ricorda più dove è stato lasciato). Si può inoltre attivare la *Modalità smarrito*, che blocca l'accesso al dispositivo e visualizza informazioni di contatto utilizzabili da chi eventualmente ritrovasse il dispositivo per riconsegnarlo al legittimo proprietario. L'ultima opzione, da utilizzare quando si ha la certezza che il device è stato rubato e non sarà restituito volontariamente, è chiamata *Inizializza iPhone* e cancella in modo irreversibile tutte le informazioni personali. Le stesse funzioni sono accessibili anche via Web: basta raggiungere la pagina *www.icloud.com/#find* e sfruttare le opzioni offerte dall'interfaccia.

Anche Android offre funzioni simili, anche se non tutti i produttori le hanno implementate nello stesso modo: nel caso dei dispositivi Samsung, per esempio, la funzione di default offerta da Google è sostituita da quella collegata all'account Samsung. Per accedervi bisogna raggiungere la sezione *Impostazioni/Sicurezza* e attivare la funzione *Trova dispositivo personale*. È un peccato che non tutti i produttori offrano le stesse funzioni, sia perché l'implementazione proposta da Google (accessibile anche dal sito Web *https://android.com/find)* è oggi più potente e completa rispetto al passato, sia perché si genera una confusione che rende più difficile agire in modo risoluto nei momenti concitati che seguono un furto o uno smarrimento. Nel caso degli smartphone e dei dispositivi con modem per la rete cellulare, è anche utile recuperare e salvare il codice Imei, che può essere comunicato al gestore telefonico per bloccare l'accesso alla rete cellulare. Il codice è riportato, in genere a caratteri microscopici, sulla scatola del telefono, ed è accessibile anche dal sistema operativo: nel caso di iOS basta raggiungere la sezione *Impostazioni/Generali/Info/IMEI*, mentre con Android bisogna aprire le Impostazioni e poi individuare la sezione *Info sul dispositivo/Stato/Informazioni IMEI*. Nel caso di Android le informazioni sono accessibili facilmente anche via Web: basta raggiungere la pagina *https://myaccount.google.com/dashboard* e aprire la sezione *Android*, che elenca i dettagli sui dispositivi collegati al proprio account Google.

Le funzioni di individuazione e cancellazione remota che abbiamo appena illustrato non sono invece patrimonio comune per i sistemi operativi desktop: per ottenere funzioni simili bisogna affidarsi a software e servizi di terze parti, con risultati non sempre perfetti. Una delle soluzioni più interessanti è Prey *(www.preyproject.com)*, disponibile con una formula freemium che propone un livello di servizio basilare gratuito, a cui sono associati alcune offerte commerciali più flessibili e ricche di funzioni. Più in dettaglio, la versione gratuita permette di controllare fino a tre dispositivi organizzati in un'unica zona, offre le funzioni di notifica e reporting standard e include le opzioni di tracciamento e sicurezza più importanti, tra cui l'individuazione della posizione geografica, l'allarme, il blocco dell'accesso e l'attivazione della webcam. Passando alle formule di abbonamento commerciale, invece, si aggiungono anche le funzioni di cancellazione remota e recupero dei file. Gli abbonamenti partono da 5 dollari Usa al mese per la versione Personal, che supporta fino a tre dispositivi, mentre l'abbonamento Home amplia a un massimo di dieci il numero di device supportati. Prey è disponibile per tutti i principali sistemi operativi: iOS e Android sul fronte mobile, Windows, Linux e Mac OS per i computer tradizionali. Può dunque rappresentare, specialmente nelle versioni commerciali, un ottimo sistema centralizzato per il monitoraggio e la sicurezza di tutti i dispositivi di una famiglia o di una piccola azienda. •



La Google Dashboard permette di recuperare velocemente il codice Imei di tutti i dispositivi Android associati a un determinato account Google.