

Paolo Attivissimo

Facebook e Twitter

manuale di autodifesa

Edizione 2012.03



Paolo Attivissimo

Facebook e Twitter

manuale di autodifesa

Conoscere i social network
per usarli in modo sicuro

Edizione 2012.03

L'edizione digitale aggiornata di questo libro
è disponibile presso
<http://disinformatico.info>

Permesso d'autore

Il testo originale di questo libro è © 2012 by Paolo Attivissimo. Alcuni diritti sono riservati. *Some rights reserved.*

Quest'opera è distribuita alle seguenti condizioni, basate sulla licenza Creative Commons *Attribuzione - Non commerciale - Non opere derivate 2.5 Italia*. I dettagli legali di questa licenza di distribuzione sono disponibili in italiano presso <http://creativecommons.org/licenses/by-nc-nd/2.5/it/legalcode>.



In sintesi, chiunque è libero di riprodurre, distribuire, tradurre, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire e recitare pubblicamente, purché senza lucro o profitto, quest'opera alle seguenti condizioni:

- **Attribuzione.** La paternità dell'opera va attribuita a Paolo Attivissimo e si deve indicare il sito <http://disinformatico.info> come fonte. Non si deve fare nulla che suggerisca che l'autore avalli il modo in cui viene usata l'opera o chi la usa.
- **Senza lucro o profitto.** Senza l'autorizzazione scritta esplicita dell'autore, non è permesso usare quest'opera per fini commerciali. Non è permesso stamparla, duplicarla o distribuirla per venderla a terzi o per trarne un vantaggio economico. È invece permesso stamparla, duplicarla e distribuirla a titolo gratuito.
- **Non opere derivate.** Non è permesso alterare o trasformare quest'opera, né usarla per crearne un'altra. Ne è però permessa la traduzione fedele e integrale.

È permessa la deroga a ciascuna di queste condizioni se si ha il permesso esplicito scritto del titolare dei diritti, con il quale è possibile concordare anche utilizzi di quest'opera non previsti da questa licenza.

Ogni volta che si usa o distribuisce quest'opera, questo va fatto secondo i termini di questa licenza, che va comunicata con chiarezza.

Questa licenza lascia impregiudicati i diritti morali.

Gli usi consentiti dalla legge sul diritto d'autore e gli altri diritti non sono in alcun modo limitati da quanto sopra. È specificamente consentita la libera citazione, anche di ampi brani, purché siano indicati fonte e autore.

Quest'opera si avvale del diritto di citazione a scopo accademico e di critica previsto dall'Articolo 10 della Convenzione di Berna sul diritto d'autore.

Photo credits: All pictures are believed to be used to the extent allowed by fair use. Should any copyright issues arise, please contact the author, Paolo Attivissimo, by e-mail at paolo.attivissimo@gmail.com or by post at the following address: via Prati Botta 16B, CH-6917 Lugano Barbengo, Switzerland.

Indice breve

Note tecniche.....	3
1. “Autodifesa”? Sul serio?.....	5
2. I concetti di base.....	9
3. Precauzioni generali per i social network.....	13
4. Impostazioni sicure di Facebook.....	23
5. Comportamenti sicuri in Facebook.....	43
6. Impostazioni sicure di Twitter.....	55
7. Comportamenti sicuri in Twitter.....	63

Note tecniche

Ringraziamenti

Vorrei ringraziare tutti i lettori e autori del blog *Disinformatico.info* per l'aiuto nelle ricerche, per la verifica dei dati, per i test ai quali hanno collaborato e per aver snidato molti miei errori e refusi. Quelli che restano sono esclusivamente colpa mia.

Distribuzione libera e gratuita

L'edizione digitale di questo libro è liberamente duplicabile e distribuibile *tale e quale*. Non avete il permesso di spacciarla per vostra o di stamparla per rivenderla; il diritto d'autore resta in vigore. I dettagli della licenza d'uso sono all'inizio del testo nella sezione *Permesso d'autore*.

Non ho scritto questo libro per diventare ricco, ma per dare al maggior numero possibile di persone l'occasione di usare in modo sicuro Internet e tutte le sue ricchezze. Tuttavia scrivere un libro come questo costa tempo e fatica. Quindi se vi va di darmi una mano e incoraggiarmi a scrivere ancora, non dico certo di no: potete farlo segnalando errori o frasi non chiare, contribuendo con indagini per ampliarlo oppure offrendomi un trancio di pizza e una birra tramite una donazione via PayPal come incentivo per scrivere altri libri. I dettagli sono sul sito *Disinformatico.info*.

Commenti, correzioni e aggiornamenti

Questo libro è un progetto in continua lavorazione. Le modalità di funzionamento dei social network cambiano frequentemente e periodicamente vengono scoperte o corrette vulnerabilità di ogni sorta. Cercherò di tenere aggiornato questo manuale il più possibile, ma se notate qualche aspetto mancante o qualche errore in questo testo, scrivetemi a paolo.attivissimo@gmail.com. Buona lettura.

1. “Autodifesa”? Sul serio?

Parlare di *autodifesa* dai social network, come se si trattasse di un nemico o di un aggressore, può sembrare eccessivo. Ma i fatti parlano molto chiaro:

- I giornali segnalano spesso **equivoci, liti e imbarazzi** scaturiti da conversazioni o immagini private caricate sui social network e poi trafugate e rese pubbliche.
- Fra i giovanissimi, e anche fra gli adulti, è di moda **scambiarsi foto molto intime sui social network**, pensando (erroneamente) che le garanzie di privacy di questi servizi siano credibili.
- I datori di lavoro e i selezionatori hanno sempre più spesso l'abitudine di **valutare i candidati tramite i social network**, in base a quello che gli aspiranti lavoratori vi scrivono e vi pubblicano.
- Attraverso i social network, i già assunti criticano l'azienda, rivelano dettagli riservati o si fanno cogliere a simulare malattie e così si trovano **licenziati a causa dei social network**, perché non si rendono conto di essere letti anche dai colleghi, dal datore di lavoro o dalla concorrenza.
- Gli avvocati divorzisti usano la cronologia delle attività sui social network del coniuge avversario per ricostruirne amicizie, legami e spostamenti sospetti: è quasi un **pedinamento digitale**.
- Nei social network, come nella vita, ci sono anche i **molestatori** e i **predatori sessuali**, ma in questo ambiente sono più spavaldi e invadenti, perché sanno (o credono) di essere anonimi e impossibili da rintracciare.
- Si creano anche **nuove forme di bullismo** (il cosiddetto *cyberbullismo*), come le **videorisse**, vale a dire scontri organizzati e pianificati per riprenderli con i telefonini e poi pubblicarli sui social network, o il **trolling** (provocazione a distanza per il puro gusto di rovinare i rapporti sociali di una vittima o farla arrabbiare).
- Con poche eccezioni, **non siamo abituati a scrivere in pubblico**, come avviene spesso nei social network, e non ci rendiamo conto di chi ci sta leggendo o ci potrebbe leggere, dal partner all'ex partner al datore di lavoro al molestatore al pedofilo. Non siamo mentalmente avvezzi a soppesare tutto quello che scriviamo

pensando a tutte le persone possibili che potrebbero sfogliare i nostri scritti pubblici su Facebook.

- Nei social network non c'è il diritto all'oblio e quindi idee scritte o immagini pubblicate anni fa possono tornare a **tormentarci per sempre**, dando agli altri un'idea del tutto distorta e obsoleta di noi.
- Anche la forma di comunicazione dei social network, che è uno strano ibrido fra scrittura tradizionale e conversazione (c'è chi lo chiama *discorso scritto*), si presta a **equivoci linguistici**. Chi scrive costruisce la frase sentendone mentalmente l'intonazione, come se stesse parlando; ma chi la riceve vede solo caratteri privi di inflessione emotiva e spesso non può sapere se chi gli ha inviato la frase stava scherzando o facendo del sarcasmo o era serio.
- La **disinformazione** grande e piccola (dalle bufale alle tesi di complotto) prospera nei social network: c'è chi la fabbrica e chi la legge e diffonde per tornaconto ideologico o economico, e i controlli sono davvero scadenti.
- Ci sono anche questioni di **sicurezza informatica**: la popolarità di questi social network, la vulnerabile complessità dei loro sistemi ricchi di opzioni e la scarsa attenzione alla sicurezza degli utenti vengono sfruttate dai criminali informatici per disseminare virus, rubare credenziali d'accesso ai social network e da lì lanciarsi verso altri crimini, oppure compiere **truffe** ai danni degli utenti. Non è un fenomeno raro: Facebook ha dichiarato che vengono "compromessi" (e quindi bloccati) circa 600.000 login di suoi utenti ogni giorno.
- C'è poi la **microservitù**, ossia il fatto che noi utenti lavoriamo gratuitamente (aggiornando i nostri profili sui social network, per esempio) per dare ai proprietari dei social network spazi nuovi nei quali inserire pubblicità e guadagnare cifre enormi sulle nostre fatiche.
- Da ultima, ma non meno importante, c'è la **privacy**. Gli utenti regalano spontaneamente ai social network un dettagliatissimo grafico delle loro amicizie e parentele e l'elenco dei loro gusti personali e dei loro spostamenti. La STASI (la polizia segreta dell'ex Germania Est) avrebbe dato tutto per avere quello che oggi stiamo regalando volontariamente a delle società commerciali prevalentemente americane.

Per contro, i social network hanno molti **aspetti positivi**, soprattutto in termini di possibilità d'interazione sociale di gruppo, senza barriere architettoniche, senza problemi di distanza e di orari e in molti casi in for-

ma anonima. Sono anche una fonte d'informazione e di notizie sempre più popolare. Di conseguenza non si possono liquidare come mode passeggiere: ormai Facebook, tanto per fare un esempio, ha oltre 845 milioni di utenti attivi. È una popolazione paragonabile a quella delle più grandi nazioni della Terra.

Questo non vuol dire che ci si debba arrendere supinamente all'orda sociale che avanza: anzi, lo scopo di questa guida è proprio permettervi di sfruttare al meglio le opportunità dei social network senza farsi travolgere dai loro numerosi svantaggi.

2. I concetti di base

Se siete già utenti di un social network, sentitevi liberi di saltare questo capitoletto, che riassume alcuni principi generali di funzionamento di questi servizi e introduce un po' di terminologia.

Cosa vuol dire “social network”?

Il nome *social network* significa “rete sociale”: è un servizio di gestione dei rapporti sociali basato su Internet e sull'uso di dispositivi elettronici d'accesso.

I social network sono uno dei tanti servizi di Internet, ma spesso vengono percepiti come se fossero entità distinte e separate dal resto di Internet. La differenza fondamentale fra un social network e gli altri servizi di Internet è che nel social network si interagisce principalmente con altre persone, mentre Internet è spesso uno spazio di consultazione o acquisizione d'informazioni nel quale si interagisce non con altre persone, ma con dati preconfezionati (enciclopedie come Wikipedia, archivi di foto, musica o video, testate giornalistiche, banche dati).

Dispositivi d'accesso

I social network sono accessibili da qualunque computer moderno (non importa se usa Windows, Mac OS X o Linux) anche senza dover installare nulla: è sufficiente digitare nel *browser* (il programma di navigazione nelle pagine Web, per esempio Internet Explorer o Safari o Firefox o Opera) il nome del sito che ospita il social network. In alcuni casi si può scaricare un programma gratuito che consente di interagire in modo più efficiente o compatto.

Per accedere ai social network si possono usare anche i *tablet*, come per esempio l'iPad, e gli *smartphone*, ossia i telefonini evoluti (iPhone, Android) che possono navigare in Internet e installare appositi programmi d'interazione con il social network (le *applicazioni*).

Account, login e password

Praticamente tutti i social network vi chiedono di iscrivervi o *registrarvi* e creare un'utenza (*account* o *profilo*) che vi identifichi univocamente. In questo account vi viene richiesto di immettere alcuni dati personali che vi identificano ulteriormente. L'account viene identificato da un nome (*login*) e viene protetto utilizzando un codice segreto, noto soltanto a voi: di solito è una *password* (parola d'ordine), ma alcuni social network usano anche altri sistemi di protezione.

Di norma i social network non consentono l'iscrizione a chi ha meno di 13 anni d'età, per ragioni dettagliate nel Capitolo 3.

Post, aggiornamento o messaggio di stato

Una volta creato l'account, potete cercare sul social network i vostri amici e colleghi oppure le organizzazioni o le fonti di notizie che vi interessano e abbonarvi alla ricezione gratuita e in tempo reale dei loro *aggiornamenti* (o *messaggi di stato* o *post*): nuove notizie, nuove foto, eccetera. Nel caso di Facebook, questo "abbonamento" si chiama "*dare l'amicizia*"; su Twitter, invece, si chiama più asetticamente "*seguire*" o "*followare*" (neologismo infelice ma popolare).

Quando una persona o un'organizzazione alla quale siamo abbonati pubblica qualcosa sul social network, la riceviamo direttamente nel nostro profilo e quindi compare sullo schermo del nostro computer, telefonino o tablet.

Allo stesso modo, possiamo scrivere qualcosa nell'apposita casella del nostro profilo oppure pubblicare un *elemento* (un commento, una battuta, una notizia, una fotografia o un video): questo si chiama *postare* e rende visibile agli utenti del social network quello che abbiamo pubblicato.

Postare in un social network è un sistema molto comodo per la *comunicazione uno-a-molti*: una persona pubblica una notizia e molti la leggono. Per esempio, la nascita di un bambino può essere annunciata tramite social network a tutta la cerchia dei familiari in un solo colpo; un'azienda può informare di un evento tutti i dipendenti di un gruppo; un giornale può inviare una notizia di cronaca a tutti i suoi lettori.

Ogni elemento che viene *postato* può essere commentato dagli altri utenti (se sono stati autorizzati a farlo da chi ha postato l'elemento).

I post vengono solitamente presentati in ordine cronologico inverso (il primo è il più recente): questa disposizione viene chiamata *diario* da Fa-

cebook. I vari social network si distinguono anche per l'estensione di questa cronologia, che in alcuni è limitata (in Twitter sono visibili agli utenti comuni solo i messaggi dell'ultima settimana, se non se ne conosce l'indirizzo esatto o almeno in parte il testo) e in altri è illimitata (come nel caso di Facebook).

Livelli di privacy

Molti social network permettono di definire un livello di privacy per ciascun elemento creato dall'utente. In questo modo, una foto di una festa può essere condivisa con il partner o con gli amici ma non con i colleghi o con tutti gli utenti del social network.

La privacy proposta dai social network, tuttavia, non è sempre assoluta, per cui è opportuno usare queste funzioni con molta cautela e precauzione.

Funzioni accessorie

Spesso i social network offrono anche delle funzioni di messaggistica istantanea o *chat*, che permettono di conversare (per iscritto o anche a voce e in video) con uno o più utenti.

Alcuni propongono giochi o strumenti, simili a programmi, che si "installano" nel nostro profilo: si chiamano *applicazioni* o *app*.

3. Precauzioni generali per i social network

Lo scopo di questa guida non è descrivere minuziosamente tutte le funzioni offerte dai vari social network (per farlo non basterebbe un libro intero), ma dare al lettore gli strumenti di conoscenza necessari per usare i social network in maniera sicura. Pertanto le varie opzioni e modalità proposte da Facebook e Twitter non verranno presentate qui in dettaglio. Questa guida è dedicata a fornirvi le impostazioni di sicurezza e le regole di comportamento consigliabili.

Età minima: perché 13 anni?

Molti social network vietano esplicitamente ai minori di tredici anni di iscriversi. Si tratta di un divieto largamente ignorato oppure violato consapevolmente e dovuto a una legge statunitense per la protezione online dei bambini, il *Children's On-line Privacy Protection Act (COPPA, www.coppa.org)*, che pone limiti molto severi al tipo di informazioni che possono essere raccolte e soprattutto diffuse se riguardano bambini al di sotto dei tredici anni. I principali social network sono nati negli Stati Uniti e quindi si basano innanzi tutto sulle leggi statunitensi per l'impostazione dei propri servizi.

In particolare, qualunque raccolta di informazioni personalmente identificabili (per esempio un messaggio che annuncia lo stato attuale dell'utente) richiede per legge, negli Stati Uniti, il consenso parentale verificabile. Dato che questa verifica è complessa e onerosa, la maggior parte dei servizi Internet statunitensi che raccolgono dati personali risolve il problema vietando ai minori di tredici anni di usarli.

Iscriversi a un social network sotto i tredici anni, insomma, significa far commettere a quel social network un atto illegale secondo la legge degli Stati Uniti. Lo stesso atto potrebbe non essere illegale nel paese nel quale vive l'utente, ma questo in genere non interessa ai gestori dei social network, che operano quasi esclusivamente sulla base delle leggi e delle consuetudini statunitensi.

Scelta del nome

La prima scelta fondamentale è il nome con il quale ci si vuole presentare in un social network. È meglio usare quello vero oppure adottare uno pseudonimo?

Non c'è una risposta universale. L'uso del nome vero (obbligatorio secondo le norme di Facebook ad eccezione delle celebrità, facoltativo in altri social network) consente alle altre persone di trovarci facilmente, e spesso lo scopo dell'iscrizione è proprio rendersi reperibili per riprendere contatti con amici di cui si erano perse le tracce. Tuttavia permette di trovarci facilmente anche a molestatori, ex partner, creditori e altre persone che forse non vorremmo ritrovare.

L'uso di un nomignolo o di un nome inventato (*nickname* o *nick*) ha il vantaggio di renderci anonimi e quindi non reperibili da molestatori e simili, ma ci impedisce di farci trovare anche da chi vorremmo che ci trovasse. Si tratta di un anonimato relativo, nel senso che gli amici che ci conoscono sono in grado di dedurre chi siamo in base alle amicizie online che abbiamo, ma è un buon modo per difendersi dai molestatori sconosciuti.

La scelta è quindi molto personale, ma va soppesata con attenzione, perché una volta che si è su un social network con il proprio nome vero si è un bersaglio facile.

Probabilmente la soluzione migliore è iscriversi inizialmente con uno pseudonimo: si fa sempre in tempo a sostituirlo con il proprio nome vero, mentre il contrario non è quasi mai fattibile. Una volta che si è scelto di apparire in un social network con il proprio nome e cognome, non si può più tornare indietro facilmente.

Tenete presente, inoltre, che alcuni social network usano i nomi degli utenti come inconsapevoli sostenitori di campagne pubblicitarie. Per esempio, se in Facebook cliccate su un pulsante *"Mi piace"* di un sito, i vostri amici vedranno il vostro nome comparire fra i sostenitori di quel sito. Volete davvero diventare sponsor gratuiti di una marca di automobili o di un supermercato?

Furto d'identità

Un malintenzionato può creare senza problemi un account usando il vostro nome, una vostra foto e i vostri dati personali (facilmente reperibili con un po' di ricerca e di astuzia). I controlli sono ridicolmente scarsi. Pertanto non potete fidarvi di un account anche se è intestato a qualcuno che conoscete: potrebbe essere un impostore. Per sapere se

l'account è autentico, usate un canale di comunicazione diverso da Internet. Per esempio, telefonate alla persona in questione e chiedete conferme.

Per la stessa ragione, anche se non volete iscrivervi a uno specifico social network, vi conviene controllare se esiste già in quel social network un account a vostro nome e con i vostri dati. In tal caso potete segnalare questo furto d'identità ai gestori.

Scelta della password

La password è molto spesso l'unica chiave che abbiamo per mantenere il controllo del nostro account sui social network. Se qualcuno la indovina o ce la ruba, può impersonarci e causarci ogni sorta di imbarazzi e guai. Ci vuole, insomma, una password *robusta*:

- lunga almeno otto caratteri
- priva di senso compiuto
- contenente lettere maiuscole e minuscole, cifre e preferibilmente anche segni di punteggiatura
- unica per ciascun servizio che utilizziamo

Il problema delle password robuste è che di solito sono difficili da ricordare. Per fortuna ci sono dei trucchi che facilitano questo compito.

Per esempio, si può prendere la lettera iniziale di ogni parola di una filastrocca o di una frase descrittiva: *“Sotto la panca la capra campa, Sopra la panca la capra crepa”* diventa *“SlplccSlplcc”*; aggiungiamoci alcune cifre della targa della nostra auto o del nostro numero di telefonino o di un altro numero che ci ricordiamo facilmente e otterremo una password robusta come *“17SlplccSlplcc”*.

Un altro trucco è usare una parola straniera scritta come la si pronuncia (*soscialnetuorc*) oppure parole gergali o dialettali. Mi raccomando, però: non usate *“17SlplccSlplcc”* o *“soscialnetuorc”* come vostre password.

Non riciclate le password!

È estremamente importante adottare una password distinta per ciascuno servizio di Internet. Se si usa la stessa password per più di un servizio, l'intruso che dovesse riuscire a scoprirla avrebbe in un sol colpo accesso a tutti i servizi protetti da quella password.

Questa è una delle tecniche d'intrusione più diffuse: si infetta il computer della vittima, o se ne intercetta il traffico di dati, si cattura la password per esempio della casella di mail e poi si prova a usare la stessa password sugli altri servizi della vittima. È come avere un *passepourtout* che apre tutte le porte: i risultati sono devastanti.

Come si ruba una password?

Per difendersi dai furti di password è indispensabile sapere come avvengono: in questo modo saprete riconoscere i sintomi di un tentativo di furto di password e potrete evitare di cadere nella trappola tesa dal malfattore. Un'opportuna regolazione delle impostazioni del social network vi permetterà inoltre di prevenire più efficacemente questi attacchi.

Il metodo più frequente per rubare una password si chiama *phishing* (non è un errore di battitura: si scrive proprio così, con la *ph* iniziale, per distinguerlo dal *fishing*, che è l'attività della pesca). Funziona così:

- ricevete una mail o un messaggio di altro tipo che sembra provenire dai gestori del social network; il mittente sembra legittimo e spesso c'è anche il logo del social network, ma in realtà è facilissimo includere in una mail un logo copiato e falsificarne il mittente, perché Internet non compie alcuna verifica di autenticità su questa parte del messaggio (molti utenti non lo sanno e quindi si fidano);
- questo messaggio vi avvisa che c'è stato un problema con il vostro account e che per ripristinarlo dovete rispondere inviando la vostra password per un controllo (non è vero: se lo fate, inviate la password al malfattore) oppure aprire l'allegato che contiene la vostra nuova password (non è vero: l'allegato è in realtà un virus che ruberà la vostra password) oppure cliccare su un link che vi porta all'apposita pagina del social network (non è vero: è una pagina di un altro sito che imita il social network e vi ruba la password se la immettete).

Di conseguenza, **non fidatevi mai di messaggi che vi chiedono la password e non seguite link che promettono di portarvi alle pagine di accesso a un social network se vi chiedono la password.**

La cosa giusta da fare, se ricevete messaggi di questo genere, è ignorarli e digitare a mano nel vostro browser l'indirizzo del social network, per poi accedervi immettendo login e password nella maniera consueta. Solo a quel punto potete fidarvi degli eventuali messaggi d'avviso che compaiono sullo schermo.



*Una falsa pagina di accesso a Facebook.
Credit: Massimo Milazzo, per gentile concessione.*

Come regola generale, **conviene sempre evitare di accedere al proprio profilo in un social network cliccando su un link.** È più prudente digitare a mano il nome del social network oppure memorizzarlo nei Preferiti del proprio browser.

Le password di Facebook vengono rubate anche usando un altro trucco insidioso: i malfattori creano finti siti che promettono di offrire lo scaricamento di musica o film (specialmente a luci rosse) e che richiedono un'iscrizione gratuita. Molti utenti usano, per quest'iscrizione, lo stesso indirizzo di mail e la stessa password che usano su Facebook e quindi regalano ai gestori del sito-trappola le proprie credenziali d'accesso.

Un'altra tecnica molto diffusa di furto di password richiede un'azione fisica e non può avvenire a distanza, ma è comunque comune: un ladro o un malfattore (o un amico in vena d'impicciarsi, di farvi dispetti o di compiere vendette) può approfittare del vostro computer o telefonino lasciato momentaneamente incustodito con la sessione di social network aperta. La soluzione è **non lasciare mai incustoditi i dispositivi che hanno accesso ai social network e proteggerli con una password o un PIN.** Questo vale anche in caso di furto dell'apparecchio.

Domanda di recupero password

Di solito quando ci iscriviamo a un social network c'è un'opzione che ci consente di recuperare la password dimenticata se rispondiamo correttamente a una domanda di cui solo noi conosciamo la risposta esatta.

Quest'opzione va usata con attenzione per non rendersi vulnerabili: infatti spesso la domanda di recupero riguarda un'informazione che è in realtà facile scoprire anche per altri e magari sono addirittura presenti fra i dati che abbiamo pubblicato nel social network (il cognome da nubile della madre, il nome della prima insegnante di scuola, l'anno di matrimonio).

Con questa vulnerabilità, presente in molti servizi di Internet, nel 2005 furono rubate le foto private di Paris Hilton (che aveva usato come risposta il nome del proprio cagnolino, notissimo grazie alle riviste di *gossip*) e nel 2008 furono divulgate le mail private di Sarah Palin (che aveva scelto come domanda il luogo in cui aveva conosciuto il marito).

Convienne quindi immettere una risposta senza senso (non veritiera) e segnlarla su un quadernetto delle password, custodito in luogo sicuro.

Mail separate

Durante l'iscrizione a un social network viene chiesto di solito un indirizzo di e-mail. Se date un indirizzo che adoperate altrove, è inutile scegliere di presentarvi sul social network con uno pseudonimo, perché il vostro indirizzo di e-mail sarà visibile a tutti (se non c'è l'opzione di nascondere o limitarne la visibilità) e permetterà di identificarvi.

Se ci tenete all'anonimato, quindi, vi conviene attivare una casella di e-mail distinta da quella di lavoro o di uso comune e adottarla per l'iscrizione ai social network.

Va da sé che se volete l'anonimato, è meglio non iscriversi usando un indirizzo di e-mail del tipo *nome.cognome@provider.com*, altrimenti ancora una volta diventa inutile adottare pseudonimi, dato che l'indirizzo di e-mail d'iscrizione è spesso accessibile a chiunque.

Approccio trasparente

La maggior parte dei social network offre livelli di privacy distinti: è possibile, in altre parole, condividere un contenuto (un messaggio, un video o una foto) soltanto con una o più persone specifiche.

Tuttavia queste forme di privacy sono scavalcabili abbastanza facilmente, per cui è assolutamente consigliabile partire da un presupposto completamente diverso: **date per scontato che tutto quello che fate su un social network sia leggibile e visibile a chiunque.**

Dati personali

È fortemente sconsigliabile fornire ai social network il proprio indirizzo di abitazione o di lavoro o la scuola frequentata, perché questo consente ai malintenzionati di sapere dove si trova il loro potenziale bersaglio e rende inutili tutte le altre misure prese per restare anonimi.

Per esempio, annunciare un'imminente vacanza consente ai ladri di sapere che la vostra abitazione sarà vuota per un certo periodo e sapere quale scuola viene frequentata da voi o dai vostri figli permette ai molestatori di selezionare le vittime da sedurre in base alla convenienza geografica.

È prudente immettere un indirizzo o un nome di scuola inventati che corrispondano solo vagamente a quelli veri: la regione può essere quella reale, ma è meglio non indicare nulla di più preciso per non dare appigli agli utenti ostili dei social network.

Foto

Pensateci bene prima di pubblicare qualunque foto, anche apparentemente innocua e innocente. Per esempio, le foto scattate in spiaggia da un'insegnante possono essere viste dai suoi studenti, con conseguenze facilmente immaginabili. Tenete presente, inoltre che i giornalisti hanno la macabra abitudine di saccheggiare i social network per cercare foto delle persone morte sulle quali vogliono scrivere un articolo: quindi scegliete bene la foto del vostro profilo.

Geolocalizzazione

Quasi tutti i social network permettono di includere automaticamente nei post delle informazioni di *geolocalizzazione*, ossia le coordinate geografiche del luogo dal quale pubblicate un post. Inoltre molti telefonini e alcune fotocamere includono direttamente nelle foto la latitudine e longitudine del luogo in cui sono state scattate.

Questa possibilità può essere molto utile per condividere con gli amici la propria ubicazione e quindi agevolare gli incontri o per ricordarsi di dove è stata scattata una fotografia, ma in alcuni casi può essere un rischio di sicurezza o di privacy.

Per esempio:

- le informazioni di geolocalizzazione possono essere sfruttate dai ficcanaso o dai molestatori per sapere quali luoghi frequentano le loro vittime e per scavalcare la protezione dell'anonimato;
- i ladri possono approfittare di questi dati per sapere quando la vittima non è in casa;
- le coordinate geografiche annidate in una foto possono rivelare che la persona che l'ha scattata o che è inquadrata non si trovava dove ha dichiarato di essere al proprio partner, genitore o datore di lavoro;
- una foto intima in cui il volto è stato occultato per poterla pubblicare in modo anonimo (attività più frequente di quanto si possa immaginare) può contenere le coordinate dell'abitazione, rendendo vano il mascheramento ed esponendo a imbarazzi e disagi.

La geolocalizzazione automatica è disattivabile in blocco o selettivamente per i singoli post. Inoltre Facebook rimuove automaticamente dalle immagini tutti i dati di geolocalizzazione incorporati dalla fotocamera o dal telefonino.

Scelta degli amici

Vi conviene decidere con attenzione se volete usare i social network per restare in contatto soltanto con le persone che conoscete già al di fuori di Internet, nella vita reale, o se volete comunicare anche con gli sconosciuti.

Nel primo caso il rischio è molto basso; nel secondo ci possono essere conseguenze piacevoli (la scoperta di nuovi amici è sempre molto gratificante), ma c'è anche il rischio di entrare in contatto con persone poco raccomandabili.

Se volete comunicare anche con gli sconosciuti, l'anonimato è un'ottima protezione; ci sarà sempre tempo per rivelare la vostra identità se e quando sarete sicuri di volerlo fare e di potervi fidare della persona conosciuta attraverso i social network.

Nel caso dei minori, invece, è opportuno stabilire una regola ben preci-

sa: comunicare con chi si conosce già va benissimo; comunicare con gli sconosciuti è da evitare tassativamente.

Nei social network occorre stare in guardia contro il fenomeno della collezione indiscriminata di “amici”: soprattutto fra i giovani si fa a gara a chi ne ha di più, come se gli amici fossero figurine. Non avere tanti “amici” (che spesso in realtà sono persone sconosciute o quasi) fa sentire esclusi e soli, e così alcuni accettano “amicizie” da chiunque, col rischio di esporsi a contatti con malintenzionati o molestatori.

Bilancio rischi/benefici

Non dimenticate che lo scopo dei social network è convincerci a condividere il maggior numero possibile di informazioni personali: questo, infatti, ci rende più appetibili per gli inserzionisti pubblicitari e per le società di ricerca di mercato alle quali i social network vendono i nostri dati (solitamente in forma più o meno anonimizzata).

In generale, quindi, i loro servizi sono pensati per raggiungere questa finalità: sta a noi valutare se le finalità dei social network coincidono con le nostre e chiederci sempre se un singolo servizio ha più vantaggi che svantaggi.

Per esempio, la geolocalizzazione è utile ai social network per avere informazioni sulle tendenze di spostamento dei loro utenti, ed è divertente far sapere ai propri amici dove siete nel momento in cui scattate una foto e scoprire che alcuni di loro si trovano nelle vicinanze, ma l'informazione geografica è sfruttabile anche dagli *stalker*, che possono usarla per pedinarvi comodamente. Vale davvero la pena di adoperarla?

4. Impostazioni sicure di Facebook

Dati personali: il minimo indispensabile

I dati personali del vostro account sono accessibili cliccando sul vostro nome nella barra superiore di Facebook e li potete modificare a piacimento cliccando su *Aggiorna informazioni*. Come regola generale, meno dati pubblicate (e quindi regalate a Facebook per le sue analisi statistiche e a potenziali bulli, molestatore e truffatori) e meglio è. Nulla vieta di non immettere niente oltre al nome, al sesso, alla data di nascita e all'indirizzo di e-mail da associare al profilo Facebook.

Ciascuna delle informazioni personali che immettete in Facebook ha un proprio livello di privacy e visibilità regolabile. Tuttavia niente impedisce a un vostro amico di Facebook di copiare i vostri dati personali privati e condividerli anche con persone che non conoscete.

- Valutate con attenzione, comunque, se è il caso di affidare a Facebook il vostro **indirizzo di casa o di lavoro**, il vostro **orientamento sessuale, politico o religioso** e i vostri **legami sentimentali**. I vostri amici (quelli veri) già li conoscono e non c'è quindi molto bisogno di sbandierarli, col rischio di farli avere a malintenzionati, e in molti casi queste preferenze personali possono essere controverse oppure oggetto di scherno.
- Specialmente nel caso di minorenni, è consigliabile non rendere visibile a nessuno l'**anno di nascita** (che comunque è necessario immettere) o la scuola frequentata. I molestatore usano infatti questi dati per selezionare le vittime potenziali. Il giorno e il mese di nascita possono essere lasciati pubblici per consentire agli amici di fare gli auguri di compleanno, mentre l'anno si può nascondere usando l'opzione *Mostra solo mese e giorno sul mio diario*.
- È importante **non diffondere la propria data di nascita completa**, perché è uno dei dati utilizzati dai truffatori per i furti d'identità. Un altro modo per proteggere quest'informazione è immetterne una data fasulla, anche se questo comporta che gli amici potrebbero far-

vi gli auguri nel giorno sbagliato se non conoscono la data vera e si appoggiano a Facebook per saperla.

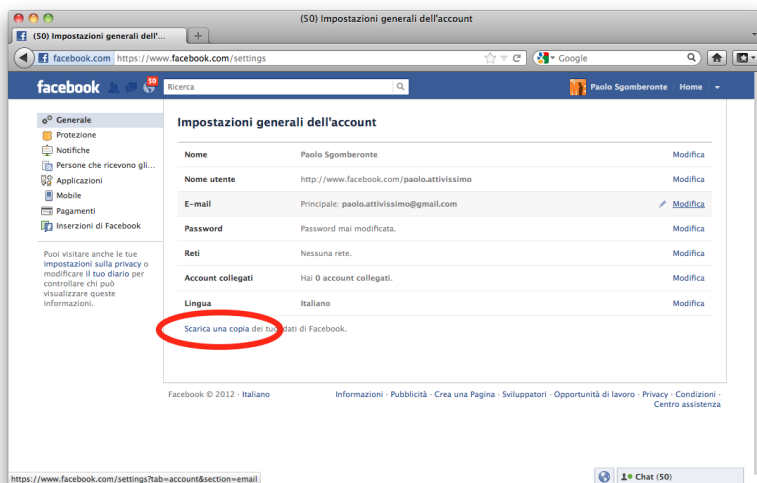
- Anche il **sex** è un dato obbligatorio, ma potete nascondere (ed è opportuno farlo, particolarmente per i minorenni e per le donne) disattivando la casella *Mostra il mio sesso nel diario*. Questo vi renderà un bersaglio molto meno appetibile per i molestatori, a patto che abbiate usato uno pseudonimo che non riveli il vostro sesso e che non abbiate pubblicato vostre foto altrettanto rivelatrici. In alternativa, indicate che siete di sesso maschile, perché gli utenti particolarmente pestiferi potrebbero interpretare il fatto che nascondete il vostro sesso come un'ammissione che siete di sesso femminile.
- Se siete lavoratori dipendenti, l'**indicazione del posto di lavoro** può essere considerata un dato sensibile dal vostro datore di lavoro, perché rende facile per concorrenti o truffatori usare Facebook per ricostruire l'organigramma di un'azienda o sapere chi occupa posizioni particolarmente significative. È quindi opportuno concordare con l'azienda la visibilità da concedere a questo dato personale.
- Per quanto riguarda l'**indirizzo di e-mail** associato al profilo Facebook, conviene usarne uno distinto da quello che usate normalmente e adoperarlo soltanto per il profilo, in modo da non essere facilmente tracciabili. In ogni caso è prudente nascondere quest'indirizzo nelle informazioni di contatto, scegliendo l'opzione di privacy massima, vale a dire *"Solo io"*, e limitarne la reperibilità nelle *Impostazioni sulla privacy*: in *Connessione da parte tua*, cliccate su *Modifica impostazioni* e scegliete *Amici* come opzione in *Chi può cercarti utilizzando l'indirizzo e-mail o il numero di telefono che hai fornito?*

Copia di sicurezza del profilo

In caso di intrusione vandalica, o se in un momento di sconforto decidete di cancellare il vostro profilo Facebook e poi vi pentite della scelta emotiva, è importante avere un *backup*, ossia una copia di sicurezza di tutti i dati che avete immesso nel vostro account Facebook.

Per eseguire questa copia cliccate sul triangolino in alto a destra nel vostro account Facebook, scegliete *Impostazioni account*, poi *Generale* (a sinistra) e *Scarica una copia dei tuoi dati di Facebook*.

Nella schermata successiva che compare, cliccate su *Avvia al mio archivio* e di nuovo su *Avvia al mio archivio*. La procedura non è immediata: verrete avvisati via e-mail quando la copia di sicurezza sarà pronta per essere scaricata.



Copia di sicurezza del profilo di Facebook.

Questa copia di sicurezza contiene le foto e i video condivisi su Facebook (anche quelli privati), i post pubblicati nella bacheca, i messaggi e le conversazioni in chat, i nomi degli amici e i loro indirizzi di e-mail (se hanno attivato quest'opzione nelle loro impostazioni); non include le foto e gli aggiornamenti di stato dei vostri amici, le informazioni personali di altre persone e i commenti fatti sui post di altri utenti.

Navigazione protetta

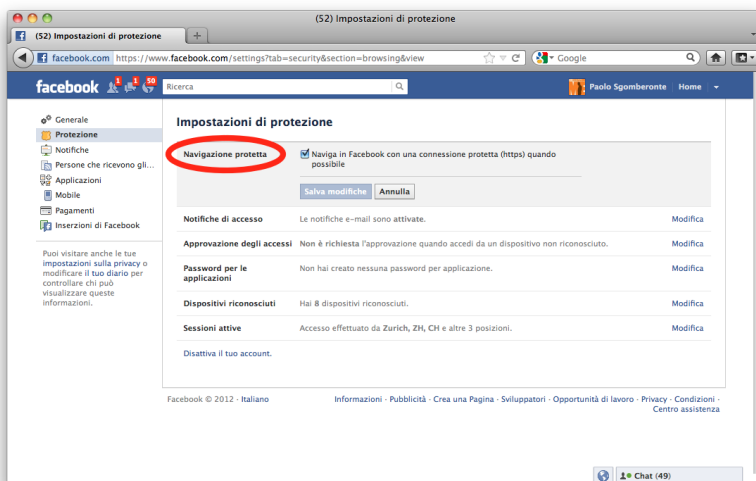
Se non attivate quest'opzione e vi collegate a Facebook usando per esempio una rete WiFi (senza fili), per esempio in casa, in ufficio o in albergo, gli altri utenti della stessa rete possono intercettare la vostra connessione e prendere il controllo della vostra sessione di attività su Facebook. Questo permette agli intrusi e ai vandali, per esempio, di leggere i vostri messaggi privati e addirittura postarne sul vostro profilo a vostro nome.

Prendere il controllo di una sessione Facebook in questo modo è molto semplice: esistono infatti programmi gratuiti, come per esempio Firesheep o WireShark, che sono installabili su qualunque computer e consentono di intercettare i dati che circolano sulla rete locale (WiFi o cablata) e di analizzarli. Quest'analisi permette poi di sostituirsi temporaneamente all'utente legittimo.

Contro questo genere d'intrusione Facebook offre la *Navigazione protetta*: per attivarla, cliccate sul triangolino in alto a destra nel vostro account Facebook, scegliete *Impostazioni account*, scegliete *Protezione* (a sinistra) e cliccate su *Modifica* in corrispondenza della riga denominata *Navigazione protetta*. Attivate la casella *Naviga in Facebook con una connessione protetta (https) quando possibile*. Cliccate su *Salva modifiche* e verificate che compaia l'indicazione *La navigazione protetta al momento è attivata*.

La precisazione *"quando possibile"* sottolinea un limite importante di quest'impostazione: alcuni metodi di accesso a Facebook (per esempio le "app" per telefonini) potrebbero non gestire la navigazione protetta. Usandole, quindi, la vostra attività su Facebook sarebbe intercettabile. Verificate che la vostra app gestisca correttamente la navigazione protetta (dovrebbe essere indicato nelle sue specifiche tecniche).

È inoltre importante tenere d'occhio la barra dell'indirizzo del programma di navigazione: deve sempre indicare, all'inizio dell'indirizzo, *https* e non *http*. La lettera S, infatti, indica che la connessione a Facebook è protetta. Se la S non c'è, potete digitarla a mano.



Attivazione della navigazione protetta in Facebook.

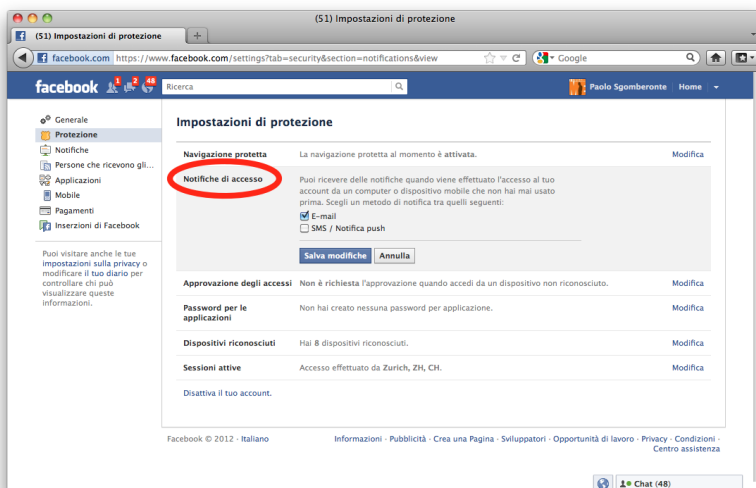
La navigazione protetta non va interpretata come un sistema contro le intercettazioni da parte delle autorità (per esempio da parte della polizia), ma solo come protezione contro i malintenzionati generici: in caso di reato, infatti, Facebook solitamente fornirà agli inquirenti un accesso diretto al vostro profilo, scavalcando qualunque protezione.

Notifiche di accesso

Le *notifiche di accesso* sono avvisi che ricevete via e-mail o SMS quando viene effettuato un tentativo di accesso al vostro profilo Facebook con un dispositivo o un programma che non avete autorizzato.

Potete infatti definire quali computer, telefonini o tablet e quali programmi volete autorizzare all'accesso al vostro profilo: se qualcuno tenta di accedervi da un altro dispositivo o programma, ne verrete avvisati e potrete prendere le contromisure del caso (per esempio cambiare subito la vostra password). L'elenco dei dispositivi e programmi autorizzati è nelle *Impostazioni account* alla voce *Dispositivi riconosciuti*, dalla quale potete rimuoverli, se occorre, cliccando su *Rimuovi*.

È consigliabile attivare queste notifiche di accesso: cliccate sul triangolino in alto a destra nel vostro account Facebook, scegliete *Impostazioni account*, scegliete *Protezione* (a sinistra) e cliccate su *Modifica* in corrispondenza della riga denominata *Notifiche di accesso*.



Notifiche di accesso in Facebook.

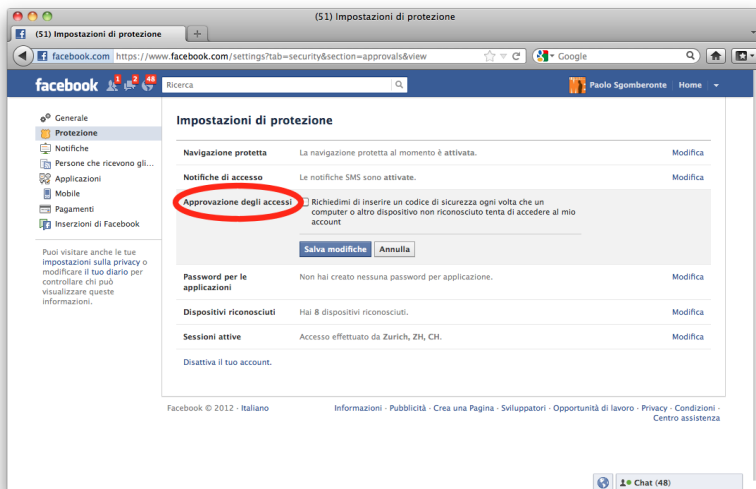
Attivate le caselle *E-mail* e/o *SMS/Notifica push* a seconda di come volete ricevere gli avvisi, poi cliccate su *Salva modifiche* e controllate che compaia l'indicazione di conferma dell'attivazione.

Approvazione degli accessi

Attivando quest'opzione, situata nelle impostazioni dell'account nella sezione *Protezione*, riceverete via SMS un codice di conferma che dovrete immettere nella schermata successiva di Facebook. Fatto questo, se qualcuno tenterà di accedere al vostro account da un dispositivo che non avete autorizzato, dovrà conoscere e immettere questo codice oltre alla consueta password. Questo rende molto più difficili i furti di account. Naturalmente quel "qualcuno" potreste anche essere voi, per esempio se state usando un dispositivo nuovo o un browser diverso dal solito.

Questa protezione non si attiva subito completamente: entra in vigore a tutti gli effetti solo dopo una settimana. Per i primi sette giorni rimane disabilitabile anche se non avete accesso al telefonino al quale avete chiesto a Facebook di inviare il codice.

Ricordatevi di segnare il codice di conferma da qualche parte: non lasciatelo sul telefonino, altrimenti in caso di furto il ladro avrà accesso facile al codice.



Approvazione degli accessi in Facebook.

Password per le applicazioni

Alcune applicazioni di Facebook non sono compatibili con l'approvazione degli accessi e potrebbero quindi risultare bloccate se attivate quest'approvazione.

Per risolvere questo problema si usano le password per le applicazioni, che in sostanza scavalcano l'approvazione degli accessi per una specifica applicazione. È un concetto piuttosto complicato, ma per fortuna si rende necessario solo in un numero abbastanza limitato di situazioni.

Occorre per prima cosa cliccare su *Modifica* alla riga *Password per le applicazioni* nella sezione *Protezione* delle impostazioni dell'account: poi si clicca su *Genera password per le applicazioni*.

Nella schermata successiva si digita il nome dell'applicazione e si clicca su *Genera password*. Al termine della generazione delle password per le applicazioni si clicca su *Fine*.

Quest'opzione è piuttosto macchinosa e solitamente non è necessaria, salvo che usiate alcune applicazioni particolari, come Xbox, Spotify o Skype, per cui non è indispensabile adoperarla se non riscontrate problemi di utilizzo delle applicazioni di Facebook dopo che avete attivato l'approvazione degli accessi.

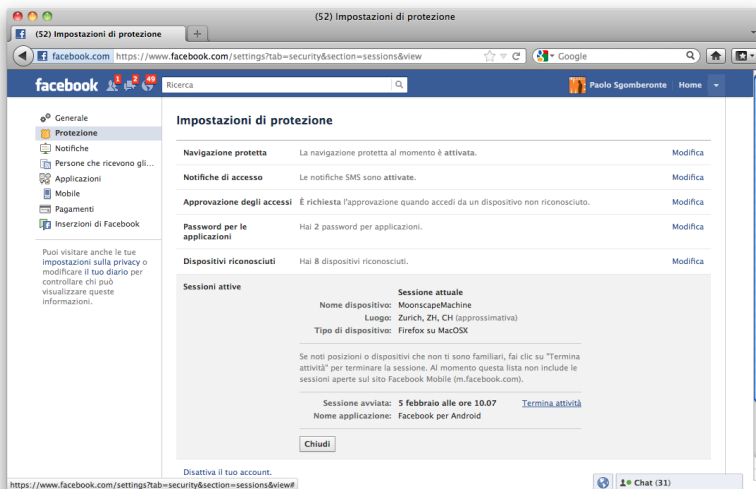
Sessioni attive

Vi può capitare di lasciare aperta una sessione nel vostro profilo Facebook su un dispositivo che non potete raggiungere facilmente: un caso tipico è tornare a casa dal lavoro dimenticandosi la sessione Facebook aperta sul computer in ufficio.

Questo potrebbe permettere a qualche ficcanaso, burlone o malintenzionato di entrare nel vostro profilo e leggerlo oppure postare qualunque cosa spacciandosi per voi, con tutti i disagi e gli imbarazzi che ne possono derivare.

Per ridurre questo rischio Facebook consente di disattivare a distanza le sessioni lasciate aperte. La procedura è semplice: si entra nel proprio account da un altro computer, si va nelle *Impostazioni account*, si sceglie *Protezione* (a sinistra) e poi si clicca su *Modifica* nella sezione *Sessioni attive*.

Questo fa comparire un elenco delle sessioni attive e dei luoghi (approssimativi) dai quali sono in corso queste sessioni. Cliccando su *Termina attività* è possibile bloccare immediatamente le sessioni indesiderate, anche se sono state aperte da un aggressore.



Gestione delle sessioni attive in Facebook.

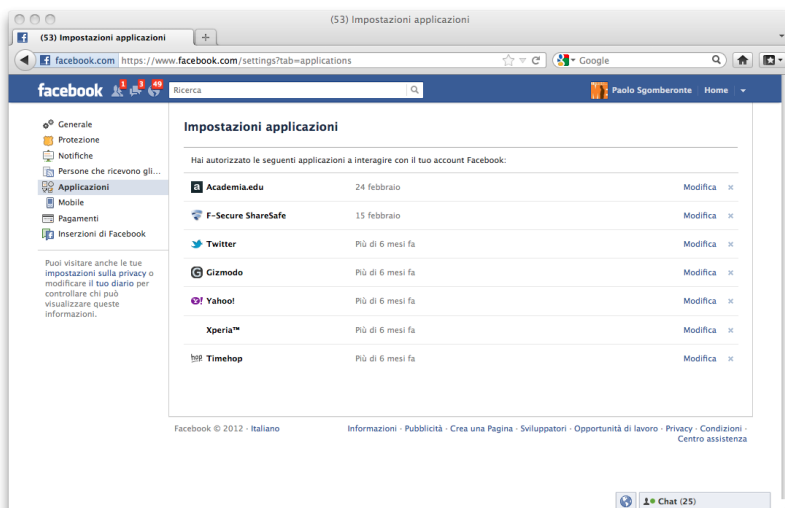
Applicazioni

Talvolta le applicazioni usano i nostri dati personali oppure intervengono sul nostro account Facebook in modi che non approviamo, per esempio pubblicando post automatici.

Per disabilitare un'applicazione che non desiderate più è sufficiente andare nelle *Impostazioni account*, scegliere *Applicazioni* dall'elenco sulla sinistra e visualizzare quali applicazioni avete autorizzato a interagire con il vostro account.

Cliccando su *Modifica* accanto a ciascuna applicazione potete:

- rimuoverla (con *Rimuovi applicazione*);
- vedere quali informazioni sono accessibili all'applicazione e quando vi ha acceduto;
- impostare il livello di privacy dell'attività dell'applicazione (per esempio il livello di privacy dei post generati dall'applicazione stessa);
- scegliere le condizioni in cui l'applicazione vi invia una notifica.



Impostazioni delle applicazioni in Facebook.

Come regola generale, sarebbe opportuno non accettare applicazioni che non siano strettamente necessarie e in ogni caso andrebbe verificato il livello di accesso ai dati personali e di privacy dell'applicazione. Per quanto Facebook vagli piuttosto attentamente le applicazioni, esse restano infatti una delle principali forme di attacco o di intrusione in questo social network.

Metodi di pagamento

È possibile registrare nel proprio profilo Facebook i dati di una carta di credito (nelle *Impostazioni account*, alla voce *Pagamenti*), ma è altamente sconsigliabile se non avete un motivo serio per farlo. In caso di furto di password, infatti, il ladro avrebbe accesso a questi dati, compreso il codice di sicurezza della carta.

Preferenze di privacy

Potete definire un livello di privacy preimpostato per tutti gli elementi che pubblicate: in questo modo, se vi dimenticate di impostare la privacy di un elemento, quell'elemento assumerà automaticamente il livello predefinito. Questo livello predefinito è utile anche per le applicazioni

Facebook che non offrono l'opzione di definire la privacy di un singolo elemento pubblicato attraverso di esse.

Per esempio, se volete che tutte le foto che caricate su Facebook siano private salvo vostra decisione contraria, potete andare nelle *Impostazioni sulla privacy*, accessibili tramite il triangolino in alto a destra nella barra standard di Facebook, e scegliere fra:

- *Pubblica* (tutto quello che postate su Facebook sarà automaticamente pubblico);
- *Amici* (tutto quello che postate sarà automaticamente accessibile soltanto agli amici);
- *Personalizzata* (ogni elemento che pubblicate sarà visibile soltanto agli utenti che selezionate o escludete secondo vari criteri che possono essere definiti nella schermata che compare scegliendo quest'opzione).

Queste impostazioni non vanno considerate come una garanzia assoluta: infatti gli elementi privati possono comunque essere copiati, ripubblicati e resi visibili a chiunque da chi è autorizzato inizialmente a vederli.

Inoltre molti elementi, come le fotografie, hanno anche un link pubblico, che li rende visibili a chiunque (compreso chi non è utente di Facebook) anche se li avete impostati come privati.

Per prudenza, conviene presumere che la privacy offerta da Facebook non esista e non funzioni e che tutto sia visibile a tutti. Il rischio di imbarazzi in caso di errore vostro o difetto di Facebook è troppo alto.

Di conseguenza, la scelta consigliabile per quest'impostazione è *Pubblica*: in questo modo sarete ben consapevoli che tutto quello che postate su Facebook è visibile a tutti e quindi vi abituerete a valutare con attenzione cosa pubblicare, dando per scontato che potrà essere visto o letto da tutte le persone che conoscete (amici, nemici, colleghi e concorrenti di lavoro, partner ed ex partner, genitori e figli) e anche dagli sconosciuti.

Sapere di vivere in una casa con le pareti di vetro è uno stimolo potente alla sobrietà e alla riflessione.



Impostazioni di privacy predefinite di Facebook.

Connessioni

Nelle *Impostazioni sulla privacy* di Facebook c'è la sezione *Connessione da parte tua*, che consente di scegliere quanto siete visibili e contattabili tramite questo social network. Qui, infatti, potete scegliere chi può trovarvi tramite l'indirizzo di mail o il numero di telefono che avete fornito a Facebook, chi può cercare o scrivere nella vostra cronologia (o *diario*, nel gergo di Facebook), chi vi può inviare richieste di amicizia o messaggi e chi può vedere quello che gli altri utenti pubblicano nella vostra cronologia.

Le impostazioni da usare dipendono dalle vostre esigenze personali: se desiderate l'anonimato e la tranquillità e volete essere semplici spettatori discreti di quel che accade in Facebook, evitando i molestatori (ma anche riducendo la possibilità di nuove amicizie), scegliete il massimo livello di privacy di ciascuna opzione di questa sezione. Non è possibile, tuttavia, essere del tutto introvabili: almeno gli amici possono trovarvi.

Funzionamento dei tag

I *tag* sono le etichette identificative degli utenti in Facebook: quando viene pubblicata una fotografia su questo social network è possibile

etichettare le persone ritratte nell'immagine in modo da identificarle pubblicamente e anche localizzarle geograficamente. Essere *taggati* aiuta gli altri utenti a scoprire nuove immagini che ci riguardano, ma questo può talvolta essere imbarazzante: vogliamo davvero che il nostro datore di lavoro ci veda in costume da bagno o un po' brilli a una festa in maschera? Oltretutto ci sono utenti burloni che etichettano con i nomi dei propri amici le foto di cani o altri animali.

Nelle *Impostazioni sulla privacy* c'è la sezione *Funzionamento dei tag*: qui potete scegliere varie opzioni per limitare questi rischi.



Impostazioni prudenziali del funzionamento dei tag.

- Volete evitare che un post nel quale siete taggati compaia automaticamente nel vostro diario di Facebook e preferite approvare singolarmente i post di questo tipo? Allora attivate l'opzione *Controllo del diario*.
- Preferite approvare manualmente i tag applicati dagli utenti ai vostri contenuti, in modo da evitare tag offensivi o ridicoli? Attivate l'opzione *Controllo dei tag*.
- A chi volete che siano visibili i post del vostro diario nei quali siete taggati dagli amici? Decidetelo usando l'opzione *Visibilità massima sul diario*, ma ricordate che la privacy su Facebook è sostanzialmente una chimera e c'è poco da fidarsi.
- Volete evitare che Facebook usi il riconoscimento automatico dei

volti per proporre ai vostri amici di taggarvi quando Facebook crede di avervi riconosciuto in una foto? Disattivate (scegliendo *Nessuno*) l'opzione *Suggerimenti per i tag*.

- Non volete che gli amici usino i tag per aggiungere informazioni di geolocalizzazione che vi riguardano? Impostate a *No* l'opzione *Gli amici possono registrarti nei luoghi*.

Condivisione con applicazioni, giochi e siti

La sezione *Applicazioni e siti Web* delle *Impostazioni sulla privacy* permette di regolare, entro certi limiti, le informazioni del vostro profilo che sono accessibili alle applicazioni, ai siti Web e ai giochi.

- L'opzione *Applicazioni che usi* porta alla sezione *Applicazioni* delle *Impostazioni account*, già descritta precedentemente.
- L'opzione *Modo in cui le persone condividono le tue informazioni con le applicazioni che usano* regola in realtà non il modo, ma il tipo delle informazioni che possono essere condivise con le applicazioni da parte degli utenti che avete autorizzato a vedere quelle informazioni. Se volete impedire questo genere di condivisione, disattivate tutti i tipi d'informazione in quest'opzione.

Modo in cui le persone condividono le tue informazioni con le applicazioni che usano

Le persone che possono vedere la tue informazioni, possono condividerle con le applicazioni che usano per rendere la loro esperienza migliore e più sociale. Utilizza questa impostazione per controllare le categorie di informazioni che le persone possono condividere quando usano applicazioni, giochi e siti Web.

- | | |
|--|---|
| ☐ Biografia | ☐ I miei video |
| ☐ Data di nascita | ☐ I miei link |
| ☐ Familiari e relazioni | ☐ Le mie note |
| ☐ Mi piacciono | ☐ Città natale |
| ☐ Orientamento politico e religioso | ☐ Città attuale |
| ☐ Il mio sito Web | ☐ Istruzione e lavoro |
| ☐ Se sono online | ☐ Attività, interessi, cose che mi piacciono |
| ☐ I miei aggiornamenti di stato | ☐ La mia attività nelle applicazioni |
| ☐ Le mie foto | |

Se non vuoi che le applicazioni e i siti Web accedano ad altre [categorie d'informazione](#) (come la lista dei tuoi amici, il tuo sesso o le informazioni che hai reso pubbliche), puoi disattivare tutte le applicazioni della piattaforma. Ricorda, tuttavia, che non potrai usare nessun gioco o applicazione.

Salva modifiche

Annulla

Impostazioni prudenziali delle informazioni condivise tramite le applicazioni.

- L'opzione *Personalizzazione istantanea* serve per consentire a Facebook di proporvi informazioni generate dai vostri amici quando visitate siti esterni a Facebook, come Bing, Pandora o Docs. Per esempio, in un sito di recensioni potreste vedere in evidenza i giudizi pubblicati dai vostri amici. Questa può sembrare un'opzione priva di rischi, ma tenete presente che attivarla significa consentire a siti esterni a Facebook di tracciarvi e di sapere cosa leggete.
- L'opzione *Ricerca pubblica* permette a chiunque di vedere un'anteprima del vostro diario su Facebook cercando il vostro nome in un motore di ricerca come Google. Se non desiderate essere trovabili in questo modo, disattivate quest'opzione.

Ci sono alcuni dati che vengono comunque condivisi con tutti gli utenti e anche con le applicazioni a prescindere da quello che impostate qui: il vostro nome, la vostra immagine del profilo, il vostro sesso, le vostre reti, il vostro nome utente e il vostro *ID utente* (un numero identificativo dell'account).

Visibilità dei vecchi post

Le *Impostazioni sulla privacy* includono la sezione *Restringi il pubblico per i vecchi post*, che permette di ridurre in blocco la visibilità dei post già pubblicati, rendendoli tutti visibili solo agli amici anche se prima erano visibili a tutti o agli amici degli amici.

Questa modifica può essere utile se avete pubblicato moltissimi post, non volete verificarne la visibilità singolarmente e temete che col passare del tempo qualche post sia diventato inopportuno. Per esempio, le foto di quando eravate con il vostro ex partner potrebbero essere motivo di disagio per voi o per il vostro partner attuale; anche i gusti e il modo di vestire possono cambiare col tempo e quindi i vecchi post possono dare un'impressione sbagliata della vostra personalità attuale.

Attenzione: si tratta di una modifica difficilmente reversibile. Se cliccate sul pulsante *Solo vecchi post* di quest'opzione e poi vi pentite, dovrete modificare a mano la visibilità di ciascun post.

Blocco di persone e applicazioni

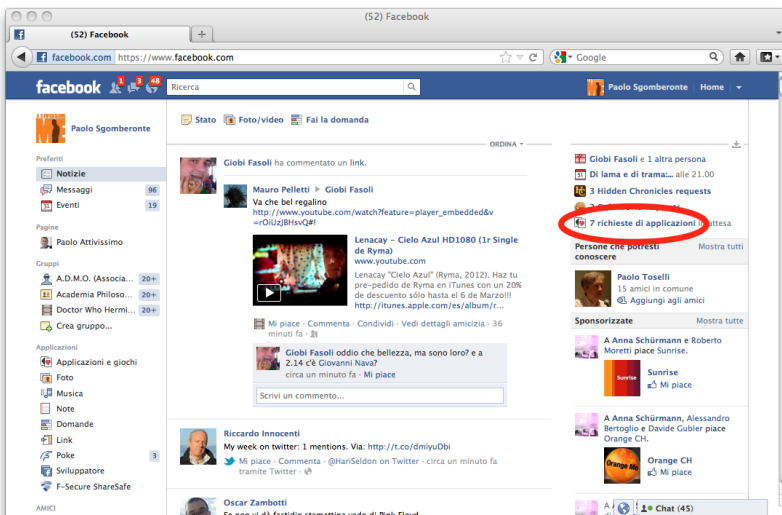
Se siete molestati da un utente di Facebook, oltre a segnalarlo al servizio di assistenza clienti di questo social network potete bloccarlo in

modo che non possa più interagire con voi. Lo stesso vale per le applicazioni che vi infastidiscono. Questi blocchi si trovano nella sezione *Persone e applicazioni bloccate* delle *Impostazioni sulla privacy*. Le varie opzioni di questa sezione consentono:

- di mettere un amico di Facebook in una *lista con restrizioni*, in modo che possa vedere soltanto i vostri post pubblici;
- di bloccare un utente in base al nome o all'indirizzo di e-mail;
- di bloccare gli inviti a usare applicazioni o a partecipare ad eventi che provengono da uno specifico utente;
- di bloccare le applicazioni indesiderate.

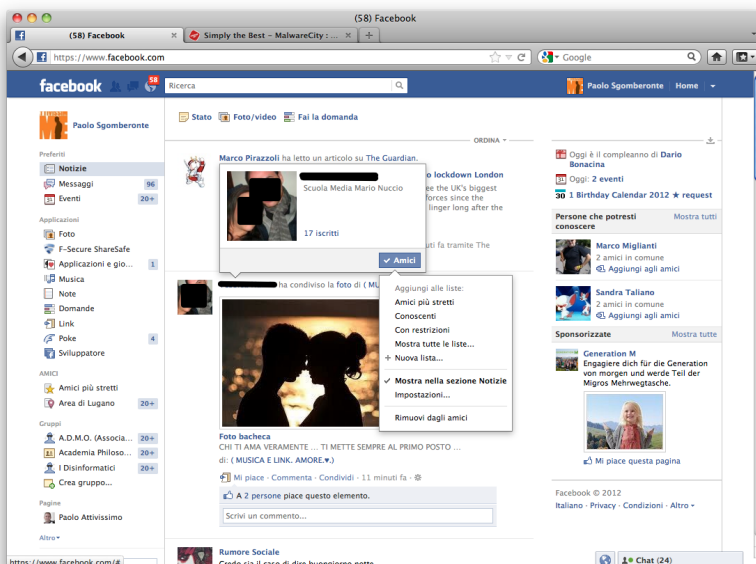
Questo può essere utile specialmente nel caso di giochi, per i quali gli utenti spesso disseminano inviti a pioggia per acquisire punti. Tutte le impostazioni di blocco sono reversibili.

Per eliminare le richieste di applicazioni in attesa che compaiono in alto a destra nella pagina di gestione (*Home*) del vostro profilo, cliccate sul conteggio delle richieste in attesa e lasciate fermo un istante la freccia del mouse sopra la richiesta che compare nella schermata successiva: cliccando sulla crocetta che viene visualizzata potete scegliere se bloccare la singola applicazione o tutte le richieste provenienti dall'utente che vi ha inviato questa richiesta. Se la richiesta è una sola, lasciate ferma la freccia su di essa e comparirà direttamente la crocetta di rimozione.



Richieste di applicazioni nella Home di Facebook.

Ricordate, inoltre, che in qualunque momento potete togliere un utente dalla vostra lista di amici: è sufficiente posizionare la freccia del mouse sul suo nome per far comparire una finestra nella quale potete cliccare sul pulsante *Amici* per selezionare l'opzione *Rimuovi dagli amici*. L'utente rimosso non verrà avvisato della rimozione.



Rimozione di un utente dagli "amici"

"Antivirus" per Facebook

Esistono delle applicazioni per Facebook che migliorano la sicurezza di questo social network, evitandovi di diffondere ai vostri amici collegamenti a siti truffaldini o infettanti, *spam* (pubblicità indesiderata) e dati personali.

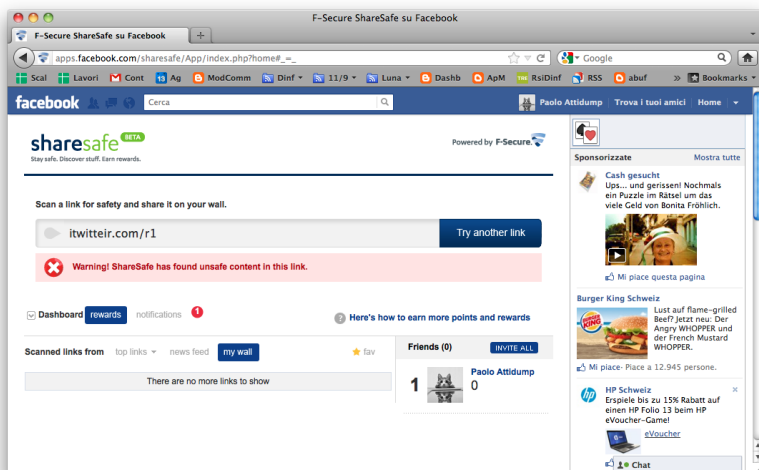
Due delle migliori applicazioni in questo campo sono ShareSafe di F-Secure e Safego di BitDefender, descritte nelle pagine seguenti.

Sharesafe

Per usare ShareSafe lo si deve per prima cosa installare: entrate in Facebook e visitate la pagina <http://apps.facebook.com/sharesafe>, dove clic-

cate su *Consenti* per accettare l'applicazione. ShareSafe propone di invitare anche gli amici a usarlo, ma non è indispensabile accettare questa proposta.

Fatto questo, il funzionamento è molto semplice: se vi imbattete in un link sospetto su Facebook, selezionatelo, copiatelo e incollatelo in ShareSafe (che è accessibile nella pagina Home del vostro account, nella sezione *Applicazioni*). Se il link è classificato fra quelli pericolosi dalla società di sicurezza F-Secure, ShareSafe lo segnalerà (per il momento quest'applicazione si esprime soltanto in inglese).



ShareSafe ha riconosciuto un link a un sito pericoloso.

Se il link non è ritenuto pericoloso, ShareSafe vi proporrà di condividerlo nella vostra Bacheca insieme a una descrizione.

Potete usare ShareSafe anche per verificare i link contenuti nei post che appaiono nella vostra Bacheca: vengono visualizzati quando accedete all'applicazione, nella parte inferiore della sua schermata, cliccando su *"My wall"*.

Per ogni sito che verificate e condividete tramite ShareSafe guadagnate dei punti che possono essere utilizzati per ricevere altri prodotti di F-Secure. Altri punti possono essere guadagnati invitando gli amici (a condizione che l'invito venga accettato) e ogni volta che qualcuno clicca su uno dei link verificati o clicca su *"Mi piace"* in un post che avete pubblicato tramite ShareSafe. Cliccando su *Dashboard* nella pagina di ShareSafe compare un elenco dettagliato dei punti raccolti. Nessuna di queste attività promozionali è indispensabile per usare l'applicazione.

Safego

L'installazione di Safego, prodotto dalla società di sicurezza BitDefender, è identica a quella di ShareSafe: entrate in Facebook, visitate <http://apps.facebook.com/bd-safego> e cliccate su *Installa l'applicazione* (a differenza di ShareSafe, Safego comunica in italiano), dando poi il consenso all'applicazione.

Al primo avvio, Safego effettua una scansione del vostro account Facebook e segnala eventuali problemi. Safego esegue anche una valutazione della protezione dei dati personali e segnala eventuali aspetti che vanno corretti. Questi controlli possono essere eseguiti nuovamente visitando la pagina Home del vostro account, nella sezione *Applicazioni*, e cliccando su *Safego*.

Queste due applicazioni di sicurezza possono coesistere tranquillamente nello stesso account e hanno funzioni differenti quanto basta per rendere utile installarle e adoperarle entrambe, considerato che sono oltretutto gratuite.



Risultati di una scansione di Safego.

Anonimato tradito dall'indirizzo Facebook

Nel vostro profilo Facebook potete scegliere un indirizzo abbreviato del tipo <http://www.facebook.com/nome.cognome>. Quest'opzione è nelle impostazioni generali dell'account, nella sezione *Generale*.

L'indirizzo abbreviato (chiamato impropriamente *nome utente* da Facebook) è un'opzione molto pratica per pubblicizzare o condividere il proprio profilo su Facebook, perché è un indirizzo facile da ricordare.

Tuttavia può rivelarsi un autogol se avete scelto l'anonimato: infatti non ha senso usare pseudonimi e foto non rivelatrici se poi il vostro indirizzo Facebook abbreviato contiene il vostro nome e cognome reale.

Quest'indirizzo è modificabile, ma una sola volta, per cui pensateci attentamente prima di attivarlo e impostarlo.

Anonimato tradito dall'indirizzo di e-mail

Se vi siete iscritti a Facebook dando un indirizzo di e-mail che contiene il vostro nome e cognome (per esempio *maria.rossi@esempio.com*) non siete anonimi ed è facile identificare il vostro profilo Facebook.

È infatti possibile digitare in Facebook, nella casella di ricerca, un indirizzo di e-mail e ottenere il profilo corrispondente, anche se l'indirizzo è impostato con il massimo livello di privacy (*"Solo io"*) nelle informazioni di contatto. Di conseguenza, chiunque conosca il vostro indirizzo di e-mail può scoprire il vostro profilo Facebook.

L'unico modo per limitare questa reperibilità tramite l'indirizzo di e-mail è andare nelle *Impostazioni sulla privacy*, scegliere la sezione *Connessione da parte tua*, cliccare su *Modifica impostazioni* e scegliere *Amici* come risposta alla domanda *Chi può cercarti utilizzando l'indirizzo e-mail o il numero di telefono che hai fornito?*

5. Comportamenti sicuri in Facebook

Attenzione alle richieste d'amicizia

Prima o poi riceverete su Facebook delle richieste di *"amicizia"*: un termine psicologicamente ingannevole e carico di valenze emotive che può sviare. In realtà sarebbe più equilibrato parlare di richieste di contatto.

Se accettate la richiesta d'amicizia di un utente, gli concedete di vedere tutto quello che avete pubblicato su Facebook ed etichettato come visibile solo agli amici. L'amicizia, quindi, non va concessa alla leggera: nemmeno quella tenue e commercializzata richiesta attraverso Facebook.

La regola consigliabile è di accettare le richieste d'amicizia soltanto se provengono da persone che conoscete già nel mondo reale e di cui potete verificare materialmente l'identità, senza cedere al desiderio di collezionare amici del tutto virtuali per sentirsi più importanti.

Non dimenticate che state regalando a una società estera l'intera rete delle vostre amicizie. Se l'idea vi infastidisce e pubblicate soltanto contenuti visibili a tutti, potreste accettare un po' di amicizie fasulle per "inquinare" gli archivi di Facebook.

Uscite sempre da Facebook correttamente

È facile pensare che chiudere la pagina di Facebook o uscire dal browser sia sufficiente per scollegarsi da questo social network e terminare la propria sessione. In realtà non è così: se vi limitate a queste due azioni, chiunque usi il computer dopo di voi si troverà automaticamente nel vostro account Facebook.

È quindi importantissimo uscire correttamente da Facebook, specialmente quando usate un computer diverso dal vostro, per esempio

quello di un albergo, quello in ufficio oppure quello di un amico.

L'uscita corretta è molto semplice: si clicca sul triangolino a destra, nella barra blu della pagina di Facebook, e si clicca su *Esci* nel menu che compare. Questo vi porterà alla pagina d'ingresso di Facebook.

Ricordate che se lasciate attiva una sessione Facebook su un computer diverso dal vostro al quale non avete più accesso, potete sempre chiudere a distanza quella sessione andando a un altro computer, entrando nel vostro account e usando l'opzione *Sessioni attive* (*Impostazioni account - Protezione - Sessioni attive - Modifica*).

Difendersi da truffe e attacchi

Le truffe su Facebook sono particolarmente ingannevoli perché i messaggi che le veicolano vi arrivano da persone di cui vi fidate e spesso hanno un aspetto del tutto innocuo: per esempio, sono inviti a guardare un nuovo video o a visitare un sito che è piaciuto moltissimo.

Per difendervi da queste truffe, che hanno lo scopo di rubare le vostre informazioni personali, il vostro account, i vostri soldi oppure di infettare il vostro computer, occorre imparare a riconoscere i sintomi di un attacco su Facebook.

Diffidate degli inviti a scaricare programmi

Se vi arriva un invito che vi propone di installare un nuovo programma, per esempio un gioco o uno strumento che vi permette di sapere chi vi ha tolto l'amicizia su Facebook, chiedetevi sempre se chi lo sta offrendo è una società seria e conosciuta e se vale la pena di installarlo, e poi controllatelo comunque con un buon antivirus aggiornato (vale anche per gli utenti Apple, che spesso si considerano invulnerabili).

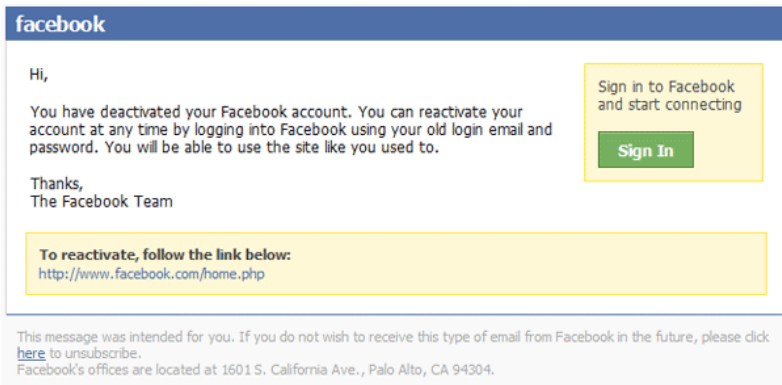
I criminali informatici usano spesso programmi-esca (denominati *cavalli di Troia*) per infettare i computer delle vittime. Il cavallo di Troia, per esempio, può bloccare il computer e chiedere un riscatto, pagabile con carta di credito, per sbloccarlo, oppure può registrare silenziosamente tutto quello che scrivete e poi inviarlo al criminale, password comprese.

Messaggi-truffa da Facebook

Non fidatevi ciecamente di messaggi o e-mail che sembrano provenire

dall'amministrazione di Facebook o da quella dei giochi di Facebook, come Farmville o Mafia Wars: il mittente è facile da falsificare in modo molto credibile.

Nel dubbio, non seguite le istruzioni e gli inviti che vi arrivano tramite questi messaggi. Usate sempre il buon senso: se un messaggio vi sembra sospetto o particolarmente sgrammaticato o troppo allettante, è probabile che si tratti di un tentativo d'imbroglione.



Un falso messaggio apparentemente proveniente dall'amministrazione di Facebook.

Attenzione alle pagine di ingresso in Facebook

Uno dei modi più frequenti per rubarvi la password di Facebook è portarvi in vari modi a una falsa pagina d'ingresso di questo social network, uguale in tutto e per tutto a quella vera.

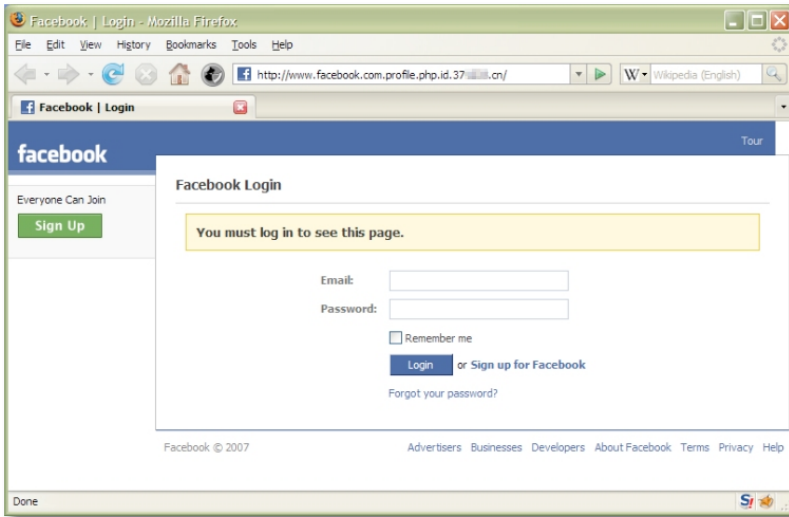
Controllate sempre che l'indirizzo mostrato nella barra dell'indirizzo del vostro browser

- inizi con *https* (non *http*)
- prosegua con *www.facebook.com/*

La barra finale (*slash*) è molto importante, perché distingue il vero sito di Facebook da tutti gli imitatori.

Ogni volta che vi compare una pagina d'ingresso, controllate anche che il nome *www.facebook.com* sia scritto correttamente. Molti ladri di password utilizzano siti dal nome visivamente simile a quello giusto (per esempio *www.facbook.com* oppure *www.faebook.com*), contando sulla distrazione degli utenti e sulla tendenza istintiva a leggere correttamente le parole familiari anche se sono scritte in modo sbagliato.

Ricordate che Facebook vi chiede di autenticarvi con login e password una sola volta per ogni sessione: se siete già entrati in Facebook e vi compare una nuova richiesta di login e password, è sicuramente una truffa e la richiesta non proviene dal social network.



Una falsa pagina d'ingresso di Facebook. Si tratta in realtà di un sito cinese.

La truffa degli script

Diffidate tassativamente di qualunque proposta di “trucco” per sapere chi vi ha tolto l'amicizia o chi ha guardato il vostro profilo oppure per scoprire altre informazioni riservate degli utenti di Facebook: si tratta di esche psicologiche che vi fanno abbassare la guardia allettandovi con promesse golose.

In particolare, su Facebook prospera la cosiddetta *truffa degli script* o *script scam*: la vittima riceve da un amico una serie di codici informatici (*script*) da copiare e incollare nella barra dell'indirizzo del browser. Questi codici permetterebbero di accedere a informazioni segrete, ma in realtà non fanno altro che impostare il vostro profilo in modo che mandi messaggi truffaldini a tutti i vostri amici.

Questa truffa è così efficace che Facebook ha attivato un sistema di verifica che vi avvisa se provate a incollare uno script nella barra dell'indirizzo e vi chiede di confermare le vostre intenzioni, spiegando anche i motivi per cui incollare codici di questo tipo è una pessima idea. Non ignorate questi avvisi.

La difesa contro questo attacco è molto semplice: non incollate mai nulla nella barra dell'indirizzo del vostro browser.

Clickjacking e likejacking: furto di clic

Può sembrare incredibile, ma esiste l'arte truffaldina di rubare i clic del mouse: in gergo si chiama *clickjacking*, ossia "dirottamento di clic". L'utente crede di cliccare su una pubblicità oppure su un pulsante che gli permetterà di vedere un video che gli interessa, ma in realtà il suo clic viene passato a un'altra pagina Web. In questo modo si può imbrogliare l'utente inducendolo inavvertitamente a cliccare su link che scaricano virus, a rispondere a sondaggi (che poi vengono venduti dai criminali alle società di ricerca di mercato) o a rendere pubbliche informazioni private che ha immesso in Facebook. Nei casi peggiori viene accesa di nascosto la webcam della vittima.

Quando il furto di clic riguarda il pulsante "*Mi piace*" di Facebook, questo inganno si chiama *likejacking* (in inglese questo pulsante si chiama infatti "*Like*"). Viene usato per far sembrare che l'utente voglia promuovere un certo prodotto dicendo che gli piace.

Per evitare questa trappola occorre tenere sempre aggiornato il proprio browser, in modo da sfruttare le difese contro *clickjacking* e *likejacking* che vengono introdotte nelle nuove versioni dei browser; se usate Firefox, installate l'estensione NoScript (scaricabile gratuitamente presso <https://addons.mozilla.org/it/firefox/addon/noscript/>).

Anche in questo caso il buon senso è un'ottima difesa: se ricevete da un amico un messaggio in cui dice che gli piace molto qualcosa che normalmente non rientra nei suoi gusti, non fidatevi e avvisatelo che forse è vittima di un *likejacking*.

Furto d'identità: il trucco dell'amico in vacanza

Attenzione ai truffatori che si spacciano per vostri amici rubandone il profilo Facebook e mandandovi messaggi in cui dicono di essere stati derubati mentre erano in vacanza all'estero e di aver bisogno che mandiate loro urgentemente dei soldi tramite Western Union.

L'emozione che si prova nel ricevere questi messaggi è molto forte: la preoccupazione per la persona cara fa abbassare la guardia e non fa notare i sintomi del raggirio. Spesso l'amico (o meglio, il criminale che si sta spacciando per lui) ci scrive in una lingua che non usa abitualmente, eppure non ci si fa caso.

Più in generale, non ha molto senso che un derubato usi Facebook per contattare gli amici: avrebbe molto più senso che andasse alla polizia locale o al consolato e telefonasse. Eppure la truffa funziona spesso.

Applicazioni? Solo se servono davvero

Valutate con cura tutte le applicazioni (giochi o altri programmi di utilità) che vi vengono proposte. Molte sono realmente utili; alcune, però, sono come virus che leggono i vostri dati personali e li inviano ai truffatori. Fate attenzione, in particolare, ai sondaggi.

Ricordate che non esistono applicazioni che permettono di sapere chi vi ha visitato: sono tutte esche, perché questa funzione è espressamente vietata da Facebook. Qualunque applicazione o “trucco” che incontrate su Internet e vi promette questo genere d’informazione è un virus o una truffa. Quando vi viene proposto di installare un’applicazione, fate molta attenzione alle autorizzazioni che chiede: se vuole accesso a troppe informazioni personali o se vuole il permesso di pubblicare qualcosa su Facebook a vostro nome, pensateci due volte.

Richiesta di Autorizzazione

Café World chiede l'autorizzazione per:



Accedere alle tue informazioni di base
Include nome, immagine del profilo, sesso, reti, ID utente, lista degli amici, e qualsiasi altra informazione io abbia reso pubblica



Accedere alle informazioni del tuo profilo
Data di nascita e Attività nei giochi e nelle applicazioni



Accedere alle informazioni che le persone condividono con me
Attività nei giochi e nelle applicazioni



Inviarti e-mail
Café World può inviarti e-mail direttamente all'indirizzo paolo.attivissimo@gmail.com - [Modifica](#)



Pubblicare su Facebook a mio nome
Café World può pubblicare messaggi di stato, note, foto e video a mio nome.



Pubblicare attività di giochi e applicazioni
Café World può pubblicare punteggi, risultati e altre attività su Facebook.



Café World

Se decidi di continuare, accetti i [Termini e condizioni d'uso](#) e la [Normativa sulla privacy](#) di Café World - [Segnala applicazione](#)

Hai effettuato l'accesso come [Paolo Sgomberonte](#) - [Esci](#)

Consenti

Non consentire

Le autorizzazioni richieste dal gioco Café World in Facebook.

Vedersi “da fuori”

Uno dei modi migliori per accorgersi di essere incappati in truffe o furti della propria password su Facebook è guardare il proprio profilo “da fuori”, ossia dal punto di vista degli altri. Molti utenti, infatti, non si accorgono di essere infettati e di mandare post pubblicitari indesiderati finché non glielo dice qualcuno dei loro amici.

Facebook aiuta a vedersi “da fuori”: nel vostro profilo c’è il pulsante “Visualizza come” che permette di vedere l’aspetto pubblico della vostra presenza su Facebook. Potete adoperarlo anche per verificare quali vostre informazioni sono visibili a uno specifico utente inserendo il nome di un amico nella casella apposita. Fatelo spesso per evitare gaffe.



L'opzione “Visualizza come” di Facebook.

Rimuovere un tag

Può capitare di essere taggati in un modo che troviamo offensivo o inopportuno, per esempio in una foto. Per rimuovere il tag potete andare alla foto in questione (consultando il Registro attività di Facebook, che è nella pagina principale del vostro profilo) e cliccare sulla foto.

In alto a destra, accanto all’immagine, compare un’icona di un ingranaggio: cliccandovi sopra appare un menu, dal quale potete scegliere

Segnala/rimuovi tag e poi specificare che volete rimuovere il tag fra le opzioni che vengono visualizzate. Vi viene chiesto, infine, se volete solo rimuovere il tag, se volete chiedere all'autore del post di eliminare l'immagine oppure se volete bloccare l'autore. Il blocco dell'autore ha il vantaggio di impedirgli di taggarvi di nuovo.

Se l'utente che ha pubblicato il post in cui siete taggati non collabora, potete inviare una segnalazione ai gestori di Facebook cliccando sempre sull'icona dell'ingranaggio e scegliendo *Segnala/rimuovi tag*; dalle opzioni che compaiono, sceglietene una adatta tranne la prima (*"Voglio rimuovere questo tag"*): tutte le altre opzioni, infatti, generano una segnalazione a Facebook.

Potete anche rimuovere un tag usando l'opzione *Rimuovi dal profilo* in un post. Ricordate che potete prevenire in blocco i tag indesiderati attivando l'opzione di controllo del profilo nelle *Impostazioni sulla privacy*.

Un po' di galateo

Non è facile rendersi conto della portata di un post su Facebook; non siamo abituati a parlare e scrivere in pubblico. Fate l'esercizio mentale di immaginarvi su un palcoscenico o in diretta TV ogni volta che pubblicate qualcosa su Facebook e vi risparmierete equivoci e imbarazzi.

Non sapete chi vi legge

Pensate sempre che fra i vostri amici su Facebook potrebbe esserci il vostro capo, il vostro partner (o ex partner) oppure il vostro insegnante. La storia di Internet è piena di esempi di persone che hanno criticato su Facebook il datore di lavoro, causando danni d'immagine all'azienda che hanno condotto al licenziamento, oppure sono stati colti a simulare malattie mentre pubblicavano su Facebook le fotografie delle loro prodezze vacanziere. Per non parlare dei giovani vandali che si sono vantati delle loro imprese pubblicandone le immagini su Facebook e in questo modo sono stati identificati.

Fate attenzione anche alle informazioni pubblicate automaticamente dalle applicazioni: per esempio, molti giochi pubblicano nel vostro profilo il fatto che li state usando. Questo può dare l'impressione che l'utente sia una persona poco seria, specialmente se compare un annuncio del tipo *"Giancarlo sta giocando ad Angry Birds! Gioca anche tu!"* mentre Giancarlo dovrebbe essere nel bel mezzo di una riunione di lavoro (e magari lo è, ma sta giocando sul telefonino di nascosto).

Se pubblicate qualcosa, resta su Facebook per sempre

Partite dall'assunto che tutto quello che pubblicate su Facebook, sia quello che riguarda voi, sia quello che riguarda gli altri, resterà su Facebook per sempre. **Le foto che mettete su Facebook rimangono accessibili a lungo, con semplici tecniche, anche se le avete cancellate**, e comunque chiunque le può copiare e conservare anche dopo che avete cancellato da Facebook l'originale.

Evitate di pubblicare immagini personali o potenzialmente imbarazzanti, vostre o dei vostri amici: oggi sembrano frivole, ma domani il futuro datore di lavoro potrebbe trovarle e farsi un'idea sbagliata.

Usate la *Regola della Nonna*: se quello che volete pubblicare turberebbe vostra nonna, non pubblicatelo.

L'amico svenduto

Non sfruttate gli amici invitandoli a partecipare a giochi online per aumentare il vostro punteggio. Molti dei giochi che trovate su Facebook sono costruiti in modo da indurvi a procacciare nuovi giocatori in cambio di punti. Non fatelo: darestes facilmente l'impressione di essere persone poco serie che svendono le proprie amicizie. Molti utenti di Facebook considerano questi inviti una forma di maleducazione.

Occhio alle bufale

Non diffondete notizie senza averle prima controllate; nel dubbio, non inoltratele, anche se provengono da amici. Le bufale prosperano su Facebook ancor più che nel resto di Internet, e non ci si può fidare ciecamente degli amici, perché magari anche loro si sono fidati dei loro amici, e così via, e nessuno ha verificato la notizia lungo la catena di Sant'Antonio.

In particolare, non abboccate agli allarmi che annunciano che Facebook diverrà a pagamento. I responsabili del social network hanno smentito categoricamente qualunque intenzione di questo genere.

Se viene violato l'account

Il sintomo più evidente di un account violato è l'impossibilità di accedere, perché il ladro ha cambiato la password, ma ci possono essere al-

tre indicazioni meno palesi. Per esempio, i vostri amici potrebbero segnalarvi che nel vostro profilo compaiono messaggi di stato che non sembrano rispecchiare i vostri gusti, oppure potreste ricevere risposte a messaggi che non avete inviato: significa che qualcuno ha avuto accesso abusivo al vostro account ma non si è ancora spinto fino al punto di cambiarvi la password.

Se vi capita un problema di questo genere, attivate la procedura di protezione dell'account presso <https://www.facebook.com/hacked>. Vi viene chiesto di eseguire una serie di controlli di sicurezza che dovrebbero permettervi di riprendere il controllo dell'account, sottraendolo al criminale.

In alternativa, potete cliccare su *Hai dimenticato la password?* nella pagina d'ingresso di Facebook e rispondere alle informazioni richieste per identificare l'account e farvi mandare una e-mail che contiene le istruzioni per reimpostare la password.

Chiudere un account Facebook

Può capitare di voler abbandonare Facebook per mille ragioni. Molti utenti pensano che questo non sia possibile perché hanno sentito raccontare dagli amici le difficoltà che hanno incontrato quando hanno provato a chiudere il proprio account.

In realtà è perfettamente possibile chiudere un account su Facebook: bisogna però fare una distinzione fra *disattivazione* ed *eliminazione*, e comunque la procedura non è molto facile.

Disattivazione o eliminazione?

Facebook usa il termine *disattivazione* per indicare quella che in realtà è una semplice sospensione dell'account: non viene cancellato o rimosso nulla, ma l'account diventa invisibile agli altri utenti. Se decidete di ricominciare a usarlo, tutto torna come prima.

L'*eliminazione* di un account è invece la cancellazione definitiva e irreversibile delle informazioni personali connesse all'account e di quasi tutto quello che è stato pubblicato tramite quell'account (sono escluse le conversazioni condivise e alcuni altri elementi).

In sintesi: se disattivate, potete pentirvene; se eliminate, non potete tornare sui vostri passi.

Come disattivare un account

Accedete al vostro account, cliccate sul triangolo nella banda blu di Facebook e scegliete dal menu la voce *Impostazioni account*. Cliccate su *Protezione* (a sinistra) e scegliete *Disattiva il tuo account*.

Compare un questionario che vi chiede le ragioni della disattivazione e, a riprova del fatto che si tratta di una semplice sospensione dell'account, viene segnalato che *“anche dopo la disattivazione, i tuoi amici potranno ancora invitarti agli eventi, taggarti nelle foto o invitarti a iscriverti ai gruppi.”* Cliccate su *Conferma*.

Disattiva account

facebook.com https://www.facebook.com/deactivate.php

facebook Ricerca

Confermi di voler disattivare il tuo account?

La disattivazione del tuo account comporterà la chiusura del tuo profilo e la rimozione del tuo nome e dell'immagine ad esso associata da qualsiasi elemento che hai condiviso su Facebook.

Motivo della disattivazione (richiesto):

- ☐ Penso che Facebook sia inutile.
- ☐ La privacy mi preoccupa.
- ☐ Non capisco come si usa Facebook.
- ☐ Ho un altro account Facebook.
- ☐ Ricevo troppe e-mail, inviti e richieste da Facebook.
- ☐ Si tratta di una misura temporanea. Tornerò.
- ☐ Passo troppo tempo su Facebook.
- ☐ Il mio account è stato violato.
- ☐ Non mi sento al sicuro su Facebook.
- ☒ Altro

Fornisci una spiegazione più dettagliata:

Interruzione ricezione e-mail: ☐ Non ricevere e-mail da Facebook in futuro

Nota: anche dopo la disattivazione, i tuoi amici potranno ancora invitarti agli eventi, taggarti nelle foto o invitarti a iscriverti ai gruppi. Se selezioni questa opzione, NON riceverai e-mail e notifiche per questi inviti da parte dei tuoi amici.

Facebook © 2012 - Italiano

Informazioni · Pubblicità · Crea una Pagina · Sviluppatori · Opportunità di lavoro · Privacy · Condizioni · Centro assistenza

Chat

L'inizio della procedura di disattivazione in Facebook.

Vi viene poi chiesta la password dell'account: immettetela e cliccate su *Disattivare ora*. Compare poi un *CAPTCHA*, ossia una coppia di parole deformate che dovete decifrare e digitare per confermare che siete un essere umano e non un programma automatico o un virus. Dopo che le avete digitate, cliccate su *Invia*.

A questo punto Facebook vi fa uscire e vi propone la schermata d'ingresso e un avviso che vi informa che il vostro account è stato disattivato. Per riattivarlo, tuttavia, è sufficiente entrare in Facebook con l'indirizzo di e-mail e la password dell'account stesso come consueto.

Non è finita: dovete fare attenzione a non entrare accidentalmente in Facebook, né dal computer né da altri dispositivi, altrimenti la disattivazione verrà revocata e tutto tornerà come prima. Tenete presente che

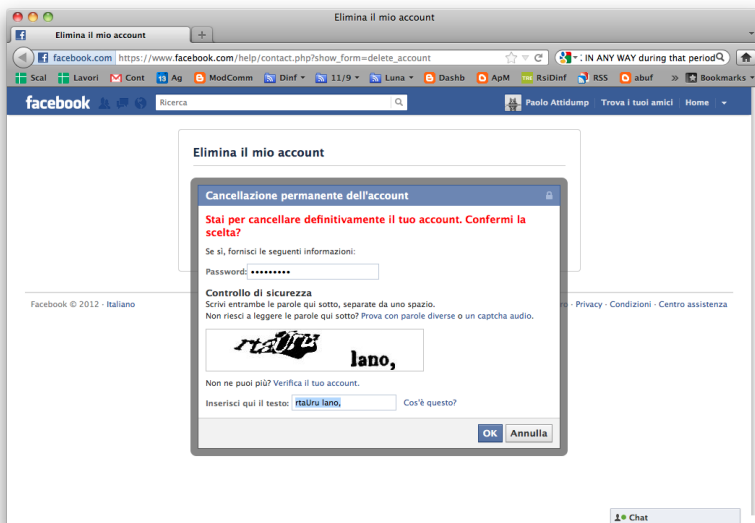
per Facebook anche cliccare su “*Mi piace*” in un sito esterno a Facebook oppure usare la password di Facebook su altri siti (Facebook Connect) significa “*entrare*” e comporta la revoca della disattivazione.

Come eliminare un account

Fate attenzione: questa procedura è irreversibile. Per eliminare un account andate a questo link:

https://www.facebook.com/help/contact.php?show_form=delete_account

Cliccate su *Elimina account*. Compare un CAPTCHA, come per la disattivazione: digitate le parole deformate, immettete la vostra password e cliccate su *OK*.



Inizio dell'eliminazione di un account.

Fatto questo, l'account non è ancora eliminato: resta *disattivato* per 14 giorni. Soltanto dopo questo periodo, se non usate questo account in alcun modo (compresi i clic sui pulsanti “*Mi piace*” su altri siti, l'accesso tramite telefonino o l'uso della password di Facebook su altri siti associati al servizio Facebook Connect), i vostri dati verranno eliminati permanentemente.

Se invece accedete all'account durante il periodo di disattivazione, vi viene proposto di revocare l'eliminazione e riattivare l'account.

6. Impostazioni sicure di Twitter

Un po' di terminologia

Twitter permette di pubblicare messaggi che hanno una lunghezza massima di 140 caratteri. Questi messaggi si chiamano *tweet*; inviare un messaggio si dice *twittare* o *tweetare*.

Ogni utente di Twitter è identificato da un nome o pseudonimo: è meglio sceglierne uno breve, visto il drastico limite di lunghezza dei messaggi. Ogni nome è preceduto dal simbolo della chiocciolina (per esempio @sgomberonte).

Salvo diversa impostazione, i messaggi che scrivete sono pubblici e quindi leggibili da chiunque: vengono inviati automaticamente a tutti gli amici, o *follower*, che vi seguono su Twitter, ma sono anche consultabili da chi non è vostro amico. Se seguite un utente e lui segue voi, potete scambiare messaggi privati.

È possibile includere in un tweet un link (un indirizzo di un sito, per esempio): verrà abbreviato automaticamente.

Nei tweet si possono anche allegare foto, cliccando sull'icona *Aggiungi un'immagine*, e si possono includere i dati di geolocalizzazione.

Se il tweet inizia con il nome di un utente, Twitter lo interpreta come una risposta rivolta a quell'utente.

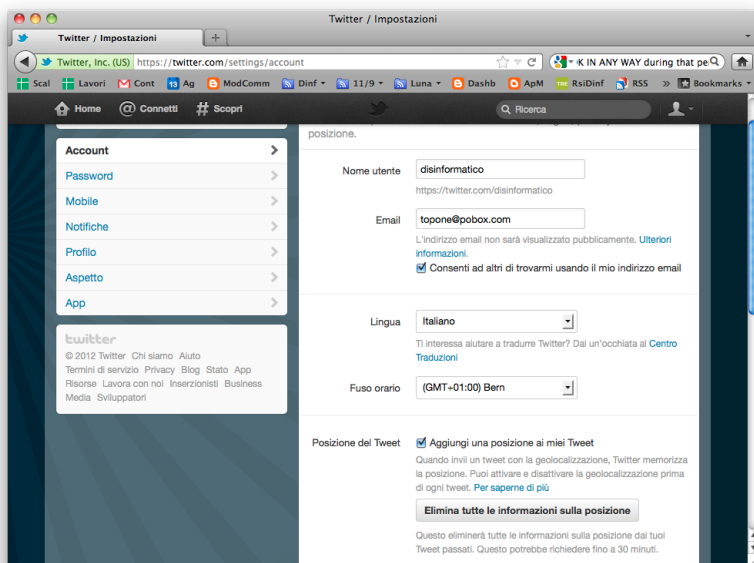
Se iniziate una parola con il simbolo "#", la contrassegnate come parola chiave (*hashtag*), che viene usata per raggruppare messaggi dedicati a un tema (per esempio #justinbieber o #terremoto).

Le impostazioni dell'account sono accessibili entrando in Twitter con la propria login e password e cliccando sul triangolino in alto a destra: questo fa comparire un menu dal quale si sceglie la voce *Impostazioni*.

Queste impostazioni sono suddivise in sezioni, che vengono descritte nelle pagine di questo capitolo soffermandosi sui loro aspetti di privacy e sicurezza.

Account

Dato che Twitter è un social network dove si dà per scontato che tutto sia pubblico, non ci sono molte considerazioni di privacy: tuttavia dovete decidere, per esempio, se volete apparire con il vostro vero nome e cognome o con uno pseudonimo (Twitter accetta entrambi) e se volete consentire agli altri di trovarvi in Twitter usando l'indirizzo di e-mail che avete usato per iscrivervi a questo social network (è consigliabile disattivare quest'opzione togliendo il segno di spunta dalla casella *Consenti ad altri di trovarmi usando il mio indirizzo e-mail*).



Prima parte della sezione Account delle impostazioni di Twitter.

Geolocalizzazione

Un'altra scelta importante in questa sezione è la *Posizione del Tweet*, ossia l'inclusione automatica dei dati di geolocalizzazione nei messaggi che inviate. Quest'inclusione può essere disattivata o attivata anche a livello del singolo messaggio: qui viene definita l'impostazione standard.

Le informazioni di geolocalizzazione possono essere rimosse in blocco da tutti i tweet già pubblicati cliccando su *Elimina tutte le informazioni sulla posizione*.

Contenuti controversi

L'opzione *Twitta il contenuto multimediale* vi permette di avvisare i vostri lettori che le immagini o i video che allegate o segnalate nei vostri tweet possono essere cruenti, scioccanti o adatti solo a un pubblico adulto.

Se pensate che qualche vostro tweet possa essere di questo genere, attivate le caselle *Mostra contenuti multimediali che possono contenere materiale sensibile* e *Segna i miei contenuti multimediali come contenenti materiale sensibile*.

Se non lo fate e poi twittate qualcosa che i vostri lettori trovano inadatto, gli stessi lettori possono segnalare il vostro account a Twitter per violazione delle norme d'uso.

Tweet privati

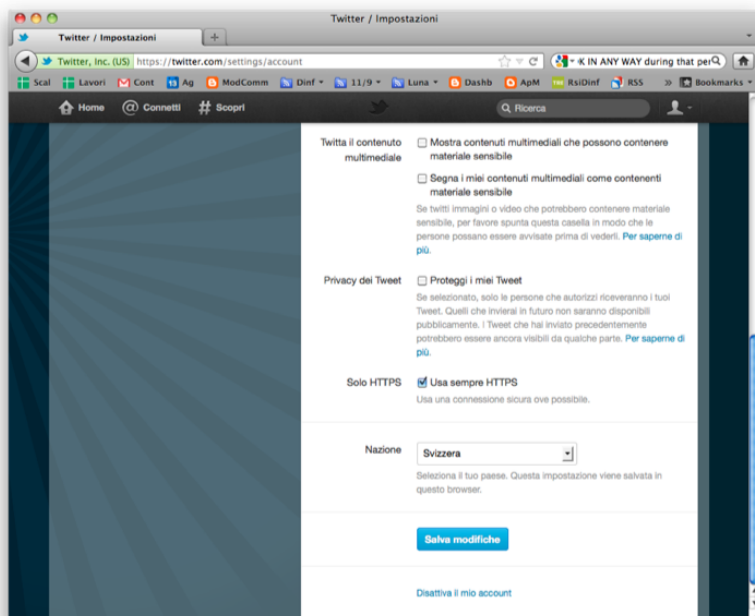
L'opzione *Privacy dei tweet* permette di rendere visibili i vostri messaggi soltanto agli utenti autorizzati. Se vi interessa questo modo di usare Twitter, attivate la casella *Proteggi i miei Tweet*. È una soluzione prudente per i minori: evita che sconosciuti possano leggere i loro tweet, che vengono invece riservati solo agli amici reali.

Tenete presente, comunque, che nulla impedisce a un vostro lettore autorizzato di prendere un vostro tweet privato e ripubblicarlo altrove su Twitter o in qualunque altro posto su Internet.

Navigazione protetta

Come per Facebook, anche in Twitter esiste il rischio che un intruso intercetti il traffico di dati della vostra sessione Twitter e si sostituisca a voi. Per ridurre questo rischio è molto importante attivare la casella *Usa sempre HTTPS* nella sezione *Solo HTTPS*. In questo modo il traffico di dati verrà cifrato per renderlo incomprensibile agli aspiranti intrusi.

Va sottolineato che non tutti i programmi per l'uso di Twitter, specialmente quelli dei telefonini e dei tablet, gestiscono la cifratura delle comunicazioni: per questo Twitter dichiara che utilizzerà una connessione sicura *“ove possibile”*.



Seconda parte della sezione Account delle impostazioni di Twitter.

Password

Per Twitter valgono le precauzioni standard sulle password:

- lunghezza di almeno otto caratteri;
- priva di senso compiuto;
- contenente lettere maiuscole e minuscole, cifre e preferibilmente anche segni di punteggiatura;
- non usata altrove per altri servizi.

Mobile

Twitter permette di inviare tweet anche da un telefonino non evoluto, usando un semplice SMS: basta registrare qui il proprio numero di telefonino e poi inviare i tweet come SMS ai numeri telefonici indicati nelle

impostazioni (attenzione: si tratta di numeri nell'Isola di Man, in Germania e in Finlandia, per cui il costo dell'SMS può essere elevato).

Qui è possibile scegliere se consentire agli altri utenti di Twitter di trovarvi in base al vostro numero di telefonino (probabilmente sconsigliabile) e se impostare un codice (PIN) da digitare all'inizio di ogni SMS per autenticare l'SMS inviato.

Notifiche

In questa sezione si impostano le notifiche che si possono ricevere via e-mail. Le varie opzioni sono da attivare o disattivare secondo i propri gusti, ad eccezione di *Inviarmi un'email quando mi viene inviata una risposta o vengo @menzionato*, che è opportuno attivare per tenere d'occhio quel che si dice di voi su Twitter.

Profilo e aspetto

Queste sezioni non comportano particolari questioni di sicurezza o privacy, salvo l'opzione di pubblicare i vostri Tweet automaticamente sul vostro profilo Facebook, presente nella sezione *Profilo*: se desiderate restare anonimi, non vi conviene attivare quest'opzione, altrimenti diventa facile correlare il vostro account Twitter con quello Facebook e quindi risalire alla vostra identità.

App

Valutate con attenzione le *app* o *applicazioni* che attivate e quali permessi date a ciascuna di esse. I permessi sono revocabili cliccando sul pulsante *Revoca l'accesso* corrispondente all'applicazione.

Privacy

Può sembrare un controsenso parlare di privacy in un social network in cui tutto, per definizione, è da considerare pubblico, ma ci sono alcune considerazioni da fare comunque, perché esporsi pubblicamente può comportare conseguenze inattese.

Per esempio, un potenziale datore di lavoro potrebbe guardare i nostri tweet e farsi un'idea sulle nostre affiliazioni politiche o religiose. Potrebbe guardare l'elenco delle persone che seguiamo su Twitter e dedurne le nostre simpatie e antipatie. Il problema di queste deduzioni, sempre più frequenti nel mondo del lavoro, è che si basano su un campione di dati estremamente ristretto e si prestano quindi a facili fraintendimenti.

Non è detto, infatti, che l'elenco delle nostre simpatie su Twitter sia completo e descriva esaurientemente la nostra personalità e i nostri interessi, ma chi lo guarda sarà portato a pensare che sia così.

Privacy degli archivi

Per gli utenti comuni, la ricerca negli archivi dei messaggi pubblicati su Twitter copre soltanto gli ultimi sette giorni o poco più, ma questo non vuol dire che dopo pochi giorni i vecchi messaggi spariscano del tutto:

- qualunque tweet pubblico è recuperabile in ogni momento se si conosce il suo indirizzo o URL specifico, che ha una struttura del tipo [http://twitter.com/#!/\[nomeutente\]/status/\[numero\]](http://twitter.com/#!/[nomeutente]/status/[numero]);
- i tweet passati possono essere trovati sfogliando la pagina Twitter di un utente;
- un tweet è recuperabile tramite un motore di ricerca (come Google o Bing) se si conosce una porzione significativa del suo testo.

Le aziende, inoltre, possono acquisire da Twitter gli archivi integrali dei tweet (esclusi quelli degli account privati).

Vi sono poi siti, come Topsy.com, che archiviano tutti i tweet pubblici e consentono a chiunque di effettuare ricerche sofisticate. Anche su Twitter, insomma, quello che pubblicate va considerato come se fosse permanente, perché anche se è possibile cancellare un tweet, può essere stato archiviato altrove.

Ricordate la regola d'oro: se non volete che qualcosa diventi pubblico e venga analizzato, aggregato e compilato statisticamente, non pubblicatelo su Internet.

“Antivirus” per Twitter

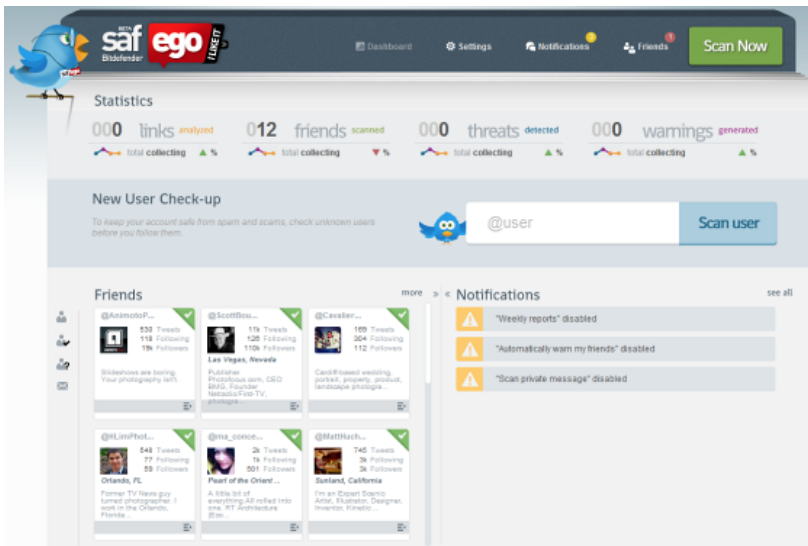
La società di sicurezza informatica Bitdefender offre gratuitamente Sa-fego per Twitter, una sorta di filtro che aiuta a bloccare le pubblicità in-

desiderate, i tentativi di furto d'identità e i tweet contenenti link a siti pericolosi.

L'installazione è semplice e vale per tutti i dispositivi usati per accedere a Twitter: andate presso <http://safego.bitdefender.com/twitter> e cliccate su *Sign in with Twitter*. Questo vi porta a Twitter, dove dovete dare l'autorizzazione a Safego tramite il vostro nome utente e la vostra password di Twitter (la password non viene inviata a BitDefender). Tenete presente che quest'autorizzazione permette a Safego di aggiornare il vostro profilo e di postare tweet a nome vostro.

Fatto questo, Safego effettua una scansione di tutti i vostri contatti. La schermata di Safego è divisa in quattro sezioni:

- *Dashboard*, dove potete chiedere la scansione di un singolo utente, vedere dati statistici, messaggi e notifiche;
- *Settings*, dove potete scegliere se ricevere avvisi automatici quando SafeGo rileva una possibile minaccia, se seguire BitDefender su Twitter, se attivare la scansione dei messaggi privati, se ricevere resoconti settimanali e se permettere a SafeGo di avvisare automaticamente gli amici se risulta che hanno inviato link pericolosi;
- *Notifications*, che informa sui cambiamenti d'impostazione di Safego;
- *Friends*, che permette di vedere quali contatti Twitter sono sicuri e quali sono ritenuti sospetti.



La sezione Dashboard di Safego per Twitter.

7. Comportamenti sicuri in Twitter

Twitter è un social network molto semplice e quindi ha meno trappole e possibili inciampi rispetto a Facebook. Tuttavia ci sono alcuni aspetti peculiari di Twitter che si prestano a imbrogli o attacchi specifici che è meglio conoscere.

Non fidatevi delle identità dichiarate

Su Twitter non c'è praticamente nessun controllo d'identità: chiunque è libero di prendere il nome che preferisce, anche se l'account può essere revocato se viene segnalato come probabile impostura.

Twitter offre degli account verificati alle celebrità, ma quest'autenticazione non è richiedibile dagli utenti non celebri. Non è quindi il caso di credere sulla parola a chi dice di essere una persona famosa o di rappresentare un'azienda, un governo o un ente.

Attenti ai tweet dissonanti

Se un vostro amico pubblica un tweet che non corrisponde ai suoi gusti o è scritto in una lingua diversa da quella consueta, o se pubblica un tweet molto vago (per esempio *"immagine scioccante, guarda qui!"* oppure *"qualcuno sta parlando male di te"*), è probabile che il suo account Twitter sia stato violato. Avvisatelo (usando un canale diverso da Twitter) e non cliccate sui link che accompagnano questi messaggi: di solito portano a siti-trappola.

Protegete la vostra password

Twitter non vi chiederà mai la vostra password in una e-mail: qualunque messaggio che ve la chieda al di fuori di Twitter è un tentativo di furto di password.

L'unico posto nel quale è necessario immettere la password è il sito www.twitter.com. Una volta che siete dentro Twitter, non vi verrà chiesta di nuovo la vostra password per tutta la durata della sessione. Se compare una richiesta di password, è una trappola (*phishing*).

Prima di digitare la vostra e-mail e password di Twitter, assicuratevi di essere sul sito autentico di Twitter e non su un sito che gli somiglia visivamente (e magari anche nel nome) ma è stato costruito da truffatori per rubarvi i codici d'accesso.

Controllate sempre che l'accesso al sito avvenga in modo protetto, usando la cifratura: il nome del sito, nella barra di navigazione del vostro browser, deve:

- iniziare con <https://> (non <http://>)
- proseguire con www.twitter.com/ (con la barra in fondo).

Se non vengono soddisfatte queste due condizioni, si tratta di un sito truffaldino che si spaccia per Twitter.

Link brevi ingannevoli

I criminali tentano spesso di ingannare gli utenti di Twitter utilizzando i link brevi (per esempio "<http://bit.ly/oTzoc>") per nascondere la vera natura dei siti ai quali vogliono portare gli utenti.

Twitter ha attivato un proprio sistema di abbreviazione dei link che conserva i primi caratteri del nome del sito originale corrispondente al link breve per consentire agli utenti di farsi un'idea della destinazione dei link, ma è comunque importante usare il buon senso e restare vigili.

Ci sono anche dei servizi di decodifica di questi link brevi, come per esempio Longurl.com: basta immettervi il link breve per sapere qual è il sito originale corrispondente.

Cancellazione dei messaggi

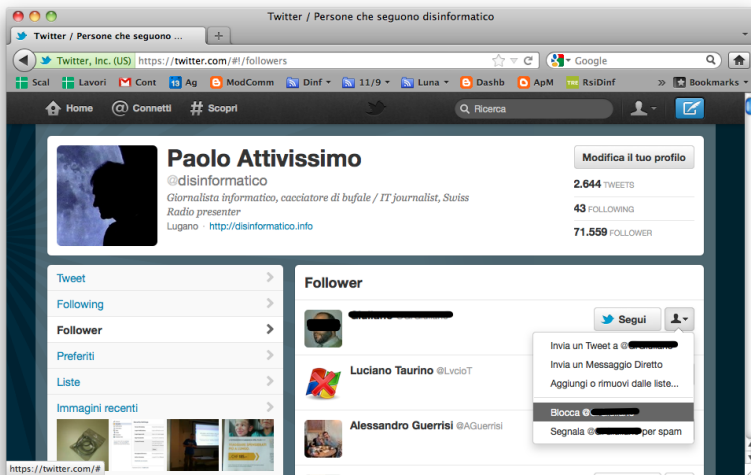
Cancellare un messaggio su Twitter è semplice ma poco intuitivo: basta visualizzarlo su www.twitter.com e lasciare ferma per qualche istante la freccia del mouse nel rettangolo che contiene il messaggio in questione. Compare l'opzione "*Elimina*": cliccatela. Twitter vi chiede "*Sei sicuro/a di voler eliminare questo messaggio?*"; cliccate su "*Sì*". Il messaggio scompare dallo schermo.

Occorre ricordare, però, che questo non elimina i *retweet* (le copie del vostro tweet inoltrate da altri utenti) e le copie pubblicate altrove, per esempio su Facebook.

Blocco di tweet e utenti offensivi o truffaldini

Conviene bloccare gli utenti che si comportano in modo offensivo o disonesto: è sufficiente cliccare sul loro nome per visualizzare il loro profilo e poi sull'icona dell'omino in alto a destra. Compare un menu nel quale si può scegliere l'opzione *Blocca* oppure *Segnala per spam*.

Nel caso di una fotografia offensiva o altrimenti inadatta si può segnalarla cliccandovi sopra per visualizzarla: in basso a destra compare l'opzione *Segnala questo contenuto*.



Blocco di un utente in Twitter.

Chiudere un account Twitter

Per chiudere definitivamente un account su Twitter occorre andare nelle *Impostazioni*, scegliere la scheda *Account* e andare in fondo alla scheda, dove si trova il link *Disattiva il mio account*.

Se lo fate, il vostro account verrà dapprima *disattivato* (reso invisibile) per trenta giorni. Scaduto questo tempo l'account verrà progressivamente eliminato nel giro di una settimana.

Indice

3 Note tecniche

- 3 Ringraziamenti
- 3 Distribuzione libera e gratuita
- 3 Commenti, correzioni e aggiornamenti

5 1. “Autodifesa”? Sul serio?

9 2. I concetti di base

- 9 Cosa vuol dire “social network”?
- 9 Dispositivi d’accesso
- 10 Account, login e password
- 10 Post, aggiornamento o messaggio di stato
- 11 Livelli di privacy
- 11 Funzioni accessorie

13 3. Precauzioni generali per i social network

- 13 Età minima: perché 13 anni?
- 14 Scelta del nome
- 14 *Furto d'identità*
- 15 Scelta della password
- 15 *Non riciclate le password!*
- 16 *Come si ruba una password?*
- 18 *Domanda di recupero password*
- 18 Mail separate
- 18 Approccio trasparente
- 19 Dati personali
- 19 *Foto*
- 19 Geolocalizzazione
- 20 Scelta degli amici
- 21 Bilancio rischi/benefici

23 4. Impostazioni sicure di Facebook

- 23 Dati personali: il minimo indispensabile
- 24 Copia di sicurezza del profilo

25	Navigazione protetta
27	Notifiche di accesso
28	Approvazione degli accessi
28	Password per le applicazioni
29	Sessioni attive
30	Applicazioni
31	Metodi di pagamento
31	Preferenze di privacy
33	Connessioni
33	Funzionamento dei tag
35	Condivisione con applicazioni, giochi e siti
36	Visibilità dei vecchi post
36	Blocco di persone e applicazioni
38	"Antivirus" per Facebook
38	<i>Sharesafe</i>
40	<i>Safego</i>
41	Anonimato tradito dall'indirizzo Facebook
41	Anonimato tradito dall'indirizzo di e-mail

43 5. Comportamenti sicuri in Facebook

43	Attenzione alle richieste d'amicizia
43	Uscite sempre da Facebook correttamente
44	Difendersi da truffe e attacchi
44	<i>Diffidate degli inviti a scaricare programmi</i>
44	<i>Messaggi-truffa da Facebook</i>
45	<i>Attenzione alle pagine di ingresso in Facebook</i>
46	<i>La truffa degli script</i>
47	<i>Clickjacking e likejacking: furto di clic</i>
47	<i>Furto d'identità: il trucco dell'amico in vacanza</i>
48	<i>Applicazioni? Solo se servono davvero</i>
49	<i>Vedersi "da fuori"</i>
49	<i>Rimuovere un tag</i>
50	Un po' di galateo
50	<i>Non sapete chi vi legge</i>
51	<i>Se pubblicate qualcosa, resta su Facebook per sempre</i>
51	<i>L'amico svenduto</i>
51	<i>Occhio alle bufale</i>

- 51 Se viene violato l'account
- 52 Chiudere un account Facebook
- 52 *Disattivazione o eliminazione?*
- 53 *Come disattivare un account*
- 54 *Come eliminare un account*

55 6. Impostazioni sicure di Twitter

- 55 Un po' di terminologia
- 56 Account
- 56 *Geolocalizzazione*
- 57 *Contenuti controversi*
- 57 *Tweet privati*
- 57 *Navigazione protetta*
- 58 Password
- 58 Mobile
- 59 Notifiche
- 59 Profilo e aspetto
- 59 App
- 59 Privacy
- 60 *Privacy degli archivi*
- 60 "Antivirus" per Twitter

63 7. Comportamenti sicuri in Twitter

- 63 Non fidatevi delle identità dichiarate
- 63 Attenti ai tweet dissonanti
- 63 Proteggete la vostra password
- 64 Link brevi ingannevoli
- 64 Cancellazione dei messaggi
- 65 Blocco di tweet e utenti offensivi o truffaldini
- 65 Chiudere un account Twitter