

Cascati nella rete

Piccola guida per genitori non digitali di figli ultratecnologici



A cura di: Stefano Provenzano, Catrin Vimercati, Stefano Gubian

www.agvergente.org www.ilvergente.com email: agvergente@gmail.com

Indice

Facebook	1
Introduzione	1
Un po' di termini	1
Utilizzo e rischi	2
Furti di identità.....	2
Installazione di applicazioni malevole o "spione"	2
Immagini difficili da rimuovere completamente	2
Informazioni sulla privacy	2
Qualche consiglio	3
Usare il buon senso	3
Facebook non è il mondo reale.....	3
Come gestire la privacy	3
Ask.fm.....	4
Cos'è.....	5
Cosa dice il regolamento.....	5
Come proteggersi?.....	6
WhatsApp.....	6
I dubbi sulla privacy.....	6
Conclusioni	6

In queste pagine abbiamo cercato di raccogliere un po' di informazioni e dati utili che possono aiutare meglio a capire il fenomeno dei social network, quelle reti di contatti delle quali i nostri figli sembrano ormai non poter più fare a meno.

Molto spesso infatti i genitori sono molto meno preparati dei loro figli e non hanno strumenti sufficienti né per capire cosa fanno i ragazzi in rete né tantomeno per dare loro un aiuto e guidarli verso un uso consapevole, sicuro e positivo.

Ecco quindi alcune informazioni riepilogative sui principali temi e strumenti. Troverete anche cenni su strumenti e argomenti di cui non si è parlato nel nostro incontro di venerdì 14 marzo 2014, ma che si spera di poter approfondire in incontri successivi.

Questo infatti vuole essere il primo passo verso l'apertura di più fronti di indagine e discussione su questi temi, e i vostri suggerimenti saranno ben accetti.

Facebook

Introduzione



Facebook nasce nel 2004 come un portale social per gli studenti dell'università di Harvard, ma nel giro di poco tempo si estende ad altri istituti, fino ad arrivare qualche anno dopo ad aprirsi completamente al mondo e a diventare pian piano il social network con il maggior numero di utenti a livello globale.

Ecco alcuni numeri che aiutano ad avere un'idea delle dimensioni:

1. Sono 1,26 Miliardi gli utenti registrati (al 29/01/2014), di cui 87 milioni in Cina anche se in questo paese l'accesso è bloccato.
2. La fascia di utenza tra 15 e 35 anni è il 66%.
3. Il 70% degli adolescenti è "amico" dei propri genitori.
4. 300 è il numero medio di "amici" che gli adolescenti hanno su FB.
5. Sono 6 miliardi i "Like" (Mi piace), in aumento ogni giorno.
6. 17 Miliardi sono i post "taggati" su Facebook.
7. 350 milioni è la media giornaliera di foto caricate su FB.

L'uso di Facebook attualmente è leggermente in calo tra i giovanissimi, che sembrano preferire altre forme di socializzazione online, come Ask e WhatsApp.

Un po' di termini


Profilo: sulla guida ufficiale si legge che un profilo deve rappresentare una persona fisica realmente esistente (quindi nome e cognome devono essere verificabili, in qualunque momento, da Facebook), ma nella realtà non è sempre così. Per avere un profilo è inoltre necessario avere 13 anni compiuti.

Bacheca o wall: è la "pagina personale", dove vengono riportate le cose che fai e i commenti che scrivi.

Stato o post: messaggio o commento scritto su FB

Gruppo: è una pagina mirata alla discussione, condivisione e collaborazione su un determinato argomento o tema. È possibile inviare messaggi, inviti ed eventi che verranno visualizzati direttamente nella casella di posta dei membri del gruppo. Offre diverse opzioni per consentire l'appartenenza al gruppo: gruppo chiuso (per partecipare occorre essere invitati), gruppo limitato, gruppo segreto, gruppo aperto.

Pagina (o anche fan page): è una pagina di FB che raggruppa i fan o gli interessati a un personaggio, un prodotto, una trasmissione radiofonica o TV o altro ancora. Sono pagine aperte al

pubblico, ovvero chiunque può diventarne fan solo cliccando il pulsante . Le pagine consentono di pubblicizzare un prodotto, un marchio, un personaggio, un'azienda o qualsiasi altra cosa immaginabile.

Taggare: significa “etichettare” e deriva dall'inglese *to tag*. Su Facebook il termine indica la possibilità di associare i nomi alle persone che appaiono nelle foto e nei video. L'utente può etichettare un volto conosciuto cliccandoci sopra con il mouse e scegliendo il nome corrispondente alla persona dalla lista dei propri amici. La foto taggata apparirà sulla bacheca dell'amico in questione e verrà indicizzata nella sua cartella “foto”.

Utilizzo e rischi

Facebook è utile, ma richiede un po' di attenzione. Offre innumerevoli possibilità, come creare nuove amicizie, socializzare e rimanere in contatto con persone care che vivono o lavorano lontano, essere informato sulle ultime notizie o addirittura trovare un lavoro attraverso il passaparola.

Tuttavia è bene essere consapevoli anche dei rischi che si possono correre usando questo potente strumento.

Furti di identità

È sempre consigliabile usare password complesse e la connessione HTTPS (che è la versione crittografata della normale connessione HTTP) soprattutto se ci si trova in una zona dove è disponibile una rete WiFi libera, come un aeroporto o un locale pubblico.

Installazione di applicazioni malevole o “spione”

Sono quelle che in gergo tecnico vengono chiamate *malware* o *spyware*. Si tratta di applicazioni che promettono di far sapere chi guarda il proprio profilo, mentre in realtà portano a sondaggi che generano introiti per chi li ha creati, oppure link che segnalano dei video-shock. In questo caso si tratta spesso di esche il cui scopo è ingannare l'utente che, convinto di vedere un filmato, sta in realtà cliccando su un pulsante invisibile che gli fa compiere azioni involontarie e consigliare la trappola ai suoi amici;

Immagini difficili da rimuovere completamente

Le foto caricate sui server di Facebook possono essere cancellate dal profilo “padrone”, ma in realtà rimangono sul server per moltissimo tempo, rimanendo quindi accessibili da parte di chiunque attraverso un apposito codice di indicizzazione (ovviamente solo se lo si conosce).

Questo comunque vale in generale non solo per FB, ma per il Web in generale: è difficile far sparire dei contenuti, soprattutto se sono passati attraverso alcuni siti.

Informazioni sulla privacy

FB offre una serie di impostazioni che permettono di controllare quali informazioni rendere visibili a tutti o solo a pochi. Ad esempio, si possono controllare:

1. **Connessioni:** puoi controllare e decidere chi può cercarti su Facebook, inviarti una richiesta di amicizia e mandarti un messaggio privato.
2. **Diario e aggiunta di tag:** puoi controllare chi può pubblicare sul tuo diario e chi può vedere i post, verificare i post dove sei taggato prima di accettare il tag e chi può vederli, consentire il tag nei commenti dei tuoi post, decidere chi può taggarti nelle foto.

È importante ricordare che le persone con cui condividi i contenuti possono sempre condividere le tue informazioni con altri.

Infine, è bene ricordare che è possibile “bloccare” gli utenti indesiderati e utilizzare la funzione “Visualizza come” per vedere un’anteprima di come il tuo profilo viene visualizzato dal tuo amico o dalla persona indesiderata.

Qualche consiglio

Usare il buon senso

Prima di postare foto, video e informazioni personali, chiediamoci se quello che vogliamo pubblicare lo racconteremmo a nostra madre o al nostro capo, se vorremmo che fosse visibile anche a persone non gradite. Se la nostra risposta è no, forse è più sicuro non pubblicare questo contenuto. Invece di affannarsi a condividere ogni istante della propria esistenza, un utente di Facebook dovrebbe prima riflettere cosa potrebbe comportare quell’azione. Oggi, soprattutto grazie agli smartphone e ai tablet, condividere informazioni, foto video è sin troppo semplice e veloce e questo può far dimenticare che ogni informazione condivisa può dire moltissimo di noi, a volte sin troppo.

Facebook non è il mondo reale

I nostri figli tendono troppo spesso a scambiare Facebook con una sorta di mondo parallelo in cui immergersi totalmente, addirittura mettendo da parte la vita reale. Inutile dire come ciò sia un grosso errore. Condividere ogni più intimo aspetto della propria vita online può essere pericoloso, soprattutto se la cosa vien fatta senza la necessaria consapevolezza dei meccanismi che seguono il proprio clic. Stringere amicizie virtuali con chiunque, non sapendo chi ci sia davvero dall’altra parte, e seguire l’istinto di socializzazione può comportare gravi rischi.

Come gestire la privacy

Oltre al buon senso, il social network offre diversi strumenti che consentono di gestire la condivisioni dei dati. Le impostazioni del profilo contengono una sezione “Privacy” sulla quale è possibile agire. Sono troppi gli utenti che non badano a questo tipo di informazioni, che sono invece un’importante garanzia della propria vita online sul social network.



The image shows a screenshot of the Facebook privacy settings page. The page title is "Impostazioni sulla privacy e strumenti". The left sidebar contains navigation options: Generale, Protezione, Privacy (selected), Diario e aggiunta di tag, Blocco, Notifiche, Per cellulare, Seguaci, Applicazioni, Inserzioni, Pagamenti, and Riepilogo segnalazioni. The main content area lists several privacy settings with their current values and a "Modifica" link for each:

Setting	Current Value	Action
Chi può vedere le mie cose?	Pubblica	Modifica
Chi può vedere i tuoi post futuri?	Pubblica	Modifica
Controlla tutti i post in cui sei taggato	Usa il registro attività	Modifica
Vuoi limitare il pubblico dei post che hai condiviso con gli amici degli amici o con il pubblico?	Limita i post passati	Modifica
Chi può contattarmi?	Tutti	Modifica
Chi può inviarti richieste di amicizia?	Tutti	Modifica
Quali messaggi vuoi filtrare nella posta in arrivo?	Filtri di base	Modifica
Chi può cercarmi?	Tutti	Modifica
Chi può cercarti utilizzando l'indirizzo e-mail che hai fornito?	Tutti	Modifica
Chi può cercarti utilizzando il numero di telefono che hai fornito?	Tutti	Modifica
Vuoi che gli altri motori di ricerca rimandino al tuo diario?	Sì	Modifica

Chi può vedere le mie cose?

In questa sezione è possibile impostare alcuni parametri molto importanti.

- *Chi può vedere i tuoi post futuri?:* qui si può scegliere chi potrà vedere le nostre condivisioni. Le opzioni disponibili sono: *Pubblico* (chiunque navighi in rete e non solo i tuoi amici), *Amici* (ai tuoi amici e agli amici degli amici), *Amici tranne conoscenti* (solo ai tuoi amici), *Solo io* (per te e per le persone taggate nel contenuto), *Personalizzata* (vengono considerate valide le impostazioni che impostate in materia di privacy), *Amici più stretti o liste* (solo le persone incluse in queste liste vedranno il contenuto).
- *Controlla tutti i post in cui sei taggato:* permette di verificare i post in cui siamo stati taggati con la possibilità di rimuovere i tag o rendere invisibili i contenuti sul diario.
- *Vuoi limitare il pubblico dei post [...]:* utilizzando questo strumento, i contenuti del diario condivisi con amici di amici o utenti pubblici diventeranno visualizzabili solo agli amici.

Chi può contattarmi?

Questa sezione consente di gestire le relazioni virtuali.

- *Chi può inviarti richieste di amicizia?:* Se non vogliamo che le richieste di amicizia arrivino da chiunque, possiamo specificare che l'invio sarà consentito solo agli amici degli amici.
- *Quali messaggi vuoi filtrare nella posta di arrivo?:* gestione dei filtri dei messaggi privati

Chi può cercarmi?

Queste impostazioni permettono di gestire il comportamento dei motori di ricerca e la possibilità che un utente possa essere rintracciato.

- *Chi può cercarti utilizzando l'indirizzo eMail che hai fornito?:* è possibile specificare se il profilo potrà essere rintracciato tramite l'indirizzo e-mail, da tutti o solo dagli amici o dagli amici degli amici.
- *Chi può cercarti utilizzando il numero di telefono che hai fornito?:* chi ha fornito il proprio numero di telefono potrà essere rintracciato mediante questo. È possibile specificare se potranno farlo tutti o solo gli amici e gli amici degli amici.
- *Vuoi che gli altri motori di ricerca rimandino al tuo diario?:* questa impostazione consente di specificare se i motori di ricerca possano indicizzare il profilo utente in modo che possa essere rintracciato dalla rete.

Oltre alla sezione *Privacy*, dalle impostazioni del proprio profilo è possibile entrare nella sezione *Diario ed aggiunta Tag*, dove è possibile specificare chi può scrivere o condividere qualcosa all'interno della Timeline e verificare quali parti gli altri vedono del nostro diario. All'interno della sezione *Blocco* è possibile bloccare utenti fastidiosi e bloccare inviti a eventi e all'uso di certe applicazioni. Dobbiamo ricordare infatti che le applicazioni che installiamo possono avere accesso ai nostri dati (e quindi utilizzarli). Rimane però sempre possibile verificare a quali applicazioni abbiamo consentito di accedere ai nostri dati e rimuovere tale consenso.

Infine, un'ultima raccomandazione: all'interno della sezione *Protezione* è importante attivare, se non già attiva, l'opzione Navigazione Protetta. E non dimentichiamoci che, per difendere la nostra identità (ed evitare furti), è fondamentale usare una password robusta e non condividerla.

Ask.fm



Sembra che negli ultimi mesi le preferenze dei ragazzi che amano interagire online si stiano rivolgendo verso strumenti diversi dai social network tradizionali, come Facebook. Ask.fm è una di queste nuove piattaforme di socializzazione.

Cos'è

Ask.fm è una community particolare, che rispetto ai vari social presenta una caratteristica particolare: gli utenti possono interagire in forma anonima, utilizzando un *nickname*.

Su Ask.fm, che è tra i siti più utilizzati dai teenager, si possono porre domande per ottenere risposte, mentre per rispondere occorre registrarsi. L'ingresso è vietato ai minori di 13 anni, ma sappiamo bene che questo tipo di divieto su Internet è quasi un'istigazione a infrangerlo.

Da qualcuno è stato definito "l'anti Facebook", proprio per la sua caratteristica di anonimato: tutti gli utenti possono condividere foto e pensieri in completa libertà e il potersi nascondere dietro a un nome falso toglie i freni e annulla ogni tipo di inibizione, permettendo ai bulli della rete di insultare chiunque senza alcun limite. Questo invece non è possibile sui social tradizionali, perché esiste un controllo, se pur sporadico, e perché la possibilità di identificare chi insulta costituisce comunque un deterrente all'uso improprio o eccessivo di opinioni personali.

Di recente Ask.fm si trova nell'occhio del ciclone: molti episodi balzati tristemente agli onori della cronaca inducono infatti a pensare che questo social network sia diventato il regno del cyberbullismo.

L'obiettivo con cui è stato creato a Riga, in Lettonia, nel giugno del 2010, non è certo quello di lasciare spazio a prepotenti e cyberbulli. Ma Ask.fm è diventato il mezzo con cui gli adolescenti si scambiano insulti, minacce e persino istigazioni al suicidio.

Ed è così che, anche se il sito registra circa trecentomila nuovi utenti al giorno ed è disponibile in 150 paesi, Italia compresa, da più parti stanno arrivando richieste e petizioni per chiuderlo.

Il punto però è: chiudere Ask.fm o capire come tutelarsi giuridicamente da social network tipo Ask.fm, visto che in Italia e più in generale nel mondo ne esistono diversi? Il sito, in fondo, era nato anche con buone intenzioni, come mettere in contatto adolescenti giovani e un po' timidi tramite il meccanismo della domanda.

Cosa dice il regolamento

Collegandosi alla pagina <http://ask.fm/about/safety/about-company> è possibile leggerlo anche senza essere iscritti, mentre i Termini di utilizzo (<http://ask.fm/about/policy/terms-of-service>) permettono di avere un quadro completo del social.

Innanzitutto è interessante leggere la sezione Politica di Abuso, che elenca le principali azioni non permesse all'utente del sito Web: nell'elenco troviamo bullismo, troll, scrivere domande o commenti maleducati o volgari, o qualsiasi altra cosa che possa turbare o mettere in imbarazzo chiunque altro, comportamenti razzisti o qualsiasi altra cosa che possa offendere la razza, la religione o la sessualità di chiunque e altro ancora. E ad un certo punto, il documento recita: "Se un utente di ask.fm ti chiede qualcosa che ti fa sentire a disagio, che ti sconvolge o che ti fa arrabbiare, è sufficiente cliccare sul pulsante Blocca utente. Questo impedirà all'utente in questione di inviarti altre domande qualora accedesse ad ask.fm dall'indirizzo IP usato originariamente" [...] "Se qualcuno ti dà fastidio, ti turba o ti fa arrabbiare, o se pensi che qualcuno che hai precedentemente bloccato, ha creato un altro account per contattarti, faccelo sapere subito, utilizzando il pulsante Segnala. Prenderemo immediatamente in considerazione la tua segnalazione. T'inverremo anche alcuni link ad organizzazioni utili che potrebbero essere in grado di aiutarti".

Per quel che riguarda l'anonimato, sempre nelle condizioni di Ask.fm si legge: "Tutti sappiamo che alcune persone potrebbero abusare della possibilità di restare anonime per comportarsi in modo scortese o per dire cose cattive, giacché l'utente non saprà la loro identità. Per questo, prenderemo le giuste misure per impedirgli di rovinare l'esperienza ad altri utenti. Potremo

aiutare la polizia o le altre forze dell'ordine con le loro richieste nella misura stabilita dalla legge. In caso contrario, se l'utente desidera restare nell'anonimato, non dovrà comunicare a nessuno la sua identità”.

Come proteggersi?

Probabilmente l'unico modo per proteggersi è non iscriversi ad Ask.fm. Su Ask.fm non c'è controllo o filtro umano a quello che viene scritto. C'è un'avvertenza molto chiara quando ci si collega al sito: nessuno monitora il contenuto, anche se i comportamenti illegali, diffamatori e lesivi dell'utenza sono proibiti.

Ma nonostante le avvertenze relative alle possibili conseguenze, la frequentazione di Ask.fm è stata associata a un numero rilevante di episodi di cyberbullismo. Utilizzando Ask.fm si è esposti da subito a domande anonime, che sono attivate di default. Per ottenere un minimo di protezione, è sufficiente che l'utente, manualmente, modifichi l'impostazione. Messaggi come “Ucciditi”, “Prenditi un cancro”, “Bevi dell'ammoniaca” sono state segnalate dagli utenti in tutto il mondo ma non c'è modo di risalire a chi insulta, soprattutto se chi insulta si iscrive con un nome fittizio.

WhatsApp



WhatsApp è un'applicazione di messaggistica istantanea per smartphone che consente di scambiare messaggi, file multimediali e altro con chiunque abbia uno smartphone connesso a Internet con una rubrica contenente diversi contatti.

WhatsApp è un'applicazione per dispositivi mobili di piattaforme diverse (Apple iOS, Android, Windows Phone, Blackberry, ecc.) che consente di scambiare messaggi con i contatti della propria rubrica, che a loro volta devono avere installato il programma sul loro dispositivo.

Per svolgere le sue funzioni ha bisogno di una connessione a Internet, la stessa tramite la quale si ricevono e-mail o si naviga in Internet, pertanto non vi sono costi aggiuntivi per mandare i messaggi e rimanere in contatto con altre persone, oltre al costo della connessione stessa.

I dubbi sulla privacy

Secondo quanto sostiene il ricercatore Bas Bosschert, WhatsApp, di recente acquistato da Facebook per 19 miliardi di dollari, tiene ben poco in conto la privacy delle conversazioni degli utenti della piattaforma.

Bosschert spiega che è possibile “rubare” il database delle conversazioni salvate dagli utenti tramite un'altra app per Android terza che sfrutta il meccanismo usato da WhatsApp per proteggere crittograficamente il suddetto database e che consiste nell'usare la stessa chiave per tutti gli utenti.

Chiunque riuscisse a individuare la chiave potrebbe quindi accedere al database di un utente salvato in locale, ripetendo poi lo stesso processo per tutti gli utenti di WhatsApp. Un problema decisamente da non sottovalutare, anche perché di natura strutturale, ma a cui la società acquisita da Facebook non ha ancora risposto in modo ufficiale.

Conclusioni

Questa è una semplice introduzione ad alcuni strumenti con cui i ragazzi hanno a che fare ogni giorno per le loro forme di comunicazione con i loro amici. Gli argomenti che rimangono da approfondire sono molti, così come gli strumenti da analizzare. Non abbiamo parlato, per esempio, di Twitter, di Instagram o di SnapChat e di altri ancora. L'intenzione comunque era di dare qualche indicazione per iniziare a muoversi in questo mondo.

Per finire, segnaliamo alcune pagine Web dove potrete trovare maggiori informazioni su questi argomenti.

Polizia Postale e delle Comunicazioni

<https://www.commissariatodips.it/da-sapere.html>

<https://www.commissariatodips.it/da-sapere/per-i-genitori/navigazione-sicura-e-consapevole-dei-minori-su-internet.html>

<https://www.commissariatodips.it/da-sapere/per-i-genitori/uso-sicuro-del-telefonino-di-tuo-figlio.html>

Potete poi trovare il manualetto *Il Web per amico - Un uso responsabile della Rete*, all'indirizzo http://img.poliziadistato.it/docs/brochure_web_amico.pdf

Il Comune di Milano ha realizzato un pieghevole contenente 10 consigli ai genitori per una navigazione sicura. L'indirizzo è

[http://www.comune.milano.it/dseserver/webcity/documenti.nsf/be5c64af5ff84136012568410060d104/825c9006ef302813c12578c50041dfd4/\\$FILE/Internet%20genitori.pdf](http://www.comune.milano.it/dseserver/webcity/documenti.nsf/be5c64af5ff84136012568410060d104/825c9006ef302813c12578c50041dfd4/$FILE/Internet%20genitori.pdf)

Potete però trovarlo facilmente inserendo come chiave di ricerca i termini comune Milano internet genitori in Google.