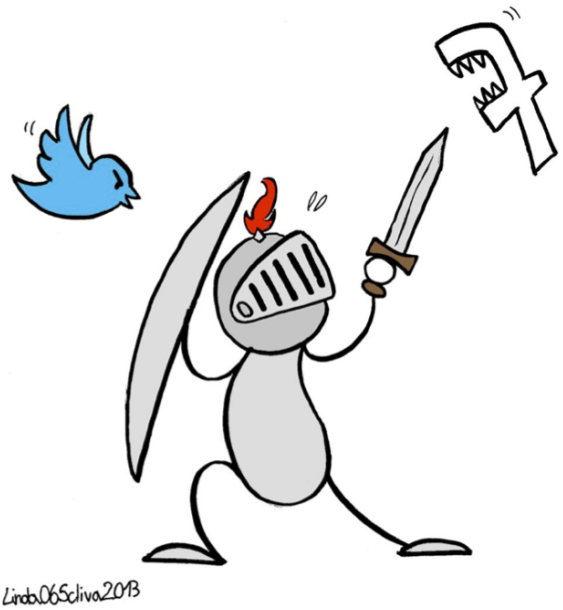
# Facebook e Twitter: manuale di autodifesa

**Paolo Attivissimo**



**Paolo Attivissimo**

# Facebook e Twitter: manuale di autodifesa

Conoscere le reti sociali
per usarle in modo sicuro

**Terza edizione**

Gli aggiornamenti a questo libro
sono disponibili presso
*http://disinformatico.info*

## Permesso d'autore






---

# Indice

# 1. Per chi ha fretta

1. Nei social network è facile fingere di essere qualcun altro e i controlli sono scarsi: non fidatevi di identità non autenticate.
2. Usate uno pseudonimo, anche se è contro le regole del social network, e datelo soltanto agli amici fidati: vi mette al riparo dalle molestie degli sconosciuti e da chi ce l'ha con voi.
3. Accettate richieste d'amicizia soltanto da chi conoscete nella vita reale e verificate di persona la loro identità: meglio avere pochi amici ma buoni.
4. Se possibile, impostate tutto, anche la lista dei vostri amici, in modo che sia visibile soltanto agli amici verificati.
5. Non fidatevi delle promesse di privacy del social network, specialmente per le foto: sono false o comunque si possono aggirare. Lo scopo dei social network non è proteggere i fatti vostri, ma venderli: non vi potete fidare che li custodiscano bene.
6. Presumete che tutto quello che fate su un social network sia visibile a chiunque, compreso il vostro peggior nemico, il vostro ex partner sentimentale, il vostro datore di lavoro, i vostri genitori. Lo è o lo può diventare molto facilmente.
7. Una volta che una cosa finisce su Internet, ci resta per sempre: rimuoverla davvero è impossibile.
8. La gente è molto più crudele di quello che immaginate. Non rendetevi vulnerabili. Siate paranoici.
9. Tutto quello che fate su Internet e nei social network è tracciabile e viene tracciato.
10. Disattivate la geolocalizzazione: serve soltanto ai pubblicitari e ai molestatori.
11. Se una persona o una proposta su un social network sembra troppo bella per essere vera, probabilmente non è vera.
12. 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: di solito sono trappole per rubarvi la password, che va custodita come le chiavi di casa.

## 1.1. 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.

## 1.2. 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.

# 2. *"Autodifesa"*? Sul serio?

Può sembrare eccessivo parlare di *autodifesa* dai social network, come se si trattasse di un nemico o di un aggressore. 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 questi ambienti digitali sono più spavaldi e invadenti, perché sanno (o credono) di essere anonimi e impossibili da rintracciare e possono raccogliere informazioni sulle vittime molto più facilmente.
- 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 e usarli contro di noi.

- Nei social network all'atto pratico non c'è 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.
- L a **disinformazione** grande e piccola (dalle bufale alle tesi di complotto) prospera nei social network: c'è chi la fabbrica e chi la legge e la diffonde per credulità o 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 digitali per disseminare attacchi informatici simili a 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: nel 2011 Facebook dichiarò che venivano *"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 e sulla vendita dei nostri dati personali.
- Da ultima, ma non meno importante, c'è la **privacy**. Gli utenti regalano spontaneamente ai social network un dettagliatissimo elenco delle loro amicizie e parentele, dei loro gusti personali e dei loro spostamenti. La temuta 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 (ma anche di altri paesi).

Per contro, i social network hanno molti **aspetti positivi**, soprattutto in termini di possibilità d'interazione sociale di gruppo, a bassissimo co-

sto, senza barriere architettoniche, senza problemi di distanza e di orari e in molti casi in forma discreta e sostanzialmente anonima. Sono anche una fonte d'informazione e di notizie sempre più popolare.

Di conseguenza non si possono liquidare come mode passeggere: ormai Facebook, tanto per fare un esempio, ha circa 1 miliardo e 230 milioni di utenti attivi.[1] 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.

1 Dato riferito a dicembre 2013 e fornito da Facebook. Con l'espressione *"utente attivo",* Facebook intende un utente che usa il social network almeno una volta al mese.

# 3. 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.

## 3.1. Cosa vuol dire *"social network"*?

Il nome *social network* significa "rete sociale": è un servizio per la 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 nel resto di Internet si interagisce prevalentemente con *informazioni* preconfezionate (enciclopedie come Wikipedia, archivi di foto, musica o video, testate giornalistiche, banche dati, eccetera).

## 3.2. Dispositivi d'accesso

I social network sono accessibili da qualunque computer moderno (non importa se usa Windows, Mac OS X, Linux o altro), di qualunque marca, anche senza dover installare nulla: è sufficiente digitare nel *browser* (il programma di navigazione nelle pagine Web, per esempio Internet Explorer, Chrome, Safari, Mozilla Firefox, Opera) il nome del sito che ospita il social network.

In alcuni casi si può anche scaricare un programma gratuito che consente di interagire con un social network specifico in modo più efficiente o compatto.

Per accedere ai social network si possono usare anche i *tablet*, come per esempio l'iPad di Apple, e gli *smartphone*, ossia i telefonini evoluti (iPhone, Android, Windows Phone) che possono navigare in Internet. Come sui computer, anche su questi dispositivi si possono installare

appositi programmi d'interazione con i social network (le *applicazioni* o *app*). L'uso dei social network tramite dispositivi mobili (principalmente telefonini) è in continua crescita e rappresenta già almeno la metà degli accessi a Facebook e Twitter.

## 3.3. *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 supplementari.

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

## 3.4. *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). Altri social network usano altri termini con lo stesso significato.

Come utenti di un social network, anche voi potete pubblicare degli aggiornamenti nel vostro profilo e permettere agli altri utenti di leggerli, in base alle impostazioni di privacy che avete scelto. Pubblicare un *elemento* (un commento, una battuta, una notizia, una fotografia o un video) si chiama *postare*.

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

I post e i commenti vengono solitamente presentati in ordine cronologico inverso (il primo è il più recente): questa disposizione viene chiamata *diario* (*Timeline*) da Facebook. 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 grosso modo solo i messaggi dell'ultima settimana, se non se ne conosce l'indirizzo esatto o almeno in parte il testo o se non si usano servizi esterni come Topsy.com) e in altri è illimitata (come nel caso di Facebook).

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. Qualche esempio:

- la nascita di un bambino può essere annunciata tramite un 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.

## 3.5. 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 ed è spesso vulnerabile, per cui è opportuno usare queste funzioni con molta cautela e precauzione.

## 3.6. 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*.

## 3.7. Autenticazione

Sia Facebook, sia Twitter offrono l'*autenticazione* degli utenti, ossia attestano che la persona corrispondente a un certo account è veramente chi dice di essere. Gli utenti autenticati sono contrassegnati da un bollino blu e sono pochissimi. Tutti gli altri, per definizione, sono non autenticati e quindi vanno trattati con circospezione. Gli altri social network principali, invece, non offrono forme di reale autenticazione.

In Facebook e Twitter, l'autenticazione non può essere richiesta: sono i gestori di questi social network a decidere di concederla, e lo fanno comunque soltanto per celebrità. giornalisti, politici e marchi e aziende popolari, non per gli utenti comuni.


*Due profili autenticati: l'astronauta lunare Buzz Aldrin su Twitter e l'attrice Lea Michele su Facebook.*

# 4. 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 volume intero), ma darvi gli strumenti di conoscenza necessari per usare questi servizi in maniera sicura. Pertanto non presenterò qui in dettaglio tutte le regole, opzioni e modalità proposte da Facebook e Twitter, ma soltanto quelle attinenti a sicurezza e privacy.

## 4.1. 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 dai minori e anche dai loro genitori ed è 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 di quel paese per l'impostazione giuridica 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, un 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 alla radice, vietando (perlomeno formalmente) 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 americane.

## 4.2. 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, anche se di solito conviene iscriversi inizialmente con uno pseudonimo: potete sempre sostituirlo con il vostro nome vero in un secondo tempo, mentre il contrario non è quasi mai fattibile. Una volta che avete scelto di apparire in un social network con il vostro nome e cognome, è difficilissimo cancellare ogni traccia della vostra identità.

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 trovarvi 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 trovarvi facilmente anche a molestatori, ex partner, creditori e altre persone che forse non vorreste ritrovare.

**Siete davvero sicuri di volervi far trovare?**
**Anche dagli ex partner e dai molestatori?**

L'uso di un nomignolo o di un nome inventato (*nickname* o *nick*) ha il vantaggio di rendervi anonimi e quindi non reperibili da molestatori e simili, ma vi impedisce di farvi trovare anche da chi vorreste che vi trovasse. Si tratta di un anonimato relativo, nel senso che gli amici che vi conoscono sono in grado di dedurre chi siete in base alle amicizie che avete nel social network, ma è un buon modo per difendersi dai molestatori sconosciuti.

La scelta è quindi molto personale, ma va fatta con attenzione, perché una volta che siete su un social network con il vostro vero nome e cognome siete un bersaglio facile.

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

### 4.2.1. 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 sull'identità nei social network 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.

**Non fidatevi dell'identità di chi incontrate sui social network. I controlli di autenticità sono scarsissimi.**

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 (non semplicemente un omonimo, ma qualcuno che fa finta di essere voi). In tal caso potete segnalare questo furto d'identità ai gestori.

## 4.3. Scelta della password

La password è molto spesso la chiave fondamentale per mantenere il controllo del vostro account sui social network. Se qualcuno la indovina o ve la ruba, può impersonarvi e causarvi ogni sorta di imbarazzi e guai. Vi serve, insomma, una password *robusta*:

- **non ovvia** (niente nomi di figli, date di nascita, cantanti preferiti)
- **lunga almeno otto caratteri** (composta magari unendo più parole, come per esempio *ApelleFigliodiApollo*)
- **priva di senso compiuto** (non una singola parola del dizionario)
- **differente per ciascun servizio che utilizzate** (per evitare che basti rubare una sola password per accedere a tutti i vostri dati, dalla mail al conto in banca).

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

- Potete prendere la lettera iniziale di ogni parola di una filastrocca, del titolo della vostra canzone preferita o di una frase descrittiva: per esempio, *"Sotto la panca la capra campa, Sopra la panca la capra crepa"* diventa *"SlplccSlplcc"*.

– Potete aggiungervi alcune cifre della targa della vostra auto o del vostro numero di telefonino o di un altro numero che vi ricordate facilmente.

– Un altro trucco è usare una parola straniera scritta come la si pronuncia (per esempio *soscialnetuorc*) oppure parole gergali o dialettali.

### 4.3.1. Non riciclate le password!

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

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

**Avere la stessa password per mail, social network e altri servizi di Internet è come avere una sola chiave per la casa, l'automobile, la bicicletta e la cassaforte: un enorme aiuto ai ladri.**

### 4.3.2. Come ricordarsi tutte queste password?

La maggior parte degli utenti usa una sola password per tutto, un po' per pigrizia e un po' perché è obiettivamente difficile ricordarsi tante password differenti, ma è un comportamento molto rischioso.

Per evitarlo, potete usare programmi salvapassword che le ricordano per voi proteggendole con una singola password principale, come 1Password (presso Agilebits.com). Ovviamente, però, se qualcuno scopre questa password principale o c'è una falla nel sito che offre il servizio salvapassword, siete a rischio.

Un altro metodo, a bassa tecnologia ma molto affidabile, è usare la classica agendina cartacea tascabile e scrivervi le password usando una regola di cifratura che conoscete soltanto voi (per esempio scrivendo

tutte le password al contrario). Abbiate cura di tenere una copia di quest'agendina in un posto sicuro, per evitare guai in caso di smarrimento.

Una variante più tecnologica è scrivere un documento contenente tutte le vostre password e salvarlo su una penna USB da portare sempre con voi. È meglio usare un formato protetto da una password e dare al documento un nome poco appariscente (per esempio non il classico *password.doc*, ma *listadellaspesa.doc* o *ricettedellanonna.odt*).

Un altro trucco è inserire nella rubrica del proprio telefonino dei nomi di persone inesistenti che sono in realtà le password dei nostri servizi su Internet. Per esempio, potreste registrare in rubrica una finta amica, Francesca Beatrice Pacchioni, e usare le consonanti del suo nome come password per Facebook (*frncscbtrc*). Sapete che è la vostra password di Facebook perché le iniziali dei suoi nomi sono FB.

### 4.3.3. 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, descritta nei capitoli successivi, 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 in inglese 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 e 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 fare una delle seguenti cose:
  - rispondere inviando la vostra password per un controllo (non è vero: se lo fate, inviate la password al malfattore);

- aprire l'allegato che contiene la vostra nuova password (non è vero: l'allegato è in realtà un virus che ruberà la vostra password);
- 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).

**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 programma di navigazione (*browser*) l'indirizzo del social network, per poi accedervi immettendo login e password nella maniera consueta. In alternativa, accedete usando la app del social network, specialmente se usate un tablet o un telefonino. Solo a quel punto potrete fidarvi degli eventuali messaggi d'avviso che compariranno 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, memorizzarlo nei Preferiti del proprio browser oppure usare la app apposita.

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 al social network.

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 non ovvio.** Questo vale anche in caso di furto dell'apparecchio.

## 4.3.4. Domanda di recupero password

Di solito quando vi iscrivete a un social network c'è un'opzione che vi consente di recuperare o reimpostare la password dimenticata se rispondete correttamente a una domanda di cui soltanto voi conoscete 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 è addirittura presente fra i dati che abbiamo pubblicato nel social network. Spesso la domanda riguarda il cognome da nubile della madre, il nome della prima insegnante di scuola o 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 scelto come domanda il nome del proprio cagnolino, notissimo grazie alle riviste di *gossip*) e nel 2008 furono divulgate le mail private della candidata alla vicepresidenza statunitense Sarah Palin (che aveva usato come domanda il luogo in cui aveva conosciuto il marito).

Conviene quindi **immettere una risposta senza senso** (non veritiera) e segnarla da qualche parte, per esempio su un quadernetto delle password d'emergenza, custodito in luogo sicuro.

### 4.3.5. Autenticazione tramite telefonino

Su Facebook e Twitter è inoltre possibile attivare la cosiddetta *autenticazione a due fattori*: in parole povere, se qualcuno vi ruba la password e cerca di usarla su un suo dispositivo, ricevete sul vostro telefonino un codice di sicurezza aggiuntivo, senza il quale l'aspirante intruso non può entrare. Lo può fare soltanto chi conosce la vostra password (primo fattore) e ha accesso al vostro telefonino (secondo fattore).[2]

L'uso di questa protezione aggiuntiva è molto consigliabile, anche se significa affidare al social network un dato personale come il proprio numero di telefonino. Se siete riluttanti a farlo, potete procurarvi un numero prepagato, tenerlo solo per queste funzioni di sicurezza e darlo al social network.

## 4.4. Mail separate

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

Se ci tenete all'anonimato, quindi, vi conviene attivare una casella di 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 mail che contenga il vostro nome e cognome (per esempio *maria.bernasconi@provider.com*, altrimenti ancora una volta diventa inutile adottare pseudonimi, dato che l'indirizzo di mail d'iscrizione è spesso accessibile a chiunque.

2 La disponibilità di quest'opzione varia da paese a paese e a seconda dell'operatore telefonico che usate.

## 4.5. 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 tutte scavalcabili abbastanza facilmente, per cui è assolutamente consigliabile partire da un presupposto completamente diverso: presumere che la privacy nei social network non esista e che tutto quello che vi scrivete e tutte le foto che vi pubblicate siano a portata dei vostri genitori, ex amici, ex partner, datori di lavoro attuali e futuri, forze di polizia, ladri e truffatori. Eviterete imbarazzi dai quali è poi difficile districarsi.

**Date per scontato che tutto quello che fate su un social network sia visibile a chiunque, compreso il vostro peggior nemico.**

## 4.6. Dati personali

**Non date ai social network il vostro 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 che avete preso 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 geografica può essere quella reale, ma è meglio non indicare nulla di più preciso per non dare appigli agli utenti ostili dei social network.

### 4.6.1. Foto

Pensateci bene prima di pubblicare qualunque foto, anche apparentemente innocua e innocente. Per esempio, le fotografie scattate in spiaggia da un'insegnante potrebbero essere viste dai suoi studenti,

con conseguenze facilmente immaginabili. Una fotografia riuscita male o in cui fate una smorfia ridicola potrebbero essere utilizzate per causare imbarazzi sul posto di lavoro o a scuola.


*Come verrà interpretata questa foto da chi la vedrà? Per esempio, da un futuro datore di lavoro, dai compagni di studi o dai colleghi? Esempio reale tratto dalle foto pubbliche presenti in Facebook.*

Tenete presente, inoltre, che molti 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.

Uno degli esempi più assurdi di come la gente spesso pubblica fotografie sui social network senza pensare alle conseguenze è offerto su Twitter da *@needadebitcard*, un account che raccoglie e ripubblica automaticamente tutti i post pubblici degli utenti di Twitter che contengono riferimenti a carte di credito o di debito di cui si stanno vantando.

Spesso questi post includono, in bella vista, una foto che mostra tutti i dati della carta, che possono essere usati da chiunque per commettere frodi. Ne vedete un esempio qui accanto.


*Esempio reale di pubblicazione di dati sensibili senza pensare alle conseguenze, tratto da Twitter.*

### 4.6.2. Geolocalizzazione

Quasi tutti i social network vi permettono di includere automaticamente nei vostri 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 molti 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 forse immaginate) può contenere le coordinate dell'abitazione, vanificando il mascheramento ed esponendo a imbarazzi e disagi.

Le agenzie di pubblicità, inoltre, usano massicciamente la geolocalizzazione per inviare spot pubblicitari su misura per il luogo nel quale si trova l'utente.

La geolocalizzazione automatica di solito è disattivabile in blocco o selettivamente per i singoli post; talvolta è possibile dare delle coordinate false. Facebook, inoltre, rimuove automaticamente dalle immagini tutti i dati di geolocalizzazione incorporati dalla fotocamera o dal telefonino e non li rende accessibili agli utenti (non è dato sapere, tuttavia, se li tenga per sé per i propri scopi).

## 4.7. 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 spesso 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 decisamente opportuno stabilire una regola ben precisa: comunicare con chi si conosce già va benissimo; comunicare con gli sconosciuti è da evitare tassativamente.

**Usare i social network per restare in contatto con gli amici reali va bene; usarli per comunicare con sconosciuti è pericoloso.**

Nei social network occorre stare in guardia in particolare 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.

**Rifiutare le richieste di "amicizia" dagli sconosciuti non è maleducazione: è legittima difesa.**

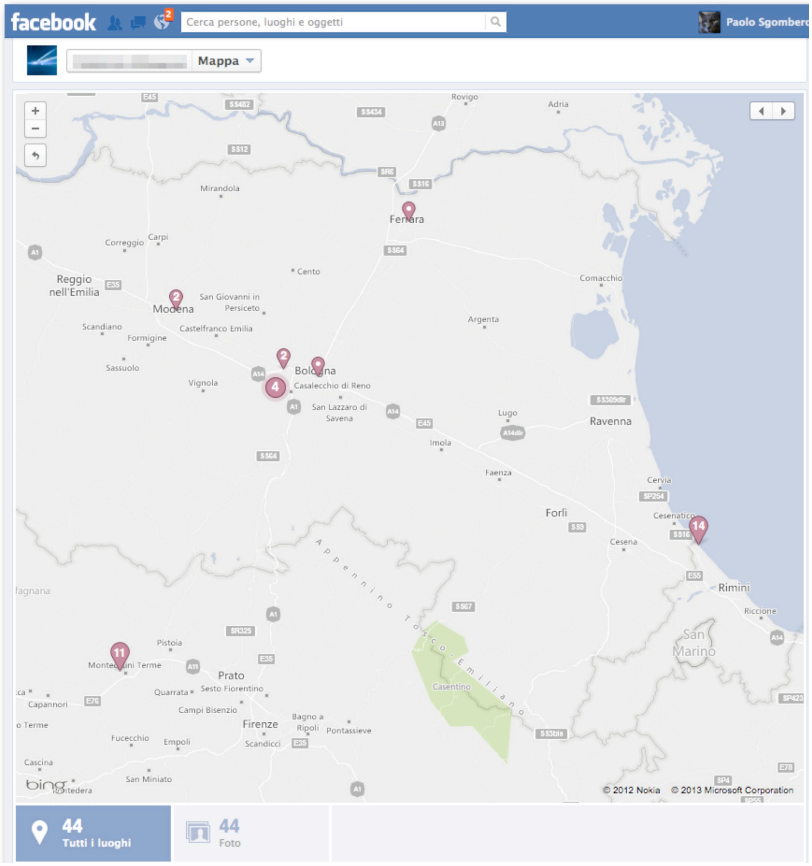
## 4.8. Bilancio rischi/benefici

Non dimenticate che lo scopo reale dei social network è convincerci a condividere con i loro gestori 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 gli scopi dei social network coincidono con i nostri e chiederci sempre se un certo servizio ha più vantaggi che

svantaggi e se ha eventuali funzioni nascoste o poco visibili che potrebbero essere problematiche.

Per esempio, la geolocalizzazione è utile ai gestori dei social network per avere informazioni vendibili sulle tendenze di spostamento dei loro utenti. Non a caso quasi tutti i social network la impostano in modo che sia attiva automaticamente e tocca all'utente scoprire che esiste e come disattivarla.




*Esempio reale di geolocalizzazioni multiple di un utente di Facebook.*

È vero che a volte 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 spesso sfruttabile non solo a fini commerciali, ma anche dagli *stalker*, che possono usarla per pedinarvi comodamente. Siete sicuri che valga davvero la pena di adoperarla?

Un altro esempio è l'elenco degli amici o contatti che abbiamo in un social network: viene spontaneo lasciarlo pubblicamente visibile perché questa scelta non sembra comportare rischi, ma in realtà un elenco pubblico può essere sfruttato dai truffatori e dai ladri d'identità per autenticarsi oppure per intimidire una vittima minacciando di mandare immagini compromettenti a tutti i suoi amici (che conosce appunto tramite l'elenco).

**In un social network non siamo clienti.**
**Siamo il prodotto in vendita.**

# 5.Impostazioni difensive di Facebook

Questo capitolo esplora in dettaglio tutte le impostazioni più importanti di un account Facebook. È scritto presumendo che l'account abbia attivato il Diario, ossia la modalità cronologica, verso la quale Facebook sta progressivamente spingendo gli utenti, e che l'utente usi questo social network tramite un browser su un computer (non tramite l'app di Facebook).

Se non avete ancora attivato il Diario, potete farlo visitando la pagina *Il tuo diario* (*http://www.facebook.com/about/timeline*) e cliccando sul pulsante *Ottieni il diario*. Il Diario di Facebook diventerà pubblico automaticamente dopo sette giorni, ma potete anche renderlo pubblico subito scegliendo l'opzione di pubblicazione immediata che compare sullo schermo.

## 5.1. Indirizzo di mail separato e segreto

Come già accennato, è prudente e preferibile usare per l'account Facebook un indirizzo di mail diverso da quello che usate pubblicamente. Questo rende più difficile il furto di password, perché permette di riconoscere più facilmente i messaggi truffaldini: arriveranno sul vostro indirizzo di mail pubblico, mentre quelli veri (effettivamente inviati dal servizio clienti di Facebook) arriveranno su quello segreto.

Per cambiare l'indirizzo di mail associato a un account e assegnare all'account l'indirizzo segreto:

- cliccate sull'ingranaggio nella barra blu superiore di Facebook;
- scegliete *Impostazioni account*;
- alla riga *E-mail*, cliccate su *Modifica*;
- cliccate su *Aggiungi un altro indirizzo e-mail*;
- immettete l'indirizzo segreto nella casella *Nuova e-mail*;

- disattivate, se non è già disattivata, la casella *Consenti agli amici di includere il mio indirizzo e-mail nel download dello strumento Scarica le tue informazioni*;
- immettete la vostra password di Facebook e cliccate su *Salva modifiche*;
- Facebook manda all'indirizzo di mail segreto un messaggio di verifica: cliccando sul link nella mail, venite portati alla pagina delle impostazioni di Facebook, dove viene indicato che la modifica è andata in porto;
- nella pagina delle impostazioni di Facebook, cliccate sul pulsante accanto all'indirizzo segreto in modo da attivare il pulsante stesso, immettete la password di Facebook e poi cliccate su *Salva modifiche*;
- sempre nella pagina delle impostazioni di Facebook, cliccate di nuovo su *Modifica* alla riga *E-mail*;
- cliccate su *Rimuovi* accanto all'indirizzo di mail originale (non quello segreto), immettete la password di Facebook e cliccate su *Salva modifiche.*


*Un messaggio di verifica per cambio indirizzo di mail in Facebook.*

## 5.2. Dati personali: il minimo indispensabile

Come regola generale, meno dati pubblicate (e quindi regalate a Facebook e a potenziali bulli, molestatori e truffatori, oltre che agli inserzionisti pubblicitari) e meglio è.

**Nulla vieta di immettere in Facebook soltanto nome, sesso, data di nascita e indirizzo di mail da associare al profilo Facebook.** Tutti gli altri dati sono facoltativi.

Molti utenti tutelano la propria privacy immettendo in Facebook informazioni personali fittizie. Questo li mette al riparo non solo dagli abusi degli altri utenti ma anche da possibili errori tecnici o comportamenti scorretti di Facebook**.**

**Immettere dati di fantasia in Facebook per difendere la propria privacy, nonostante le insistenze di Facebook, non è una scelta punibile legalmente.**

Le condizioni d'uso di Facebook esigono l'uso del proprio vero nome e cognome, ma se usate uno pseudonimo non siete punibili dalla legge: avete semplicemente violato le condizioni d'uso del social network e il peggio che vi può capitare è che Facebook vi contesti l'identità e, se non la correggete, vi disabiliti l'account; in ogni caso i controlli sono estremamente rari e superficiali.[3] L'importante è non usare i dati di qualcun altro, perché in questo caso si potrebbe configurare il reato di furto d'identità.

Potete accedere ai dati personali del vostro account e modificarli cliccando sul vostro nome nella barra superiore di Facebook e poi su *Aggiorna informazioni*.

## 5.3. Privacy dei dati personali

Ciascuna delle informazioni personali che immettete in Facebook ha un proprio livello di privacy e visibilità regolabile. Per regolarlo si accede alla sezione *Informazioni* cliccando sul vostro nome nella barra superiore di Facebook e poi cliccando su *Aggiorna informazioni*.

**I dati personali immessi in Facebook non devono essere pubblicamente visibili a chiunque senza aver ottenuto la vostra "amicizia".**

3 A ottobre 2011 Facebook mi scrisse contestando la mia *vera* identità nel social network, dichiarando che *Attivissimo* non poteva essere il mio vero cognome (lo è; non è un nome d'arte) e minacciando di disabilitarmi l'account. Risposi "confessando" che il mio vero cognome era *Sgomberonte* e Facebook lo accettò senza batter ciglio.

Impostare i propri dati personali in modo che siano visibili solo agli "amici" serve a impedire che ficcanaso o truffatori possano leggerli.

Si tratta comunque di un deterrente, non di una garanzia: Facebook ogni tanto commette errori tecnici che rendono pubblici dati impostati come privati, e comunque niente impedisce a un vostro "amico" di Facebook di copiare i vostri dati personali privati, foto comprese, e condividerli anche con persone che non conoscete. Prendete quindi l'abitudine di mettere su Facebook soltanto parole e immagini che non vi causeranno imbarazzi o problemi se diventano pubbliche.

### 5.3.1. Sezione *Lavoro e istruzione*

Se siete lavoratori dipendenti, l'**indicazione del posto di lavoro corrente** 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 se concedere visibilità a questo dato personale o se non indicarlo del tutto. Lo stesso genere di cautela va adottato per l'indicazione dei lavori precedenti.

Anche **l'indicazione della scuola frequentata è da evitare:** i molestatori usano queste informazioni per selezionare le vittime potenziali.

### 5.3.2. Sezione *Relazioni e familiari*

L'indicazione della situazione sentimentale può essere oggetto di vanto, ma può anche causare imbarazzi e si presta ad abusi, per cui è prudente ometterla: i vostri amici (quelli veri) già la conoscono e non c'è quindi molto bisogno di sbandierarla, col rischio di farla sapere a malintenzionati.

Indicare le parentele significa regalare il proprio albero genealogico a Facebook e ai suoi clienti e inserzionisti (e anche ai ficcanaso generici, se lo rendete pubblico); non sembra esserci alcun vantaggio per gli utenti nel fornire questi dati.

Uno scenario di truffa sempre più frequente basato su questi dati è quello del "cugino d'America": la vittima viene contattata da una persona che afferma di essere un lontano parente ma in realtà è un truffatore. Il criminale riesce a conquistarsi la fiducia della vittima perché dimostra di conoscere i dettagli di numerosi parenti, ma in realtà ha preso tutte queste informazioni da Facebook.

### 5.3.3. Sezioni *Su di te* e *Citazioni preferite*

Questi spazi sono a contenuto libero: valgono le consuete raccomandazioni di non includere informazioni troppo personali e di renderle comunque visibili soltanto agli amici.

### 5.3.4. Sezione *Città*

L'indicazione della città attuale di residenza offre a Facebook un riferimento geografico per le campagne pubblicitarie mirate locali. Se indicate la vostra città attuale effettiva, riceverete annunci di eventi locali che potrebbero interessarvi: per contro, se immettete una città attuale fasulla (o non immettete nulla) renderete più difficile l'attività dei molestatori d'ogni genere.

La città natale è un dato meno problematico, ma può comunque servire a identificarvi e distinguervi. Se ci tenete all'anonimato, non indicate nessun dato.

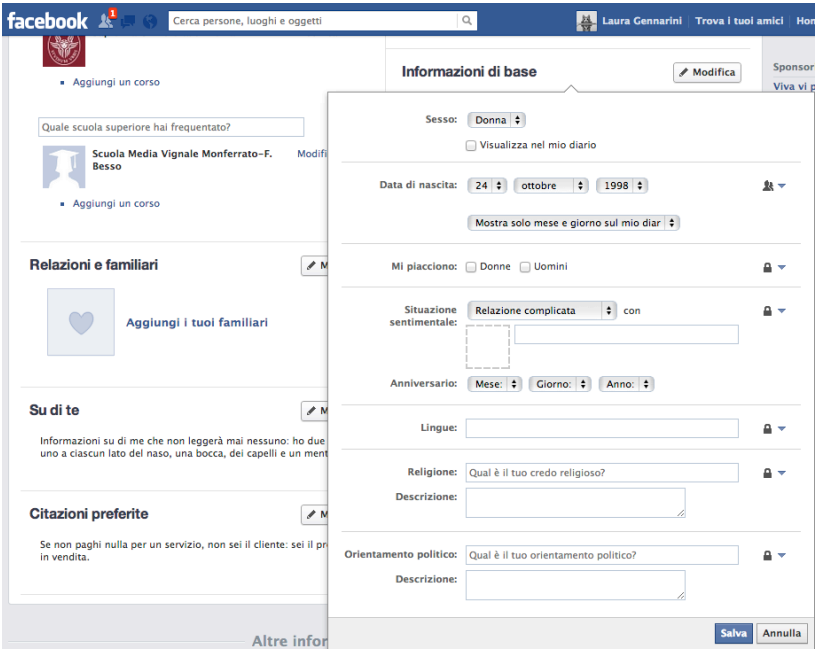
### 5.3.5. Sezione *Informazioni di base*

Il **sesso** è un dato obbligatorio, ma potete nasconderlo (ed è opportuno farlo, particolarmente per i minorenni e per le donne) disattivando la sua casella *Visualizza 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.

È importante **non rendere pubblica 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 farvi gli auguri nel giorno sbagliato se non conoscono la data vera e si appoggiano a Facebook per saperla.

Specialmente nel caso di minorenni, è consigliabile **non rendere visibile a nessuno l'anno di nascita** (che comunque è necessario immettere). Il giorno e il mese di nascita possono essere lasciati visibili agli amici per consentire loro di fare gli auguri di compleanno, mentre l'anno si nasconde usando l'opzione *Mostra solo mese e giorno sul mio diario*.

Valutate con attenzione se è il caso di affidare a Facebook il vostro **orientamento sessuale, politico o religioso** e i vostri **legami sentimentali**. In molti casi queste preferenze personali possono essere controverse oppure oggetto di scherno, molestia o bullismo.




*Impostazioni sicure delle informazioni personali.*

## 5.3.6. Sezioni *Informazioni di contatto* e *Storia per anno*

Gli **indirizzi di mail** (sia quello segreto, sia quello assegnato automaticamente da Facebook, che è del tipo *nome.cognome@facebook.com*) vanno nascosti scegliendo il livello massimo di privacy, vale a dire *"Solo io"*, e l'opzione *Non visibile sul diario*. Questo serve per non regalarli a curiosi, scocciatori e spammer.

L'indicazione del **numero di telefono cellulare** è necessaria soltanto se si intende usare Facebook sul telefonino o se si attivano le notifiche e conferme di sicurezza tramite SMS. In ogni caso è opportuno tutelare questo dato con un livello alto di privacy, rendendolo visibile per esempio solo a un gruppo selezionato di persone oppure scegliendo l'opzione *Solo io*.

Il **numero di telefono fisso** e il **nome utente di messaggistica istantanea** non sono indispensabili. Se volete immetterli, valutate se è opportuno limitarne la visibilità usando un livello alto di privacy. Potete modificare il livello di privacy rispetto al valore predefinito (*Amici*) soltanto se immettete un numero, anche fittizio (diversamente Facebook sembra accettare la modifica ma poi reimposta il valore predefinito quando cliccate su *Salva*).

L'**indirizzo di casa o di lavoro non va mai immesso**. Il rischio d'abuso e di truffa o molestia è troppo alto e non è giustificato da nessun vantaggio.

I dati del **sito Web** possono essere immessi se ne avete uno da pubblicizzare; a parte questo caso (nel quale rinunciate inevitabilmente all'anonimato eventualmente desiderato) non c'è alcun motivo di darli a Facebook o renderli pubblici.

La ***Storia per anno*** è una biografia che in parte viene generata automaticamente attingendo agli altri dati che immettete in Facebook. A meno che vogliate farvi trovare da ex colleghi con i quali avete condiviso un luogo di lavoro o da ex compagni di studi che hanno frequentato i vostri stessi istituti, non c'è motivo di immettere queste informazioni (utilissime invece al reparto marketing di Facebook) o di renderle visibili al di fuori della cerchia degli amici.

## 5.3.7. Sezioni *Film, Programmi TV, Musica, Libri*

Queste sezioni vi spingono a dichiarare e condividere i vostri gusti culturali e d'intrattenimento selezionando i film, i programmi televisivi, la musica e i libri che vi piacciono cliccando sui rispettivi pulsanti *"Mi piace":* non è opportuno rendere accessibili a tutti queste informazioni e di norma conviene lasciarle visibili soltanto agli amici.

A differenza di molte altre parti di Facebook, la privacy dei *"Mi piace"* di tutte queste sezioni si imposta cliccando sull'icona di matita situata a destra del titolo della rispettiva sezione e non imposta la visibilità della sezione ma soltanto quella dei suoi *"Mi piace"*. Anche cliccando su *Modifica sezioni* e nascondendole tutte, le loro informazioni potranno continuare ad apparire nel Diario e altrove su Facebook.

## 5.3.8. Sezioni *Foto, Amici, Luoghi* e *"Mi piace"*

La **sezione Foto** elenca le fotografie che avete pubblicato e quelle eventualmente nascoste.

La **sezione Amici** visualizza l'elenco degli "amici" (nel senso in cui Facebook usa questo termine) e permette di gestire i livelli di "amicizia". L'icona di matita accanto al titolo della sezione regola parzialmente la privacy di quest'elenco, che non dovrebbe mai essere pubblicamente visibile, in modo da ostacolare ficcanaso e ladri d'identità (che usano spesso i nomi dei vostri amici per carpire la vostra fiducia). Le amicizie restano comunque parzialmente visibili altrove su Facebook, ma perlomeno non offrite a tutti la lista completa bell'e pronta.

La **sezione Luoghi** include le località che avete citato o immesso in Facebook e la sua privacy non è modificabile da qui.

La **sezione "Mi piace"** permette di definire chi potrà vedere che abbiamo cliccato *"Mi piace"* su un oggetto o un concetto in base alla sua categoria. Per esempio, si possono rendere visibili soltanto agli amici i *"Mi piace"* riguardanti il cibo e rendere invisibili quelli riguardanti lo sport o altri interessi. Tutti i *"Mi piace"* restano comunque visibili ai dipendenti di Facebook e vengono utilizzati per catalogare i vostri gusti e analizzare la vostra personalità.

## 5.4. Impostazioni generali dell'account

Potete accedere a queste impostazioni cliccando sull'icona dell'ingranaggio che si trova a destra nella barra superiore della schermata di Facebook e scegliendo la voce *Impostazioni account*.

### 5.4.1. Sezione *Generale*: impostazioni generali dell'account

In questa sottosezione delle Impostazioni account dovete prendere delle decisioni molto importanti per la vostra identità e reperibilità su Facebook. Purtroppo la terminologia di Facebook non è sempre molto chiara e va capita bene per evitare passi falsi. Ecco le voci significative dal punto di vista della privacy e della sicurezza.

#### 5.4.1.1. Nome

Qui definite il vostro **nome pubblico** su Facebook: quello con il quale vi farete conoscere sul social network. Potete modificare questo nome pubblico anche ripetutamente (ma non all'infinito). Potete anche includere un *nome alternativo* (di solito un nomignolo o un appellativo) e scegliere se renderlo visibile o meno nel vostro profilo.

Le regole di Facebook vogliono che usiate il vostro nome e cognome effettivi, ma se volete tutelare la vostra privacy e usare Facebook in modo anonimo dovete immettere dati diversi da quelli reali.

**Pensateci bene prima di usare il vostro vero nome e cognome su Facebook. Usare uno pseudonimo aiuta a proteggersi dai molestatori e dai ficcanaso.**

### 5.4.1.2. Nome utente

Il **nome utente** è diverso dal nome pubblico, è modificabile una sola volta e di norma ha il formato *nome.cognome*, ma in caso di omonimia è necessario modificarlo, aggiungendo per esempio dei numeri, per renderlo unico.

Il nome utente determina l'**indirizzo abbreviato** del vostro profilo Facebook, che è del tipo *www.facebook.com/nome.cognome*, e anche il vostro indirizzo di mail presso Facebook, che è del tipo *nome.cognome@facebook.com* (con eventuali numeri in coda per renderlo unico in caso di omonimia).

Occorre fare molta attenzione alla differenza fra *nome* e *nome utente* nella terminologia di Facebook. Se cambiate il vostro *nome*, per esempio per smettere di usare il vostro vero nome e cognome, tenete presente che il *nome utente* non cambia automaticamente di conseguenza, ma va modificato a mano, altrimenti mantiene il vostro nome e cognome precedenti e li usa come indirizzo abbreviato e come indirizzo di mail.

Per esempio,:

- se l'utente Giuditta Corda si è iscritta a Facebook con il proprio nome e cognome, il suo *nome utente* le assegna un indirizzo abbreviato *www.facebook.com/giuditta.corda* e un indirizzo di mail *giuditta.corda@facebook.com*;
- se Giuditta modifica il proprio *nome* in *Gianna Sgomberonte* per rendersi anonima, il suo indirizzo abbreviato su Facebook rimane comunque *www.facebook.com/giuditta.corda* e il suo indirizzo di mail nel social network continua a essere *giuditta.corda@facebook.com*, tradendo quindi la sua vera identità. Giuditta deve quindi cambiare anche il proprio *nome utente*.


*Giuditta Corda ha cambiato il proprio nome in Gianna Sgomberonte, ma l'indirizzo abbreviato del suo profilo e l'indirizzo di mail rivelano il suo vero nome.*

### 5.4.1.3. E-mail

Qui viene indicato l'indirizzo di mail che avete usato per attivare l'account. È possibile aggiungere un altro indirizzo di mail e renderlo *principale*, cioè usarlo per le comunicazioni da parte di Facebook.

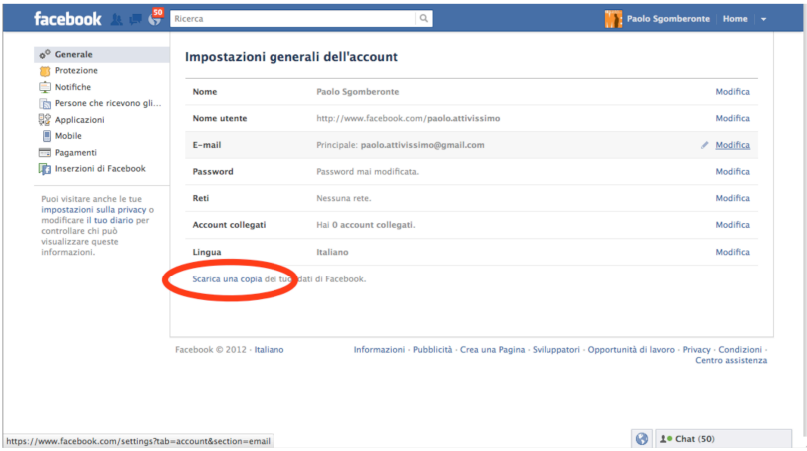
Il significato della casella *Consenti agli amici di includere il mio indirizzo e-mail nel download dello strumento Scarica le tue informazioni* non è intuitivo e richiede una spiegazione. In sostanza, ciascun utente può scaricare da Facebook una copia dei contenuti che ha caricato e delle conversazioni fatte in *chat*; se questa casella è attivata, quando i vostri amici scaricano questa copia dei propri contenuti, la copia include anche il vostro indirizzo di mail. **Se volete il massimo della privacy, non attivate questa casella.**

### 5.4.1.4. Scarica una copia dei tuoi dati di Facebook (copia d'archivio del profilo)

In caso di intrusione da parte di un vandalo 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 d'archivio di tutti i dati che avete immesso nel vostro account Facebook.

Per creare questa copia cliccate su *Scarica una copia dei tuoi dati di Facebook*. Nella schermata successiva che compare, cliccate su *Avvia il mio archivio* e di nuovo su *Avvia il mio archivio*. La procedura non è immediata: verrete avvisati via mail quando la copia sarà pronta per essere scaricata.

Questa copia d'archivio contiene quasi tutto quello che avete pubblicato o condiviso su Facebook e comprende anche i contenuti privati: l'elenco completo dei contenuti viene aggiornato frequentemente ed è presso *www.facebook.com/help/405183566203254*.




*Copia d'archivio del profilo di Facebook.*

**Queste copie vanno custodite con molta attenzione:** chiunque riesca a leggerle ha accesso a *tutte* le vostre informazioni personali condivise su Facebook.

## 5.4.2. Sezione *Protezione*: impostazioni di protezione

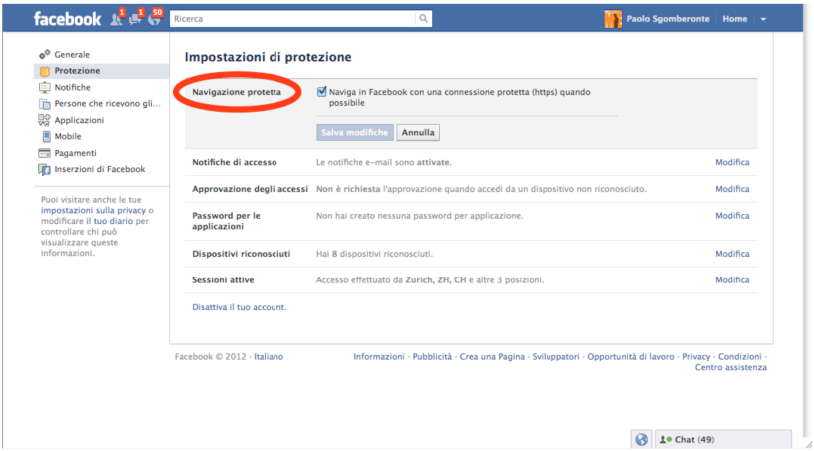
### 5.4.2.1. Navigazione protetta

Vi conviene decisamente attivare l'opzione *Naviga in Facebook con una connessione protetta (https) quando possibile*. Se non lo fate e vi collegate a Facebook usando una rete locale (specialmente se WiFi, cioè senza fili), come può capitare in casa, in ufficio o in albergo, gli altri utenti della stessa rete possono facilmente **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 di postare 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, FaceNiff o WireShark, che sono installabili su qualunque computer e molti dispositivi portatili (tablet e smartphone) e consentono di intercettare i dati che circolano sulla rete locale (WiFi o cablata) e di analizzarli dettagliatamente. Quest'analisi permette poi di sostituirsi almeno temporaneamente all'utente legittimo.

Contro questo genere d'intrusione Facebook offre appunto la *navigazione protetta*: cliccate su *Modifica* in corrispondenza della riga denominata *Navigazione protetta, a*ttivate 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*.

Non è un rimedio perfetto, perché con i programmi-spia opportuni è comunque possibile prendere il controllo di una sessione Facebook anche quando quest'opzione è attiva, ma è meglio di niente e di certo rende più difficile il lavoro di un eventuale intruso.




*Attivazione della navigazione protetta in Facebook.*

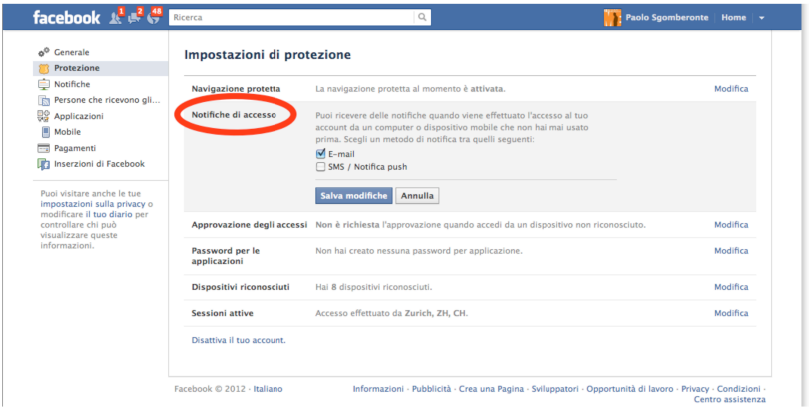
La precisazione *"quando possibile"* sottolinea infatti un limite importante di quest'impostazione: alcuni metodi di accesso (per esempio le "app" per telefonini) potrebbero non gestire la navigazione protetta. Usandole, quindi, la vostra attività su Facebook sarebbe intercettabile. Verificate che la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

**Accedete sempre a Facebook usando *https://*. Se non c'è la S, la connessione è molto insicura e il rischio di farsi rubare l'account è maggiore.**

La navigazione protetta non va interpretata come un sistema contro le intercettazioni da parte delle autorità (per esempio da parte della polizia), ma soltanto 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.

### 5.4.2.2. Notifiche di accesso




*Notifiche di accesso in Facebook.*

Le *notifiche di accesso* sono avvisi che ricevete via mail o SMS se viene tentato un accesso al vostro profilo Facebook con un dispositivo o un programma che non avete autorizzato. Potete infatti definire quali specifici computer, telefonini o tablet e quali programmi volete autorizzare all'accesso al vostro profilo: se qualcuno prova 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 modificabile dei dispositivi e programmi autorizzati è alla voce *Dispositivi riconosciuti* di questa stessa sezione *Protezione*.

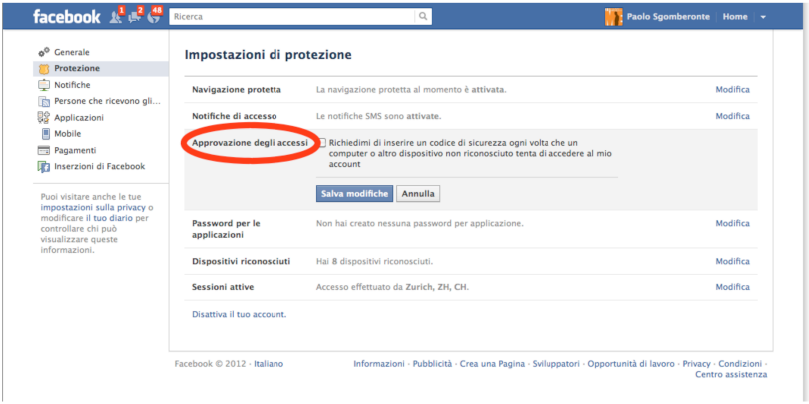
**È consigliabile attivare queste notifiche di accesso** cliccando su *Modifica* alla riga denominata *Notifiche di accesso*.

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.

Per ricevere le notifiche via SMS occorre affidare a Facebook un numero di cellulare, se non lo avete già fatto. Il numero verrà indicato nelle informazioni di contatto, per cui impostate il suo livello di privacy andando al vostro profilo, scegliendo *Aggiorna* informazioni e accedendo a *Informazioni di contatto*.

### 5.4.2.3. Approvazione degli accessi

Se avete immesso in Facebook un numero di telefonino e usate Facebook su quel telefonino, potete attivare quest'opzione per ricevere SMS un codice di sicurezza supplementare: se qualcuno tenterà di accedere al vostro account da un dispositivo o da un browser che non avete autorizzato, dovrà conoscere e immettere questo codice oltre alla consueta password. Questo rende molto più difficili i furti di account.




*Approvazione degli accessi in Facebook.*

Naturalmente quel *"qualcuno"* potreste anche essere voi, per esempio se state usando un dispositivo nuovo o un browser diverso dal solito, per cui non è detto che quest'allarme indichi un'intrusione.

Normalmente questa protezione non si attiva subito: entra in vigore a tutti gli effetti soltanto dopo una settimana che l'avete richiesta e per i primi sette giorni rimane disabilitabile anche se non avete accesso al telefonino al quale avete chiesto a Facebook di inviare il codice. Se la volete attivare subito, attivate la casella *No grazie, richiedi subito un codice* quando impostate l'approvazione degli accessi.

### 5.4.2.4. Generatore di codici

Questa funzione è legata all'Approvazione degli accessi e all'uso di Facebook sul telefonino. Il generatore di codici è un sistema di autenticazione presente nell'applicazione Facebook per smartphone e tablet. Normalmente funziona dietro le quinte senza richiedere l'interazione dell'utente, per cui non è necessario descriverne il funzionamento in dettaglio.

### 5.4.2.5. Password per le applicazioni

Alcune applicazioni interne 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 soltanto in un numero abbastanza limitato di situazioni. Se non usate le applicazioni interne di Facebook (giochi e simili), non avete bisogno di quest'impostazione.

Occorre per prima cosa cliccare su *Modifica* alla riga *Password per le applicazioni* e poi cliccare 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.

### 5.4.2.6. Contatti fidati

In caso di problemi nell'accesso al vostro account (per esempio in seguito a un furto di password o se avete dimenticato la vostra password), potete chiedere aiuto ai *contatti fidati*, ossia altri utenti di Facebook di cui vi fidate assolutamente.

Potete sceglierne da tre a cinque: saranno custodi di codici di sicurezza che vi forniranno se glieli chiedete e che vi permetteranno di accedere di nuovo al vostro account. Scegliete quindi con attenzione questi contatti e assicuratevi che siano capaci di verificare la *vostra* identità quando li contattate chiedendo i codici.

### 5.4.2.7. Dispositivi riconosciuti

Questa voce è collegata alla precedente voce *Notifiche di accesso* della stessa sezione *Protezione* ed elenca i dispositivi e i programmi che avete preautorizzato a usare il vostro account Facebook.

Se accedete all'account da uno di questi dispositivi, non vi verrà chiesta alcuna conferma di autorizzazione e non vi verrà mandata alcuna noti-

fica. In sostanza, **qui devono essere indicati i dispositivi che usate normalmente per accedere all'account Facebook.**

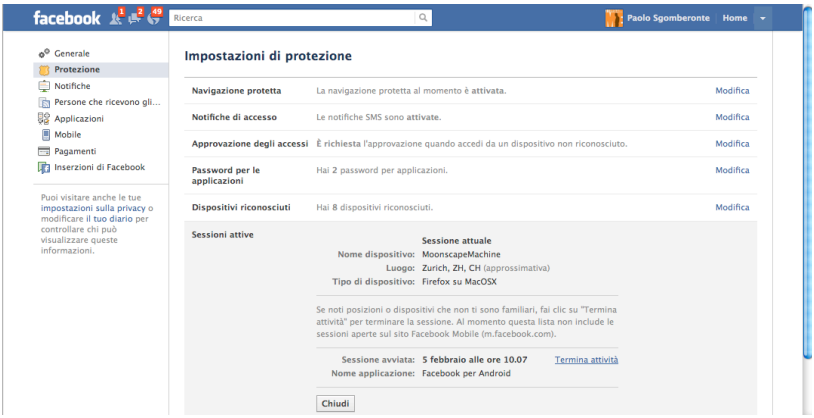
Se volete togliere l'autorizzazione a uno dei dispositivi elencati, per esempio perché l'avete perso, regalato, venduto, rotto o sostituito, potete toglierlo da quest'elenco cliccando su *Rimuovi*. In questo modo, se il dispositivo è finito in mani inaffidabili, non potrà essere usato per accedere al vostro account Facebook senza la vostra approvazione.

### 5.4.2.8. 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 accede a questa voce delle impostazioni dell'account 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.*

Va sottolineato che questo blocco non sempre funziona alla perfezione talvolta le sessioni restano aperte o perlomeno visibili. In ogni caso è meglio di niente e vale la pena di provarlo.

#### 5.4.2.9. Disattiva il tuo account

Questa voce consente di disattivare l'account, ossia sospenderne la visibilità agli altri utenti. Vista l'importanza di una funzione di questo genere, verrà descritta in dettaglio nel capitolo 10.

### 5.4.3. Sezione *Privacy* (impostazioni sulla privacy e strumenti)

#### 5.4.3.1. Visibilità dei nuovi post

In *Chi può vedere le mie cose?*, la sezione *Chi può vedere i tuoi post futuri?* permette di definire quale livello di privacy automatico avranno tutti gli elementi che pubblicherete: se vi dimenticate di impostare la privacy individuale di un elemento, quell'elemento assumerà automaticamente il livello che scegliete qui.

Per esempio, se volete che tutte le foto che caricate su Facebook siano private salvo vostra decisione contraria, potete scegliere qui fra:

- *Pubblica*: tutto quello che postate su Facebook sarà automaticamente visibile a chiunque;
- *Amici di amici*;
- *Amici*;
- *Amici tranne conoscenti*;
- *Solo io*;
- *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.

Questo livello predefinito è utile anche per le applicazioni Facebook che non consentono di definire la privacy di un singolo elemento pubblicato attraverso di esse.

**Queste impostazioni non vanno considerate come una garanzia assoluta:** infatti anche gli elementi privati possono comunque essere

copiati, ripubblicati e resi visibili a chiunque da chi è autorizzato inizialmente a vederli. Lo scenario tipico è questo: lei manda foto sexy a lui, impostandole come private; lui fa una copia delle foto e le manda a tutti i propri amici. Succede spesso, purtroppo.

Inoltre **molti elementi, come le fotografie, hanno anche un link alternativo nascosto** ma facilmente rivelabile, **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 più consigliabile per quest'impostazione è *Pubblica* per i maggiorenni e *Amici di amici* per i minorenni: può sembrare un controsenso, ma in realtà 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 moderazione e alla riflessione.**

### 5.4.3.2. Visibilità dei vecchi post

Le *Impostazioni sulla privacy*, nella sezione *Chi può vedere le mie cose?*, includono la sottosezione *Vuoi limitare il pubblico dei post che hai condiviso con gli amici degli amici o con il pubblico?*, che permette di ridurre in blocco la visibilità di tutti i post già pubblicati, rendendoli visibili soltanto agli amici e alle persone taggate (e ai loro 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, gli atteggiamenti 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 su *Limita i post passati* e sul pulsante *Solo vecchi post* di quest'opzione e poi vi pentite, dovrete modificare a mano la visibilità di ciascun post.

### 5.4.3.3. Chi può contattarvi per richieste d'amicizia e messaggi?

Per tenere a bada i molestatori e i ficcanaso potete impostare le due voci dell'opzione *Chi può contattarmi?* in modo che soltanto gli amici di amici, anziché tutti, possano mandarvi una richiesta di amicizia o un messaggio via Facebook.


*Scelta di chi può inviarvi richieste di amicizia.*

### 5.4.3.4. Chi può cercarvi usando il vostro indirizzo di mail e numero di telefono?

Alla voce *Chi può cercarmi?* potete decidere chi vi può trovare in Facebook immettendo il vostro indirizzo di mail (in *Chi può cercarti utilizzando l'indirizzo e-mail che ha fornito?*) o il vostro numero di telefonino (o meglio, l'indirizzo e il numero che avete affidato a Facebook). L'impostazione consigliabile è solitamente *Amici* per entrambi, a meno che ci teniate a farvi trovare da chiunque.

### 5.4.3.5. Visibilità nei motori di ricerca

Qui potete decidere se i contenuti pubblici del vostro profilo Facebook sono reperibili attraverso i motori di ricerca (Google, Bing, Yahoo e simili). Per impostazione predefinita, Facebook consente questa reperibilità soltanto dopo che l'utente ha compiuto 18 anni (in base alla data di nascita immessa in Facebook).

Se ci tenete alla privacy, è sconsigliabile attivare questa visibilità.

### 5.4.4. Sezione *Diario e aggiunta di tag*

Qui potete definire varie restrizioni del vostro Diario, come per esempio chi ha il permesso di scriverci dentro e di leggerlo. Potete anche scegliere come gestire i *tag*, ossia le identificazioni del vostro volto in Facebook, fatte automaticamente dal social network oppure manualmente dagli utenti (identificare in questo modo un utente si dice *taggare*). I tag sono molto utili come strumento di socializzazione e condivisione, ma si prestano anche a molti scherzi pesanti e a molestie e rendono molto più facile a chiunque capire chi siete.

Queste sono le impostazioni consigliate:

- ***Chi può scrivere sul tuo diario?*** *Solo io.* Serve per evitare atti vandalici e scherzi.
- ***Vuoi controllare i post in cui ti taggano gli amici prima che vengano visualizzati sul tuo diario?*** *Sì*. In questo modo potrete filtrare preventivamente eventuali "taggaggi" inopportuni, indesiderati o imbarazzanti.
- ***Chi può vedere i post in cui sei taggato sul tuo diario?*** *Amici*. Questa scelta è un compromesso ragionevole se la aggiungete, come è opportuno fare, al fatto che controllate preventivamente tutti i post in cui siete taggati.
- ***Chi può vedere cosa pubblicano gli altri sul tuo diario?*** *Solo io.* Si tratta di una misura di ulteriore precauzione, visto che comunque nessuno tranne voi dovrebbe poter pubblicare sul vostro diario. Meglio avere due protezioni che una sola.
- ***Vuoi controllare i tag aggiunti dai tuoi amici ai tuoi post prima che vengano visualizzati su Facebook?*** *Sì*. Serve a evitare, anche qui, scherzi e vandalismi.
- ***Quando qualcuno ti tagga in un post, vuoi poter aggiungere dei destinatari se non sono già inclusi nel pubblico?*** *Solo io*. L'impostazione predefinita, *Amici*, significa che se qualcuno vi tagga in una foto, la foto diventa visibile ai vostri amici, e questo può causare facilmente imbarazzi e si presta a molestie e scherzi pesanti.
- ***Chi vede i suggerimenti dei tag quando vengono caricate foto che ti assomigliano?*** *Nessuno* oppure *Solo io*. Facebook usa il riconoscimento automatico dei volti per proporre di taggarvi quando crede di avervi riconosciuto in una foto; qui, se siete maggiorenni, potete scegliere a chi verranno mostrate queste proposte.


*Impostazioni raccomandate del Diario e dei tag.*

## 5.4.5. Sezione *Blocco*

La *Lista limitata* offerta in questa sezione permette di bloccare l'accesso di uno o più amici ai vostri contenuti accessibili agli amici. È una funzione che può rivelarsi utile per esempio se volete impedire a una persona alla quale avete dato l'amicizia di leggere i vostri contenuti riservati agli amici ma non volete togliere l'amicizia a quella persona.

Le funzioni più importanti della sezione *Blocco*, però, riguardano le possibilità di bloccare varie cose:

- gli utenti indesiderati e gli scocciatori;
- gli inviti a usare applicazioni che vi arrivano da una persona specifica;
- gli inviti a eventi che vi arrivano da una persona specifica;
- le applicazioni indesiderate.

Per attivare questi blocchi è sufficiente immettere rispettivamente il nome o l'indirizzo di mail dell'utente da bloccare o di cui volete bloccare gli inviti a eventi oppure il nome di un'applicazione che desiderare bloccare.

### 5.4.6. Sezione *Notifiche*

Qui scegliete in pratica quanto volete che Facebook vi assilli con le sue *notifiche* (avvisi che è successo qualcosa): per esempio, potete attivare o disattivare l'avviso sonoro emesso in caso di ricezione di una notifica e potete scegliere quali notifiche ricevere via mail o sul telefonino.

Per la ricezione via mail è consigliabile attivare l'opzione *Solo le notifiche sul tuo account, su sicurezza e privacy* per non essere sommersi di mail. in Facebook ci sono infatti ben 140 tipi diversi di notifica via mail.

Le *Notifiche push* riguardano l'uso eventuale di Facebook su dispositivi mobili (smartphone e tablet) e vanno impostate nell'applicazione Facebook presente su questi dispositivi, se li usate.

La notifica alla voce *Attività che ti riguardano* è sempre attiva, in modo da essere avvisati quando qualcuno vi tagga in una foto oppure commenta un vostro post.

Potete inoltre impostare le notifiche degli aggiornamenti pubblicati dagli amici più stretti, dei gruppi e delle applicazioni interne di Facebook (giochini e simili), scegliendo se riceverle sia quando consultate Facebook sia via mail oppure soltanto quando entrate nel social network. Potete anche scegliere di non riceverle mai.

Dato che alcune applicazioni interne di Facebook sono poco rispettose della privacy e possono postare automaticamente sul vostro profilo, facendovi diventare sponsor pubblicitari involontari, vi conviene tenere attive le notifiche per la voce *Richieste e attività delle applicazioni*.

### 5.4.7. Sezione *Per cellulare*

Qui gestite l'eventuale numero di telefonino associato all'account: potete indicarne anche più di uno oppure rimuovere quello esistente.

L'opzione *Attiva SMS* serve per usare Facebook tramite SMS: consente per esempio di aggiornare il proprio stato o di mandare e ricevere messaggi e post altrui come SMS, così anche chi non ha un telefonino evoluto (*smartphone*) può usare Facebook mentre è in giro. Tuttavia l'opzione non è disponibile in alcuni paesi (manca in Svizzera, per esempio, mentre in Italia c'è) e con alcuni operatori telefonici.

Se smarrite il telefonino, cliccate su *Hai perso il telefono* e poi su *Esci sul telefono*: si chiuderà l'app Facebook sul cellulare. Per riaprirla occorrerà digitare la password dell'account, così se qualcuno vi ha rubato il telefonino troverà difficile rubarvi anche l'account Facebook e magari ricattarvi con la minaccia di pubblicare le vostre foto private.

### 5.4.8. Sezione *Persone che ti seguono*

Se volete che i vostri post siano leggibili da chiunque senza dover chiedere la vostra amicizia, per esempio per diffondere notizie riguardanti la vostra attività pubblica o commerciale, potete scegliere in questa sezione l'opzione *Tutti*. In questo modo chi vuole seguire i vostri post deve soltanto cliccare *Segui* nel vostro Diario (può comunque chiedervi l'amicizia; in tal caso vi seguirà automaticamente) e vedrà i vostri post apparire nella sua sezione *Notizie* di Facebook.

Se non avete esigenze di visibilità pubblica, la scelta prudenziale è *Amici*.

### 5.4.9. Sezione *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.

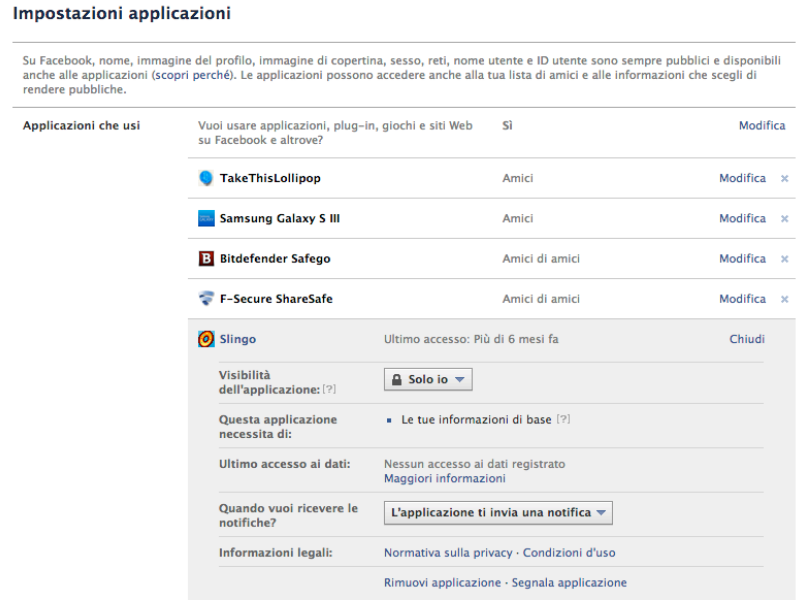
Per disabilitare un'applicazione che non desiderate più è sufficiente usare questa sezione: otterrete l'elenco delle applicazioni che avete autorizzato (consapevolmente o meno) a interagire con il vostro account.

Cliccando su *Modifica* accanto a ciascuna applicazione potete:

- rimuoverla (con *Rimuovi applicazione*); se lo fate, valutate anche se eliminare da Facebook tutte le tracce del vostro uso dell'applicazione attivando la casella *Elimina tutte le attività*.
- 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);
- limitare l'accesso dell'applicazione ai vostri dati: spesso conviene disattivare opzioni come *Pubblicare a tuo nome*, per non consentire a un'applicazione di scrivere nel Diario o pubblicare automaticamente contenuti potenzialmente imbarazzanti, come l'annuncio pubblico che avete vinto a un gioco mentre tutti credono che stiate studiando o siate in riunione di lavoro.
- scegliere le condizioni in cui l'applicazione vi invia una notifica.

Come regola generale, sarebbe opportuno non accettare applicazioni che non siano strettamente necessarie e in ogni caso è prudente verificare il livello di accesso ai dati personali e di privacy dell'applicazione e

soprattutto i permessi di pubblicazione a nome vostro. Per quanto Facebook le vagli piuttosto attentamente, le applicazioni restano infatti una delle principali forme di attacco o di intrusione in questo social network.




*Impostazioni delle applicazioni in Facebook.*


*Esempio di imbarazzo causato da applicazione: il nonno non s'è reso conto che Viddy pubblicava notifiche dei video che aveva guardato.*

**Evitate il più possibile di attivare applicazioni frivole: spesso pubblicano o rubano dati personali o fanno pubblicità imbarazzante usando il vostro nome.**

Non conviene disattivare l'opzione *Vuoi salvare applicazioni, plug-in, giochi e siti Web su Facebook e altrove*: senza entrare troppo nei dettagli, disattivarla rende inutilizzabili quasi tutte le funzioni più popolari di Facebook.

In questa sezione trovate inoltre:

– **Applicazioni usate dagli altri:** qui decidete quali vostri dati personali possono essere letti e analizzati dalle applicazioni usate dagli utenti ai quali avete concesso l'accesso ai dati stessi: solitamente conviene disattivare tutte le categorie, in modo da rendere più difficile alle società che sviluppano giochi e app acquisire i vostri dati senza il vostro consenso esplicito.


*Impostazioni prudenziali delle informazioni condivise tramite le applicazioni.*

– **Personalizzazione istantanea**, per consentire o meno a Facebook di proporvi informazioni generate dai vostri amici quando visitate siti esterni a Facebook, come Bing, TripAdvisor o altri (principalmente legati ai giochi). 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.

– **Versioni più vecchie di Facebook per dispositivi mobili:** serve soltanto per regolare la visibilità dei contenuti per chi usa Facebook

tramite telefonini BlackBerry adoperando vecchie versioni dell'applicazione per Facebook. Normalmente non ha alcun effetto pratico, ma se volete essere ipersicuri impostate la privacy a *Solo io* o a un altro livello molto restrittivo.

### 5.4.10. Sezione *Inserzioni*

**Siti di terzi**: conviene impostare quest'opzione a *Nessuno* invece di *Solo i miei amici* (che è il valore predefinito) per limitare l'eventuale uso futuro del vostro nome e della vostra immagine nelle inserzioni da parte di applicazioni e reti pubblicitarie: è una precauzione in più per chi preferisce prevenire ed essere lungimirante.

**Inserzioni e amici:** qui potete decidere se i vostri amici vedranno i vostri *"Mi piace"* legati a prodotti o servizi pubblicizzati. In altre parole, potete scegliere se diventare *testimonial* inconsapevole di una marca, per cui i vostri amici vedranno il vostro nome associato a un oggetto pubblicizzato che vi è piaciuto (con un richiamo pubblicitario molto persuasivo) oppure no. Se non vi piace questo sfruttamento del vostro nome o se non siete sicuri di voler condividere proprio tutti i vostri gusti personali con tutti i vostri conoscenti, vi conviene scegliere *Nessuno*.

### 5.4.11. Sezione *Pagamenti*

Qui la voce da tenere sott'occhio è *Metodi di pagamento*. Potete infatti registrare nel vostro profilo Facebook i dati di una carta di credito, ma è altamente sconsigliabile farlo se non avete un motivo serio per affidare a Facebook informazioni così delicate e sfruttabili.

In caso di furto del vostro account Facebook, infatti, un ladro avrebbe accesso non solo a tutte le vostre informazioni private, ma anche a questi dati, compreso il codice di sicurezza della carta, e potrebbe usarli per acquisti fraudolenti.

## 5.5. Impostazione delle app per dispositivi mobili

Se usate Facebook su un dispositivo mobile, per esempio un telefonino evoluto oppure un tablet o un iPod touch, normalmente interagite con Facebook usando un apposito programma, cioè una *app* in gergo tecnico.

Oltre all'app di base di Facebook esiste anche *Facebook Messenger*, un'altra app ufficiale, che consente di mandare messaggi e di fare chiamate a voce via Internet.

Molte delle impostazioni che avete definito tramite il vostro computer vengono adottate anche dalle app; viceversa, se cambiate un'impostazione sulle app, viene cambiata anche nell'accesso via computer.

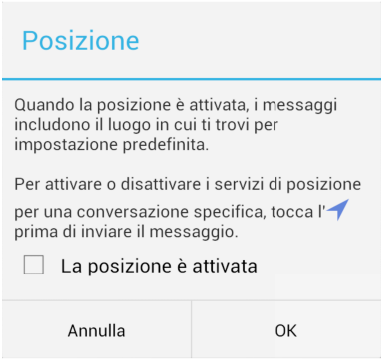
Le app di Facebook hanno però anche delle impostazioni specifiche, che è opportuno regolare per evitare violazioni della privacy e della sicurezza.

Per prima cosa, quando installate l'app di base di Facebook (o quando la attivate per la prima volta), valutate se volete sincronizzare il vostro calendario digitale (presso servizi come Google o Apple) e la vostra galleria di foto. Nel dubbio è solitamente meglio disattivare tutto, per evitare condivisioni inattese o inopportune.

## 5.5.1. Geolocalizzazione

È opportuno tenere disattivata quest'opzione.

**Dispositivi Android:** andate all'app principale di Facebook, toccate le tre barrette orizzontali in alto a sinistra e poi toccate *Impostazioni applicazione* nel menu a scorrimento che compare. Toccate *Servizi sulla posizione di Messenger* e assicuratevi che sia vuota la casella *La posizione è attivata*.




*Disattivare la geolocalizzazione nell'app di base di Facebook per Android.*

**Dispositivi iOS (iPhone, iPad, iPod touch):** andate all'icona *Impostazioni* del dispositivo (non l'icona dell'app di Facebook) e toccate *Privacy* e infine *Localizzazione*. Fatto questo, disattivate i selettori di Facebook e Messenger.

## 5.5.2. Sincronizzazione foto

Quest'opzione copia automaticamente su Facebook le foto scattate con il dispositivo. Le foto vengono impostate come private, ma è meglio non fidarsi e tenere disattivata questa sincronizzazione.

**Dispositivi Android:** andate all'app principale di Facebook, toccate le tre barrette orizzontali in alto a sinistra e poi toccate *Impostazioni applicazione* nel menu a scorrimento che compare. Assicuratevi che la voce *Sincronizza foto* indichi *Non sincronizzare le mie foto*. Se non indica questa dicitura, toccate la voce *Sincronizza foto* e scegliete *Non sincronizzare le mie foto* dal menu.

**Dispositivi iOS (iPhone, iPad, iPod touch):** nell'app di Facebook, accedete al Diario, toccate *Foto* e poi *Sincronizzate*. Toccate l'icona a forma di ingranaggio e scegliete *Disattiva la sincronizzazione delle foto* e infine *Non sincronizzare le mie foto*.

## 5.5.3. Sincronizzazione contatti

Potete decidere se permettere a Facebook di acquisire i dati dei vostri contatti memorizzati sul dispositivo mobile (foto, stato e informazioni di contatto): normalmente non conviene dare questo permesso, perché fra i vostri contatti possono esserci facilmente persone o aziende che vi hanno dato il loro numero e le loro altre coordinate in via confidenziale e non ci tengono a condividerlo con un social network che ne potrebbe fare usi imponderabili.


*Impostazione della sincronizzazione contatti in iOS7.*

**Dispositivi iOS (iPhone, iPad, iPod touch):** nelle Impostazioni di iOS, toccate la voce *Facebook*, immettete la password dell'account Facebook e verificate che sia disattivato il selettore di consenso per Facebook, come mostrato qui accanto. Se non lo è, disattivatelo.

**Dispositivi Android:** accedete all'app di base di Facebook, toccate le tre barrette orizzontali in alto a sinistra e poi toccate *Impostazioni applicazione* nel menu a scorrimento che compare. Assicuratevi che la voce *Sincronizza contatti* indichi *Non sincronizzare*. Se non indica questa dicitura, toccate la voce *Sincronizza contatti* e scegliete *Non sincronizzare* dal menu. Infine toccate *Fine*.

### 5.5.4. Riproduzione automatica dei video

I video di Facebook si avviano automaticamente, ma questo può essere un inconveniente se si è connessi a Internet tramite la rete cellulare in condizioni di segnale scarso: il caricamento automatico rallenta la navigazione e può causare addebiti anche molto elevati a seconda del vostro contratto telefonico e delle vostre impostazioni di roaming. Guardare un video di Facebook mentre si è su una rete cellulare estera può diventare un salasso economico indimenticabile.

Per fortuna questo automatismo si può disattivare almeno parzialmente, in modo che i video partano da soli soltanto se si è connessi a una rete WiFi.

**Dispositivi iOS (iPhone, iPad, iPod touch):** nelle Impostazioni di iOS, toccate la voce *Facebook*, toccate *Impostazioni* e attivate il selettore *Riproduci automaticamente solo su Wi-Fi*. Valutate anche se tenere disattivato il selettore *Carica in HD*: questo eviterà di caricare le versioni in alta definizione dei video, che possono pesare ancora di più dei video normali sulla velocità e sui costi di connessione.

**Dispositivi Android:** accedete all'app di base di Facebook, toccate le tre barrette orizzontali in alto a sinistra e poi toccate *Impostazioni applicazione* nel menu a scorrimento che compare. Attivate il segno di spunta nella casella *Riproduci automaticamente video solo su Wi-Fi.*

### 5.5.5. SMS

Nella versione iOS7 dell'app di Facebook c'è la sezione *SMS*, che consente di ricevere SMS di notifica sul telefonino per ogni messaggio, post in bacheca e richiesta d'amicizia e di inviare SMS che diventano aggiornamenti di stato. Il servizio non è disponibile in tutti i paesi e richiede un'attivazione iniziale, che si effettua in questa sezione dell'app inviando un SMS a un numero nazionale gestito da Facebook.

## 5.6. Test delle impostazioni: PrivacyFix

Potete fare una verifica generale delle vostre impostazioni di privacy tramite PrivacyFix, che potete scaricare dall'App Store o da Google Play (se usate Facebook su un dispositivo Android o iOS come iPhone, iPod o iPad) oppure presso Privacyfix.com (se usate Facebook in un browser come Chrome o Firefox per Mac o Windows) ed è realizzata dal produttore di antivirus AVG.

L'app è in inglese, ma i suoi avvisi sono molto chiari: verde se tutto va bene, arancione se c'è qualcosa da sistemare cliccando su *Fix*.

Effettua un ripasso globale periodico delle impostazioni, trovando anche cose che è facile dimenticare di controllare, come le sessioni Facebook lasciate attive (che possono essere usate per prendere il controllo del vostro account).


*Un account Facebook ben impostato supera i test di PrivacyFix.*

# 6. Comportamenti difensivi in Facebook

Una volta che l'account Facebook è stato impostato correttamente, come descritto nel capitolo precedente, in modo da esporvi il meno possibile ad attacchi informatici o a violazioni di privacy, vi resta da gestire e rinforzare l'altro elemento debole di qualunque sistema informatico: l'utente e i suoi comportamenti. In altre parole, **voi**. Non c'è tecnologia protettiva che tenga se la scavalcate perché vi infastidisce o se vi fate ingannare o sedurre e adottate abitudini pericolose.

Il guaio è che la pericolosità di molti comportamenti su Internet non è affatto intuitiva e va imparata, spesso sul campo. Ecco qualche suggerimento in proposito per evitare di scottarsi.

## 6.1. Diffidare delle richieste d'amicizia

Prima o poi riceverete su Facebook da utenti sconosciuti 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 soltanto agli amici. **L'amicizia, quindi, non va concessa alla leggera**: nemmeno quella tenue e commercializzata che vi viene chiesta attraverso Facebook.

La regola consigliabile è 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 sentirvi più importanti, come fanno invece in tanti.

## 6.2. Uscire 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, è probabile che 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: cliccate sull'ingranaggio in alto a destra, nella barra blu della pagina di Facebook, e poi 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 - Termina attività*).

## 6.3. 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.

### 6.3.1. 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. Questo

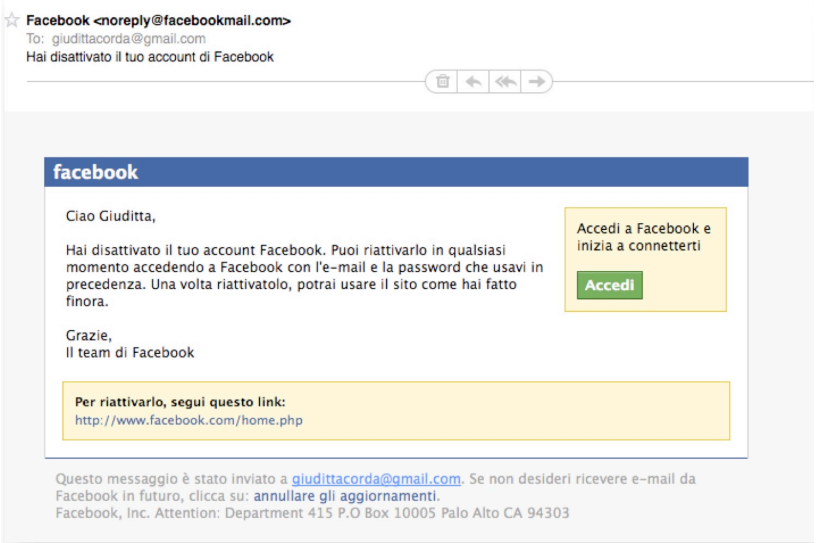
controllo è indispensabile e vale anche per gli utenti Apple, che spesso si considerano invulnerabili.

I criminali informatici usano spesso programmi-esca (denominati *cavalli di Troia* o *trojan*) 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.

## 6.3.2. Messaggi-truffa da Facebook

Non fidatevi ciecamente di messaggi o 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 e non cliccate sui link ma accedete a Facebook manualmente per vedere se il messaggio è presente davvero su Facebook. Usate sempre il buon senso: specialmente se un messaggio vi sembra sospetto o particolarmente sgrammaticato o troppo allettante, è probabile che si tratti di un tentativo d'imbroglio.




*Un falso messaggio apparentemente proveniente dall'amministrazione di Facebook.*

### 6.3.3. Finte pagine d'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.

Per fortuna c'è un trucco semplice per capire se una pagina d'ingresso a Facebook è autentica o no: basta guardare l'indirizzo mostrato nella barra dell'indirizzo del vostro browser e assicurarsi che:

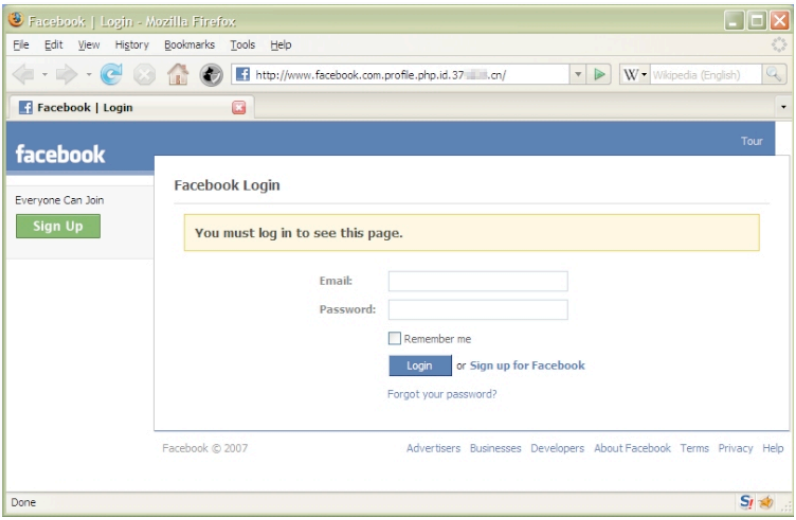
– inizi con *https* (non *http*)

– 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.*

### 6.3.4. 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 promettono di darvi accesso 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.

### 6.3.5. *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*.

### 6.3.6. 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 raggiro. 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.

### 6.3.7. 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.


*Le autorizzazioni richieste dal gioco Café World in Facebook.*

## 6.3.8. Password monouso

Per rendere sicuro l'accesso a Facebook da un computer che non è il vostro, per esempio a scuola, in biblioteca o in altri luoghi pubblici, in alcuni casi potete usare le *password monouso*. Anziché immettere la vostra password abituale, ne immettete una speciale che vale una sola volta e scade dopo venti minuti.

Per ricevere una password monouso, che arriverà sotto forma di SMS sul telefonino di cui avete dato il numero a Facebook, dovete inviare un SMS con la sigla *"otp"* (abbreviazione di *"one time password"*, ossia *"password monouso"*) al numero speciale che corrisponde al vostro operatore cellulare. L'elenco dei paesi nei quali è disponibile presso *https://www.facebook.com/help/www/447046021986895*. Per usare questa funzione dovete ovviamente aver affidato il vostro numero di cellulare a Facebook.

### 6.3.9. Bufale

Non credete a tutto quello che leggete su Facebook. Su questo social network, come del resto in tutte le forme di comunicazione fra persone, circolano allarmi e notizie false di ogni genere. Non inoltrate e non condividete nulla che non abbia una fonte autorevole e sicura o se non siete in grado di controllarne la veridicità.

Il fatto che una notizia o una segnalazione d'allarme sia stata pubblicata da un vostro amico non garantisce nulla: può essersi fidato a sua volta di qualche suo amico, e così via, senza che nessuno abbia mai verificato i fatti 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.

### 6.3.10. Se viene violato l'account Facebook

Il sintomo più evidente di un account violato è l'impossibilità di accedervi, perché il ladro ha cambiato la password, ma ci possono essere altre 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 mail che contiene le istruzioni per reimpostare la password.

Un'altra soluzione è usare i Contatti fidati, descritti nel Capitolo 5: un gruppo di utenti dei quali vi fidate e ai quali avete affidato dei codici d'emergenza.

# 6.4. Difendersi da ficcanaso, scocciatori e molestatori

## 6.4.1. Taggaggio selvaggio

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 simili, così chi cerca vostre immagini si trova quelle di questi animali.

Le impostazioni descritte nel capitolo precedente vi mettono al sicuro da molte forme di "taggaggio" scorretto od offensivo e vi allertano quando venite taggati, ma potete anche chiedere la rimozione dei tag dalle immagini alle quali non volete essere associati. Procedete come segue:

- Andate al Registro delle attività, cliccando sul vostro nome nella banda superiore blu di Facebook e poi cliccando su *Registro attività* e infine su *Foto* (sulla sinistra) e *Foto in cui ci sei tu*.
- Compare un elenco di foto nelle quali siete stati taggati. Cliccate sul triangolo dell'impostazione di privacy a destra della foto per far comparire un menu a tendina, dal quale scegliete *Segnala/Rimuovi tag* e poi chiedete la rimozione del tag (è immediata) o della foto (richiede tempo).

## 6.4.2. 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 mail;

– di bloccare gli inviti a usare applicazioni o a partecipare ad eventi che provengono da uno specifico utente;

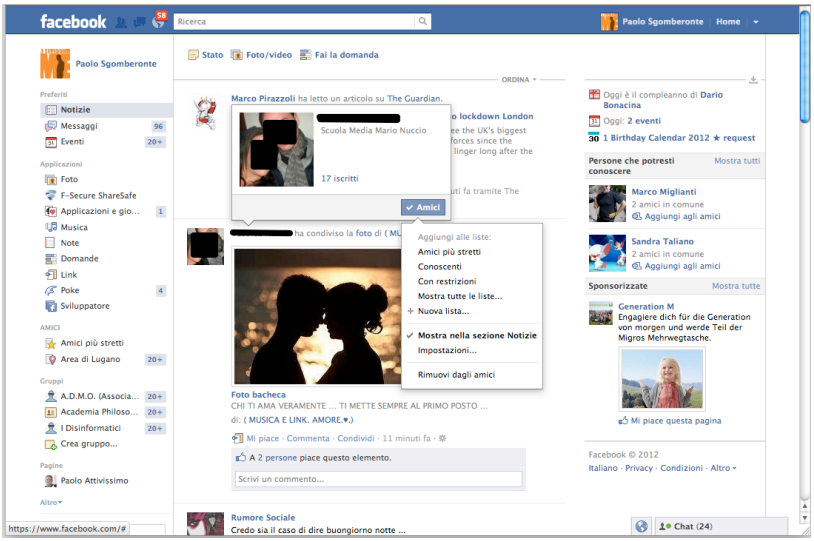
– di bloccare le applicazioni indesiderate.

Questo può essere utile specialmente nel caso di giochi, per i quali gli utenti spesso disseminano inviti a pioggia per acquisire punti. Tutte queste 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".*

Potete anche *bloccare* una persona, comprese le persone alle quali non avete concesso l'amicizia su Facebook: cliccate sul nome della persona da bloccare e visualizzate il suo profilo Facebook. Accanto al pulsante *Messaggio* c'è un triangolino. Cliccandovi sopra compare un menu dal quale potete scegliere *Segnala/blocca* e poi l'opzione *Blocca*.

Quando bloccate qualcuno, vengono rimossi da Facebook tutti i legami esistenti tra voi e la persona bloccata, se ce ne sono. Inoltre non potete più vedere il diario dell'altra persona (e viceversa), non potete trovarvi nei risultati di ricerca e l'altra persona non potrà più taggarvi.

## 6.4.3. Blocco di contenuti o immagini

A volte gli utenti pubblicano foto o post testuali scioccanti od offensivi. Potete segnalarli a Facebook: se violano le condizioni di pubblicazione previste dal social network, verranno rimossi.

Il modo più diretto per fare questa segnalazione è il seguente:

– **Foto:** visualizzate la foto a tutto schermo e cliccate sul menu *Opzioni* in basso: questo fa comparire l'opzione *Segnala*: se vi cliccate sopra, compare una finestra di dialogo nella quale scegliete il motivo della segnalazione. Se Facebook concorda con la vostra segnalazione, rimuoverà la foto.

– **Post:** visualizzate il post cliccando sulla sua data e poi mettete il cursore sull'area bianca del post: questo fa comparire una crocetta in alto a destra. Se vi cliccate sopra, potete scegliere *Segnala/Contrassegna come spam*. Il post scompare subito alla vostra vista e Facebook valuterà se rimuoverlo del tutto.

Con questo sistema potete anche chiedere alla persona che ha pubblicato la foto di rimuoverla volontariamente. Se non la volete contattare direttamente, fatelo fare a un amico fidato, a un genitore o a un'altra persona di fiducia.

### 6.4.4. Vedersi "da fuori"

Uno dei modi migliori per accorgersi di essere incappati in truffe o furti della propria password o di aver condiviso un po' troppo su Facebook è guardare il proprio profilo "da fuori", ossia dal punto di vista degli altri. Molti utenti non si accorgono di essere infettati, di mandare post pubblicitari indesiderati o di aver reso erroneamente pubblica un'immagine imbarazzante finché non glielo dicono i 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 suo nome nella casella apposita. Fatelo spesso per evitare gaffe.


*L'opzione "Visualizza come" di Facebook.*

## 6.4.5. Disseppellire gli scheletri: Graph Search

Graph Search (in italiano *"Strumento di ricerca tra le connessioni"*) è una sorta di Google per Facebook: consente di effettuare ricerche approfonditissime all'interno di Facebook usando un metodo simile a quello dei comuni motori di ricerca.

Per esempio, potete chiedere a Graph Search di elencarvi tutte le donne iscritte a Facebook che abitano nel raggio di quindici chilometri da voi, hanno meno di 25 anni e sono fan della cantante Rihanna. Potete anche chiedere ricerche molto più personali e rivelatrici: per esempio, tutte le foto pubblicate da una persona, o tutte quelle che ha commentato o sulle quali ha cliccato *"Mi piace"*, oppure tutti i luoghi visitati da quella persona o tutti i video che sono piaciuti ai nostri amici. La ricerca incrociata permette di far emergere risultati potenzialmente imbarazzanti come *"cattolici italiani ai quali piace la Durex"* (con nomi, cognomi e foto), *"donne single nelle mie vicinanze alle quali piacciono gli uomini e piace ubriacarsi*" o *"persone alle quali piace il razzismo"*.

Con Graph Search scompare il naturale oblio dovuto al passare del tempo e all'accumulo di nuovi contenuti: anche immagini e post pubblicati anni fa riemergono con estrema facilità, perché basta chiedere *"foto scattate prima del 2008"* indicando il nome della persona ritratta.

Non tutti gli utenti hanno accesso a Graph Search, almeno per ora: per averlo si visita *https://www.facebook.com/about/graphsearch* e si clicca s u *Iscriviti alla lista d'attesa*. Se si imposta l'inglese come lingua dell'interfaccia di Facebook le probabilità che venga attivato il servizio aumentano nettamente, dato che lo sviluppo delle funzionalità di Facebook avviene prima in questa lingua e poi in tutte le altre.

Per evitare l'occhio onniveggente di Graph Search dovete rendere privato l'elenco degli amici, delle relazioni e dei familiari e poi spulciare i *"Mi piace"* (tramite il Registro attività) e decidere se cancellare quelli obsoleti o imbarazzanti e in generale renderli visibili solo agli amici.

Rendere meno pubblici e scandagliabili i vecchi post è molto semplice: cliccate sull'icona dell'ingranaggio, scegliete *Impostazioni sulla privacy*, cliccate su *Limita i post passati* e poi su *Solo vecchi post*: tutti i post che prima erano visibili agli amici di amici o a tutti diventeranno visibili solo agli amici.

Nascondere le foto agli occhi di Graph Search è un po' più complicato: dovete andare nella sezione *Foto* del profilo, scegliere *Album* e poi definire la privacy di ciascun album. Ma non basta, perché se qualcuno vi ha taggato in una foto, quella foto rimane cercabile con Graph Search: per impedire che venga trovata bisogna togliere il tag (visualizzate la foto e scegliete *Opzioni* > *Segnala/Rimuovi tag*).

### 6.4.6. Statistiche con Wolfram Alpha

Potete ottenere una quantità impressionante di dati statistici sul vostro utilizzo di Facebook tramite WolframAlpha.com: digitate nella sua casella le parole "*facebook report*", cliccate su "*Analyze my Facebook data*" e attendere qualche decina di secondi intanto che Wolfram Alpha esplora la vasta rete interconnessa di dati che avete creato in Facebook. Potete anche attivare le analisi storiche (*historical analytics*) per vedere come si evolve nel tempo la propria attività su Facebook.

Il risultato è impressionante: statistiche sul numero di foto, link e messaggi di stato che avete pubblicato, il numero e la media dei *"Mi piace"* e dei commenti che gli amici hanno assegnato ai vostri post, le parole che usate più frequentemente, il vostro post che è piaciuto di più e quello più commentato.

Ci sono anche informazioni sui vostri amici: quelli che commentano più assiduamente, la ripartizione percentuale in uomini e donne, il grafico delle proporzioni fra amici single, legati sentimentalmente, fidanzati o sposati (a sua volta suddivisibile per età), le loro fasce d'età e località dichiarate, persino la distribuzione mensile dei compleanni, i nomi più comuni e gli amici con il maggior e minor numero di amici in comune con voi. E poi ci sono i grafici delle "isole" di relazioni fra persone.

Questa marea di dati, presentata in questo modo, rende bene l'idea di quanto i social network siano miniere immense di dati sulle persone, pronti per essere vagliati e sfruttati dalle agenzie di marketing e dai governi.

## 6.5. 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.

### 6.5.1. 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 colte 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 dalla polizia.

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 siate persone poco serie. Immaginate l'effetto che può avere 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).

### 6.5.2. 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, conservandole 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.

### 6.5.3. 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: dareste facilmente l'impressione di essere persone poco serie che svendono le proprie amicizie. Molti utenti di Facebook considerano questi inviti una forma di maleducazione.

### 6.5.4. Un commento è per sempre

Vi rode il fatto di aver appena pubblicato su Facebook un commento di rara finezza ma afflitto dal neo di un banale errore di battitura? Stavate consolando una persona cara sul social network e vi è scappato di scri-

vere che volete darle un *coniglio* dal profondo del cuore? Facebook vi capisce e soffre con voi. Per questo offre la possibilità di modificare i commenti.

L'operazione è molto semplice: per correggere un commento dopo averlo inviato, cliccate sulla matita che compare in alto a destra nel riquadro del commento e scegliete *Modifica*. Correggete il commento a vostro piacimento e poi premete Invio: al posto della versione precedente comparirà quella nuova.

Attenzione, però, a non pensare di poter far sparire per sempre i refusi o i commenti imbarazzanti, oppure di atteggiarvi a luminosi profeti e chiaroveggenti, usando questo sistema. Infatti quando si modifica un commento, Facebook ne conserva anche le versioni precedenti, che sono accessibili a tutti (o perlomeno a chi ha il diritto di vedere il commento in questione) cliccando sulla parola *Modificato* che sta sotto il commento.

Per eliminare definitivamente un commento bisogna invece cliccare sulla matitina e scegliere *Elimina*.

# 7. 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 fondamentale fra *disattivazione* ed *eliminazione*, e comunque la procedura non è molto facile.

## 7.1. 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 (che possono comunque continuare a mandarvi inviti e taggarvi). 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).

La cancellazione diventa attiva e definitiva 14 giorni dopo che l'avete richiesta ma è revocabile durante questo periodo semplicemente rientrando in Facebook.

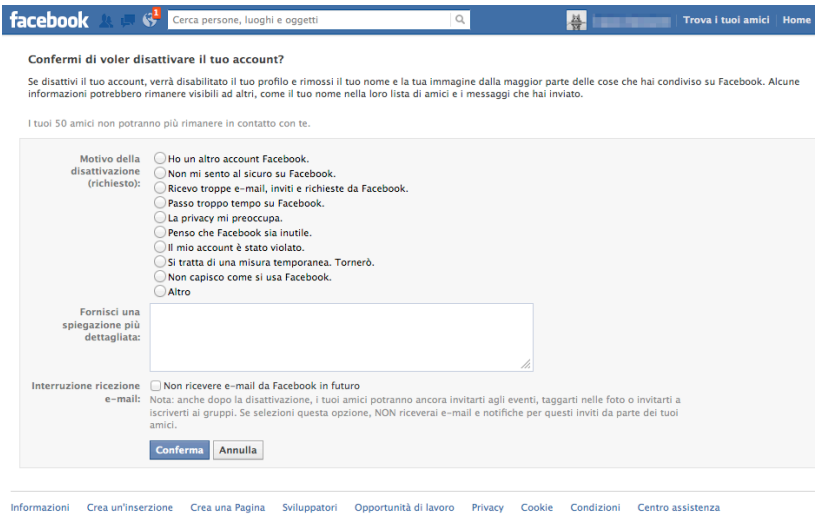
In sintesi:

- se *disattivate* l'account, potete sempre pentirvene;
- se *eliminate* l'account, non potete tornare sui vostri passi dopo che è scaduto il periodo di ripensamento.

## 7.2. Come disattivare un account

Accedete al vostro account, cliccate sull'ingranaggio 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*.




*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 mail e la password dell'account stesso come consueto.

Fate attenzione a non entrare accidentalmente in Facebook, né dal computer né da altri dispositivi (per esempio con la app sul telefonino o sul tablet), altrimenti la disattivazione verrà revocata e tutto tornerà come prima. Per Facebook anche cliccare su *"Mi piace"* in un sito ester-

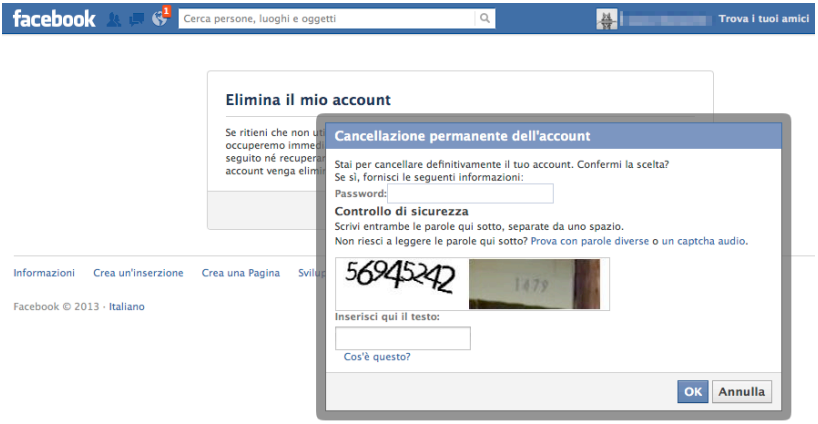
no a Facebook oppure usare la password di Facebook su altri siti (Facebook Connect) significa *"entrare"* e revoca la disattivazione.

Un trucco molto semplice per evitare che un'app rientri per sbaglio è cambiare tramite browser la password dell'account prima di iniziare la disattivazione.

## 7.3. Come eliminare un account

**Fate attenzione: questa procedura è irreversibile dopo che è stata completata.**

- Per prima cosa entrate in Facebook usando un browser (non un'app) e **cambiate la vostra password.** Questo serve a impedire che le app entrino automaticamente nel vostro account, interrompendo così la procedura di eliminazione: non ci riusciranno perché avranno in memoria la password vecchia. Per eliminare un account, infatti, Facebook esige che non vi accediate più in nessun modo per quattordici giorni dopo che avete inoltrato la richiesta di eliminazione.
- Se siete veramente decisi a eliminare l'account e volete rinunciare al periodo di ripensamento, potete **cancellare subito i vostri dati** cliccando su *Aggiorna informazioni* nel vostro profilo e azzerando manualmente tutte le informazioni immesse. Potete eliminare subito le foto selezionando i singoli album (alla voce *Foto* del vostro profilo) e poi cliccando sull'ingranaggio e sulla voce *Elimina album;* per le foto singole vi tocca procedere una per una con un clic su *Opzioni* e poi su *Elimina questa foto*.
- Disattivate tutte le app che hanno il permesso di postare su Facebook a nome vostro.
- Se possibile, disinstallate dai tablet e dai telefonini le app di Facebook.
- Andate a questo link: *https://www.facebook.com/help/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*.
- Compare un avviso che informa che il vostro account verrà eliminato permanentemente entro quattordici giorni se non vi rientrate: cliccate su *OK*.
- Facebook vi scollega e vi porta alla sua pagina d'ingresso: non rientratevi.




*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 in qualunque modo all'account durante il periodo di disattivazione, vi verrà proposto di revocare l'eliminazione e riattivare l'account.

# 8. Impostazioni difensive di Twitter

## 8.1. 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* (grafia ufficiale di Twitter in italiano) o *tweetare*. Gli informatici di lungo corso come me preferiscono la seconda grafia perché nell'era pre-Twitter il termine *twittare* significava grosso modo *"dare del cretino"*.[4]

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.

Ai tweet si possono anche allegare foto, cliccando sull'icona *Aggiungi un'immagine*, e 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*).

4 Più precisamente, significava togliere i privilegi a un utente di una rete informatica, degradandolo a utente semplice, perché aveva commesso qualcosa di scorretto o inaccettabile e quindi si era dimostrato troppo stupido per meritarsi i privilegi che gli erano stati dati.


*Un tweet da un posto speciale: l'astronauta Luca Parmitano scrive dalla Stazione Spaziale Internazionale. Il tweet contiene un hashtag* (#Volare) *e un link a una foto.*

Potete condividere un tweet ricevuto usando l'opzione *Retweet* e potete indicare il vostro gradimento cliccando su *Aggiungi ai preferiti*. Alla voce *Altro* di ogni tweet potete inoltrare un tweet via mail e soprattutto segnalarlo come spam o messaggio offensivo oppure come messaggio di un account che sospettate sia stato rubato; la segnalazione permette anche di bloccare un utente non desiderato.

Le impostazioni dell'account sono accessibili entrando sul sito di Twitter con la propria login e password e cliccando sull'ingranaggio 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 seguenti di questo capitolo soffermandosi sui loro aspetti di privacy e sicurezza.

## 8.2. Sezione *Account*

In questa sezione delle impostazioni definite gli elementi di base: il vostro nome utente, l'indirizzo di mail da associare all'account, la lingua dell'interfaccia, il fuso orario e la nazione con la quale vi identificate (non è necessariamente quella in cui abitate).

### 8.2.1. Indirizzo di mail

L'indirizzo di mail che immettete nelle impostazioni resta privato e non viene visualizzato pubblicamente. È consigliabile usare, se possibile, un indirizzo di mail diverso da quello che usate pubblicamente: in questo modo eventuali aspiranti intrusi avranno un dato segreto in più che dovranno scoprire e sarà più difficile rubarvi l'account Twitter.

### 8.2.2. Gestione dei contenuti sensibili

La voce *Contenuti dei tweet* ha due caselle di spunta che servono per la gestione dei *contenuti sensibili*: immagini e video di violenza, crudezza, sessualità, shock, turpiloquio o altre situazioni non adatte a tutti i palati e a tutte le età.

- La prima, *Non informarmi prima di mostrare contenuti potenzialmente sensibili*, serve per scegliere se vedere un avviso prima di vedere immagini e video che gli altri utenti hanno etichettato come potenzialmente sensibili. Se volete tutelarvi contro questo tipo di contenuto, lasciatela disattivata.
- La seconda, *Segna i contenuti che twitto come materiale potenzialmente sensibile*, vi permette di avvisare gli altri utenti che quello che pubblicate su Twitter può essere inadatto a tutti i gusti. Attivatela se pensate che le immagini o i video che pubblicate siano sensibili. 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.

### 8.2.3. Scaricamento di una copia d'archivio

Cliccando su *Richiedi il tuo archivio* potete ottenere una copia completa di tutti i tweet che avete mai inviato da quell'account. Quando fate questa richiesta, ricevete entro qualche minuto via mail, all'indirizzo che avete immesso nell'account, un link dal quale scaricare la copia d'archivio.

### 8.2.4. Disattivazione dell'account

Un clic su *Disattiva il mio account* fa esattamente quello che immaginate: disattiva il vostro account Twitter. I dettagli sono nel Capitolo 10, ma comunque la procedura è semplicissima.

## 8.3. Sezione *Sicurezza e privacy*

Qui cominciano le decisioni più corpose: la visibilità dei vostri tweet, la protezione della password, la geolocalizzazione, il tracciamento e altro ancora. Procediamo con ordine.

### 8.3.1. Verifica d'accesso

Alla voce *Verifica d'accesso* avete la possibilità di proteggere il vostro account usando un codice di sicurezza supplementare che vi viene inviato tramite SMS sul numero di telefonino che affidate a Twitter. Quest'opzione non è ancora attiva in tutti i paesi: lo è per esempio in Italia ma non in Svizzera.

Se il vostro account Twitter è importante (avete molti follower e/o rappresentate un'azienda, per esempio), conviene proteggerlo con questa verifica d'accesso se è attiva nel vostro paese (o se avete un telefonino con un numero di un paese nel quale è attiva). Tecnicamente si chiama *autenticazione a due fattori*: all'intruso non basta scoprire la vostra password, ma deve anche mettere le mani sul telefonino sul quale ricevete il codice di verifica.

Per attivare quest'opzione dovete per prima cosa dare a Twitter un numero di telefonino, cliccando su *"aggiungere un telefonino"*. Questo vi porta alla sezione *Cellulare*, descritta più avanti, nella quale immettete i dati del vostro telefonino.

Fatto questo, attivate l'opzione *Invia una richiesta di verifica d'accesso*: vi viene mandato un SMS di test. Se lo ricevete e ne confermate la ricezione cliccando su *Sì*, da questo momento in poi per poter accedere al vostro account dovrete immettere non solo la vostra password ma anche il codice supplementare che riceverete gratuitamente tramite SMS.

Se usare Twitter su un dispositivo iOS o Android, potete anche scegliere *Invia una richiesta di verifica d'accesso all'app Twitter*: in questo modo riceverete un codice d'emergenza (*backup code*), che va copiato e custodito con cura, perché servirà per accedere all'account in caso di smarrimento del dispositivo mobile. Al successivo accesso al vostro account, Twitter invierà al vostro dispositivo mobile una notifica e la dovrete aprire per poter usare l'account.

### 8.3.2. Reimpostazione password

Conviene attivare quest'opzione, etichettata *Richiedi informazioni personali per reimpostare la mia password*, perché in questo modo chiun-

que cerchi di rubarvi l'account tramite una reimpostazione della password non potrà tentare questa reimpostazione digitando nella schermata d'ingresso di Twitter il nome del vostro account (un dato pubblico) ma dovrà anche conoscere l'indirizzo di mail o il numero di telefonino che avete associato all'account (due dati che possono essere resi privati).

Quest'impostazione vale anche per voi: se attivate quest'opzione e vi dimenticate la vostra password, non potrete reimpostarla immettendo nella schermata d'ingresso di Twitter il nome del vostro account ma dovrete immettere anche l'indirizzo di mail o il numero di telefono associati all'account.

### 8.3.3. Privacy dei tweet

Quest'opzione serve per rendere privati tutti i vostri tweet: se la attivate, saranno visibili su Twitter soltanto agli utenti che autorizzate. Questo può essere utile per adoperare Twitter come sistema di comunicazione riservato fra un gruppo di persone, per esempio per i minori, perché evita che sconosciuti possano leggere i loro tweet, che vengono invece riservati solo agli amici reali.

Tuttavia, come per qualunque social network, l'idea dei messaggi privati è da prendere con molta cautela e diffidenza, per cui non è opportuno ricorrere a Twitter per comunicazioni delicate e strettamente confidenziali. Per esempio, 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.

### 8.3.4. 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*.

### 8.3.5. Reperibilità

Se ci tenete alla privacy e non volete essere trovati dagli sconosciuti, vi conviene disattivare entrambe le caselle di questa sezione, che consentono a chiunque di trovare il vostro account Twitter immettendo il vostro indirizzo di mail e/o il vostro numero di telefonino che avete affidato a Twitter.

### 8.3.6. Personalizzazione e contenuto sponsorizzato

L'opzione *Personalizzazione* serve a scopi pubblicitari e cerca di adattare i contenuti di Twitter in base alle vostre visite ad altri siti. Si tratta di una forma di tracciamento piuttosto invasiva che è normalmente opportuno disattivare.

Anche le *Sponsorizzazioni* hanno una funzione pubblicitaria di tracciamento dell'utente e come tali sono solitamente da disattivare, anche se offrono pubblicità basate sui gusti (presunti) dell'utente stesso.

## 8.4. Sezione *Password*

Qui immettete la password quando desiderate cambiarla. Per Twitter valgono le precauzioni standard sulle password:

- lunga 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.

## 8.5. Sezione *Cellulare*

Se l'operatore del vostro telefonino è fra quelli gestiti da Twitter, in questa sezione potete immettere il numero di telefonino che volete associare all'account Twitter, allo scopo di poter inviare e ricevere tweet via SMS e utilizzare la verifica d'accesso tramite SMS.

Vi viene chiesto di inviare un SMS dal telefonino che avete indicato a un numero specifico (per esempio, in Italia con TIM dovete mandare il messaggio *"vai"* al numero +39 339 9940 424). Se l'operazione ha suc-

cesso, vi viene presentato un elenco di opzioni di notifica tramite SMS: valutate se attivarle o disattivarle. Potete anche scegliere di limitare gli orari durante i quali ricevete le notifiche via SMS.

## 8.6. Sezione *Notifiche email*

In questa sezione impostate le notifiche che volete ricevere via mail. Le varie opzioni sono da attivare o disattivare secondo i vostri gusti, ad eccezione di *I miei Tweet ricevono una risposta o vengo menzionato in un Tweet,* che è probabilmente opportuno attivare per tenere d'occhio quel che si dice di voi su Twitter, e *Notizie su Twitter e sugli aggiornamenti delle funzioni,* che conviene tenere attiva per sapere quando ci sono novità nell'uso di questo social network.

Le notifiche via mail, fra l'altro, hanno il vantaggio non trascurabile di generare automaticamente un archivio dell'attività su Twitter.

## 8.7. Sezioni *Profilo* e *Aspetto*

Queste parti delle impostazioni 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.

## 8.8. Sezione *App*

Qui potete elencare e valutare con attenzione le *app* o *applicazioni* che attivate e quali permessi date a ciascuna di esse. I permessi sono revocabili cliccando sul pulsante *Revoca accesso* corrispondente all'applicazione. È consigliabile dare periodicamente un'occhiata a quest'impostazione per assicurarsi che non ci siano state attivazioni inopportune di applicazioni inutili o troppo invasive.

Tenete presente che alcune applicazioni possono pubblicare tweet a nome vostro senza preavvisarvi, con risultati imbarazzanti o sconvenienti. Non installate app che non siano strettamente indispensabili.

## 8.9. Sezione *Widget*

Nessun aspetto di sicurezza: si tratta semplicemente di una sezione delle impostazioni di Twitter nella quale potete definire un *widget*, ossia delle istruzioni da inserire in un sito o in un blog per farvi comparire il flusso progressivo dei tweet che scrivete, l'elenco dei vostri tweet preferiti, liste di cui siete proprietari oppure una casella di ricerca.

## 8.10. Archiviazione dei tweet

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:

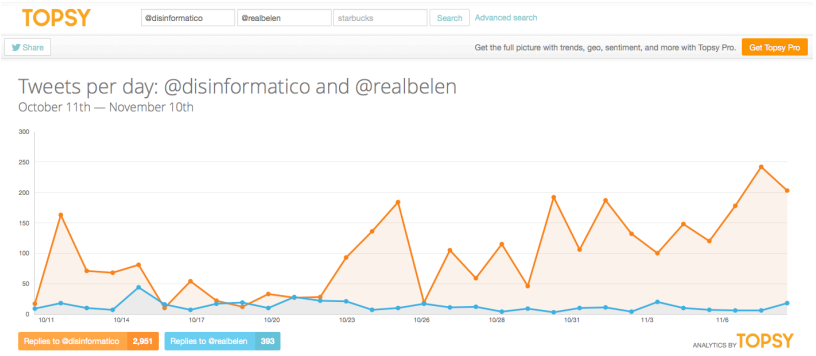
– qualunque tweet pubblico è recuperabile in ogni momento se si conosce il suo indirizzo o URL specifico, che ha una struttura del tipo *http://twitter.com/#!/[nomeutente]/status/[numero]*;

– 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.




*Un grafico statistico generato da Topsy.*

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

# 9. Comportamenti difensivi in Twitter

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

## 9.1. 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.

## 9.2. 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 ha un contenuto 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, magari da qualche app di gioco. Avvisatelo (usando un canale diverso da Twitter) e non cliccate sui link che accompagnano questi messaggi: di solito portano a siti-trappola.

## 9.3. Proteggete la vostra password

Twitter non vi chiederà mai la vostra password in una 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 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.

**Se accedete a Twitter da un computer o altro dispositivo che non è il vostro, assicuratevi di non accettare nessuna richiesta di ricordare la password.**

## 9.4. Privacy

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. A differenza di Facebook, Twitter accetta entrambi.

Può sembrare un controsenso porsi questioni 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 vostri tweet e farsi un'idea sulle vostre affiliazioni politiche o religiose. Potrebbe guardare l'elenco delle persone che seguite su Twitter e dedurne le vostre 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 vostre simpatie su Twitter sia completo e descriva esaurientemente la vostra personalità e i vostri interessi, ma chi lo guarda sarà portato a pensare che sia così.

## 9.5. 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. Se vedete un tweet che contiene uno di questi link, non fidatevi e non cliccate sul link.

Se siete curiosi, potete usare uno dei servizi di decodifica di questi link brevi disponibili su Internet, come per esempio Longurl.com: basta immettervi il link breve per sapere qual è il sito originale corrispondente.

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 sempre vigili.


*Twitter abbrevia i link ma ne lascia visibile la prima parte.*

## 9.6. Cancellazione dei messaggi

Cancellare un messaggio che avete pubblicato su Twitter è semplice: basta visualizzarlo su *www.twitter.com* o nella app e cliccare su *Elimina* o sull'icona del cestino.

Twitter vi chiede di confermare la richiesta: pensateci bene e poi, se siete sicuri, cliccate su *Elimina*. Il tweet scompare dal vostro flusso di messaggi.

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

## 9.7. 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 contenuto*. La segnalazione è irrevocabile.

C'è una serie di criteri molto affidabile per riconoscere un utente Twitter truffaldino:

- ha spessissimo l'icona predefinita (l'uovo) nel proprio profilo;
- ha un nome impronunciabile e farcito di numeri;
- segue parecchie centinaia di persone ma non ha altrettanti follower;
- ha scritto pochissimi tweet o non ne ha scritto nessuno.

Questo avviene perché questi account sono generati in massa e in modo automatico da parte dei criminali informatici, e hanno una vita molto breve prima di essere bloccati da tutti, per cui i loro creatori mettono poca cura nei dettagli.

## 9.8. Bufale

Anche su Twitter le bufale prosperano: oltre alle categorie tradizionali degli allarmi e degli appelli fasulli ma ritenuti veri e ritrasmessi senza controllarli c'è un genere specifico di bufala che prospera in particolare su questo social network: gli annunci di morte di celebrità. La rapidità della circolazione delle notizie che caratterizza Twitter, tramite i retweet quasi istantanei, fa sì che una notizia-shock faccia il giro del mondo in men che non si dica.

Fra le celebrità dichiarate morte erroneamente su Twitter ci sono George Clooney, Aretha Franklin, Charlie Sheen, Mick Jagger, Eddie Murphy, Adam Sandler, Bill Cosby, Morgan Freeman, Jon Bon Jovi, Denzel Washington e Will Smith. Per qualche strana ragione, molti di questi decessi fasulli vengono attribuiti, nei tweet che li annunciano, a un incidente di snowboard.

In altre parole, non credete a tutto quello che leggete su Twitter.

## 9.9. Se viene violato l'account Twitter

Se vi accorgete che il vostro account Twitter sta inviando tweet pubblici o privati senza il vostro permesso, diffondendo per esempio notizie false o messaggi pubblicitari o inviti a visitare siti di cui non sapete nulla, probabilmente l'account è stato violato.

Un altro sintomo frequente di violazione dell'account è che non riuscite ad accedere all'account tramite il sito Twitter.com, ma non fatevi prendere dal panico: ci potrebbero essere altre cause. Per esempio:

- state cercando di accedere dando il *nome* del vostro account Twitter e il sito vi respinge perché l'avete digitato senza la chiocciolina davanti o perché avete sbagliato a digitare la password;
- avete sbagliato troppe volte la password e Twitter vi ha sospeso l'accesso per un'ora circa, per precauzione, e durante questo periodo non potrete accedere neanche con la password giusta;
- avete lasciato in un'app una password non aggiornata e l'app ha tentato ripetutamente di accedere a Twitter, col risultato che Twitter ha pensato che siete sotto attacco e ha sospeso gli accessi per un'oretta.

### 9.9.1. Cosa fare se riuscite ancora ad accedere all'account

Per prima cosa uscite da Twitter, svuotate la cache del browser, riavviate il browser e rientrate in Twitter: serve ad annullare il *cookie* della sessione corrente, che può essere un appiglio usato da eventuali virus o altre forme di attacco. Poi cambiate la vostra password. Ricordate che dovrete cambiarla anche nelle app che usate e di cui vi fidate.

Fatto questo, andate nelle Impostazioni, scegliete la sezione *Applicazioni* e verificate che l'elenco di applicazioni che hanno accesso al vostro account non contenga voci che non conoscete. Se ne contiene, cliccate sul pulsante *Revoca accesso* accanto all'applicazione sospetta.

Andate poi a sfogliare il vostro flusso di tweet ed eliminate i tweet che non riconoscete. Cogliete l'occasione per una scansione del vostro computer con un buon antivirus aggiornato e per scaricare gli aggiornamenti di sicurezza dei vostri sistemi operativi.

### 9.9.2. Cosa fare se non riuscite più ad accedere all'account

Prima di tutto chiedete un *reset* della password andando all'indirizzo *https://twitter.com/account/resend_password*. Riceverete una mail con le istruzioni per reimpostare la password. Se avete affidato a Twitter il vostro numero di telefonino, potete immetterlo nella richiesta di reset per attivare la reimpostazione tramite SMS. Questo è solitamente sufficiente a riprendere il controllo dell'account.

Se però l'intruso ha cambiato l'indirizzo di mail e il numero di cellulare associati all'account, la mail con le istruzioni di reimpostazione e l'SMS di reset non arriveranno a voi ma all'intruso. In questo caso andate a *https://support.twitter.com/forms/signin* e preparatevi a comunicare con Twitter in inglese (unica lingua attualmente gestita dall'assistenza utenti): dapprima vi verrà proposto di reimpostare la password.

Poi, se anche questo non risolve il problema, avrete la possibilità di mandare un messaggio all'assistenza utenti, nel quale fornirete il maggior numero possibile di prove che siete il vero titolare dell'account: per esempio la mail di benvenuto che Twitter vi ha mandato quando avete aperto l'account, un elenco di persone alle quali avete mandato un tweet diretto o altri dati di questo genere.

Una volta risolto il problema, cancellate gli eventuali tweet abusivi, fate un controllo antivirus del vostro computer e scaricate gli aggiornamenti di sicurezza dei vostri dispositivi.

# 10. Chiudere un account Twitter

Per chiudere definitivamente un account su Twitter occorre andare al sito Twitter.com con un browser: non si può usare un'app su tablet o smartphone.

Preliminare importante: se intendete usare lo stesso nome utente o lo stesso indirizzo di mail per un altro account, cambiateli *prima* di disattivare l'account corrente.

Accedete alle *Impostazioni*, scegliete la sezione *Account* e andate in fondo alla schermata, dove trovate il link *Disattiva il mio account*. Cliccatevi sopra e confermate la richiesta cliccando su *OK* e dando la vostra password.

Se lo fate, il vostro account verrà dapprima *disattivato* (reso invisibile) nel giro di pochi minuti, anche se qualche elemento potrà restare visibile per qualche giorno.

Se non rientrate nell'account per trenta giorni, l'account verrà cancellato. Se cambiate idea, potete riattivare l'account semplicemente rientrandovi entro i trenta giorni successivi alla richiesta di disattivazione. Scaduto questo tempo l'account verrà eliminato. Tutto qui.

# 11. Impostazioni prudenti in breve

Qui sono riassunte le principali impostazioni consigliate per Facebook e Twitter, descritte in dettaglio nelle pagine precedenti. Se volete fare un controllo veloce del vostro account e vi fidate delle motivazioni descritte nel resto del libro, siete nel capitolo giusto.

## 11.1. Facebook: impostazioni via Web

Di seguito vengono elencate le impostazioni accessibili visitando il sito Facebook.com tramite un computer dotato di browser (per esempio Firefox) e immettendo nome utente e password del vostro account. Le impostazioni disponibili tramite l'app di Facebook su un telefonino o tablet sono elencate nella sezione 11.2.

Accedete a queste impostazioni cliccando sull'ingranaggio nella barra blu superiore di Facebook, poi su *Impostazioni account* e infine sulle voci della colonna di sinistra della schermata di Facebook.

### 11.1.1. Generale

**Nome:** Preferibilmente diverso da quello reale.

**Nome utente:** Preferibilmente diverso da quello reale.

**E-mail:** Preferibilmente un indirizzo di e-mail che solo voi conoscete, diverso da quello che usate abitualmente. La casella *Consenti agli amici di includere...* va disattivata.

### 11.1.2. Protezione

**Navigazione protetta:** attivata.

**Notifiche di accesso:** attivate.

**Approvazione degli accessi:** attivata.

**Generatore di codici:** attivato.

**Password per le applicazioni:** non indispensabile.

**Contatti fidati:** impostati.

**Dispositivi riconosciuti:** verificare periodicamente che non contengano dispositivi che non usate più.

**Sessioni attive:** controllare periodicamente che non ci siano sessioni diverse da quelle che usate abitualmente. Se ci sono, scegliete *Termina attività* per ciascuna sessione non vostra.

### 11.1.3. Privacy

**Chi può vedere le mie cose?** *Amici*; l'opzione *Limita i post passati* va preferibilmente attivata (*Solo vecchi post*).

**Chi può contattarmi?** *Amici di amici* per entrambi i parametri.

**Chi può cercarmi?** *Amici* per le prime due opzioni, *No* per la terza.

### 11.1.4. Diario e aggiunta di tag

**Chi può aggiungere cose sul mio diario?** *Solo io*; *Sì.*

**Chi può vedere le cose che sono sul mio diario?** *Amici*; *Solo io.*

**Come faccio a gestire i tag aggiunti dalle persone e i suggerimenti di tag?** *Sì*; *Solo io*; *Amici* (obbligatorio per minorenni) oppure *Nessuno*.

### 11.1.5. Blocco

Questa sezione non ha impostazioni preliminari da definire.

### 11.1.6. Notifiche

**Modalità di ricezione delle notifiche:** disattivare *Emetti un suono alla ricezione di ogni notifica*; in *E-mail*, attivare *Solo le notifiche sul tuo account, su sicurezza e privacy*.

***Notifiche push:*** *Sì* per *Attività che ti riguardano*; Mai o *Su Facebook* per *Attività degli amici più stretti*; *Post degli amici* oppure *No* per *Attività nei gruppi*; tutto attivo per *Richieste e attività delle applicazioni*.

### 11.1.7. Per cellulare

Facoltativamente, immettere un numero di telefonino da usare con Facebook.

### 11.1.8. Persone che ti seguono

**Chi può seguirmi?** *Amici*, se non si tratta di un account di lavoro (in questo caso scegliete *Tutti*).

### 11.1.9. Applicazioni

**Applicazioni che usi:** In *Vuoi usare applicazioni*, scegliere *Sì*. Esaminare periodicamente l'elenco delle applicazioni ed eliminare quelle indesiderate o non più usate oppure regolare per ciascuna applicazione i permessi e la visibilità. Evitare applicazioni inutili.

**Applicazioni usate dagli altri:** tutto disattivato.

**Personalizzazione istantanea:** *No*.

**Versioni più vecchie:** *Solo io*.

### 11.1.10. Inserzioni

**Siti di terzi:** *Nessuno*.

**Inserzioni e amici:** *Nessuno*.

**Pubblico personalizzato:** Disattivato.

### 11.1.11. Pagamenti

**Metodi di pagamento:** non salvarne nessuno.

## 11.2. Facebook: impostazioni dell'app

Qui vengono elencate soltanto le impostazioni dell'app per cellulari e tablet che sono accessibili soltanto tramite l'app stessa. Quelle impostabili anche tramite l'interfaccia Web (ossia visitando il sito Facebook.com) sono descritte nella sezione precedente. Le stesse

impostazioni vanno fatte anche nell'app ausiliaria di Facebook, denominata *Messenger*.

**Chat di Facebook:** No.

**Servizi sulla posizione di Messenger:** disattivati.

**Sincronizza foto:** disattivato.

**Riproduci automaticamente video solo su Wi-Fi:** Sì.

**Notifiche:** inattive.

**Sincronizza contatti:** Non sincronizzare.

**SMS:** disattivato.

## 11.3. Twitter: impostazioni via Web

Accedete a queste impostazioni cliccando sull'ingranaggio in alto a destra e scegliendo *Impostazioni*.

### 11.3.1. Account

**Nome utente:** Preferibilmente diverso da quello reale.

**Email:** Preferibilmente un indirizzo di e-mail che solo voi conoscete, diverso da quello che usate abitualmente

**Non informarmi prima di mostrare contenuti sensibili:** disattivato.

### 11.3.2. Sicurezza e privacy

**Verifica d'accesso:** attiva su telefono (se disponibile) o su app.

**Proteggi i miei tweet:** attivato se volete scegliere i destinatari dei vostri tweet.

**Posizione dei tweet:** disattivata.

**Reperibilità:** disattivata.

**Personalizzazione:** *Non tracciare* attivato.

**Contenuto sponsorizzato:** *Personalizza gli annunci* disattivato.

### 11.3.3. Cellulare

Se l'opzione è disponibile nel vostro paese e con il vostro operatore cellulare, immettete il numero del vostro telefonino; meglio ancora, quello di un cellulare riservato che usate solo per l'autenticazione.

### 11.3.4. Notifiche email

Tutto disattivato tranne *I miei Tweet ricevono una risposta o vengo menzionato in un Tweet* (scegliendo *Da chiunque*) e *Notizie sul prodotto Twitter e sugli aggiornamenti delle funzioni*.

### 11.3.5. Profilo

**Connettiti a Facebook:** disattivato se volete tenere separato il vostro account su Twitter da quello su Facebook.

### 11.3.6. App

Controllate periodicamente che vengano elencate soltanto applicazioni che usate e conoscete e revocate l'accesso a tutte le altre.