Università degli Studi di Perugia

Dipartimento di Matematica ed Informatica

Corso di laurea in Matematica

A.A. 2010/11

Social Network Forensics

Studenti:

Paola Ginnasi
Andrea Burattini

Docente:

Stefano Bistarelli

INDICE

INTRODUZIONE

I Social Network hanno cambiato il modo in cui interagiamo nella nostra vita personale, il nostro modo di conoscere e presentarci agli altri, generando un mondo parallelo al mondo reale. Anche nella vita professionale stanno acquistando sempre maggior spazio, permettono infatti alle aziende di incrementare i servizi, mantenere e rafforzare le relazioni, svolgere iniziative di marketing e generare nuovi contatti. Con centinaia di milioni di utenti ogni giorno, i Social Network hanno attratto “aggressori” più di ogni altro obiettivo negli ultimi anni. Dato che il loro successo dipende dal numero di utenti che attirano e dalle loro connessioni, il principale obiettivo degli sviluppatori è stato quello di incrementare tale numero tralasciando alcune priorità come la sicurezza. Di conseguenza ai numerosi vantaggi offerti dai Social Network si contrappongono significativi rischi per gli utenti.

Oltre ad analizzare le minacce che possono derivare dall’uso dei Social Network, è importate offrire agli utenti strumenti per impedire che diventino vittime di tali minacce e infine, se un crimine è stato commesso, dare la possibilità di rintracciare l’autore del reato.

Che cosa sono i Social Network

Si definiscono siti di Social Network quei servizi web-based che permettono agli individui di costruire un profilo pubblico o semi-pubblico all’interno di un sistema limitato, articolando un elenco di contatti con altri utenti con cui condividere informazioni di qualsiasi tipo.

Come funzionano

Ai social network ci si partecipa registrandosi e compilando un profilo più o meno dettagliato. Una volta registrato, possiamo "*socializzare*" con i vari membri della community iniziando a: leggere i profili e i blog di altri utenti, aggiungere o eliminare amici, visionare video e foto personali, comunicare tramite Messaggi Privati o Live chat ed iscriversi a Gruppi di persone che condividono i tuoi stessi interessi od hobby. E' comunque quasi sempre possibile visionare i profili degli utenti iscritti anche se non si è registrati.

PROBLEMI DI SICUREZZA LEGATI AI SOCIAL NETWORK

Tra i numerosi problemi di sicurezza che caratterizzano i Social Network, alcuni tra i più frequenti sono:

Cross Site Scripting

Permette ad un hacker di inserire un codice e modificare il contenuto della pagina web visitata, è così possibile sottrarre dati sensibili nel browser degli utenti che successivamente visiteranno la pagina.
Gli attacchi alle vulnerabilità XSS hanno effetti dirompenti per i siti con un elevato numero di utenti, dato che è sufficiente una sola compromissione per colpire chiunque visiti la stessa pagina.

Spear Phishing e Social Network specific Phishing

Il phishing è una truffa mirata al furto di identità e di dati sensibili come password, numero di carta di credito ecc. La truffa si esegue tramite email false, ma anche contatti telefonici, che riproducono l'apparenza grafica dei siti di banche, poste, ecc…
Lo spear phishing impiega una strategia di phishing molto più mirata. Gli autori di questo tipo di frode inviano messaggi di posta elettronica, link e contatti che sembrano attendibili a tutti gli impiegati o i membri di una determinata società, ente statale, organizzazione o gruppo.
La struttura del messaggio lascia intendere che il mittente è il datore di lavoro o un altro dipendente o collega e può includere richieste di nomi utente e password.
In realtà le informazioni sul mittente vengono falsificate o ricavate tramite "spoofing". Mentre il phishing tradizionale si propone lo scopo di sottrarre informazioni da singoli utenti, le frodi che si basano sullo spear phishing hanno come obiettivo quello di penetrare all'interno dell'intero sistema informatico di una società.
Se fornisci il nome utente o la password oppure selezioni dei collegamenti o apri gli allegati in un messaggio di posta elettronica, in una finestra a comparsa o in un sito Web di spear phishing, diventi vittima di un furto d'identità ed esponi a rischi gli altri dipendenti o membri del tuo gruppo di lavoro.
Le frodi tramite lo spear phishing sono rivolte anche agli utenti che utilizzano un determinato prodotto o sito Web. Gli autori di tali frodi utilizzano qualsiasi informazione a disposizione per personalizzare un messaggio di phishing, in modo da restringere il più possibile il gruppo di utenti a cui è rivolto.

Cyber Bullying

Nell'era di Internet, della posta elettronica, dei blogs, e dei telefoni cellulari sempre più tecnologici, il fenomeno generale del bullismo ha assunto perciò nuove forme, tutte riconducibili all'espressione cyberbullying, o "bullismo elettronico". Il bullo non agisce più esclusivamente all'interno del "mondo reale": oggi molesta le sue vittime anche attraverso il "mondo virtuale" offerto dalla rete.

Alla base di queste nuove forme di bullismo vi è la possibilità di trasmissione elettronica delle informazioni. L'informazione specifica, come ad esempio il pettegolezzo offensivo, l'insulto, o la minaccia, non viene più trasmessa oralmente, o per via cartacea, ma attraverso l'utilizzo di moderni e sofisticati strumenti, come ad esempio i siti di Social Network, l'e-mail, i blogs , gli SMS, i messaggi multimediali per cellulari (MMS), ecc.
Il bullo ha perciò nuove vie e nuovi strumenti per perseguitare le sue vittime: è così che il fenomeno del bullismo è cresciuto in maniera impressionante, varcando velocemente i confini fisici dei corridoi e delle mura delle scuole, per svilupparsi nello spazio ben più indefinito e vasto del web. Le offese, le minacce, i pettegolezzi, gli attacchi verbali, le botte, le aggressioni, episodi assai frequenti all'interno del sistema-scuola, sono stati così trasportati rapidamente nelle pagine web visibili in tutto il mondo. Le molestie verbali inoltre, vengono sempre di più inviate attraverso l'uso delle nuove tecnologie messe a disposizione dei telefoni cellulari, delle videocamere e dei PC.
Il cosiddetto "Cyber Bullying" ha anche un'altra caratteristica molto pericolosa che è quella di consentire al bullo di mantenere in rete il quasi totale anonimato, rendendo difficile sia rintracciarlo che perseguirlo con mezzi legali.

CBIR (Content-based Image Retrival)

I CBIR sono sistemi di recupero di immagini, digitali e fisse, basati su attributi visuali del contenuto di tali immagini.
I sistemi CBIR considerano essenzialmente gli elementi formali intrinseci che caratterizzano l'immagine, ovvero il livello formale o plastico. Tra gli elementi formali grafici di carattere intrinseco, che possono essere estratti e analizzati da questi sistemi si trovano colori, texture, figure e relazioni topologiche tra questi attributi. Con l'analisi di questi attributi, si producono automaticamente le strutture di composizione dell'immagine. Il recupero dei dati non è altro che un processo di estrazione dei tratti visuali, considerati come il vero contenuto dell'immagine.

Si possono distinguere tre fasi del funzionamento dei sistemi CBIR:

- Fase di archivio: Le caratteristiche intrinseche delle immagini vengono analizzate automaticamente. Si generano vettori di caratteristiche grafiche per ciascuna immagine. L'indice visuale vincola ciascun attributo all'immagine che lo contiene.
- Fase di consultazione: l'utente specifica una o più caratteristiche visuali mediante le opzioni che sono disponibili sull'interfaccia:
    - Consultazione attraverso esempi visivi.
    - Consultazione attraverso l'immagine indice mostrata.
    - Consultazione mediante l'esempio realizzato.
    - Uso del linguaggio visivo.
- Fase di recupero: Le immagini vengono mostrate in ordine decrescente di somiglianza.

Vi è un interesse crescente nei sistemi CBIR dovuto alle limitazioni presenti nei sistemi basati sui metadati, come la grande offerta di impieghi possibili per il recupero efficiente delle immagini.

La necessità di questo sistema si riassume in tre idee:

- La crescente quantità delle immagini digitali.
- Il fatto che il Web sia una risorsa aperta.
- Che il motore di ricerca attuali si basino sul titolo delle immagini, con la limitazione che questo suppone.

Sfruttando questi sistemi è possibile scansionare gli album fotografici personali degli utenti dei Social Network (almeno quelli non protetti dal filtro della privacy) rintracciando foto che hanno determinate caratteristiche e sfruttandole poi per i motivi più svariati.

Spam

Il termine trae origine da uno sketch comico del Monty Python's Flying Circus ambientato in un locale nel quale ogni pietanza proposta dalla cameriera era a base di Spam (un tipo di carne in scatola). Man mano che lo sketch avanza, l'insistenza della cameriera nel proporre piatti con "spam" ("uova e spam, uova pancetta e spam, salsicce e spam" e così via) si contrappone alla riluttanza del cliente per questo alimento, il tutto in un crescendo di un coro inneggiante allo "spam" da parte di alcuni Vichinghi seduti nel locale.
Al di là delle note di colore, il significato del termine “spam” risulterà noto a tutti. La maggior parte degli utenti di internet che possiedono una comune casella di posta elettronica ogni giorno ricevono con decine di email pubblicitarie che riempiono la “posta in arrivo”.
Il principale scopo dello spamming è la pubblicità, il cui oggetto può andare dalle più comuni offerte commerciali a proposte di vendita di materiale pornografico o illegale, come software pirata e farmaci senza prescrizione medica, da discutibili progetti finanziari a veri e propri tentativi di truffa. Uno spammer, cioè l'individuo autore dei messaggi spam, invia messaggi identici (o con qualche personalizzazione) a migliaia di indirizzi e-mail. Questi indirizzi sono spesso raccolti in maniera automatica dalla rete (articoli di Usenet, pagine web) mediante spambot ed appositi programmi, ottenuti da database o semplicemente indovinati usando liste di nomi comuni.
Nei Social Network accade la stessa cosa: le pagine personali degli utenti vengono inondate di annunci pubblicitari e link a siti di e-commerce. Questo è possibile per svariate ragioni:

- La prima e la più importante è che spesso molti degli utenti dei Social Netork condividono informazioni con chiunque, anche sconosciuti. Sicuramente questo è uno dei lati “attraenti” di un Social Network, ma favorisce la divulgazione del proprio account e dà accesso alla nostra pagina a svariati soggetti fra i quali ci possono essere degli spammer.

- La seconda è che alcuni Social Network consentono a chiunque di inviare o pubblicare messaggi agli utenti senza che questi ne abbiano dato il permesso.
- La terza, è legata all'esistenza dei malaware e del phishing. Tali strumenti sfruttano espedienti per poter acquisire permessi di accesso al nostro sistema o al nostro account. Una volta ottenuti tali permessi (concessi direttamente dall'utente ignaro del pericolo) inviano messaggi e link agli utenti contenuti nella nostra cerchia di contatti.

Worms

Un worm (letteralmente "verme") è una particolare categoria di malware in grado di autoreplicarsi. È simile ad un virus, ma a differenza di questo non necessita di legarsi ad altri eseguibili per diffondersi.
Il termine deriva da un romanzo di fantascienza degli anni 1970 di John Brunner: i ricercatori che stavano scrivendo uno dei primi studi sul calcolo distribuito notarono le somiglianze tra il proprio programma e quello descritto nel libro e ne adottarono il nome. Uno dei primi worm diffusi sulla rete fu Internet Worm, creato da Robert Morris, figlio di un alto dirigente della NSA il 2 novembre 1988, quando internet era ancora agli albori. Tale virus riuscì a colpire tra le 4000 e le 6000 macchine, si stima il 4-6% dei computer collegati a quel tempo in rete.
Il mezzo più comune impiegato dai worm per diffondersi è la posta elettronica: il programma maligno ricerca indirizzi e-mail memorizzati nel computer ospite ed invia una copia di sé stesso come file allegato (attachment) a tutti o parte degli indirizzi che è riuscito a raccogliere. I messaggi contenenti il worm utilizzano spesso tecniche di social engineering per indurre il destinatario ad aprire l'allegato, che spesso ha un nome che permette al worm di camuffarsi come file non eseguibile.
Analogamente alla posta elettronica, gli worms agiscono sui Social Network ricercando gli account degli utenti e inviando loro delle richieste di adesione a gruppi o accesso ad applicazion. Nel momento in cui l'utente accetta tali richieste riceve in automatico il dawnload sul proprio computer del malaware.

Furto di identità

In termini strettamente legali, il furto d'identità è il reato che viene commesso quando qualcuno usa l'identità di un'altra persona per una qualsiasi attività con valore legale (la sottoscrizione di un contratto per esempio). Nei Social Network in particolare e in Internet più in generale questo fenomeno ha trovato un terreno fertilissimo. Per iscriversi a un social network basta infatti un indirizzo di posta elettronica ed è molto semplice fingere di avere una mail come *pinco.pallino@hotmail.it*. Un pò meno facile è trovare la password di una mail già esistente e usarla a proprio piacimento. Una volta in possesso di tale password ci si può spacciare per la persona interessata dal furto e sfruttare i suoi contatti per ottenere informazioni. Oppure, con l'aiuto di un po' di ricerche sulla vittima, truffare persone e società

A differenza dei forum e delle chat, nei Social Network la maggior parte degli utenti è identificabile con il proprio nome di battesimo e non con un soprannome. Perciò altri utenti possono reperire rapidamente il profilo, inoltre chiunque conosca il vostro nome può reperire rapidamente svariate informazioni sulla vostra persona. Alcuni network come Facebook, MySpace o Twitter permettono ai motori di ricerca l'accesso ai dati. Di conseguenza, chi digita il nome di una persona, per esempio su Google, può trovare un rimando al corrispondente profilo, o addirittura leggerne gli estratti. Solo pochi Social Network (e nessuno di quelli più diffusi) proibiscono ai motori di ricerca di frugare all'interno dei loro contenuti.

Spionaggio Industriale (Corporate Espionage)

Le problematiche legate a questo fenomeno nei Social Network sono in rapida espansione. Le cause sono imputabili all'imperizia degli impiegati che durante le ore di lavoro, utilizzando i sistemi aziendali, si connettono alla rete ed entrano in contatto con persone esterne all'azienda.
Le strategie aziendali relative ai Social Network e le policy di sicurezza spesso trascurano la necessità di un piano di gestione della crisi per affrontare le problematiche che emergono dal loro utilizzo, in termini di autenticità, sicurezza e privacy. Come citato nel report di Panda, Facebook è "eletto" come massimo colpevole di infezioni di malware con il 71.6% e di violazioni della privacy (73.2%), Twitter dà il proprio contributo nelle violazioni della privacy con il 51%. Secondo le opinioni delle aziende che hanno subito perdite finanziarie a seguito di queste violazioni, Facebook è stato il sito più sfruttato (62%), seguito da Twitter (38%), YouTube (24%) e LinkedIn (11%).

Stalking

Configura il reato di stalking la persecuzione attuata con l'invio di video e messaggi tramite un Social Network.
Anche il Diritto italiano si "adegua" all'evoluzione dei mezzi di comunicazione. Ad esempio, tenendo in considerazione l'importanza dei *S*ocial Network, come il famoso facebook, sempre più utilizzato per condividere stati d'animo, trovare nuovi amici, riallacciare vecchi contatti.
È infatti reato di "atti persecutori", o stalking, così come stabilito dall'art. 612-bis del codice penale, la condotta di chi vessa la vittima provocando in lei uno stato di profondo disagio e paura utilizzando Facebook.
L'estrema facilità di comunicazione con utenti sparsi in tutto il mondo è la causa principale di questo fenomeno; raggiungere il potenziale bersaglio è abbastanza semplice e una volta ottenuto il contatto, per la vittima risulta difficile controllare lo stalker che può agire indisturbato, sfruttando le enormi potenzialità di comunicazione che i Social Network offrono.

PRIVACY E SOCIAL NETWORK

Quello della privacy è sicuramente un dei problemi cardine legato dall'uso dei Social Network. Il semplice fatto che gli utenti sono tenuti a compilare un proprio profilo, contenente dati più o meno sensibili, costituisce una minaccia per gli utenti stessi, poiché spesso tali profili sono di dominio pubblico e consultabili anche da chi non è registrato come utente del Social Network.
Alcuni sistemi offrono dei servizi che cercano di limitare e/o controllare la diffusione di dati persolali inseriti nel proprio profilo:

Filtro della privacy

Uno strumento efficace, comune ormai a quasi tutti i Social Network, per tutelare il più possibile la propria identità è il: Filtro della Privacy.
All'interno del pannello di controllo del proprio profilo è possibile impostare, di norma, il Filtro della Privacy e scegliere fra tre livelli di sicurezza predefiniti: Basso, Medio, Alto (consigliato.)
Basso: Il vostro profilo è visualizzabile da tutti, anche ai visitatori non registrati.
Medio: Il vostro profilo è visualizzabile dai vostri amici e dalle persone facenti parte dei Gruppi a cui vi siete iscritti, vale a dire tutte quelle persone legate dai vostri stessi interessi.
Alto (consigliato): Il vostro profilo è visualizzabile solo dai vostri amici.
Per i più esperti è anche possibile scegliere quale informazione far visualizzare e a chi.

Visitor Tracker

Il Visitor Tracker è uno strumento offerto solamente da alcuni Social Network che consente agli utenti di conoscere chi e quando ha visualizzato il proprio profilo. Questa opzione aumenta la protezione e facilita l'utente nel monitoraggio del proprio account.

Scripting

Alcuni Social Network offrono la possibilità agli utenti di inserire parti di codice HTML o script Java all'interno della propria pagina. Se sfruttata con criterio, questa opportunità consente di monitorare con estrema precisione gli accessi e i contatti sulla nostra pagina personale, tuttavia diventa un problema quando questa opportunità viene consentita anche ai visitatori. Alcuni Social Network infatti permettono a chiunque di pubblicare codice html o script sulla pagina personale di un utente, consentendo così a terze persone di monitorare il traffico sulla nostra pagina, acquisire contatti di altri utenti.
Come è possibile vedere dalla tabella sotto, alcuni Social Network non offrono un servizio di Visitor Tracker, tuttavia per quei siti che consentono di inserire parti di codice sulla nostra pagina, crearsene uno è molto semplice: si posiziona un pezzo di codice (HTML o

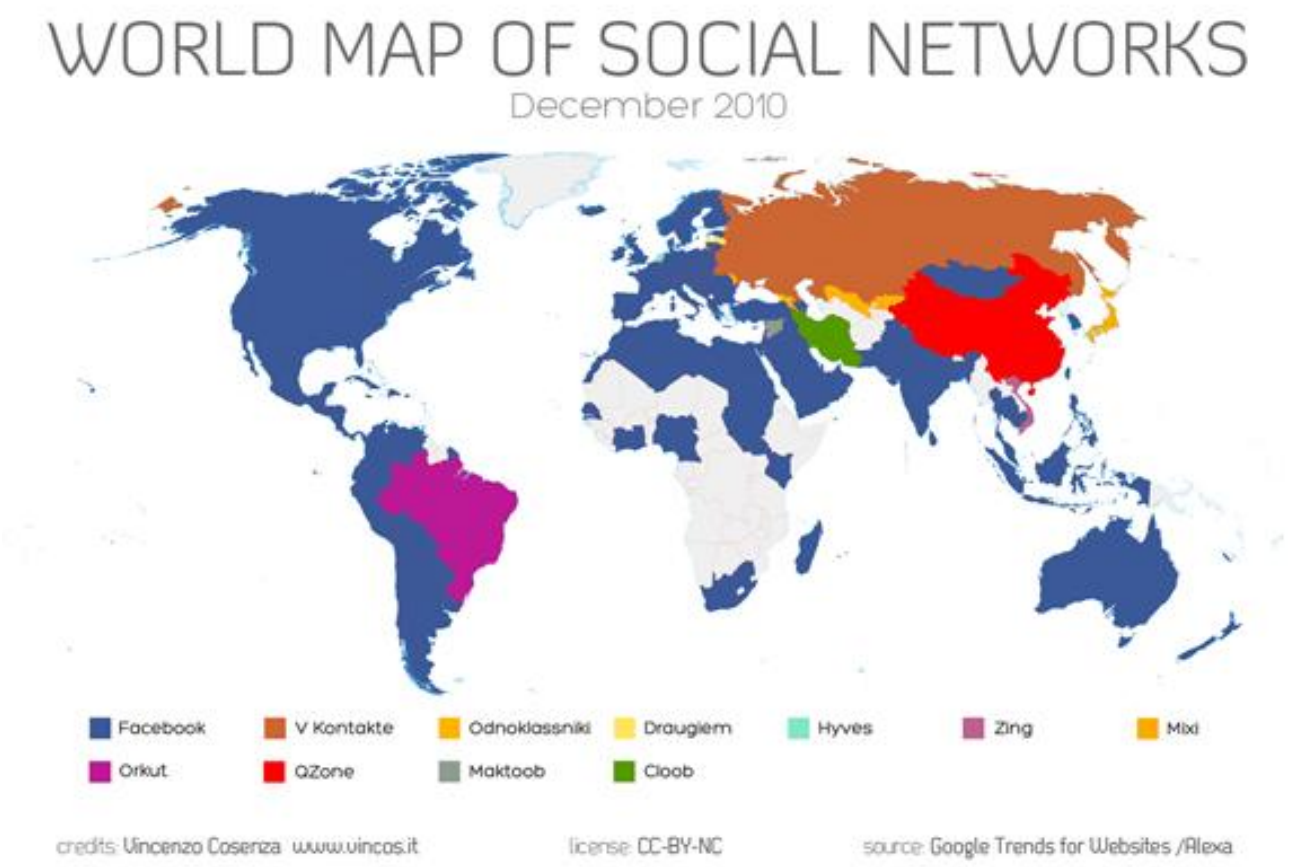
Java di solito) sul vostro sito, quando qualcuno visita la pagina e il codice viene eseguito, questo analizza e memorizza i dati pubblici del visitatore (indirizzo IP, browser, sistema operativo, referrer, titolo di pagina e url ecc). Un Visitor Tracker registra anche i visitatori in caso di ritorno alla stessa pagina più di una volta ed offre una cifra realistica degli ospiti del sito web.

Vediamo quali fra i 10 Social Network più diffusi offrono i servizi descritti:

Social Network	Filtro della Privacy	Visitor Tracker	Supporto codice HTML o JAVA
Bebo	Si	No	No
Facebook	Si	No	No
Friendster	Si	Si	No
Hi5	Si	Si	Si
MySpace	Si	No	Si
Netlog	Si	No	No
Orkut	Si	Si	No
PerfSpot	Si	Si	Si
Yahoo!360	Si	No	Si
Zorpia	Si	No	No

(fonte "Virtual Forensics: Social Network Security Solutions" Seidenberg School of CSIS, Pace University)

IL SOCIAL NETWORK PER ECCELLENZA: FACEBOOK



*Una mappa nuova del mondo, che mostra i social network più diffusi del paese, secondo Alexa e Google Trends per il traffico del sito web * dati (dicembre 2010).*

Facebook è senza alcun dubbio il Social Network più diffuso ed utilizzato in tutto il mondo. Rispetto ad altri siti è stata dedicata una maggior attenzione alla sicurezza ed alla privacy, fornendo una enorme possibilità di personalizzazione delle proprie impostazioni di account che diversi altri concorrenti non offrono. Tuttavia, pur risultando sotto vari aspetti un Social Network all'avanguardia, Facebook ha i suoi "punti deboli" che tutti gli utenti dovrebbero conoscere per poter usufruire del servizio in totale sicurezza.

Iscrizione e creazione del proprio profilo

Per iscriversi a Facebook sono necessarie : una casella di posta elettronica, una password, nome e cognome. Per gli utenti questo è sicuramente un vantaggio poiché non sono costretti ad inserire altri dati personali per accedere al servizio, tuttavia, come già detto in precedenza, questo risulta anche la causa principale di un dei problemi che affligge irrimediabilmente Facebook e praticamente tutti i Social Network in circolazione: il

furto di identità. Chiunque può creare un profilo con un nome qualsiasi e fingersi un'altra persona, contattare utenti fingendosi magari un amico o un conoscente, con intenzioni più o meno legali, sottrarre dati sensibili dai profili degli utenti stessi, il tutto mantenendo il proprio completo anonimato.
Purtroppo in questo caso ben poco si può fare per ovviare al problema se non prestare estrema attenzione alle persone con le quali scambiamo informazioni, evitando di divulgare dati sensibili o personali anche se siamo sicuri dell'identità dell'utente con il quale stiamo interagendo.

Protezione del profilo, il Filtro della Privacy di Facebook

Facebook offre un Filtro della Privacy molto efficace e personalizzabile.
Si può scegliere tra la condivisione con tutti, amici di amici, solo amici, e personalizza (nessuno o solo certi amici).
Ecco una lista delle possibiità di personalizzazione più importanti:

- Non voglio andare sui motori di ricerca. I motori di ricerca conservano le informazioni personali dove la privacy è stata impostata su "tutti". Per scegliere di non comparire occorre andare, nel menu privacy, su "ricerca". Poi togliere l'opzione "consenti" in "risultati di ricerca pubblica".
- Scelgo io chi può accedere alle mie foto. Per fare in modo che la foto del profilo non sia visibile sui motori di ricerca o impostare diversi livelli di privacy bisogna andare su "informazioni personali", poi "album fotografici" e "profilo".
- Quell'utente è indesiderato. Di fronte a richieste insistenti (e indesiderate) c'è l'opzione "elenco utenti bloccati" dal menu generale "impostazioni sulla privacy". Una volta inserito il nome, la persona non potrà più stringere amicizia o interagire su Facebook.
- Personalizzazione istantanea. E' una funzione che ha suscitato diverse polemiche fra gli utenti. Permette di condividere i dati personali con alcuni siti esterni. Per eliminarla, dal menu privacy, occorre andare su "applicazioni e siti web" e barrare personalizzazione istantanea.

Non tutti i gestori dei servizi dicono chiaramente cosa faranno con i dati relativi agli utenti. La legge italiana vi consentirebbe di rifiutare esplicitamente il trasferimento dei dati a terzi al momento dell'iscrizione, ma Facebook non offre alcun modo per farlo. Alcuni Social Network si offrono di esaminare la vostra casella di posta elettronica, per verificare se le persone di cui avete l'indirizzo in rubrica sono già iscritte, e includerle direttamente nella lista dei vostri amici.

Servizio BEACON

Il servizio Beacon di Facebook tiene traccia delle attività di tutti gli utenti in siti partner di terze parti, comprese le persone non iscritte a Facebook o che hanno cancellato il loro account. Beacon cattura dettagli legati agli utenti e alle loro attività sul sito di un partner esterno, memorizza quindi l'indirizzo IP, la data del contatto, gli indirizzi delle pagine

visitate ecc. Chiaramente questo servizio ha i suoi lati negativi e positivi: se da una parte offre la tracciabilità degli utenti e da quindi alle autorità la possibilità di rintracciare gli autori di qualsiasi fatto illecito commesso su Facebook, dall'altra costituisce una riserva preziosa di informazioni e dati sensibili che potrebbero rappresentare l'obiettivo di hacker e spammer.

Facebook: aggiunto il protocollo HTTPS (HTTP Secure) per migliorarne la sicurezza

La novità è stata resa nota dopo un avvenimento abbastanza clamoroso, in cui una pagina dei fan di Mark Zuckerberg, CEO di Facebook, era stata hackerata, una situazione che non è che abbia fatto una buona pubblicità al social network.
In teoria sarebbe già possibile effettuare l'accesso mediante il protocollo HTTPS attivandolo dalle impostazioni dell'account, ed anche se non è visibile, una volta settato, la connessione sarà sicura a tutti gli effetti. Come agirebbe questo nuovo protocollo? Mediante una sorta di filtro per applicazioni di terze parti, che non potranno accedere mediante connessione HTTPS; da un lato viene migliorata la sicurezza, ma dall'altra il Social Network perderebbe gran parte del suo fascino.
In passato c'era la possibilità di effettuare un accesso HTTPS, mediante un plugin di Firefox, ma questo non era compatibile con la maggior parte delle altre feature di Facebook.

Differenza tra protocollo http ed https

Il normale traffico effettuato attraverso il browser si basa sul protocollo HTTP (*Hyper Text Transfer Protocol*), un'applicazione che si preoccupa solo del trasferimento delle informazioni tra il mittente ed il destinatario, senza porre in relazionare i dati tra le sessioni precedenti e le successive. Questo, in termini pratici, significa minore quantità di dati da trasferire e dunque maggior velocità. Il traffico HTTP avviene, in ricezione e trasmissione, mediante protocollo TCP (*Transmission Control Protocol*) sulla porta 80 del nostro computer.
Sintatticamente identico al protocollo impiegato per la normale navigazione in rete, l' HTTPS (*Secure HyperText Transfer Protocol*) impiega, oltre ad i protocolli TCP e HTTP, un ulteriore livello che si occupa della crittografia ed autenticazione dei dati trasmessi, chiamato SSL (*Secure Sockets Layer*). I dati transitano sulla porta 443 anziché 80.
Ipotizziamo di esser seduti davanti al nostro PC e navigare in internet con un browser qualsiasi come Internet Explorer, Firefox, Chrome… Il software di navigazione non fa altro che interpretare le istruzioni che giungono via HTTP e trasformarle secondo il disegno di chi ha creato la pagina web che visitiamo. Oltre a sapere cosa fare se clickiamo su un link (e poche altre operazioni) il browser non è in grado di fare altro. Come i dati transitino da un punto all'altro o se questi siano più o meno completi, non è compito che gli riguarda. E' il prezzo da pagare se vogliamo che la trasmissione dei dati sia molto veloce; in fondo non sempre è necessario crittografare le informazioni che stiamo cercando sul web.

Con l'HTTPS la situazione è diversa. La sicurezza diventa necessaria e dunque rendere univoci i mittenti ed i rispettivi destinatari delle informazioni diventa indispensabile. Il protocollo SSL prende i dati, in entrata come in uscita, e li cripta attraverso un algoritmo matematico che li rende praticamente indecifrabili. Più è complesso l'algoritmo più risultano *blindati* i dati trasmessi, più risulta difficile violarne la riservatezza.
L'operazione di criptaggio avviene quando il proprietario di un sito web acquista un certificato da un'autorità di certificazione o lo genera in proprio. Questo certificato non è altro che un codice di notevole complessità creato *ad hoc* per uno specifico utente e per uno specifico sit, in una specifica sessione. Oltre il codice vengono acquisite anche informazioni aggiuntive relative alle entità interessate, come ad esempio il nome del server che ospita il sito o gli indirizzi IP.
Tutto ciò allo scopo di rendere evidentemente il più affidabile possibile il sito al quale ci apprestiamo ad inviare le nostre informazioni riservate. Il browser in presenza di una connessione HTTPS visualizza una finestra con tutti i dati caratteristici della connessione e chiede all'utente l'eventuale accettazione del certificato.

CONCLUSIONE

"Il web è a un punto di svolta molto importante. Fino a poco tempo fa, la normalità sul web era che la maggioranza delle cose non erano sociali e la maggior parte delle persone non usava la propria identità reale. Stiamo costruendo un nuovo web in cui alla base vi è il "sociale". "

Sono queste le parole di Mark Zuckerber, fondatore di Facebook, riguardo un nuovo modo di vivere il web dove, un ruolo principale spetta sicuramente ai Social Network. In questa relazione abbiamo cercato di porre l'attenzione su tutti i problemi che questo mondo virtuale riserva ai suoi numerosissimi utenti spesso del tutto inconsapevoli dei rischi che possono nascondersi dietro la condivisione di immagini, informazioni personali, applicazioni ed ogni altra azione che può sembrare la più banale e "sociale".

In ultimo non possiamo non riportare una analisi pubblicata alcuni giorni fa sul blog ufficiale di *Symantec*, società specializzata in sicurezza informatica. Una specifica vulnerabilità delle API sfruttate da Facebook, attive fin dal primo lancio nel 2007, avrebbe permesso ad un numero spropositato di applicazioni di avere accesso, in maniera quasi totale, alle informazioni contenute in milioni di profili. Date di nascita, indirizzi fisici e di posta elettronica, album fotografici, addirittura conversazioni avvenute tramite messaggi privati o chat. Contenuti ed informazioni finite nelle mani di terze parti, consegnate inavvertitamente da almeno 100mila applicazioni presenti sul gigantesco Social Network. La *Symantec* non è riuscita a quantificare la possibile mole di dati e informazioni che potrebbero essere ancora in possesso di società terze.

Questi dati ci mostrano quanto il problema sia rilevante e quanto sia fondamentale sviluppare e potenziare strumenti per la tutela di tutti gli utenti.