Internet e figli

insegniamo ai nostri figli a navigare in sicurezza

Ed. 25 settembre 2016

Stefano Ramacciotti
C.I.S.S.P. | 357229
Membro Direttivo (ISC)2 Italy Chapter
Coordinatore GdL Educazione alla Sicurezza Informatica

premessa.

premessa

perchè un ennesimo ebook sulla sicurezza informatica?

Perché spesso, quando andiamo nelle scuole a fare le nostre presentazioni ci viene chiesta la consegna del materiale.

Molti di noi relatori del Gruppo di Lavoro di "Educazione alla Sicurezza Informatica" di (ISC)^2 Chapter Italy che fanno attività nelle scuole, in comunità e in centri ricreativi, viene chiesto di poter consegnare le presentazioni mostrate. Quest'ultime però sono volutamente povere di contenuti scritti per permettere al relatore di trattare più proficuamente i vari punti.

Abbiamo, così, pensato di creare un ebook organizzando in modo più strutturato i contenuti. Questo lavoro è rivolto principalmente a genitori e insegnanti che pensiamo abbiano un po' di dimestichezza con gli strumenti informatici. E' stato, infine, adottato un formato *ebook* orizzontale, più idoneo ad essere visualizzato su uno schermo di computer o su un *tablet* senza trascurare di dare una mano all'ecologia.

Buona lettura!

introduzione.

ovvero: chi siamo

(ISC)²®

La *International Information Systems Security Certification Consortium* (ISC)²® è un'associazione no-profit internazionale leader mondiale nella formazione e certificazione delle competenze di professionisti della sicurezza informatica, la più conosciuta delle quali è la CISSP.

Wikipedia la descrive come la più grande organizzazione del genere nel panorama mondiale. Ha infatti più di 100.000 membri e 60 capitoli distribuiti in 135 Paesi.

Per maggiori informazioni su (ISC)²® e sulle sue certificazioni, visitare il sito https://www.isc2.org/

(ISC)²® ovvero International Information Systems Security Certification Consortium.

(ISC)^2 Chapter Italy

(ISC)^2 Chapter Italy è un'associazione no-profit Italiana nata nel 2012; è il capitolo di (ISC)$^{2®}$ International che opera sul territorio italiano.

E' organizzata in Gruppi di Lavoro (G.d.L.) che affrontano molteplici temi per professionisti e non, tra cui l'Educazione alla Sicurezza Informatica nelle scuole.

Per maggiori informazioni su (ISC)^2 Chapter Italy, visitare il sito http://www.isc2chapter-italy.it/

ISC)² Chapter Italy è il capitolo di (ISC)²® International che opera sul territorio italiano.

G.d.L. “Educazione alla Sicurezza Informatica” di (ISC)^2 Chapter Italy

Il Gruppo di lavoro “Educazione alla Sicurezza Informatica” del Capitolo Italiano di (ISC)^2 offre le seguenti risorse gratuite a scuole e comunità:

- professionisti della sicurezza informatica con conoscenze idonee per rispondere alle insidiose domande dei ragazzi
- presentazioni innovative corredate da video
- materiale divulgativo sulla sicurezza nel mondo virtuale
- linee guida per studenti e genitori

Con l’A.S. 2014-2015 stati raggiunti 13.465 tra ragazzi, docenti, personale ATA e genitori

Il G.d.L. “Educazione alla Sicurezza Informatica” è uno dei gruppi di lavori sui quali si articola (ISC)^2 Chapter Italy.

panoramica del programma di “Educazione alla Sicurezza Informatica”

Per gli insegnanti e i genitori di alunni e studenti e per il personale ATA delle segreterie:

- presentiamo i nuovi media
- mostriamo quali sono i rischi di una navigazione senza la giusta consapevolezza
- forniamo informazioni sui corretti comportamenti da tenere in rete (community online, chat, blog, social network…)
- mostriamo ai ragazzi quali sono le conseguenze di un loro comportamento errato quando si trovano su Internet, della pubblicazione di contenuti digitali e soprattutto della condivisione di questi ultimi online, spiegando le relative problematiche di natura legale

Panoramica del programma del G.d.L. “Educazione alla Sicurezza Informatica”.

attività in pratica del G.d.L. “Educazione alla Sicurezza Informatica”

I Relatori, in genere, in una giornata effettuano più presentazioni, da 1,5 a 2 ore a seconda dell’età, a più gruppi.

Durante i contatti preliminari, verranno definiti i dettagli degli interventi, quali:

- dettaglio di eventuali elementi specifici da includere nelle singole presentazioni e l’adozione del registro linguistico più appropriato
- stabilire le date
- stabilire un punto di contatto
- Quali sono le predisposizioni disponibili per l’effettuazione delle presentazioni (aula, auditorium o palestra, schermo, proiettore, microfono, ecc.)

Rendiamo il mondo virtuale un posto più sicuro per tutti.

programmi e contenuti disponibili

Tutti i volontari sono preparati e dotati di materiali interattivi e di presentazioni differenziate per fascia d'età, realizzate con il supporto e il contributo di avvocati, psicologi, esperti di sicurezza informatica e sotto la supervisione di docenti con anni di esperienza.

Sono disponibili **cinque presentazioni differenti** per fascia d'età. Tra queste se ne annovera una per genitori, insegnanti e personale ATA ve ne è un'altra che fornisce le conoscenze e le competenze necessarie per garantire la sicurezza e il controllo dei minori.

Le **fasce d'età prese in considerazione per i ragazzi** sono quelle:

- IV Elementare (Sc. Primaria) - I Media (Sc. Secondaria di 1° grado)
- II - III Media (Sc. Secondaria di 1° grado)
- I - III Secondaria di 2° grado
- IV - V Secondaria di 2° grado

Permetteteci di aiutarvi!

per far sì che le nostre comunità siano più sicure e protette online

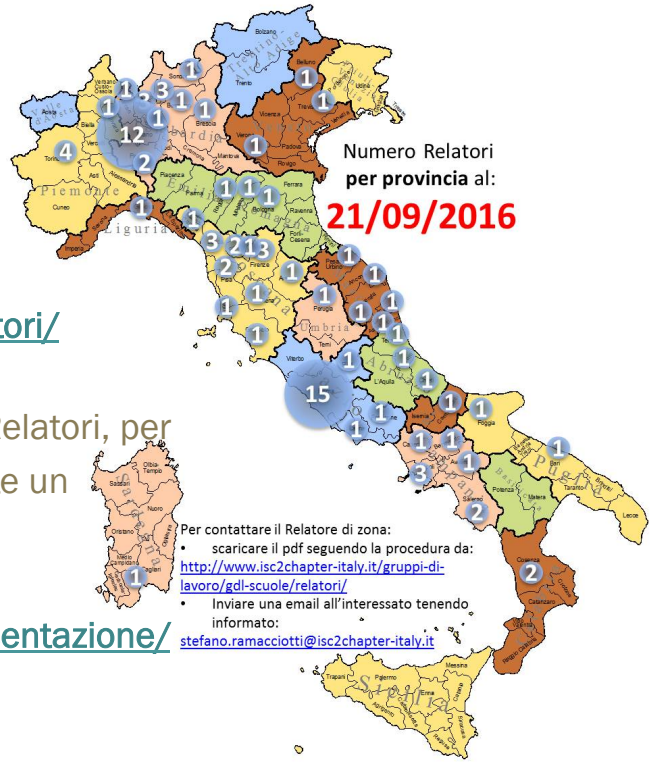
Se desiderate che un volontario venga nella vostra scuola, comunità o parrocchia, vi chiediamo di andare al link:

http://www.isc2chapter-italy.it/gruppi-di-lavoro/gdl-scuole/relatori/

e da lì seguire le istruzioni per scaricare il file con l'elenco dei Relatori, per verificare se la vostra zona è coperta. Nel caso che sia presente un Relatore vi chiediamo di compilare il modulo online su:

http://www.isc2chapter-italy.it/gruppi-di-lavoro/gdl-scuole/presentazione/

oppure di contattarci all'indirizzo: scuola@isc2chapter-italy.it



indice.

Indice dei contenuti

sicurezza

cosa vedremo

Da cosa nasce la necessità di un *eBook* sulla sicurezza informatica

Sezione a cura di:

- Stefano Ramacciotti, CISSP

perché un programma di Educazione alla Sicurezza Informatica?

Bambini sempre più piccoli sono quotidianamente esposti alle violenze di un mondo virtuale che affrontano troppo spesso da soli. Per permettere loro di auto proteggersi è essenziale insegnare loro i rudimenti della sicurezza e aiutarli a sviluppare abitudini online responsabili.

A loro supporto offriamo diverse decine di volontari esperti di sicurezza informatica, sparsi in tutta Italia, che sono desiderosi di condividere gratuitamente le personali conoscenze e competenze con coloro che ne hanno maggiore necessità.

Man a mano che il gruppo di volontari cresce, sempre più scuole ne richiedono l'intervento in considerazione delle riconosciute capacità di qualificati professionisti. Costoro offrono il loro tempo e le loro competenze per aiutare gli studenti a proteggersi da cyberbullismo, abusi, *grooming*, *trolling*, *malware*, truffe, e altro ancora.

Gli studenti così imparano, da un vero esperto di sicurezza informatica, quali sono i rischi ma soprattutto imparano...

come difendersi!

perché c'è da temere?

	mondo reale	mondo virtuale
Criminalità	Localizzata	Diffusa
Corpo di leggi interno	Chiare e conosciute	Chiare ma poco conosciute
Corpo di leggi diritto internazionale	Sufficienti	Diverse da Paese e Paese
Giurisdizione	Definita	Poco definita
Anonimità (possibilità di essere perseguiti)	Più difficile	Più facile
Possibilità di individuare zone rischiose	Alta	Bassa
Persone "normali" che commettono illeciti	Limitata	Medio-alta (es. pedofilia, furto di canzoni, sexting, ecc.)
Tecnologia per proteggersi	Facile impiego, prodotti disponibili	Difficile da configurare, disponibili prodotti e linee guida, scarsa propenzione degli utenti a manternersi aggiornati
Percezione del rischio	Elevata	Limitata

comportamento offline e online

percezione del crimine	mondo reale	mondo virtuale
Gravità del comportamento	Sentita	Limitata (ad es.: facilità con la quale si può scaricare software, non si vedono gli effetti delle nostre azioni per ignoranza sulle leggi in materia)
Timore della sanzione sociale e legale	Alta	Bassa (“tanto lo fanno tutti”, disinibizione)
Percezione del danno inferto alla vittima	Coscienza	Incoscienza (è un soprannome, un nickname o avatar, non una persona)
Anonimità (possibilità di perseguire)	Più difficile	Più facile da realizzare
Stima dei rischi di essere scoperto, denunciato e catturato	Alta	Bassa (falso anonimato, protezione mura domestiche/ufficio)
Persone “normali” che commettono crimini o illeciti	Limitata	Medio-alta (es. Pedofilia, furto di canzoni, sexting, ecc.)

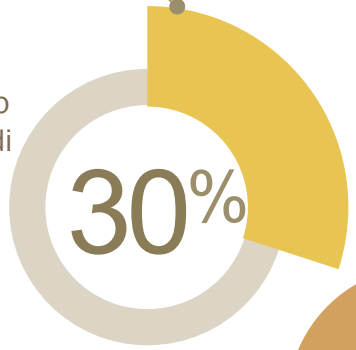
dati su cui riflettere

ricerca Doxakids e Telefono Azzurro

Il 50% dei ragazzi vuole più consigli da parte degli adulti perché li ritiene utili per saper contrastare atti di cyberbullismo e *sexting*

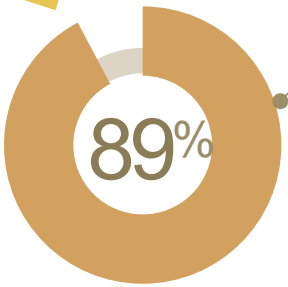
Europe Anti-Bullying Project

Chi subisce il bullismo è esposto al rischio di suicidio con una probabilità doppia rispetto ai coetanei: il 10% tenta di togliersi la vita, il 30% compie atti di autolesionismo



ricerca Doxakids e Telefono Azzurro

Nell'89,2% delle case dei ragazzi intervistati è presente almeno un pc portatile



malware

cosa vedremo

che cos'è il *malware*, come si caratterizza e come si combatte

Sezione a cura di:

- Stefano Ramacciotti, CISSP
- Luigi Cristiani

malware

virus & co.

Con la parola “*malware*” si intende non un oggetto software specifico ma una categoria di diversi tipi di software che sono diffusi allo scopo o di arrecare danni a chi viene “infettato” o ottenere un vantaggio per chi li ha diffusi.

I modi per contrastare ogni specifico tipo di *malware* sono rappresentati nella seguente tabella, non esaustiva, come rappresentazione delle principali tipologie di *malware*:

Nella tabella successiva si offre un riassunto di quanto sarà specificato nelle prossime pagine.

malware

tipo di malware	file che hanno effetti dannosi sul computer della vittima	come proteggersi (AV=antivirus, SO=sistema operativo)
Virus	E' un file parassita che ha bisogno di un file ospite per riprodursi, al quale si concatena, per poi propagarsi infettando altri file	AV e SO aggiornati, educazione utenti
Worm	*Malware* in grado di auto replicarsi e saturare il sistema ospite	AV e SO aggiornati, educazione utenti
Trojan	File con funzionalità nascoste in un altro file apparentemente utile	AV e SO aggiornati, educazione utenti
Spyware	Software che raccoglie informazioni riguardanti le attività online di un utente senza il suo consenso per trasmetterle via Internet a chi le userà per trarne profitto	AntiSpyware aggiornato (spesso inserito in "suite" AV), educazione utenti
Rootkit	Software per ottenere il controllo del computer senza bisogno di autorizzazione da parte di un utente	Antirootkit, SO e applicazioni aggiornati, educazione utenti

virus

virus & co.

E’ un file che infetta altri file per riprodursi.

I virus rappresentano il *malware* per antonomasia, e sono tanto famosi da essere identificati con il termine *malware* stesso e sostituirlo nell’immaginario collettivo.

Tra i vari tipi di virus ce n’è uno molto pericoloso e "di moda" negli ultimi tempi, il *ramsonware*, che è un tipo di virus che cifra i file dell’utente per i quali i criminali chiedono poi un riscatto in cambio della password per decifrarli.

Ci si difende : usando un antivirus e un sistema operativo aggiornato ma soprattutto educando gli utenti.

E’ un file che infetta altri file per riprodursi e rappresenta il *malware* per antonomasia.

ma cos’è esattamente un virus?

La caratteristica distintiva di un virus è il fatto che si replica inserendo una copia di se stesso all’interno di programmi o file di dati o nel MBR (Master Boot Record) di un disco.

Da questo comportamento sorge l’analogia con i virus come li si intende in campo medico: questi ultimi diffondono infatti il proprio codice genetico all’interno delle cellule sane che, a loro volta, assimilano il codice virale e trasformano il proprio pool genetico.

L’intervento umano è necessario per l’attivazione del virus, che rimane dormiente fino a quando un utente esegue o apre il file o il programma contenenti il codice malevolo, che viene eseguito a sua volta.

L’infezione si diffonde quando il file o il programma “ospitanti” il virus vengono trasferiti da un computer ad un altro attraverso la rete, un drive USB o in allegato ad una e-mail.

Una sottocategoria degna di nota fra i virus è quella dei macrovirus, ossia le infezioni scritte in uno dei linguaggi "macro",

I linguaggi “macro”, sono quei linguaggi caratteristici dei software di tipo “word processor” o “fogli di calcolo”. All’interno dei documenti possono infatti risiedere le cosiddette “macro” pronte anch’esse ad essere attivate allo stesso modo dei file eseguibili di cui abbiamo appena parlato. Un virus può compromettere la normale operatività di un computer, danneggiare il contenuto del disco, causare frequenti crash del PC, prosciugarne le risorse (CPU o memoria) o cancellare file.

ramsomware

ramsomware il software che chiede un riscatto

Un *ransomware* in sostanza è un sottotipo di virus che impedisce all'utente di poter accedere ai suoi dati (ne limita, perciò, la disponibilità). Questa aggressione può avvenire in due modi: il più comune è quello di cifrare il contenuto di un disco (rendendo illeggibile parte di esso o dei file memorizzati) oppure impedendo all'utente l'utilizzo del PC. In ogni caso, a fronte dell'indisponibilità dei dati, l'utente viene costretto a pagare un riscatto (*ransom*) all'estorsore che ha infettato il PC vittima. In genere vengono chiesti 1 o 2 Bitcoin, la moneta irrintracciabile di Internet, cioè dai 300 ai 500 € circa.

Ci si difende: antivirus e un sistema operativo aggiornati, regolare esecuzione dei backup, ed educazione utenti.

Ransomware il software che ci estorce un riscatto.

worm

worm, rabbit, ecc.

Caratteristica distintiva dei worm è la loro capacità di autopropagarsi da un computer all'altro senza bisogno dell'intervento umano, essi non necessitano di essere inclusi in un altro programma. Una volta entrati in un computer i *worm* penetrano negli altri sistemi remoti e si autoreplicano utilizzando *e-mail*, *Instant-messaging*, programmi *peer-to-peer*, canali IRC e altri metodi di trasferimento. L'effetto di un *worm* può essere devastante sia nei confronti delle macchine colpite che sulla rete LAN/WAN che subisce l'attacco.

Ci si difende: usando un antivirus e un sistema operativo aggiornato ma soprattutto educando gli utenti.

Malware in grado di auto-replicarsi e saturare il sistema ospite.

trojan

trojan horse o cavallo di Troia o semplicemente Trojan

I cosiddetti *“trojan”* devono il loro nome proprio al cavallo di Troia descritto da Virgilio nell’Eneide, un dono o un oggetto utile che in realtà racchiude al suo interno un pericolo o il nemico stesso.

Sono programmi apparentemente utili che celano al loro interno file pericolosi per l’utente finale. Sono spesso incautamente scaricati da utenti alla ricerca di software utili ai loro scopi, magari di dubbia provenienza o, spesso, “crackati”. Lo scopo finale dei *trojan* è quello di aprire una “*backdoor*” (porta di servizio) sul PC, tramite la quale i malintenzionati sono in grado di accedere alla macchina infetta e assumerne il controllo.

Ci si difende: usando un antivirus e un sistema operativo aggiornato ma soprattutto educando gli utenti.

File con funzionalità nascoste in un altro file apparentemente utile.

r.a.t.

Remote Access Trojan (RAT)

È un sottotipo di *trojan* che introduce una *"backdoor"* che consente il controllo da remoto con i privilegi dell'amministratore della macchina infetta. Una volta che il sistema risulta compromesso, l'intruso può utilizzarlo, ad esempio, per distribuire a sua volta il *malware* stesso su altri computer vulnerabili e costituire una *"botnet"* (una rete composta da PC denominati *"zombie"* sotto il controllo di criminali). Considerato il fatto che il RAT consente un controllo amministrativo sulla macchina vittima, rende possibile all'intruso praticamente qualsiasi tipo di attività sul sistema infetto.

Ci si difende: antivirus e un sistema operativo aggiornati, ed educazione utenti.

Per la creazione di eserciti di *"zombie"* al servizio dei cyber criminali.

spyware

spyware o software spia

Questo tipo di *malware* essenzialmente spia la vittima inconsapevole e colleziona differenti tipi di dati, da quelli finanziari a quelli riguardanti le nostre abitudini di navigazione, i siti da noi visitati e i nostri interessi. Tutte queste preziose informazioni, non escluse eventuali password o numeri di carte di credito digitati dall'ignaro utente, vengono inviate ai creatori/utilizzatori dello *spyware*. Uno dei danni più nefasti degli *spyware* è il "furto di identità" della vittima.

Ci si difende: AntiSpyware aggiornato (spesso inserito in "suite" antivirus) ma soprattutto educazione utenti.

File con capacità di raccolta di dati sugli utenti.

rootkit

rootkit: operazione a cuore aperto

Un *rootkit* è un *malware* nascosto che opera al livello più "profondo" del sistema operativo (normalmente definito *"root"*). Operando ad un livello privilegiato i *rootkit* sono estremamente difficili da rilevare ed eradicare dal sistema, richiedono infatti metodi speciali che vanno oltre le capacità dei normali software antivirus o *antimalware*. Il metodo più sicuro, in taluni casi, è la formattazione, la cancellazione sicura (sovrascrittura con software di *erasing*) della partizione e la creazione di una nuova partizione pulita. In altri casi invece i *rootkit* sono stati usati da aziende di risonanza mondiale per proteggere i propri sistemi da violazioni del copyright.

Sistemi che permettono di accedere alle parti più nascoste dei nostri sistemi.

Ci si difende: Antirootkit, un sistema operativo e applicazioni aggiornati, educazione utenti.

keylogger

keylogger i top dei software spia, che sanno tutto di noi

È un *malware* che "gira" in background e registra ogni singolo carattere digitato dall'utente della macchina infetta. Ciò che viene digitato include nomi utente, password, numeri di carta di credito e qualsiasi altro dato sensibile. Il *malware* effettua l'upload di ciò che "cattura" verso un server controllato dai malintenzionati che provvedono ad analizzare il materiale ricevuto utilizzandolo per i propri scopi fraudolenti. Altri tipi di "*keylogger*" possono essere utilizzati a scopo di mero monitoraggio della vittima, ad esempio da mariti o mogli gelose, ma anche per controllare illegalmente i figli.

Ci si difende: Antirootkit, SO e applicazioni aggiornati, tastiera virtuale (da utilizzare per l'home banking) e educazione utenti.

Con questi software nessuno ha più segreti.

virus & co.: ma quanti sono?

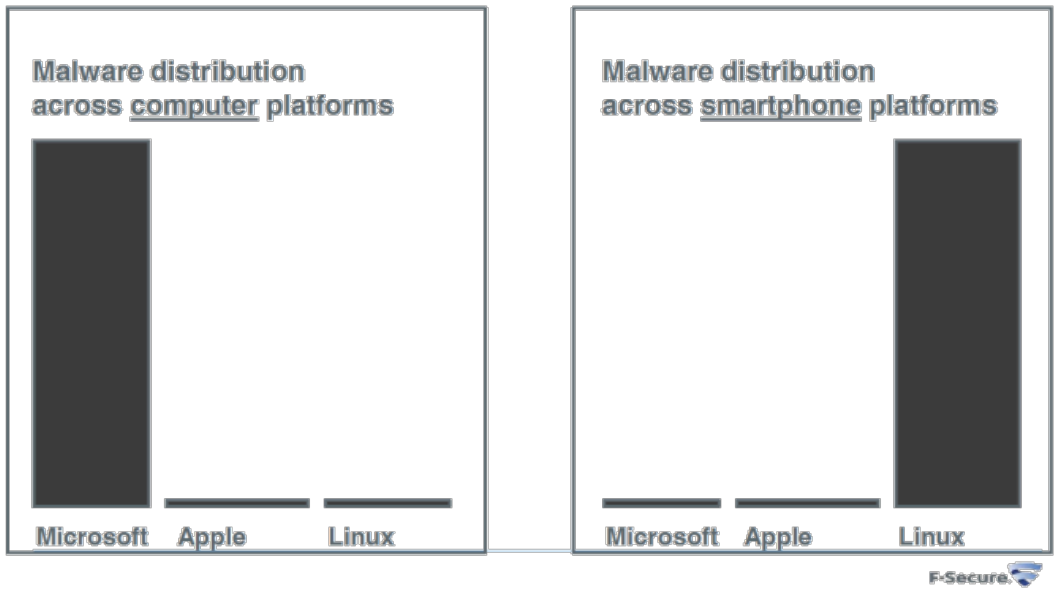
Fino a cinque anni fa era possibile fare una stima del numero di *malware* in circolazione. Fino al 2013 si parlava di una media di 65.000 nuovi *malware* al giorno e un totale di 40.000.000. Adesso che di *malware* ne vengono prodotti di nuovi circa 160.000 al giorno non ha più senso tenere certi conti. E' notizia recente (TrendMicro, OTT 2015) che dopo un'ora che un nuovo *malware* è stato diffuso si contano già 127 varianti. E mentre il trend per i *malware* dei PC è elevato ma abbastanza costante, quello per i sistemi che impiegano Android (*smartphone* e *tablet*) è in crescita esplosiva e si stima che rappresenti più del 99% del *malware* per il settore *smartphone*.

Sostanzialmente la situazione è quantitativamente (in percentuale) invariata rispetto a quanto F-Secure ha riassunto nel 2012 con l'immagine successiva.

Gli antivirus sono indispensabili almeno su PC che installano MS Windows® e *smartphone* che installano Android.

virus & co.: ma quanti sono?

I sistemi più colpiti sono quelli **maggiormente** diffusi



La situazione di F-Secure del 2012 qua raffigurata è sostanzialmente invariata. Con Apple si considera un generico sistema MAC OS X su computer e iOS su *smartphone*, per Linux deve intendersi una qualsiasi distribuzione su PC e Android per gli *smartphone*.

Windows, Apple o Linux?

Un Antivirus è sicuramente essenziale su:

- PC con sistema operativo Microsoft Windows
- Smartphone con sistema operativo Android

E', però, sempre meglio avere l'antivirus anche su PC che installano Mac OS X (per iOS non ne esistono ancora) e Linux (sia le distribuzioni su PC che Android), quantomeno per non comportarsi da "untore" e distribuire il malware ad altri utenti che usano sistemi operativi diversi. Inoltre il *malware* per Mac esiste, anche se non nelle quantità per PC (il rapporto è un migliaio a qualche decina di milioni), e Linux è stato addirittura il primo sistema operativo ad essere infettato da *worm* e *virus*.

Non esiste un sistema più sicuro di altri, solo sistemi più diffusi e che pertanto sono più interessanti per i potenziali attaccanti.

mi dica dottore ho la febbre?

Anticamente, che nei tempi dell'informatica vuole dire al massimo una decina di anni fa, l'utente si accorgeva di avere preso un virus in tanti modi diversi quale era la fantasia dello sviluppatore del virus. I sintomi erano i più diversi:

- comparsa di immagini o di messaggi;
- il PC emetteva suoni strani o i programmi si attivano da soli e cercavano di collegarsi a Internet, o si aprivano lentamente;
- i nostri amici ricevevano nostre email senza che gliele avessimo inviate;
- il PC si bloccava, o ripartiva continuamente o si ricevevano messaggi d'errore;
- il software di protezione, come antivirus o il firewall, veniva disabilitato e non era più possibile riattivarlo né installarne altri sostitutivi;
- alcuni file o cartelle divenivano inaccessibili, o venivano modificati, o l'hard disk si riempiva di file in poco tempo.

Oggi, purtroppo e sempre più spesso, non accade nulla! Almeno in apparenza.

Da tempo i vecchi creatori di virus, che il più delle volte realizzavano virus per puro spirito goliardico o come dimostrazione della loro capacità di attaccare sistemi protetti, sono stati soppiantati da nuove generazioni di programmatori il cui unico intento è fare soldi. Ovviamente costoro non hanno alcun interesse a rendere visibili le loro attività e pertanto i nuovi virus mantengono, quasi sempre, un profilo particolarmente basso per non essere intercettati dagli antivirus (AV).

considerazioni finali sul malware

Per riassumere, i vettori con cui i PC possono essere infettati dal *malware* sono gli allegati delle e-mail (attenzione a non cliccare su qualsiasi cosa riceviamo!) o le chiavette USB, ma anche un semplice “click” su un annuncio pubblicitario che appare su Internet potrebbe essere pericoloso (abbiamo veramente bisogno di quel prodotto così scontato?!). Attenti anche a giochi, toolbar o altre cosiddette “utilities” che molte volte non sono solamente ciò che dichiarano di essere…

Quindi prudenza, accortezza, consapevolezza della minacce e … un pizzico di diffidenza in più.

Quando piove ci proteggiamo con l'ombrello.

E quando navighiamo in Internet?

https://www.flickr.com/photos/toastkid/5419046095/

antivirus

cosa vedremo

gli antivirus, sono ancora utili o non servono più a niente?

Sezione a cura di:

- Stefano Ramacciotti, CISSP
- Luigi Cristiani

antivirus

L'antivirus: software che permette di proteggere il PC, *tablet* e *smartphone*, dalle principali minacce,.

Che cos' è un antivirus

L'antivirus è un software che permette di proteggere il PC, e sempre più spesso il *tablet* e lo *smartphone*, dalle principali minacce. In realtà, visti gli attuali trend che vedono in rapidissima crescita il *malware* per *tablet* e *smartphone* sarebbe ben più importante proteggere per primi questi ultimi, ma pochi lo fanno.

Inoltre la relativa limitata potenza di questi *device* non permette di impiegare al meglio le limitate risorse per complessi sistemi di protezione, ergo questi sistemi sono in genere molto più vulnerabili, tanto che si stima che l'87% dei dispositivi che utilizzano Android sia a rischio (fonte "ictbusiness.it" del 15 Ottobre 2015 http://goo.gl/7b1K9y).

antivirus: principi di funzionamento

Gli antivirus funzionano in base a **due principi complementari**. Il primo ad essere stato utilizzato è quello del **riconoscimento della cosiddetta "firma" del *malware***. Quando si parla di firma si parla di quella parte del codice del software immutabile che può essere presa a riferimento per l'identificazione del *malware*, è una sorta di impronta digitale che lo rende unico. Questa modalità funziona ancora per i virus che si auto-modificano, i cosiddetti polimorfi, anche se con minore efficacia, perché in genere rimangono riconoscibili, proprio perché, invece di una stringa di codice, si prende a riferimento l'algoritmo che ne consente la mutazione.

Questo sistema ha un evidente limite che il *malware* può essere riconosciuto solo se catalogato come virus da qualche ricercatore, mentre è **completamente inutile nei confronti di nuovi virus**.

Il secondo sistema, più recente, ed evoluzione dei cosiddetti antivirus euristici, è quello che osserva il **comportamento del computer alla ricerca di accessi anomali e operazioni inattese** che fanno sorgere il sospetto che del software voglia danneggiare il sistema ospite, isolandolo come *malware*. Anche questo sistema ha una sua importante debolezza che è quella dei cosiddetti **"falsi positivi"**, che segnalano anche operazioni del tutto lecite come potenziali minacce bloccando il sistema e richiedendo all'utente cosa fare. Spesso l'utente, infastidito da questi continui avvisi, autorizzerà qualsiasi operazione, comprese quelle effettivamente illecite.

antivirus: garanzia limitata (ma comunque necessari)

I nuovi antivirus generalmente adottano **entrambe le soluzioni**, viste in precedenza, in sinergia tra loro.

Purtroppo la produzione di nuovi *malware* è di centinaia di migliaia al giorno e non esiste antivirus in grado di analizzarli tutti, estrarne le firma e aggiornare così velocemente i database. Inoltre gli sviluppatori di *malware* studiano sempre nuove soluzioni per riuscire a passare inosservati anche dalle trappole rappresentate di sistemi che impiegano l'analisi comportamentale.

Alcuni *antivirus* (ad es. Panda e Kaspersky), nel dubbio che un qualsiasi software possa essere un *malware*, inseriscono qualsiasi cosa scaricata e che si vuole inviare in esecuzione in una *sandbox*. Una ***sandbox*** è una porzione di disco isolata in cui viene fatto girare il software in modo che non possa interagire con il sistema.

Una versione gratuita di software *sandbox* si trova su www.sandboxie.com, ed è utile sia per studiare il codice che per la protezione dell'utente.

Per quanto detto, è opportuno perciò essere consapevoli che comunque **gli antivirus riescono solo a garantire una protezione parziale** e che la protezione più importante dal *malware* è quella di non mettersi nelle condizioni di riceverne. Come al solito, la prima linea di azione è quella di una adeguata educazione degli utenti.

Ad esempio quanti sanno che il **sistema più facile per prendersi qualche virus** è quello di installare **software "craccato"**, o banali suonerie e altri gadget "free"?

come impiegare bene un antivirus

- Scaricare sempre i programmi antivirus da siti ben conosciuti, **mai affidarsi ai suggerimenti di email o pop-up pubblicitarie che dichiarano che siete infetti e che dovete installare un software per la disinfezione**;
- **aggiornare automaticamente il software antivirus**. Se il PC è stato lasciato spento per molto tempo attendere che il sistema si sia aggiornato prima di continuare a impiegarlo. Se l'antivirus è a pagamento **non lasciare mai scadere l'abbonamento**;
- **mai disattivare l'antivirus** (anche se perché rallenta troppo il computer e o perché richiesto dal programma che stiamo installando o dopo avere visitato una pagina web, nel qual caso sarà probabilmente un *malware*);
- **leggere attentamente tutti gli avvisi** che l'antivirus mostra a schermo e applicate tutti i suggerimenti;
- **mai installare due AV diversi** perché si potrebbero verificare conflitti;
- **verificare che l'antivirus scansioni sempre automaticamente:**
  - **le eMail**
  - **tutti i dispositivi rimovibili** che vengono collegati al PC
    - chiavette USB
    - hard-disk USB
- **configurare l'antivirus** per le proprie esigenze/abitudini;
- **associargli sempre un firewall** che permette di controllare i file in ingresso/uscita dal PC da e verso Internet secondo particolari parametri;
- **attenzione ai link sui quali cliccate**. E' sufficiente passare con il mouse sul link e verificare che il link che appare in sovrimpressione sia esattamente uguale a quello scritto o che il dominio del link sia lo stesso della mail ma, meglio ancora, sarebbe **scaricare plug-in o usare AV che automaticamente verificano l'attendibilità dei siti** che visitiamo.

l'antivirus serve?

"L'antivirus è morto!".
Viva l'antivirus!

Gli antivirus da soli ormai non garantiscono più, ammesso che in passato lo abbiano mai fatto, un livello di sicurezza adeguato per far fronte a tutte le minacce informatiche.

A riprova di ciò è sufficiente dire che già nel 2014 **Brian Dye**, il vicepresidente anziano per la sicurezza delle informazioni di Symantec, uno dei principali produttori al mondo di antivirus, diceva in un'intervista al *"The Wall Street Journal"*: **"L'antivirus è morto!"**, dato che stimava che un antivirus non riuscisse a riconoscere più del 45% di tutte le minacce esistenti.

Nonostante ciò, l'antivirus è il primo prodotto che viene in mente all'utente medio quando pensa a come difendersi. E' allora naturale che quando andiamo nelle scuole, sia dagli studenti che dai genitori e che dagli insegnanti ci sentiamo rivolgere la domanda: qual è l'antivirus che devo scaricare per proteggermi al meglio? Vediamo come rispondere.

quale antivirus scegliere?

Non è una domanda semplice a cui rispondere per più di un motivo:

1. occorre sapere qualè il **sistema operativo** in uso e la sua **versione**. In genere l'utente medio italiano nella quasi totalità dei casi utilizza sistemi Microsoft Windows (in genere da Windows XP a Windows 10), ma alcuni utilizzano anche Mac con le varie versioni del suo OS X, pochi usano Linux e moltissimi usano sistemi operativi per *tablet* e *smartphone* come Android (basato su Linux), iOS (per iPhone e iPad) e Winphone;
2. in Italia sono ancora diverse le **persone che cercano di procurarsi del software senza acquistarlo** dai canali ufficiali. Questo porta spesso con se cavalli di troia, virus e, nella migliore delle ipotesi, semplici *adware/spyware* (questi ultimi talvolta presenti anche in software free ma anche a pagamento). Per tener conto anche di queste minacce in modo integrato senza dover installare prodotti diversi, normalmente **consigliamo di acquistare e installare delle *suite* integrate**.

   L'acquisto garantisce una **migliore continuità di aggiornamento e una maggiore facilità di utilizzo** delegando agli esperti che hanno realizzato il software molte delle azioni che il singolo utente dovrebbe fare da solo;
3. gli **antivirus non sono sempre costantemente efficaci**, ma la loro capacità di rivelare le minacce varia nel tempo;

... continua

quale antivirus scegliere?

... continua dalla pagina precedente...

4. **alcuni antivirus** risultano particolarmente **"pesanti"** in termini di prestazioni e, a seconda del computer in uso, talvolta è più opportuno installare un antivirus con minori capacità di riconoscimento, ma che rallenta meno le sue performance, che non un antivirus che rallenti eccessivamente il computer tanto da renderne l'uso difficoltoso;
5. semplicemente **non esiste il "miglior antivirus"**, ma esiste l'antivirus che risponde meglio alle nostre esigenze specifiche;
6. (ISC)^2 Chapter Italy, l'Associazione cui apparteniamo, è ***"vendor-indipendent"*** e pertanto potrebbe sembrare un interesse personale quello di consigliare un determinato prodotto.

Dunque, per rispondere alla domanda di qual è l'antivirus più efficace, se l'inglese non è un problema, invece di un nome suggeriamo di **visitare i siti della tabella alla pagina successiva** prima di fare l'acquisto.

Sono dei **siti che periodicamente effettuano prove comparative tra tutti i principali antivirus** disponibili (sia *free* che a pagamento). E' allora meglio vedere i risultati di ogni AV su ognuno di essi, perché ogni servizio va alla ricerca di caratteristiche diverse dei vari antivirus. **Confrontiamo i risultati ottenuti nelle prove comparative per poi scegliere il prodotto che meglio si attaglia alle nostre esigenze**.

principali siti per test comparativi su AV

logo e nome	link	note
AV comparatives	http://www.av-comparatives.org/	Uno dei test più completi. Verifica sia le capacità di rilevazione delle minacce che l'individuazione di siti infetti nonché le performance dei test per rilevare quanto l'antivirus influisce sulle prestazioni del pc
AV-TEST The Independent IT-Security Institute	https://www.av-test.org/en/antivirus/home-windows/	Prove comparative tra antivirus per i sistemi operativi più diffusi: Android, Windows e Mac OS X
DENNIS TECHNOLOGY LABS	http://www.dennistechnologylabs.com/reports/s/a-m/2015/	I laboratori Dennis verificano come gli antivirus reagiscono alle minacce Internet e come gestiscono i programmi legittimi degli utenti. Infatti verificano anche se gli antivirus generano dei falsi positivi impedendo all'utente di utilizzare programmi legittimi e senza problemi
virus BULLETIN	https://www.virusbtn.com/vb100/rap-index	RAP sta per *Reactive And Proactive*, che significa che il test verifica la capacità dell'antivirus di reagire alla minaccia, cioè alla capacità del *vendor* di tenere aggiornato il prodotto, e di prevenirla, ovvero la capacità di individuare nuovo *malware*. Le prove comparative vengono svolte su base bimestrale
no logo	http://ilmigliorantivirus.com/il-miglior-antivirus-free/	Tra i pochi in italiano. Focalizzato solo sui prodotti gratuiti
ProgrammiFree.com	http://www.programmifree.com/confronti/confronto-antivirus2015.htm	Tra i pochi in italiano. Focalizzato solo sui prodotti gratuiti

rimuovere un virus dal PC

Passi per rimuovere un virus dal nostro PC.

1. disconnettere il PC da Internet/dalla rete;
2. avviare il PC in modalità provvisoria (in genere si attiva questa modalità premendo F8 all'avvio) o avviarlo da un CD/DVD di soccorso (ricordarsi che l'antivirus non sarà aggiornato con le ultime firme virali);
3. eseguire la scansione completa del PC.
   - se l'antivirus non trova nulla occorrerà scaricare gli aggiornamenti dell'antivirus (possibilmente da altro PC) e poi effettuare di nuovo la scansione. Se ancora non trovasse nulla ricollegarsi a Internet e scaricare gli aggiornamenti del Sistema Operativo e delle applicazioni.
   - se l'AV ha trovato un virus eliminarlo (se proprio necessario inserirlo in quarantena, ma è un rischio) e valutare la possibilità di scaricare dal produttore di antivirus software specifici per il virus (talvolta più efficaci dell'antivirus stesso, non tanto nell'eliminazione ma quanto nella ricerca di eventuali residui del *malware*).

antispyware

L' antispyware: è una sorta di antivirus specializzato nello spyware.

Che cos' è un antispyware

L'*antispyware* è un po' l'alter ego dell'antivirus.

E' specializzato nel ricercare lo *spyware*.

I migliori antivirus offrono garanzie anche nei confronti degli *spyware* ma difficilmente ciò avviene nel caso dei prodotti gratuiti.

Occorre fare attenzione ad eventuali incompatibilità con altri antivirus free.

per *smartphone* più sicuri

	iPhone/iPad (iOS)	Android
Store alternativi	No (no jailbreak)	No (no rooting)
Feedback	Controllare cosa dicono gli altri delle App	
Accesso dati	Negare accesso ai dati alle App	
Geolocalizzazione	Disabilitarla	
Blocco schermo	PIN (cifra dati)/PSWD	PIN/PSWD
Upload foto	Disabilitarlo (tx dati posizione)	
Bluetooth-WiFi	Disabilitarlo quando non serve	
SMS/MMS da sconosciuti	Non aprirli e non cliccare sui link presenti («Olympic live stream in Sochi hxxp://mms****.ru/ olympic.apk»)	
AV/FW	//	Sempre
Aggiornamento App	Sì	Sì

N.B.: dato che non tutti gli smartphone/tablet (per ragioni di sicurezza) consentono l'installazione di un antivirus, nella tabella soprastante si fornisce la **configurazione di base da adottare**

password

cosa vedremo

come crearle e usarle nel modo corretto

Sezione a cura di:

- Stefano Ramacciotti, CISSP

Autentichiamoci

Dal film: "Non ci resta che piangere" con Benigni e Troisi

"Alt! Chi siete? Cosa portate?
Sì, ma quanti siete?
Un fiorino!"

password: ORRORI da evitare

Per garantirsi un discreto livello di sicurezza:

- evitare di impiegare come password nomi o parole di senso compiuto, come:
  - nomi propri di calciatori / cantanti / attori / animali di casa
  - date di nascita / matrimonio / fidanzamento / ricorrenze varie
- proteggere anche gli account del PC di casa o di scuola
- modificare le password almeno ogni 3 mesi
- La password va ricordata a memoria e non trascritta su:
  - post-it sul monitor
  - rubrica telefonica
  - a matita dietro la tastiera o nel primo cassetto

User ID: pippo
Password: 123456
non ci credereste mai, ma sono quelle più comunemente utilizzate

20 password più comuni al mondo

RANK	PASSWORD	CHANGE FROM 2014			
1	123456	Unchanged	13	abc123	1 ↗
2	password	Unchanged	14	111111	1 ↗
3	12345678	1 ↗	15	1qaz2wsx	NEW
4	qwerty	1 ↗	16	dragon	7 ↘
5	12345	2 ↘	17	master	2 ↗
6	123456789	Unchanged	18	monkey	6 ↘
7	football	3 ↗	19	letmein	6 ↘
8	1234	1 ↘	20	login	NEW
9	1234567	2 ↗	21	princess	NEW
10	baseball	2 ↘	22	qwertyuiop	NEW
11	welcome	NEW	23	solo	NEW
12	1234567890	NEW	24	passw0rd	NEW
			25	starwars	NEW

Non ci credete?

https://mobilejazz.com/blog/wp-content/uploads/2016/02/image08.jpg

password: how-to

Una buona password dovrebbe essere composta da:

- minimo 8 ma sarebbe meglio più di 15 caratteri (per i più "smanettoni": per evitare un attacco a forza bruta o con le Rainbow Tables)
- lettere MAIUSCOLE e minuscole
- segni di punteggiatura come !?]
- Simboli come *, ‘, ^

User ID: pippo
Password: password
non ci credereste mai, ma sono quelle più comunemente utilizzate

tool di cifratura delle password

Può essere utile:

- scrivere le password e conservarle in un luogo segreto
- scrivere le password e conservarle utilizzando *tool* di cifratura delle password come:
  - KeePass,
  - LastPass,
  - ecc....

  Ma attenzione talvolta i *tool* stessi sono risultati "baggati" e se li vogliamo usare proteggiamoli con una password veramente ben fatta. Non ha senso proteggere servizi con una password di 15 carattere e proteggere il tool che conserva quelle "chiavi" con "1234"!

Mettiamo le password in cassaforte.

esempio di buona password

NMdcdN5MR*1SOkld53S

Caratteristiche:

- 19 caratteri
- lettere MAIUSCOLE e minuscole
- caratteri speciali

Decisamente un'ottima password!

Domanda: è semplice o difficile ricordarsi una password del genere?

Tutto dipende da come l'ho creata. Nella pagina seguente sarà mostrato l'algoritmo (OVVIAMENTE non deve essere riutilizzato ma ne deve essere inventato uno personale)

Cosa ve ne pare? E' una buona password

come costruire una buona password

passaggio	link	note
1	“Nel mezzo del cammin di nostra vita mi ritrovai per una selva oscura ché la diritta via era smarrita” (Canto I – Inferno – Comedìa – Dante)	Creare una piccola poesia facile da ricordare o prendere una frase di una canzone o di una poesia poco conosciuta (questa seconda possibilità è meno sicura della prima)
2	nel mezzo del cammin di nostra vita mi ritrovai * 1 selva oscura k la diritta via era smarrita	Sostituire, quando possibile, parole intere con lettere dello stesso suono o numeri (* invece di "per", 1 invece di "uno/a", ecc.).
3	nel mezzo del cammin di nostra vita mi ritrovai * 1 selva oscura k la diritta via era smarrita	Evidenziare la prima lettera di ogni parola eventualmente sostituendo le lettere facilmente rimpiazzabili con un numero (0 invece di "o", 3 invece di "e", 5 invece di "v", ecc.).
4	nmdcdn5mr*1s0kld53s	Creare una parola con le sole lettere evidenziate.
5	NMdcdN5MR*1S0kld53S	Cambiate le lettere dalla M in poi in MAIUSCOLO

Non usare mai la stessa password per più UserID o account. Gli hacker lo sanno e per questo vi attaccano sull’account sul quale siete più vulnerabili (quello al quale attribuite meno peso), vi sottraggono la password e poi la usano null’account della carta di credito o altro importante.

Se vogliamo sapere come a Jennifer Lawrence nel 2014 sono state sottratte molte foto intime:
http://nypost.com/2016/03/16/how-the-jennifer-lawrence-nude-picture-hack-really-went-down/

passphrase - alternativa alle password

Sistema più rapido:

- prendere una foto
- prendere particolari tra loro slegati
- unire le parole.

Es.
vacca+tetto +automobile+ sari (il vestito indiano) =
vaccatettoautomobilesari
È più sicura di una password complessa da 18 caratteri

https://www.flickr.com/photos/betta_design/2078005654/in/pool-creative_commons-_free_pictures/

social network come minaccia

cosa vedremo

i social network visti non come utile strumento per far comunicare le persone fra loro ma come minaccia

Sezione a cura di:

- Stefano Ramacciotti, CISSP

social network e social media

I social network:
- Facebook;
- Linkedin;
- Twitter.

I social media:
- YouTube;
- Blogger;
- Slideshare.

Con **social network** si intendono **servizi che mettono in relazione singoli e gruppi con la spiccata propensione a favorire conversazioni digitali**, come:
- Facebook;
- Linkedin;
- Twitter.

Con **social media** si intendono invece **contenitori con la spiccata propensione alla socialità**, come:
- YouTube;
- Blogger;
- Slideshare.

social network e social media

I social network:
- Facebook;
- Linkedin;
- Twitter.

I social media:
- YouTube;
- Blogger;
- Slideshare.

Nel seguito si parlerà genericamente di social network per intendere entrambi se non diversamente indicato.

Molte persone li additano come pericolosi.

In quanto strumenti tecnologici non sono di per sé né positivi né negativi. Dipende dall'uso che se ne fa.

Si può ragionevolmente dire che i social network sono strumenti eccezionali per far si che le persone rimangano collegate tra loro. Ovviamente, essendo strumenti potenti dal punto di vista della comunicazione, un loro impiego errato o fraudolento può portare a vederli come una minaccia.

il “numero di Dunbar”

Uno dei primi problemi è non rendersi conto proprio delle potenzialità di questi strumenti. La Sociologia ci insegna che esiste un numero massimo di possibili collegamenti efficaci tra le persone e questo numero massimo, il “numero di Dunbar” è pari a 150 collegamenti interpersonali. Alcuni autori asseriscono che le capacità dell’uomo non sono cambiate da quando ha iniziato a riunirsi nei primi villaggi in epoca preistorica.

Allora il gruppo era formato da circa 150 individui e ancora oggi questo numero rappresenta il massimo dei possibili contatti che anche l’uomo moderno è in grado di mantenere. Invece, è molto frequente incontrare dalla III media in poi, ragazzi che hanno anche 2 o 3 mila contatti e già qualche volta è capitato di sentire che qualcuno abbia raggiunto il limite massimo di contatti permessi da un social network come Facebook che è pari a 5 mila.

E’ evidente che, per quanto detto prima, avere più di 150 contatti non permette di seguirli tutti, anzi molti contatti distrarranno l’attenzione dalle informazioni più importanti per l’utilizzatore e sarà praticamente inevitabile che perfetti conosciuti, tra cui delinquenti, possano venire in contatto con l’utente. Sono delle folle di persone talmente vaste che molti ragazzi, paradossalmente, soffrono di solitudine anche se ancora di più patiscono quando ne sono esclusi. In sostanza: fermiamoci a 150 contatti e non andiamo oltre.

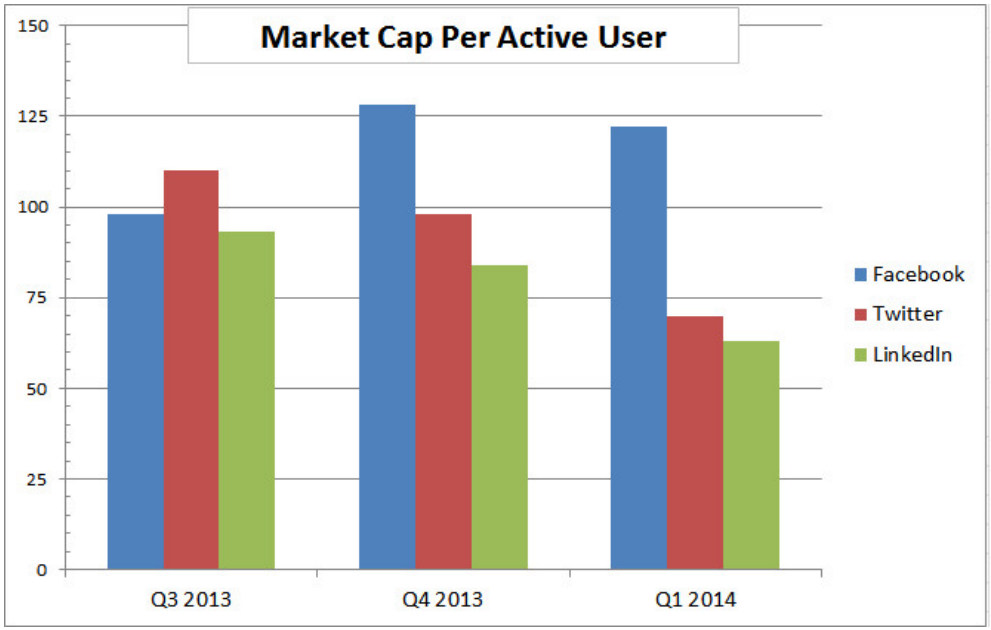
chi paga i social network "gratuiti"?

Molti dei servizi disponibili su Internet sono gratuiti e tra questi spiccano i Social network. Non si può pensare però che le server farm (vasti ambienti pieni di server) dai costi elevatissimi siano una generosa concessione da parte dei loro gestori. In realtà i vari proprietari come Mark Zuckerberg di Facebook e WhatsApp o il duo Larry Page o Sergey Brin di Google e YouTube, per citare i più famosi, hanno costruito veri e propri imperi economici apparentemente "regalando" servizi ai loro utenti. Ma come hanno fatto?

Molto semplice: hanno, con il consenso degli utilizzatori, sistematicamente scandagliato tutto quanto i loro utenti mettevano in rete allo scopo di carpirne i desideri più nascosti e rivendere le informazioni a caro prezzo ai pubblicitari, i quali li pagano anche per mostrare banner pubblicitari mirati all'utente nei vari profili.
Oramai siamo tutti pesantemente "schedati". Sono numerose le aziende che categorizzano i vari utenti in stereotipi chiamati "personas" allo scopo di ricondurli a gruppi ("target" in gergo) suddivisi in base ai comportamenti tipici per permettere ai pubblicitari di fare pubblicità mirata nei loro confronti.

E questo è un mercato particolarmente redditizio. È così che non solo ripagano le loro costose server farm ma ci guadagnano anche molto, tanto che si stima che per una società come Facebook le informazioni relative a ogni singolo utente abbiano un valore pari a circa 190 € (ad oggi). Il ritorno economico delle informazioni varia nel tempo e la tabella di seguito ci mostra l'andamento in 3 successivi quadrimestri per i tre social network più conosciuti nel mondo occidentale.

valore singolo account



In questo grafico è possibile vedere quanto vale un singolo account in tre diversi trimestri.
Ad esempi nel quarto trimestre del 2013 un account Facebook valeva più di 125 dollari americani.

cessione volontaria

Come detto precedentemente, dal punto di vista formale, non è possibile sollevare alcuna obiezione sulla condotta di queste aziende perché sono gli utenti che cedono, spesso inconsapevolmente, ma volontariamente i propri dati.
Come può presentarsi una cessione volontaria e, nello stesso tempo, inconsapevole di informazioni personali?
Purtroppo gli utenti sono pigri e, invece di leggere le informative che le varie aziende invitano a sottoscrivere, cliccano sula casella "accetta" senza leggere alcunché.

Cioè, quando l'utente medio vede la classica casellina quadrata da spuntare per accettare un nuovo servizio, lo fa senza leggere il contenuto dell'informativa sulla privacy e in questo modo consegna inconsapevolmente, ma volontariamente, i diritti sui propri dati ad altri. Ad esempio nella **Dichiarazione dei diritti e delle responsabilità** (di seguito **DDR**), la sorta di "contratto" che l'utente sigla con Facebook al ***Paragrafo 9.1.*** "Informazioni su pubblicità e altri contenuti commerciali pubblicati o supportati da Facebook" si legge:

"Gli utenti forniscono a Facebook l'autorizzazione a utilizzare il loro nome, l'immagine del profilo, i contenuti e le informazioni in relazione a contenuti commerciali, sponsorizzati o correlati (ad esempio i marchi preferiti) pubblicati o supportati da Facebook. Tale affermazione implica, ad esempio, che l'utente consenta a un'azienda o a un'altra entità di offrire un compenso in denaro a Facebook per mostrare il nome e/o l'immagine del profilo di Facebook dell'utente con i suoi contenuti o le sue informazioni senza ricevere nessuna compensazione." (alla data del 16/04/2016).

Ma quante persone hanno letto finora la DDR?

Io facciamo per il vostro (nostro) bene

In linea di massima le aziende asseriscono con forza di volere i dati degli utenti per migliorare i loro servizi ma, allo stesso tempo sottacciono il fatto che ciò che fanno è principalmente a loro beneficio.
Per ottenere ciò, analogamente a come fanno certe assicurazioni che scrivono i contratti con caratteri microscopici per evitare di farli leggere agli utenti, queste aziende impiegano vari sistemi per frustrare l'impegno di utenti volenterosi di approfondire la lettura dei contratti adottando sistemi simili. Pertanto, utilizzano o caratteri troppo piccoli o particolarmente distanziati e carichi di insulse clipart per far stancare l'utente oppure cambiano frequentemente i termini dei contratti, o anche suddividono il contratto su pagine diverse, il tutto per far desistere l'utente dalla lettura.

Chiariamo subito, Facebook, WhatsApp e gli altri citati non sono né peggiori e né migliori di altri e non vi è alcuna intenzione di colpevolizzarli. Sono stati presi a riferimento perché, al momento, sono i più utilizzati social network a livello nazionale. Anche altri si muovono sostanzialmente sulla stessa linea ed in definitiva la colpa vera è dell'utente poco scaltro o poco informato che non si rende conto di cosa succede quando:

- si iscrive a un servizio online "free" sottovalutando l'importanza e sottostimando il valore delle proprie informazioni;
- adotta configurazioni non restrittive;
- utilizza in maniera inappropriata le tecnologie;
- concede l'amicizia a persone sconosciute, senza impostare limitazioni di visibilità;
- ricorre all'interazione fra social media (ad esempio impiegando lo stesso account per Google e YouTube o per Facebook e WhatsApp sempre per pigrizia);

... continua

Io facciamo per il vostro (nostro) bene

... continua dalla pagina precedente...

- impiega eccessive applicazioni (DDR Facebook ***Paragrafo 2.3***. *"Quando l'utente usa un'applicazione, questa può richiedere l'autorizzazione per accedere a contenuti e informazioni dell'utente, nonché a contenuti e informazioni condivise da altre persone"*).

Adesso dovrebbe essere abbastanza chiaro che nulla viene concesso gratuitamente.
Un discorso a parte meritano i cosiddetti **"amici".**

Ognuno di noi, ognuno dei nostri figli, ha un numero limitato di amici, amici veri, intimi. Molti altri invece sono semplici conoscenti e poi vi è una vastità di sconosciuti.

Purtroppo, i social network si sono appropriati del termine e abusandone ne hanno deliberatamente modificato il significato aggiungendone uno in contrasto con il precedente. Adesso gli "amici" non sono solo i veri amici e nemmeno i conoscenti ma anche dei perfetti sconosciuti che si presentano via web chiedendo la nostra amicizia. Questa subdola manovra è stata fatta al solo scopo di far si che le persone, sentendo la parola "amici", abbassassero le difese e fossero più propense a condividere informazioni personali o intime con perfetti sconosciuti al solo scopo di aumentare i guadagni delle citate multinazionali.

Tutto è aggravato per gli adolescenti tra i quali si instaura spesso una sorta di gara ad avere quanti più "amici" possibile.

Questo senza rendersi conto che, inevitabilmente, consentiranno a dei perfetti sconosciuti e potenziali disturbatori (troll e quant'altro) di entrare nella nostra cerchia di amicizie "internettiane".

cosa dire e cosa non dobbiamo dire

Ladri moderni.

E’ ovvio che se uno pubblica foto dell’ultima vacanza alle Maldive probabilmente ha un tenore di vita che lo identifica come benestante e se l’utente dice che invece partirà tra un mese per una vacanza in USA non solo si avrà la certezza delle sue possibilità ma gli interessati sapranno anche quando andare a svaligiargli casa. Analogamente se i nostri ragazzi saranno prodighi di informazioni e lasceranno online il loro numero di telefono o l’indirizzo di casa e un pedofilo li ha presi di mira immaginiamoci cosa potrà accadere loro.
Non illudiamoci poi che se abbiamo insegnato ai nostri figli ad essere guardinghi non possa succedere loro alcunché. Se anche, come dovremmo fare, abbiamo costretto nostro figlio a creare un account con uno pseudonimo, e non con nome e cognome, basta che un amico “tagghi”, cioè metta una etichetta con il vero nome e il cognome di nostro figlio, una fotografia online per rendere vani i tentativi di proteggere i nostri cari. Ergo serve una sorveglianza continua delle attività che fanno online.

cosa dire e cosa non dobbiamo dire

Sì	Meglio EVITARE	ASSOLUTAMENTE NO!
Nome	Cognome	Indirizzo e telefono
“Amicizia” solo a conoscenti o, meglio, a veri amici e solo dopo attenta verifica di persona, via email o telefono per evitare casi di omonimia o profili "fake"	Foto/video di persone (solo di maggiorenni)	Scuola/palestra frequentata
	Foto/video e notizie su vacanze (passate)	Contatti con sconosciuti (non dare “amicizia” a sconosciuti)
	App eccessive o app con geolocalizzazione (FourSquare, AroundMe)	Notizie sulle vacanze future o su allontanamenti da casa
	Account collegati (Facebook per YouTube)	Tag non autorizzati
Foto/video di paesaggi	Appuntamenti (dipende)	Flame e profili falsi ("fake")
		Foto proprie o di proprietà e oggetti di valore (casa, auto, ecc.)
		Video (Periscope, Vine, ecc.)

Ladri tecnologicamente più avanzati dell’utente medio hanno ormai compreso che non occorre più sorvegliare un possibile obiettivo direttamente con il rischio di essere individuati. E’ sufficiente vedere cosa l’utente posta online, o cosa gli altri dicono di lui, i discorsi che fa, le immagini che riprendono l’ultimo costoso gadget tecnologico, per comprendere se è benestante o meno.

geolocalizzazione

A cosa può servire a un'app di ricette sapere dove ci troviamo?

Occorre sapere che varie app chiedono all'utente di poterne determinare la posizione per potergli offrire servizi legati a queste. App come Google Maps o Mappe non avrebbero senso senza la geolocalizzazione così come app come AroundMe che permettono di trovare locali come ristoranti, gelaterie, ecc. nelle proprie vicinanze.

Ma ci sono anche app, come ad esempio alcune di ricette di cucina, che richiedono di attivare la geolocalizzazione e l'utente, spesso senza nemmeno leggere la richiesta, accetta tutto. E' evidente che non serve a loro per migliorare il servizio che forniscono a noi ma serve a loro solo per aumentare le loro finanze.

geolocalizzazione delle nostre foto

Esempio

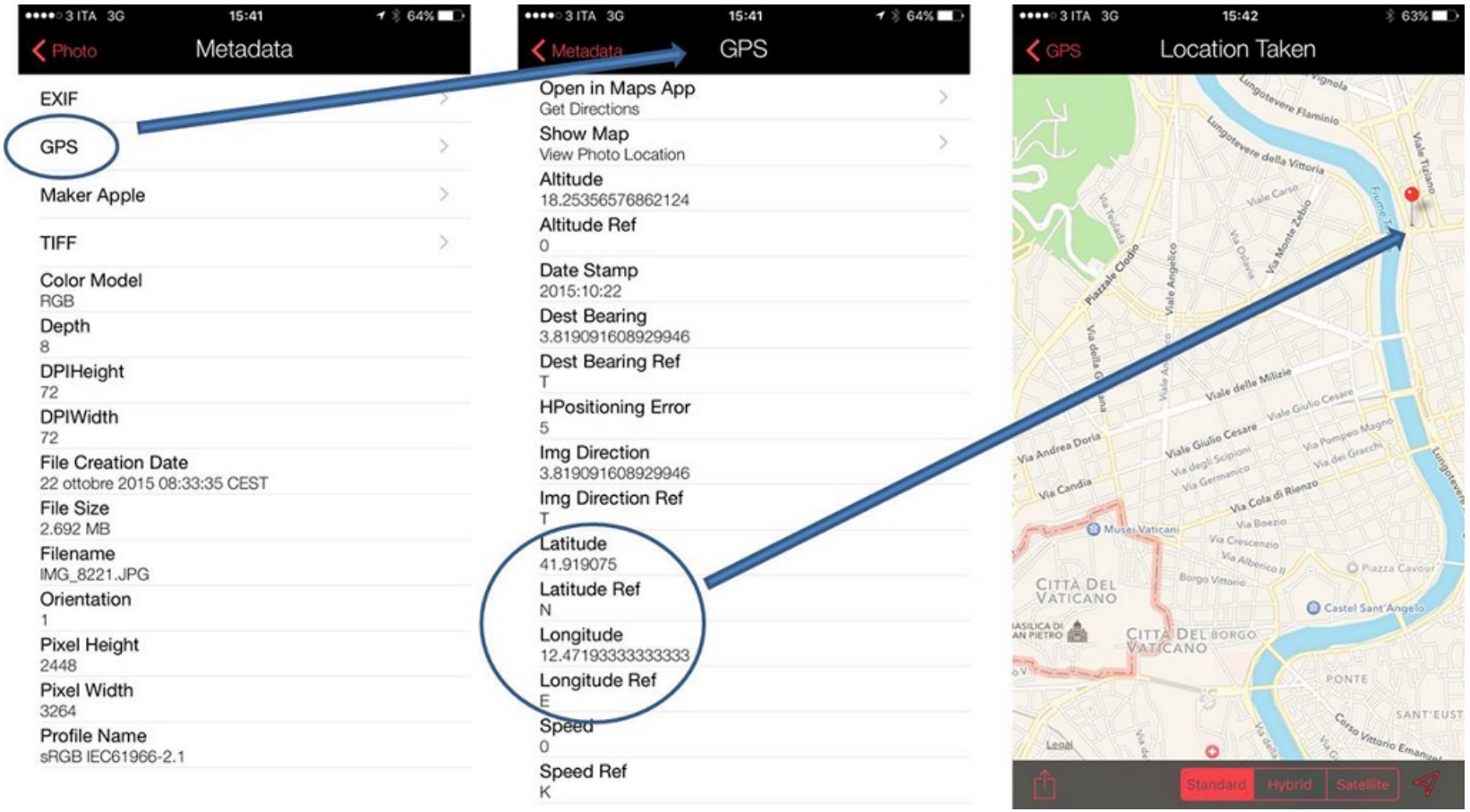
A volte forniamo informazioni in grado di geolocalizzarci anche senza saperlo. E' il caso delle foto acquisite con gli *smartphone*.

Spesso gli utenti non disdegnano di sapere dove è stata scattata una foto oppure non sanno nemmeno che le foto, come i video e molti altri file, sono corredate dai cosiddetti meta-dati.

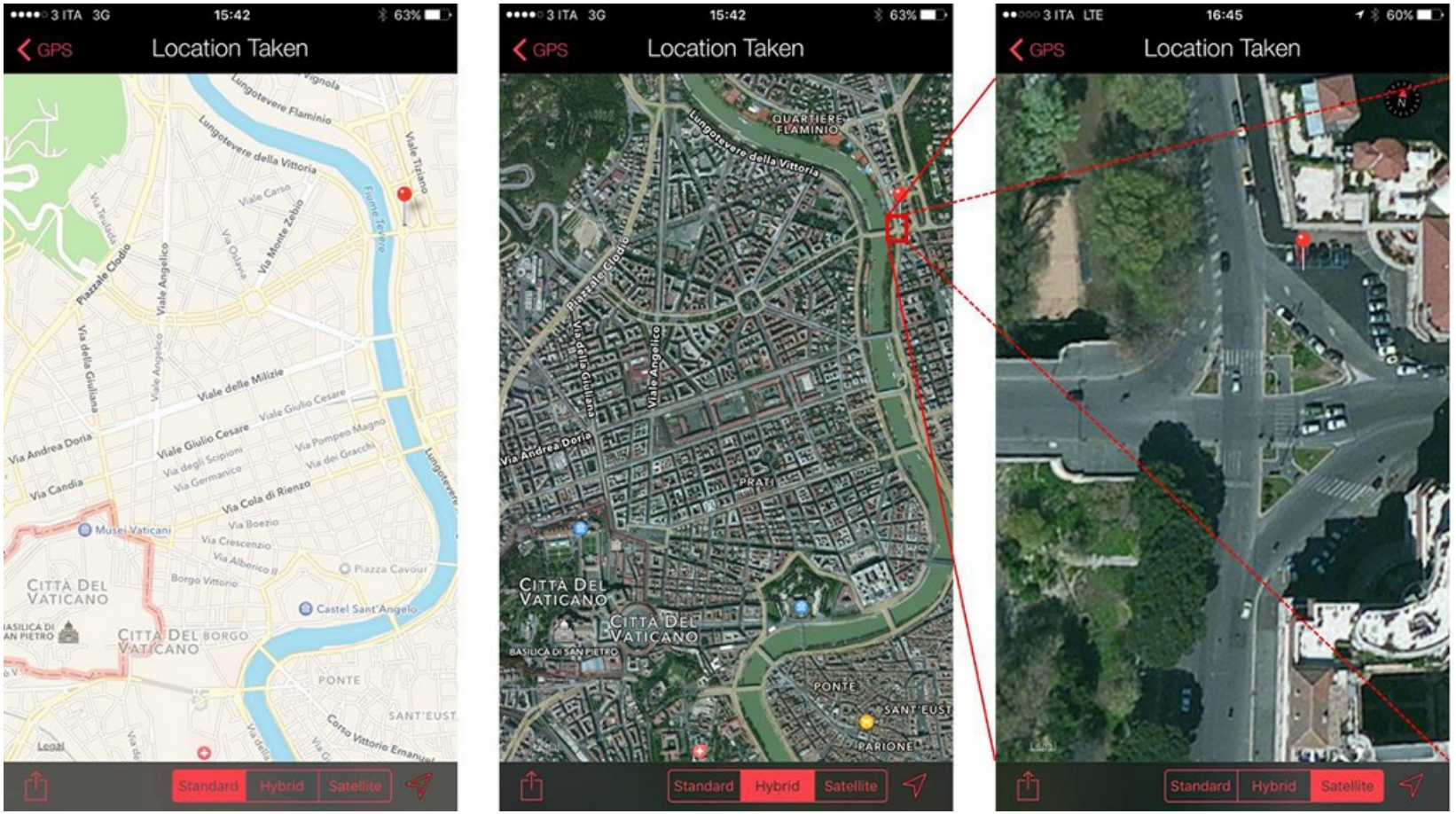
Questi meta-dati servono a memorizzare numerose informazioni, molte di più di quanto si possa immaginare. Vediamo questa sequenza di immagini che mostra quanti dati si possono estrarre da una singola foto scattata a Roma.

Impiegando una delle tante app che permettono di leggere i meta-dati si apre la scheda relativa al GPS (Global Positioning System, sistema satellitare per la determinazione precisa della posizione). In base alla latitudine e longitudine l'app ci mostra il dato su una mappa.

geolocalizzazione delle nostre foto



geolocalizzazione delle nostre foto



geolocalizzazione delle nostre foto

Pensiamo attentamente prima di pubblicare una nostra foto e, se proprio vogliamo farlo, almeno eliminiamo i metadati (Exif) che ogni immagine mantiene nel proprio file.

In pratica si può vedere come il sistema fornisca la posizione del fotografo con una precisione molto spinta, dell'ordine delle decine di centimetri. Pensiamo un po' cosa accadrebbe se una scrupolosa mamma, molto attenta alla privacy, fotografasse i propri figli in salotto nel corso di una festicciola o se una ragazzina, attenta a non dare informazioni in eccesso, si facesse un *selfie* nella propria cameretta di casa e entrambi postassero la foto su un social network.
Sarebbe possibile per un eventuale pedofilo sapere esattamente dove poter trovare la ragazzina con una precisione migliore che non se avesse l'indirizzo di casa, dato che il sistema fornisce anche l'altezza che permetterebbe di ritrovare un appartamento anche in un condominio affollato.
Per eliminare almeno i dati di posizione da una foto scattata con un iPhone; Impostazioni > Privacy > Localizzazione individuate l'app Fotocamera e disattivatela.

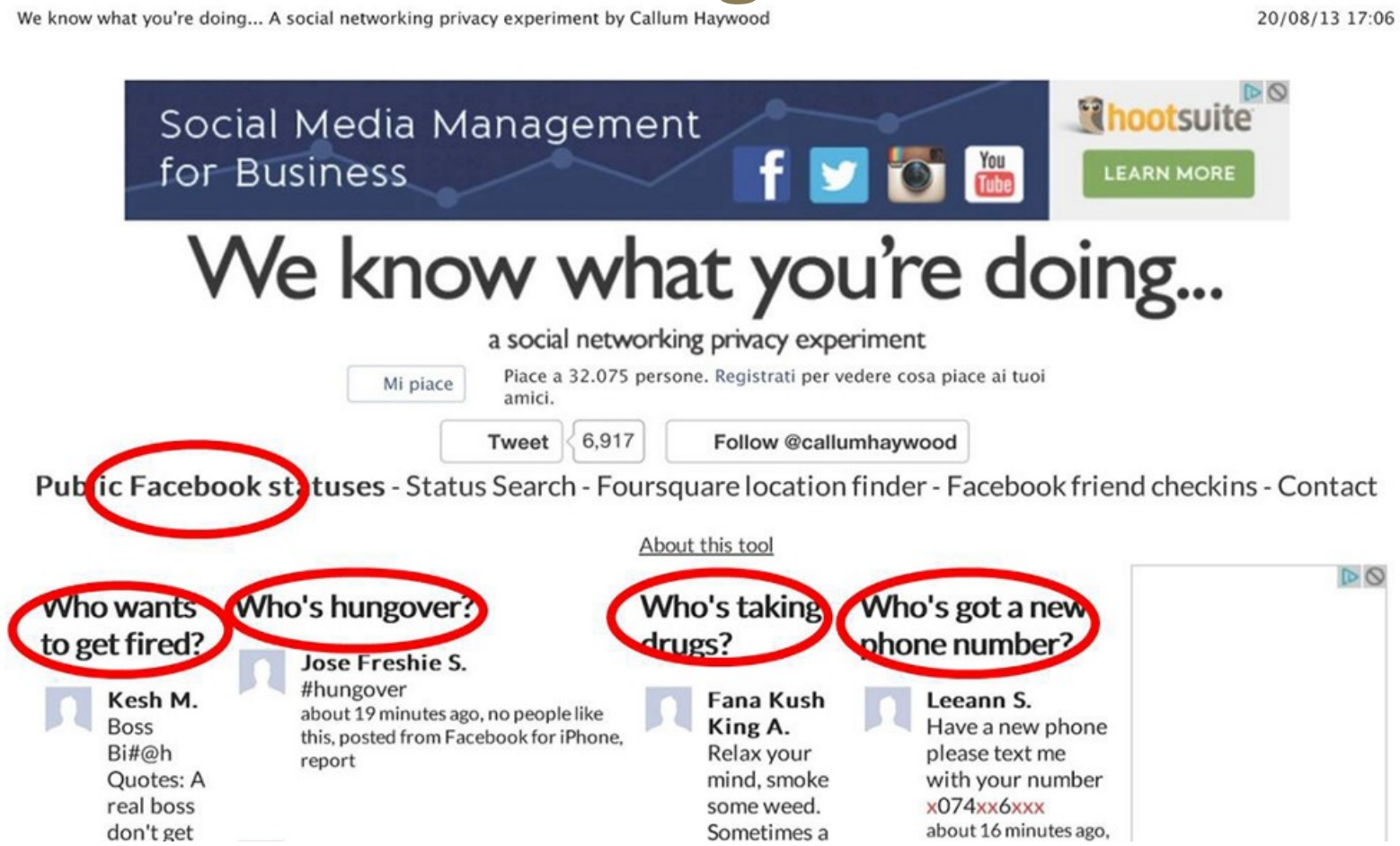
ma cosa interessa agli altri di me?

Siamo proprio sicuri di non suscitare interesse anche in chi non conosciamo?

Anche la convinzione che agli altri non importi niente dei nostri fatti è errata. Sono numerosi gli esempi di chi, o per questioni di ricerca o di semplice curiosità, “pesca a strascico” osservando cosa fanno gli individui su Internet.

Un esempio è rappresentato dal sito rappresentato nella foto alla pagina seguente e dal titolo evocativo “We know what you're doing…” (2013, ormai off-line) che mostra: gli utenti che fanno uso di droghe, chi parla male del proprio datore di lavoro, chi lascia il proprio numero di telefono online, ecc.

ma cosa interessa agli altri di me?



possiamo pubblicare foto liberamente?

	immagine dannosa	immagine non dannosa
Persona famosa (VIP)	Pubblicabile senza autorizzazione ma con le dovute accortezze	Pubblicabile senza autorizzazione
Persona non famosa	Chiedere autorizzazione alla pubblicazione	Pubblicabile senza autorizzazione
Minore	Mai	Chiedere autorizzazione alla pubblicazione ai genitori

… e comunque:	immagine dannosa
se fornisce indicazioni su: stato di salute - orientamento politico - credo religioso - vita sessuale	Richiesta autorizzazione e comunicazione al Garante
Se è per finalità: promozionali - pubblicitarie - merchandising o comunque non di prevalente informazione o gossip	Chiedere autorizzazione alla pubblicazione

social network famosi per essere pericolosi

Alcuni social network sono tristemente famosi non perché sono pericolosi in se stessi ma per come vengono usati. In genere avviene perché permettono di anonimizzare gli interlocutori o perché permettono di collegare perfetti sconosciuti fra di loro.

Attenzione ai social network/applicazioni tristemente famose tra ragazzi e ragazze per la supposta anonimità che fa dire loro tutto quello che pensano, come:

- **Ask.fm** (messaggi anonimizzati che sono spesso usati male per diffondere odio in Rete);
- **Chat roulette / Omegle** (video chat che mettono in comunicazione persone sconosciute in modo casuale);
- **Snapchat** (messaggi che si autodistruggono, usato spesso per il sexting);
- Kik Messenger;
- Voxer;
- Formspring.

stralcio da una discussione su Ask.fm

avvenuta dopo il suicidio di una ragazza

era troia però

Muori cazzo, ora sono io che dico a te muori, per il tuo cazzo di gioco, perchè per te solo questo era, è costata la vita ad una ragazza stupenda come . Siete solo degli stronzi bastardi di merda che pensano solo al divertimento e non alla fragilità delle persone. Meritate di morire soffrendo al più lungo possibile.

circa 3 ore fa

tu lo sapevi cosa voleva fare?

No, cioè sapevo che non riusciva più a sopportare gli anonimi di ask perchè me lo diceva lei, poi per il ragazzo ecc..
Ma soprattutto per la storia dei tagli, le avevano rotto cazzo, vabe non la conosco stra bene ma in quattro anni ho fatto a tempo a parlarci. Non meritava di fare sta fine, no e tutto per colpa di anonimi del cazzo

circa 3 ore fa

perchè si è suicidata??mi dispiace:(

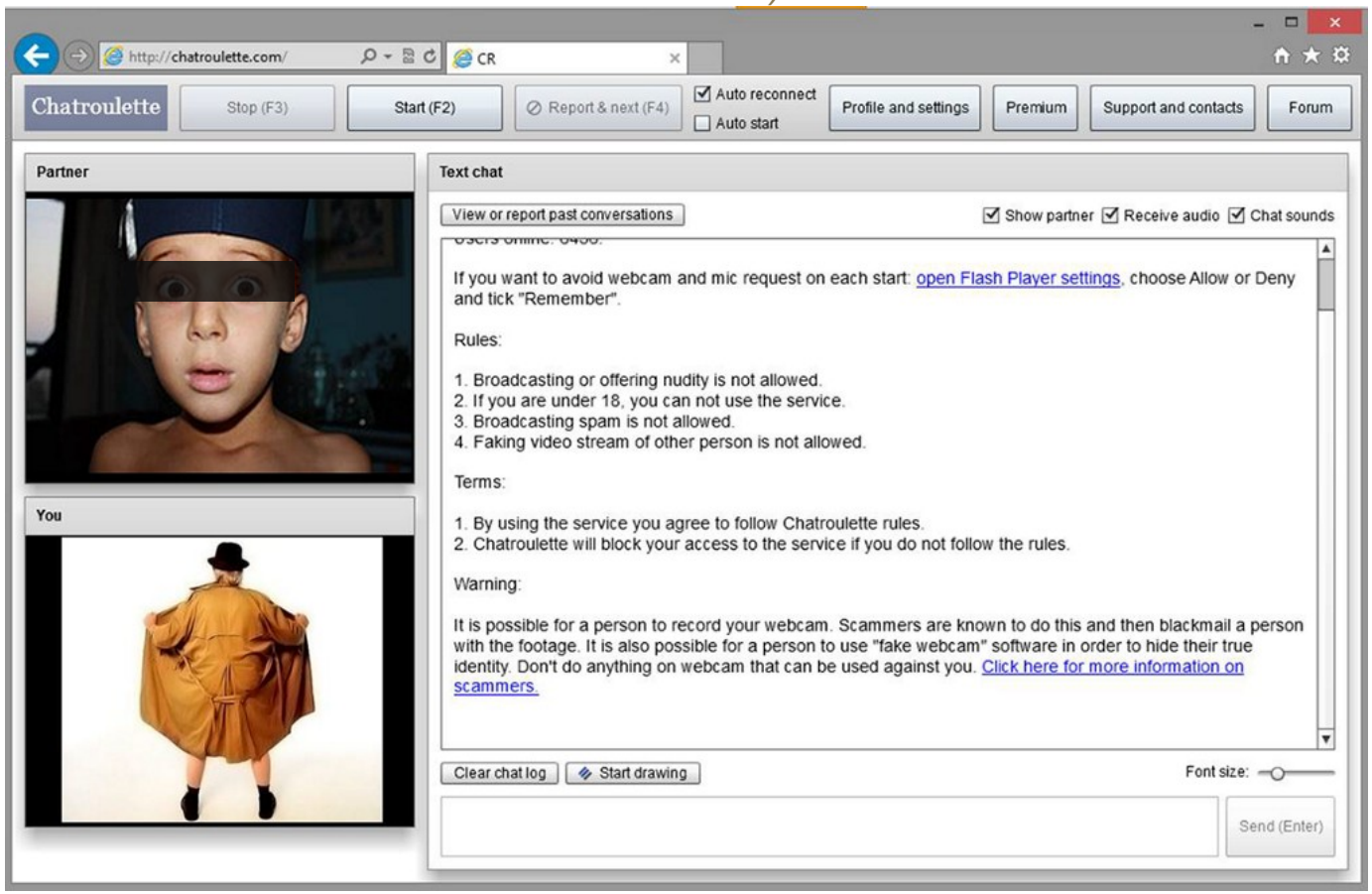
Non sono tenuta a parlare

circa 5 ore fa

conosci la ragazzina che è morta?

Sì.

Chatroulette, simile a Omegle *(le immagini del bambino e dell'esibizionista sono di fantasia)*



varie “mode” su Internet

I pericoli spesso si annidano anche in vere e proprie mode lanciate sui Social Network.

A fronte dell’“Ice Bucket Challenge” una campagna virale lanciata nell’estate 2014 dalla ALS Association (Associazione statunitense contro la SLA) con lo scopo di sensibilizzare l'opinione pubblica sulla sclerosi laterale amiotrofica e di stimolare le donazioni per la ricerca, ve ne sono state altrettante negative, molto negative, sempre nel 2014. Tra queste ultime la “Neknomination” che prevede che il nominato beva una ingente quantità di alcol tutta d'un fiato per poi pubblicare il filmato sul web con la nomina di altre due persone a fare altrettanto. Inizialmente veniva usata solo birra poi le persone sono passate ai superalcolici o a fare bravate dopo la bevuta. Ciò ha comportato almeno 5 morti in Gran Bretagna nel solo 2014. Purtroppo la fantasia malata di certe persone ha diffuso anche altri “giochi” pericolosi come il “Knockout Game!” che consiste nello sferzare pugni e calci ai passanti, a caso, senza motivo, gioco che ha mietuto vittime anche in Italia, ovviamente sempre facendosi riprendere con una videocamera per mostrare il proprio gesto sconsiderato.

“mode” su Internet positive

’“Ice Bucket Challenge”.

Foto di: Stefan Brending, Lizenz: Creative Commons by-sa-3.0 de, CC BY-SA 3.0 de, https://commons.wikimedia.org/w/index.php?curid=35072238

“mode” su Internet negative

“Nek nomination”.	
	“Knockout Game!”

http://www.ohtuleht.ee/565212/rumal-joomismang-kogub-tuure#1

'Why Neck It?' - Documentary On Neknominations - Abi Hoskins

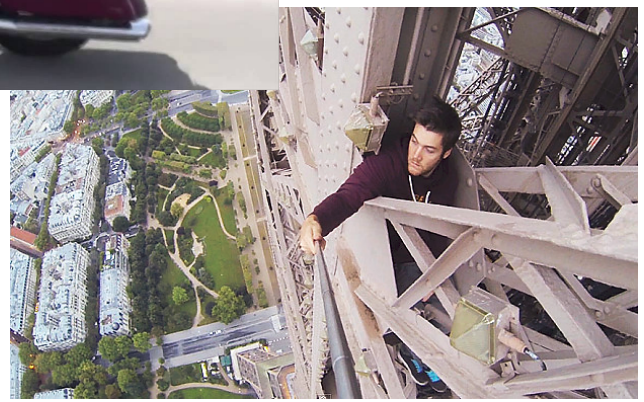
https://www.youtube.com/watch?v=E4hj03LaGvg

http://www.snopes.com/wordpress/wp-content/uploads/2016/02/knckout.jpg

selfie estremi

Distrarsi in movimento.	
	"Darwinismo tecnologico: morire per un selfie" (Web news, 6.7.2016).

https://jafrum.files.wordpress.com/2014/11/distractions-while-riding.jpg



http://i.telegraph.co.uk/multimedia/archive/03496/effiel1_3496434b.jpg

Internet non dimentica

Da Internet non scompare mai niente.

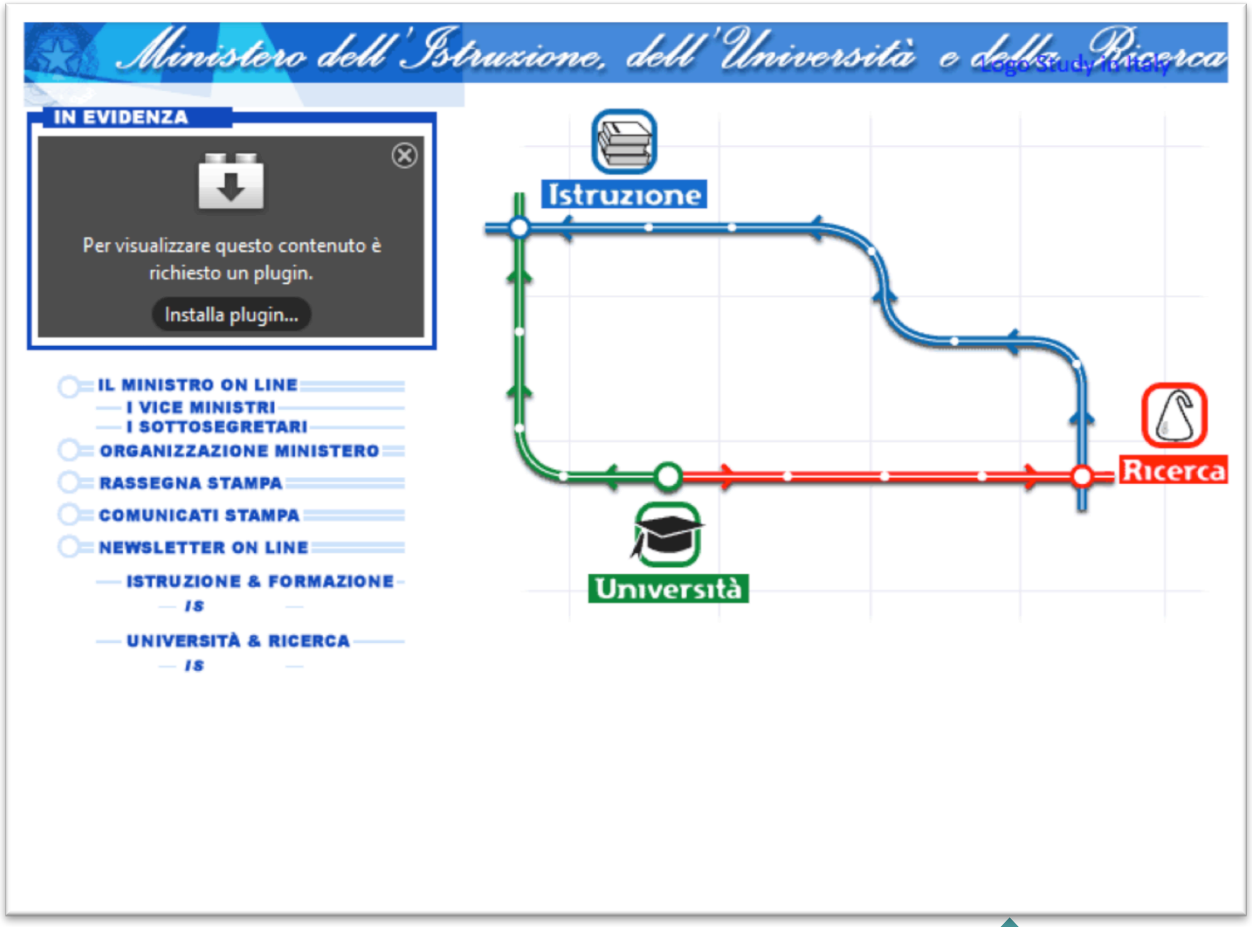
Il problema è ulteriormente ingigantito dal fatto che da Internet si può affermare che **non scompare mai niente**, sia perché:

- chiunque può avere salvato "quelle" immagini o "quel" video particolarmente intrigante sul proprio computer;
- vari fornitori di servizi effettuano numerosi backup in siti sparsi per il mondo per evitare che i propri utenti possano perdere propri dati (si dice che Gmail mantenga costantemente almeno 6 copie di backup di ogni singola mail sui suoi server proprio per questo);
- sia perché ci sono servizi che effettuano il cosiddetto *mirroring* dei siti e li archiviano per studio o futura memoria.

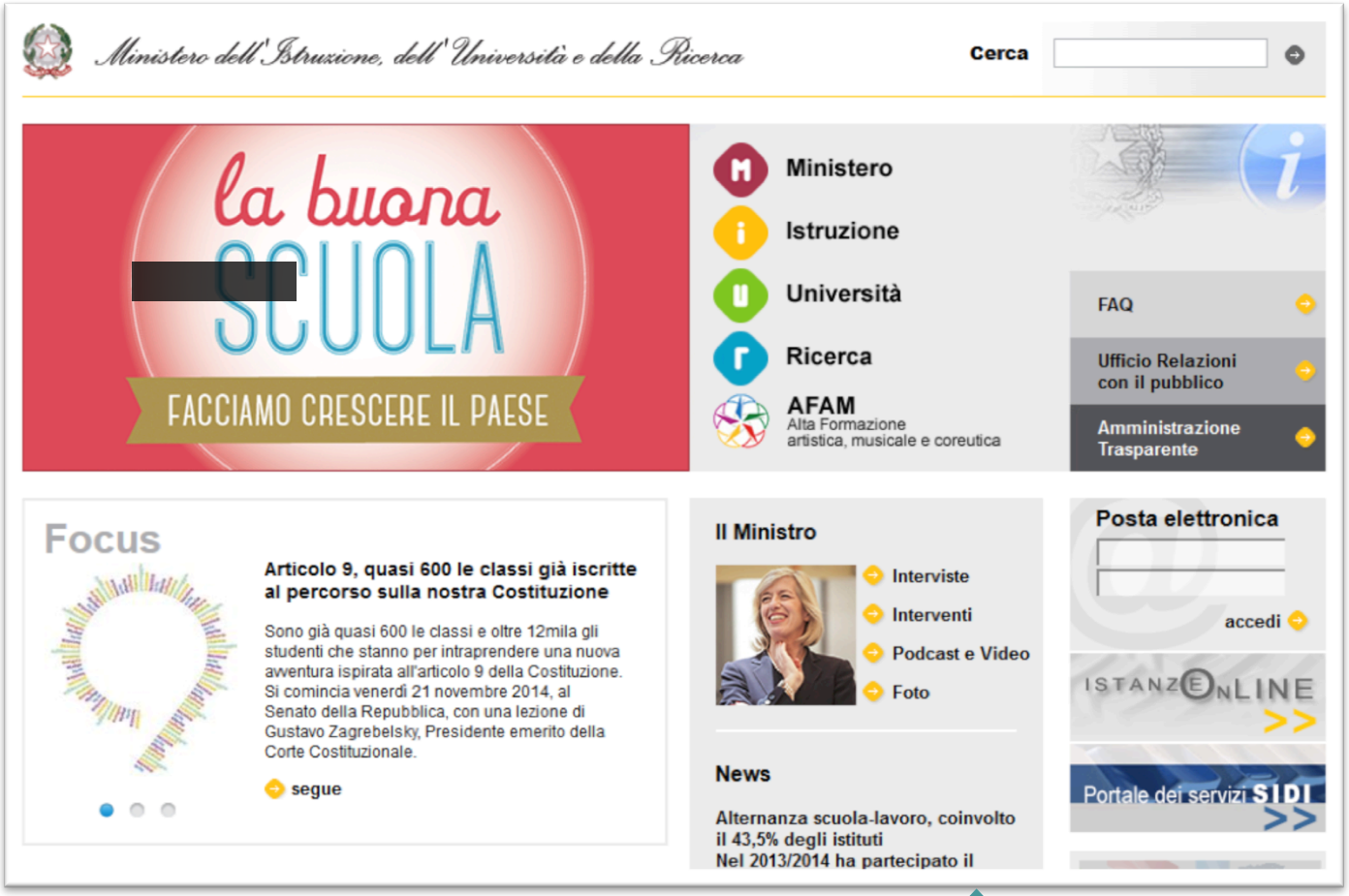
Sapendo dove cercare è possibile, ad esempio, vedere l'evoluzione del sito del Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) negli anni.

MIUR www.istruzione.it (05.11.1998)

MIUR www.istruzione.it (14.07.2005)



MIUR www.istruzione.it (22.11.2014)



sezione 05

iperconnessi

Oggigiorno è quasi più facile enumerare gli oggetti che non permettono di connettersi.

I giovani d'oggi sono sempre più connessi, anzi iperconnessi.

Molto spesso i genitori si preoccupano della sicurezza del solo computer ("mi dica quale Parental Control posso installare sul PC di mio figlio?") anche quando sanno benissimo che per usare Internet al PC i propri figli preferiscono lo *smartphone* oppure usano *tablet*, *smart* TV, consolle giochi come Playstation, Wii, Xbox, ma anche navigatori, orologi, GoogleGlass e chi più ne ha più ne metta.

Oggigiorno è quasi più facile enumerare gli oggetti che non permettono di connettersi che non quello che sono costantemente collegati alla rete ridenominata IoT ("Internet of the Things", Internet delle cose).

dal device fingerprint al cross-device tracking

Purtroppo ogni sistema che impieghiamo lascia sempre delle tracce evidenti che permettono ad altri di sapere che cosa stiamo facendo in ogni istante.

Innanzitutto occorre dire che non esiste un sistema esattamente uguale ad un altro. Si stima che se si effettua una installazione da zero di un sistema operativo senza apportare alcuna personalizzazione esista una sola possibilità su qualche milione di trovare un altro sistema uguale. Se poi effettuiamo una qualsiasi personalizzazione possiamo essere ragionevolmente certi che i nostri apparati siano riconosciuti come oggetti unici.

Vediamo quali sono i mezzi per seguirci.

- Stack **TCP-IP**: a seconda del sistema operativo in uso la cosiddetta pila TCP/IP è diversa, quantomeno lo sono l'indirizzo della scheda di rete (l'indirizzo MAC) e l'indirizzo IP del computer;
- Parametri **HW PC** (Serial number, caratteristiche, risoluzione schermo);
- Parametri **SW PC** (sistema operativo, fuso orario, software installati ognuno con un numero seriale diverso).
- Attività di **navigazione**:
  - Uso di un particolare **browser** (font, pixel video);
  - Impiego di certi **plug-in**;
  - **Cookies**: ve ne sono di vari tipi tra i quali:
    - HTML5 storage;
    - HTTP Cookies: First o Third Party;
    - Flash LSO: First o Third Party;
    - Flash Cookies;
    - Session Cookies;
    - HTML5 LSO;
    - Supercookies;
    - Web bug.

cookie

Per chi non sapesse cos'è un cookie deve pensare che non è altro che una stringa di dati, cioè una serie di caratteri alfanumerici, utili per memorizzare alcune informazioni importanti. I cookie servono per operazioni fondamentali. Ad esempio: per mantenere traccia di cosa stiamo acquistando da un negozio online, il cui carrello della spesa senza cookie si azzererebbe ogni volta che scegliessimo un nuovo oggetto da acquistare; per memorizzare le password di accesso a un sito senza costringerci ogni volta a digitarle di nuovo; ecc..

In realtà i tanto vituperati cookie, per come sono stati pensati, sarebbero stati un sistema abbastanza sicuro perché possono essere letti dal solo server che ce li ha inviati. Solo che le persone sono abilissime a scovare utilizzi alternativi.

Praticamente da subito venne trovato il modo di ingannarli. Società come Doubleclick.com (acquistata recentemente da Google) pensarono che se al posto del server X, del server Y e del server Z fossero state loro a metterli per tutti avrebbero potuto sapere le nostre abitudini di navigazione sui server citati, ai quali loro avrebbero distribuito le informazioni dietro pagamento.

Quando, ancora oggi vediamo nella barra in basso a sinistra dei vari browser rapidamente passare la scritta doubleclick.com prima di raggiungere il sito di nostro interesse, e magari molti altri siti, possiamo essere certi che stiano attuando quanto citato. E' per questo che i cookie sono divenuti un argomento spinoso per la nostra privacy, perché commercianti con pochi scrupoli e molta immaginazione hanno trovato un ottimo sistema per sapere le nostre abitudini online.

cookie

Internet: la privacy questa sconosciuta.

In sostanza possiamo essere sicuri che ciò che digitiamo:

- sui vari motori di ricerca (Google, Bing, Yahoo!, ecc.)
- nei vari social network (Facebook, Twitter, Instagram, Snapchat, del.icio.us, reddit, Ask.fm, WhatspApp, ecc.)
- nei vari social media (Scribd, YouTube, Blogger, Slideshare)
- in altri servizi

da qualcuno viene opportunamente correlato e collegato a discapito della privacy.

cosa dicono di noi i nostri browser

How well are you protected against non-consensual Web tracking? After analyzing your browser and add-ons, the answer is ...

Mixed results: you have **some protection** against Web tracking, but it has **some gaps**. We suggest re-configuring your protection software, or consider **installing extra protections**. Privacy Badger isn't available for your browser / OS, but Disconnect may work for you.

Test	Result
Is your browser blocking tracking ads?	✓ yes
Is your browser blocking invisible trackers?	! partial protection
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✗ no
Does your browser protect from fingerprinting?	✗ your browser has a unique fingerprint

Show full results for fingerprinting

Note: because tracking techniques are complex, subtle, and constantly evolving, Panopticlick does not measure all forms of tracking and protection.

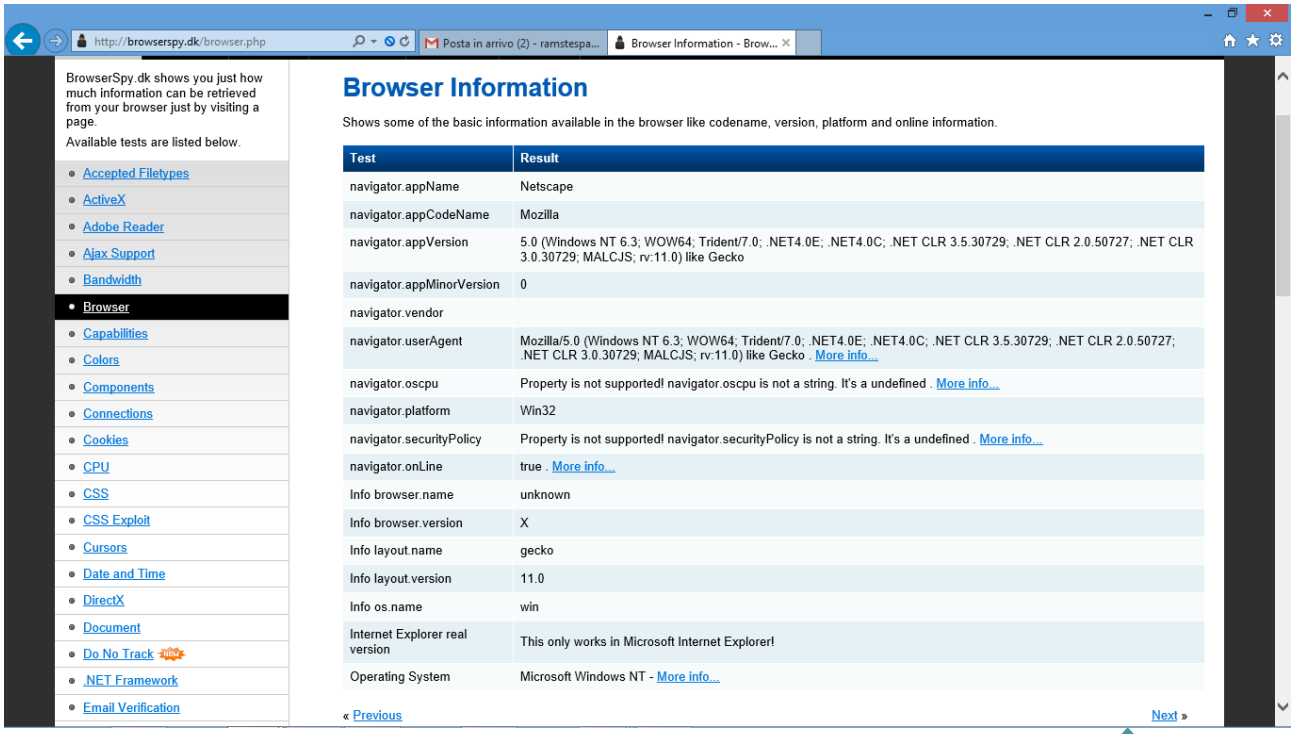
Se vogliamo sapere quali informazioni specifiche il nostro browser, sia esso Internet Explorer, Firefox, Safari, Opera, ecc., rende disponibili ai siti che visitiamo è sufficiente visitare dei siti predisposti per mostrare le informazioni che i nostri browser raccolgono su di noi, come:

http://panopticlick.eff.org/

cosa dicono di noi i nostri browser

...oppure su http://browserspy.dk/

e ci renderemo conto del perché dopo avere fatto una ricerca di un berretto da baseball, quando nuovamente andremo sullo stesso motore di ricerca, ma anche su altri siti che non dovrebbero averci niente a che fare, invariabilmente verremo bombardati con pubblicità sui berretti da baseball.



caso limite... ma pur sempre un caso

File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto

La tecnologia ci spia? Man...

www.lettera43.it/tecnologia/web/la-tecnologia-ci-spia-manuale-di

Cerca

MENU FOTO VIDEO FIRME BLOG CERCA LOGIN

STRAGE DI ORLANDO | EURO 2016 | CRISI CENTRODESTRA | AMMINISTRATIVE 2016 | EMERGENZA MIGRANTI

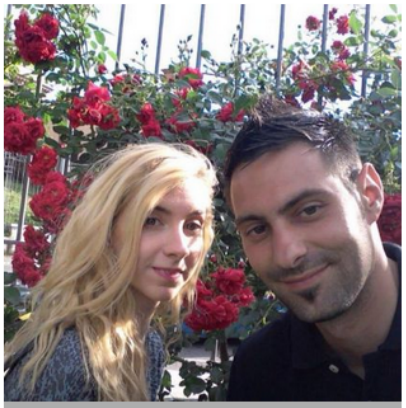
Home » tecnologia » La tecnologia ci spia? Manuale di sopravvivenza

La tecnologia ci spia? Manuale di sopravvivenza

Sara localizzata e uccisa con "Trova il mio iPhone". E anche noi lasciamo tracce. WhatsApp, cellulari, mail, social: due esperti spiegano come proteggersi in Rete.

di Fabrizio Colarieti | 12 Giugno 2016

In molti vivono nella convinzione, e alcuni anche nella paura, che i propri strumenti digitali lascino dietro di sé molte tracce che messe insieme da mani malintenzionate consentano di svelare informazioni personali di ogni tipo.
È sicuramente tutto vero, al netto delle leggende metropolitane - «se senti l'eco della tua voce sei intercettato» -, tanto che gli esperti lo hanno soprannominato "effetto Pollicino".
Uno di questi incubi è legato alla possibilità - ormai non più remota e, come vedremo, molto facile da attuare - che qualcuno ci pedini



Sara Di Pietrantonio e l'ex fidanzato Vincenzo Paduano.

Ultima ora | Le TOP 5 di oggi

10:51 Frana vicino Cortina, interrotta statale

09:08 Borsa, Milano apre in rialzo dell'1,15%

06:52 Furbetti cartellino, 9 arresti a Caserta

06:48 Obama riceve Dalai Lama a Casa Bianca

00:34 Bimba in adozione anche a

plugin che evitano il tracciamento

Le tue scelte online.

I plugin sono dei moduli software, di per se non autonomi, che interagiscono con altri programmi o applicazioni per ampliarne le funzioni. Si trovano numerosi plugin per Firefox, così come estensioni per Internet Explorer o altri browser, che permettono di fare da filtro e limitare il tracciamento. Purtroppo, nel caso di Firefox, all'inizio di aprile 2016 è stato riscontrato che plugin diffusi come: No Script, Firebug, Greasemonkey e altri add-on (come sono anche chiamati) molto diffusi rappresentano una vulnerabilità per il browser mentre solo AdBlock Plus sembrava non essere vulnerabile (per allora... e adesso?).

Un meccanismo che limita la diffusione di dati che disperdiamo verso soggetti terzi è rappresentato da questo link: http://www.youronlinechoices.com/it/le-tue-scelte.

In questa pagina è possibile agire su degli interruttori che inibiscono l'acquisizione di numerose informazioni da parte di terzi.

la Privacy: questa sconosciuta

Spesso si parla di privacy ma non ci siamo nemmeno presi la briga di sapere come le norme la definiscono. Le vari informazioni relative alla privacy sono suddivise in categorie che qui si elencano da quelle meno importanti a quelle più importanti:

- i **dati personali**: nome e cognome della persona, la ragione sociale della ditta, l'indirizzo o i numeri di telefono o di cellulare, codice fiscale e partita IVA;
- i **dati identificativi** sono i dati personali che permettono l'identificazione diretta dell'interessato, come la fotografia di una persona;
- i **dati giudiziari**;
- i **dati sensibili**, che sono dati personali idonei a rivelare: l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale.

Quante volte ci sarà capitato di vedere su un social network persone parlare di problemi di salute o sessuali o fare discussioni politiche che permettono di comprendere le opinioni di una persona senza dargli eccessivamente peso fermo poi inalberarci quando qualcuno impiega tali informazioni?

Anche una semplice ricerca su un motore di ricerca di un farmaco per un raffreddore mette a rischio la nostra privacy come si può evincere dall'articolo alla pagina seguente tratto da "La Repubblica" del 20 marzo 2015 a pagina 42.

la Privacy e la Rete

R2/ LA COPERTINA

Il medico spia viaggia su Internet così ci rubano i segreti della salute

FABIO CHIUSI E MAURIZIO RICCI

I malati nella rete

Quando cerchiamo sul web i sintomi di un disturbo che sospettiamo di avere, nove volte su dieci un software trasmette le domande a un circuito parallelo, dove le autorità pubbliche e le imprese pescano a nostra insaputa informazioni riservate e preziosissime. Uno studioso americano spiega come funziona l'ultimo Grande fratello di internet. Che ora l'Unione europea sta cercando di fermare con un nuovo codice della privacy

Basta effettuare una ricerca sull'influenza per far sapere a molti di non sentirsi bene

Perfino associazioni umanitarie condividono dati sensibili, per esempio sull'aborto

MAURIZIO RICCI

per le ricerche su Internet relative a 2 mila comuni malattie.

uno fa se ha un dito gonfio, il colesterolo alto o un mal di testa ricor-

Articolo tratto da "La Repubblica" del 20 marzo 2015 a pagina 42.

In sostanza l'**identificazione di una persona può condizionare:**

- il **lavoro**;
- la possibilità di **accendere un mutuo** (credito);
- la possibilità di avere una **copertura assicurativa**;
- i **nostri acquisti** (variazioni di prezzo a seconda censo);
- le **informazioni** a cui si può accedere;
- Ecc.

reputation on-line

Un uso sbagliato dei Social network avrà sicure ripercussioni su quella che è denominata “Reputation on-line” e che sta assumendo sempre maggiore importanza e rappresenta un argomento importante per il futuro dei nostri ragazzi. Società, pubblica amministrazione e singoli utenti devono la loro reputazione a ciò che "sono" online.

“La reputazione (o nomea) di un soggetto (una persona, un'istituzione, un'azienda e così via) è la considerazione o la stima di cui questo soggetto gode nella società. A differenza di "stima", il termine reputazione ha valenza neutra; si può cioè godere di una buona o di una cattiva reputazione” (da Wikipedia).

La reputazione condiziona pesantemente le nostre vite e mentre in passato si veniva giudicati principalmente dalle nostre azioni, oggigiorno lo siamo anche da ciò che scriviamo o postiamo online. E’, pertanto, normale che se una persona deve cercare lavoro il suo curriculum vitae sia vagliato anche in base alle informazioni della persona che si possono reperire online. Anzi, oggi almeno i CV del 70% delle persone che chiedono un lavoro viene vagliato e verificano ricorrendo a ricerche sul web. Per poter comprendere cosa un futuro datore di lavoro, o un semplice curioso, potrebbe trovare su di noi online si vedano i seguenti siti per avere una prima idea di cosa è possibile trovare:

- http://pipl.com;
- http://snitch.name;
- http://www.twilert.com;
- http://www.google.it (e stabilire un “alert” con il proprio nome)

Ovviamente un “cacciatore di teste” non si limiterà a verificare questi link ma potrà ricorrere a siti specializzati

... continua...

reputation on-line

... continua dalla pagina precedente...

in grado di scovare molto di più di quanto ci possiamo aspettare grazie anche alla capacità di incrociare dati provenienti da molte fonti diverse.

La nostra reputazione non è importante solo per cercare un lavoro ma anche per vedersi accendere un mutuo nel caso che una persona non dimostri di offrire sufficienti garanzie.

Anche essere considerate persone con possibili problemi di salute potrebbe crearci qualche difficoltà con le assicurazioni che potrebbero alzare molto il premio assicurativo nel caso che venissero a conoscenza che stiamo effettuando qualche ricerca di troppo in campo medico. Cosa che potrebbe far pensare che soffriamo di qualche malattia, anche a livello familiare. E' infatti questo uno dei motivi del perché il DNA di una persona viene considerato una informazione molto delicata dal punto di vista della privacy tanto che le banche dati che conservano queste informazioni sono tra quelle che vantano i migliori sistemi di protezione.

Non strettamente legato alla reputazione ma alla privacy è il discorso della variazione del prezzo degli acquisti online a seconda di come e da dove viene fatto l'accesso alla rete. E' ormai da molti anni, e lo si può verificare facilmente, che se un utente fa più ricerche su uno stesso argomento (ad esempio un viaggio in aereo da Milano a New York) a distanza di poco tempo vede crescere progressivamente il prezzo (in genere di un 10%), ma se cambia PC o semplicemente browser il prezzo magicamente scende di nuovo su valori normali. Ciò accade in virtù del tracciamento. La compagnia aerea vede che siamo interessati e

... continua

reputation on-line

... continua dalla pagina precedente...

artificialmente fa salire il prezzo. Un sistema simile sta prendendo piede nelle grandi città ed è, invece, basato sull'indirizzo di provenienza di una richiesta. Se a New York un utente fa una richiesta da un indirizzo IP che risulta provenire da Harlem (noto quartiere dove le persone hanno spesso difficoltà economiche) il prezzo visualizzato nel carrello sarà probabilmente inferiore a quello di un utente che vive sulla Fifth Avenue (una delle strade più chic e importanti di Manhattan).

Dobbiamo anche parlare di informazione e qui il discorso sarebbe lungo ma la sostanza è che è inutile pensare che l'informazione venga distribuita a livello mondiale nella stessa forma. Lasciando perdere i regimi dittatoriali che condizionano direttamente le news, la stessa informazione diffusa in Paesi con forme di governo democratiche viene condizionata dai media. Per rendersene conto è sufficiente accedere alla stessa pagina dei media internazionali facendo finta di provenire da Paesi diversi dal nostro (cosa facilmente attuabile utilizzando dei proxy anonimizzatori), vedremo quasi certamente delle differenze eclatanti nel modo in cui viene proposta una stessa notizia, azione che spesso porta a diverse conclusioni da parte dei lettori.

In sostanza per non subire i social network e i social media e ridurre i rischi per la propria sicurezza e gli attentati alla propria privacy occorre impiegare quello che è chiamato lo Human Firewall (Firewall: "componente passivo di difesa perimetrale di una rete informatica, che può anche svolgere funzioni di collegamento tra due o più tronconi di rete, garantendo dunque una protezione in termini di sicurezza informatica della rete stessa" da Wikipedia).

… e allora?

E allora **"Turn on your Human firewall"** (accendiamo il nostro firewall umano, ndr: il cervello) e chiediamoci sempre:

- Lo/la conosco?
- Cosa vuole questo/a?
- Sono sicuro chi sia lui/lei?
- Quali dati gli sto consegnando?
- Che danno mi potrebbe arrecare?

https://i.ytimg.com/vi/QYNR_F4SDMw/hqdefault.jpg

guida ai principali social network

(n.d.r.: se richiesto siamo disponibili a realizzare altre schede per ulteriori social network/media).

Di seguito una serie di slide relative ai principali social network:

- Facebook
- Instagram
- Snapchat
- Twitter
- WhatsApp

Facebook

cosa vedremo

siamo proprio sicuri di
conoscere bene Facebook?

Sezione a cura di:

- Sylvio Verrecchia
- Stefano Ramacciotti, CISSP

Facebook: cos'è?

https://www.facebook.com/

Facebook è una rete sociale creata da Mark Zuckerberg nel 2004 in un primo momento per i soli studenti dell'Università di Harvard. Ha poi avuto una crescita esponenziale fino a raggiungere un livello planetario.
In realtà parlare di social network, per i nostri scopi, è fuorviante. Sarebbe più opportuno parlare di una macchina per fare soldi che ha fatto di Mark Zuckerberg il giovane più ricco del mondo.
Ciò lo si deve al particolare modello di business adottato e sconosciuto alla gran parte delle persone che "credono" di non averne pagato l'accesso. In realtà il pagamento c'è stato con il conferimento della facoltà a Facebook di impiegare le informazioni che immettiamo sui nostri profili. E' grazie alle informazioni lì contenute che vengono rivendute a terzi, e non tanto per la pubblicità inserita nelle nostre pagine, che Facebook è un'azienda da 3.688 .000.000.000 $ netti (2015, https://www.bamsec.com/filing/132680116000043?cik=1326801) generati da 1.650.000.000 di utenti.

Facebook: età minima

"Termini di utilizzo": non è permesso utilizzare i servizi di facebook da parte dei minori di 13 anni.

Regola ampiamente disattesa ma che andrebbe valutata quando i ragazzi chiedono di poter installare facebook.

Facebook: privacy & security

Parlare di privacy su Facebook è, in un certo modo, un paradosso o meglio un ossimoro, perché se uso Facebook è proprio per mostrare agli altri i momenti più significativi della mia vita e non solo. Rivelare cosa mangiamo a colazione non è però obbligatorio e dovremmo stare molto più attenti alle informazioni che vi mettiamo.
Purtroppo sempre più persone condividono una grande quantità di dati personali e non è escluso che lo facciamo perché affetti da una forma di Fear Of Missing Out, ovvero FoMO. Come spiega Wikipedia si tratta dell'"apprensione diffusa che altri potrebbero avere esperienze gratificanti da cui si è assenti. [...] Questa angoscia sociale è caratterizzata da "un desiderio di rimanere costantemente in contatto con ciò che gli altri stanno facendo".»
Per controllare ciò che mettiamo online Facebook mette a disposizione due pagine: "Centro Assistenza" e "Profilo".

Facebook: privacy & security

"Centro Assistenza"

E' la sezione del sito dalla quale è possibile configurare le impostazioni di Facebook e gestire la possibilità di accedere alle nostre informazioni o limitarne l'accesso da parte degli altri. Vi si accede cliccando sull'ultima icona a destra della barra superiore, quella con il triangolo rivolto verso il basso e poi sulla scritta "Centro Assistenza". Cliccando poi su "Visita il Centro Assistenza" si accede a una nuova pagina. Nel menu a sinistra bisogna cliccare su "Privacy" e poi su "Impostazioni di base" dove ci sono tre voci di interesse per la privacy:

- "Strumenti e impostazioni sulla privacy di base";
- "Controlli sulla privacy avanzati";
- "I tuoi dati personali".

E' importante prendere visione di tutto per sapere come comportarsi.
Tra le situazioni che possono arrecare fastidio è quando vediamo comparire sul nostro diario una foto, fatta da altri, con il *tag* (etichetta) con il nostro nome e cognome. Per evitare che ciò avvenga dobbiamo cliccare sul triangolo rivolto verso il basso e selezionare "Impostazioni". Nel menu a sinistra cliccare su "Diario e aggiunta di tag" e modificare la voce "Privacy" su "Impostazioni". Modifichiamo "Chi può scrivere sul tuo diario?" in modo che risulti "Solo Io" e alla voce "Vuoi controllare i post in cui ti hanno taggato gli amici prima che vengano visualizzate sul tuoi diario?" clicchiamo su "Sì".

"Profilo"

Come si evince dal nome è la scheda che popoliamo con i dati che vogliamo che gli altri vedano (foto, nome e cognome, data di nascita, studi pregressi e attività lavorativa). Si accede al profilo cliccando sul nostro nome nella barra superiore. Cliccando sulla seconda voce "Informazioni" della barra superiore dei menu possiamo accedere ai nostri dati.

... continua...

Facebook: privacy & security

Spostando il cursore del mouse su una qualsiasi riga compare l'icona di una matita ("Modifica"), cliccando sulla quale si possono modificare le informazioni.

Possiamo scegliere una tra queste cinque opzioni:

1. **Tutti:** profilo potenzialmente visibile da tutti gli utenti di Facebook, cioè circa 1.65 MLD di persone lo possono vedere ma probabilmente anche di più dato che i principali motori di ricerca indicizzano anche le pagine di Facebook;
2. **Amici:** parola subdola se paragonata al vero significato di Amici nella vita reale, dove il numero di "veri" amici si conta sulle dita di una mano. Gli altri sono conoscenti con più (familiari, colleghi, compagni di classe) o meno (semplici conoscenti) accesso alle nostre informazioni personali. La dizione amici viene usata subdolamente allo scopo di farci abbassare la guardia e condividere più informazioni personali.
3. **Amici degli amici:** a rigor di logica la maggior parte dei conoscenti non sono nostri amici anche se Facebook, intenzionalmente, ne travisa il significato. Questa sarebbe l'opzione massima da scegliere per la condivisione delle informazioni.
4. **Solo Io:** questa sarebbe l'opzione giusta da impiegare sempre avendo cura di non fornire informazioni corrette al fine di non fare distribuire le nostre informazioni a terzi di cui Facebook non rivela nemmeno l'identità
5. **Personalizzata:** da impiegare nel caso volessimo definire un elenco specifico di persone che hanno accesso ai nostri dati.

Facebook: privacy & security

Facebook.

E’ bene ricordare che comunque, qualsiasi opzione scegliamo, Facebook fornirà a terzi i dati che noi inseriamo sui suoi sistemi (a partire dal Diario) come contropartita del servizio fornito.

Inoltre, anche se non siamo “loggati” su Facebook, cioè abbiamo inserito i nostri dati di nome utente e password e visitiamo semplicemente una pagina che contiene l’icona del “Mi piace” di Facebook, anche se non vi clicchiamo sopra Facebook saprà che l’abbiamo visitata grazie ai cookie sul nostro computer.

Ricordiamoci infine di disabilitare la geolocalizzazione in modo da non essere tracciati, al limite permetterla solo quando usiamo Facebook, e ricordiamo che se anche disabilitiamo oggi alcune informazioni su di noi, qualcun altro potrebbe già averle salvate sui propri sistemi sui quali possono rimanerci potenzialmente per sempre.

Facebook: how-to

Facebook.

Per avere informazioni sempre aggiornate:

iPhone:
https://www.facebook.com/help/251803581597761/

Smartphone Android:
https://www.facebook.com/help/452400401467000/

Sicurezza e Privacy su Facebook:
https://www.facebook.com/help/ e cliccare su **Privacy** o **Sicurezza**

Instagram

cosa vedremo

siamo proprio sicuri di
conoscere bene Instagram?

Sezione a cura di:

- Sylvio Verrecchia
- Stefano Ramacciotti, CISSP

Instagram: cos'è?

https://www.instagram.com/

Instagram è un'applicazione gratuita per la condivisione di foto e video. Le persone possono caricare foto o video e condividerli con i loro "*followers*" ovvero i seguaci o con un gruppo di amici selezionato. Il successo di Instagram è dovuto alla grande community di creativi, che con i loro scatti fotografici, pubblicano, condividono e raccontano momenti di vita.
Nella home dell'applicazione è possibile visualizzare le foto pubblicate dai nostri amici, commentarle ed esprimere il proprio gradimento.
Ad Instagram sono legate tre applicazioni stand-alone:

- **Layout:** app per collage fotografici. Partendo dalle foto presenti sullo *smartphone* è possibile applicare diverse modifiche prima della condivisione.
- **Boomerang:** permette di creare mini video che saranno riprodotti in *loop* mettendo insieme una serie di foto.
- **Hyperlapse:** permette di ottenere dei video ad effetto cinematografico, privi di tremolii e con possibilità di scegliere il tempo di riproduzione, senza ricorrere a costose apparecchiature professionali.

Instagram: età minima

"Termini di utilizzo": non è permesso utilizzare i servizi di Instagram da parte dei minori di 13 anni.

Il problema è che la legge italiana non permette, se non in particolari casi preventivamente autorizzati, che si pubblichino liberamente foto di minori, com'è una buona parte di utenti. Tale legge viene continuamente infranta proprio dai ragazzi che pubblicano loro foto o, come spesso accade, foto di loro coetanei.

Visto che tutti hanno la possibilità di vedere le foto e i video di un profilo pubblico, diventa importante per un genitore attivare un livello di privacy molto restrittivo in modo da assicurarsi che solo chi segue legittimamente il profilo possa vedere i post del proprio figlio e che non possa essere visto dagli sconosciuti.

Instagram: privacy & security

Instagram non rivendica la proprietà di qualsiasi contenuto pubblicato dall'utente sui servizi o tramite essi.
L'utente garantisce a Instagram una licenza non esclusiva, completamente pagata e libera da royalty, che può essere concessa come sottolicenza ed è valida in tutto il mondo, per l'uso dei contenuti che pubblica sui servizi o tramite i servizi, soggetta alla normativa sulla privacy". Questa licenza termina nel momento in cui si elimina l'account o il contenuto presente nell'account, salvo ulteriore condivisione con terzi.
Per evitare di vedere utilizzare una propria foto per fini commerciali occorre proteggerla con il sistema del *watermark*, ovvero applicare alle immagini una scritta o logo per rivendicarne la paternità.
E' sempre meglio rendere il proprio profilo privato. Per attivare tale impostazione: "Modifica profilo" > opzione "Post privati". In questo modo chi vorrà accedere ai vostri contenuti, non dovrà far altro che inoltrarvi una richiesta e sarete voi a decidere se approvarla o meno.

Instagram: how-to

Instagram.

Come impostare la propria privacy rendendo visibile i propri post solo agli utenti approvati:
https://help.instagram.com/448523408565555

Come bloccare una o più persone indesiderate:
https://help.instagram.com/426700567389543

Maggior informazioni per la tua sicurezza e privacy su Instagram al seguente link:
https://help.instagram.com/

Snapchat

cosa vedremo

siamo proprio sicuri di
conoscere bene Snapchat?

Sezione a cura di:

- Sylvio Verrecchia
- Stefano Ramacciotti, CISSP

Snapchat: cos'è?

https://www.snapchat.com/

Snapchat è un'app di messaggistica istantanea, molto diffusa tra i giovani, che diversamente dalle altre chat, fa sì che gli *snap*, ovvero le foto e video inviati, si autodistruggano qualche secondo dopo essere visualizzati (generalmente da 1 a 10 secondi), eccezione fatta per quelli archiviati nelle "Storie", che saranno visibili a tutti i vostri amici per 24 ore.

Questa particolarità sembra un modo apparentemente sicuro per inviare immagini riservate senza lasciare traccia e che il destinatario non possa avere la possibilità di conservarli o divulgarli. In realtà vi sono sistemi *"hack"* in grado di eludere queste sicurezze.

Snapchat: età minima

“Termini di utilizzo”: non è permesso utilizzare i servizi di WhatsApp da parte dei minori di 13 anni.

Pr ovviare al problema età è stata creata SnapKidz che è una versione "non social" della stessa applicazione che consente solo di fare foto e video ed editarli ma non condividerli nel web. Viene attivato dichiarando un’età inferiore a 13 anni.

Snapchat: privacy & security

Anche se la possibilità di catturare la schermata o *screenshot* dello *smartphone* o *tablet* è disabilitata, esistono vari modi di conservare le foto, tra cui il più semplice è quello di fotografare lo schermo con un altro dispositivo.

Altro pericolo per la nostra privacy è la funzione “riproduzioni” che permette di visualizzare uno *snap* più volte prima che questo venga cancellato. Le riproduzioni non sono illimitate ma devono essere acquistate nello *store*. Per cui qualcuno potrebbe visualizzarle nuovamente.

Occorre configurare correttamente le impostazioni di Snapchat relative alla privacy decidendo chi può inviare *snap* ai propri figli (selezionando l'icona di accesso alle impostazioni posta nell'angolo superiore sinistro della pagina dei “*Feed*”, e modificando le impostazioni per consentire la ricezione di messaggi solo dagli amici), oppure chi può visualizzarne la loro storia e gestire gli utenti bloccati.

Snapchat: how-to

Snapchat.

Come impostare la propria privacy rendendo visibile i propri post solo agli utenti approvati:
https://support.snapchat.com/it-IT/a/privacy-settings

Come bloccare una o più persone indesiderate:
https://support.snapchat.com/it-IT/a/block-friends

Maggior informazioni per la tua sicurezza e privacy su Snapchat al seguente link:
https://www.snapchat.com/l/it-it/safety

Twitter

cosa vedremo

siamo proprio sicuri di
conoscere bene Twitter?

Sezione a cura di:

- Luigi Cristiani
- Stefano Ramacciotti, CISSP

Twitter: cos'è?

https://twitter.com/

Twitter è un social network di livello globale che consente alle persone e alle organizzazioni di condividere pubblicamente brevi messaggi informativi istantanei di 140 caratteri chiamati "*Tweet*" (cinguettio).

È un modo semplice per ottenere le ultime notizie su argomenti che interessano.

Quello che uno dice su Twitter può essere visto istantaneamente in tutto il mondo perché la maggior parte della comunicazione che ha luogo su Twitter è visibile a tutti. Dal momento che le informazioni postate sono pubbliche, possono essere "ritwittate" (o "ripostate") da chiunque le veda. Sebbene i Tweet possano essere protetti in modo da essere visibili solo ai *follower* approvati, la maggioranza degli utenti condivide i propri Tweet con il mondo intero.

Twitter: età minima

"Termini di utilizzo": non dovrebbe essere permesso utilizzare i servizi di Twitter da parte dei minori di 13 anni.

LA COSA NON È PERÒ CHIARA E SUI TERMINI DI UTILIZZO NON È SPECIFICATO

Twitter: privacy & security

Dal sito ufficiale: *"Indipendentemente dal Paese in cui vivi, ci autorizzi ad usare i tuoi dati e conseguentemente a trasferirli e immagazzinarli, negli Stati Uniti, in Irlanda e in qualsiasi altro Paese in cui operiamo. Le leggi sulla privacy e sulla protezione dei dati personali in alcuni dei suddetti Paesi possono differire da quelle del Paese in cui vivi."*.

Chi può vedere i miei Tweet?

- I Tweet pubblici (impostazione predefinita) sono visibili da chiunque, anche da coloro che non hanno un account Twitter.
- I Tweet protetti sono visibili solo dai *follower* di Twitter.

Per ulteriori informazioni sui Tweet pubblici e protetti: https://support.twitter.com/articles/282460#

Per sapere come si applica la protezione dei Tweet vedi: https://support.twitter.com/articles/20170038#

Twitter: privacy & security

E se qualcuno pubblica informazioni private su di te (numeri di telefono, gli indirizzi o le carte di credito) e desideri eliminarle? https://support.twitter.com/articles/20170302#

Se qualcuno si accanisce contro di te, tenta di litigare con te o semplicemente non smette di infastidirti, esistono due modi per risolvere il problema: “Togli la voce” e “Blocca”.

- Per sapere come si “toglie la voce” ad un account (togli voce ti consente di rimuovere dalla cronologia i Tweet di un account senza smettere di seguirlo o bloccarlo): https://support.twitter.com/articles/20171595#
- Per sapere come si blocca un account (per impedire a determinati account di contattarti, vedere i tuoi Tweet e seguirti): https://support.twitter.com/articles/255415#

Per segnalare abusi: https://support.twitter.com/articles/20170298#

Twitter: how-to

Twitter.

Infine:

Suggerimenti per le famiglie:
https://about.twitter.com/it/safety/families

Suggerimenti per gli insegnanti:
https://about.twitter.com/it/safety/educators

Suggerimenti per gli adolescenti:
https://about.twitter.com/it/safety/teens

WhatsApp

cosa vedremo

siamo proprio sicuri di
conoscere bene WhatsApp?

Sezione a cura di:

- Sylvio Verrecchia
- Stefano Ramacciotti, CISSP

WhatsApp: cos'è?

https://www.whatsapp.com/

WhatsApp è un'applicazione nata per uno scambio di messaggi istantanei, tecnicamente parlando è un sistema di *Instant Messaging*, con il quale inviare messaggi, immagini e video ai propri contatti. Inizialmente utilizzabile solo su dispositivi mobili, cioè per *smartphone* e *tablet*, ora è utilizzabile anche sul proprio computer via *browser web* o come applicazione da installare.

Con WhatsApp è possibile chattare e chiamare gli amici in tutto il mondo senza apparenti costi aggiuntivi in quanto l'applicazione utilizza la connessione dati del telefonino 2G/3G/4G (il consumo è relativamente modesto se non si scambiano file di grandi dimensioni come sono ad esempio molti video) oppure la Wi-Fi (se uno ha una connessione senza limiti come quelle che in genere sono diffuse nelle abitazioni).

WhatsApp: età minima

"Termini di utilizzo": non è permesso utilizzare i servizi di WhatsApp da parte dei minori di 16 anni.

Regola ampiamente disattesa ma che andrebbe valutata quando i ragazzi chiedono di poter installare WhatsApp.

Ciò anche considerando che la stessa Facebook che ha acquisito WhatsApp nel 2014 per 19 miliardi di dollari, reputa il sistema ben più pericoloso di Facebook stessa che è vietata solo ai minori di 13 anni.

Età minima:

WhatsApp: privacy & security

Innanzitutto conviene sapere che al primo accesso viene trasferita tutta la propria rubrica ai server di WhatsApp per la verifica di chi fra essi appartiene già alla rete WhatsApp. E' evidente che questo rappresenta una violazione non tanto della nostra privacy ma della privacy dei nostri contatti che ancora non sono su WhatsApp. Questo in passato ha anche comportato non pochi problemi legali all'azienda con la denuncia di garanti della privacy di vari Paesi.
Ci sono regole anche sui contenuti: immagini e post non devono violare la privacy o veicolare razzismo e violenza (cyberbullismo).
A tal fine è meglio non mettere la propria foto nel profilo in modo da non attirare l'attenzione di malintenzionati.
Per impostazione predefinita, nessun contatto è bloccato, quindi tutti gli utenti possono vedere le conferme di ricezione e di lettura, l'ultimo accesso, l'immagine del profilo e lo stato. Per ogni informazione si può decidere quali utenti WhatsApp possono visualizzarla.

WhatsApp: how-to

WhatsApp.

Per avere informazioni sempre aggiornate:

iPhone:
https://www.whatsapp.com/faq/it/iphone/28041111

Smartphone Android:
https://www.whatsapp.com/faq/it/android/23225461

Sicurezza e Privacy su WhatsApp:
https://www.whatsapp.com/security/

cyber bullismo

cosa vedremo

cyberbullismo, cos'è e come affrontare una delle piaghe del nostro tempo

Sezione a cura di:

- Stefano Ramacciotti, CISSP

bullismo e cyberbullismo

Bullismo:

“Uno studente è oggetto di azioni di bullismo, ovvero è prevaricato o vittimizzato, quando viene esposto ripetutamente nel corso del tempo alle azioni offensive messe in atto da parte di uno o più compagni.” (Olweus, 1993 trad..it. pag. 11-12) (Menesini, 2004)

Cyberbullismo:

"Azione aggressiva e intenzionale, messa in atto da un individuo o da un gruppo di persone, utilizzando mezzi elettronici, nei confronti di una persona che non può difendersi facilmente" (Smith e collaboratori, 2008)

Due lati di una stessa moneta, ma con differenze precise e diverse tipologie di attori.

cyberbullismo: reato contro la persona

Molto spesso si identifica il cyberbullismo solo con azioni denigratorie e violente, ma è molto di più, ad es.:

- Battaglie verbali con utilizzo di messaggi elettronici violenti che utilizzano un linguaggio rabbioso e volgare ***(flaming)***
- Spedizione ripetuta di messaggi offensivi, insultanti, disturbanti che vengono inviati tramite SMS, chat, MMS, telefonate sgradite ***[molestie (harassment)]***
- Quando l'*harassment* diviene particolarmente insistente ed intimidatorio e le molestie includono minacce per cui la vittima comincia a temere per la propria sicurezza fisica, il comportamento offensivo assume la denominazione di cyber-persecuzione ***(cyberstalking)***
- Sparlare di qualcuno online. Diffusione di pettegolezzi e/o altro materiale offensivo con l'intento di danneggiare gratuitamente e con cattiveria la sua reputazione e/o le amicizie di un coetaneo ***[diffamazione (denigration)]***
- Farsi passare per un'altra persona per spedire messaggi o pubblicare materiale allo scopo di mettere in difficoltà o in pericolo una persona o per danneggiare la sua reputazione o le sue amicizie *[sostituzione di persona* ***(impersonation)]***
- Il cyberbullo dopo aver salvato le confidenze spontanee di un coetaneo o immagini riservate e intime decide, in un secondo momento , di pubblicarle online ***[rivelazioni (outing)]***
- Ingannare qualcuno per ottenere segreti o informazioni imbarazzanti, per poi pubblicarle online ***[inganno: (trickery)]***
- Escludere deliberatamente e crudelmente una persona da un gruppo online ***[esclusione (exclusion)]***

bullismo Vs. cyberbullismo

Differenza fondamentale tra bullismo e cyberbullismo:

Nonostante il cyberbullismo presenti elementi di continuità rispetto al bullismo tradizionale, esso mostra altrettanti elementi di novità che caratterizzano in maniera specifica il fenomeno e che derivano propriamente dalle modalità interattive mediate dalle nuove tecnologie.

Una delle differenze fondamentali, tra bullismo e cyberbullismo, è la connotazione che assume nel contesto online un elemento peculiare per la definizione di "bullismo": ***lo squilibrio di potere*** esistente tra il bullo e la vittima.

Se "faccia a faccia" il bullo solitamente è più forte in termini fisici, psicologici e/o sociali, online questo non è così necessario e il potere del cyberbullo potrà essere determinato dall'impossibilità della vittima di difendersi perché ad esempio con minori capacità informatiche, perché non sa chi è il suo persecutore e perché online tutto viene diffuso coinvolgendo un vasto pubblico e spesso si vive l'incapacità di rimuovere i contenuti dopo che questi sono stati condivisi online.

Altro elemento peculiare del cyberbullismo è la distanza tra bullo e vittima, lo schermo del PC o dello *smartphone* rappresenta una barriera che deumanizza la vittima, non fa vedere gli effetti immediati dell'azione e fa sentire meno colpevoli.

La lontananza e la supposta anonimità fa sentire il cyberbullo o la cyberbulla inattaccabile, con scarse possibilità di essere scoperto, denunciato e catturato.

Inoltre, si può sempre dire che: "Era uno solo uno scherzo!" e spesso avere così una sostanziale assoluzione sociale.

Due lati di una stessa moneta, ma con differenze precise e diverse tipologie di attori.

attori del cyberbullismo

Cyberbullo: l'aggressivo

Cybervittima ("bullizzato"): destinatario dei soprusi e delle cattiverie online dei compagni

Sostenitori del cyberbullo: -spettatori attivi- partecipano all'atto di bullismo, ad esempio condividendo immagini, video, unendosi agli insulti postati dal cyberbullo, cliccando mi piace, incitandolo

Spettatori (bystander): -spettatori passivi- osservano, sono a conoscenza di ciò che avviene, ma non intervengono

Difensori della vittima: coloro che cercano di interrompere l'azione aggressiva, ad esempio segnalando il contenuto offensivo, scrivendo di rimuovere il contenuto e/o dando sostegno emotivo alla vittima

Quante sono le persone coinvolti dai cyberbulli?

comprimario: il/la cyberbullo/a

Può sembrare strano ma le statistiche parlano chiaro. Il fenomeno è -poco- più diffuso tra le ragazze (52%) che non tra i ragazzi, ma vediamo chi sono i cyberbulli:

- il cyberbulli talvolta sono ragazzi/e insicuri/e e con una bassa autostima (e infatti si nascondono dietro a un monitor e tendono a rimanere nell'anonimato), ed hanno bisogno di prevaricare gli altri per affermare la loro forza. Talvolta, però, possono anche uscire allo scoperto se si sentono protetti dal "gruppo", che potremmo anche chiamare "branco";
- anche se si rivolgono a un gruppo di spettatori non ne fanno mai parte integrante, dato che incutono timore.

Cyberbulli.

attore principale: la cybervittima

Cybervittima («Bullizzato/a»):

- è il ragazzo o la ragazza che spesso per sue caratteristiche personali si trova in una condizione di vulnerabilità, di fragilità e si sente indifeso e solo (talvolta in conseguenza proprio degli attacchi subiti dai compagni);
- questa sensazione di impotenza e di vergogna le rende praticamente impossibile difendersi e spesso non le consente nemmeno di denunciare gli abusi e le vessazioni.

Cybervitima.

attori «quasi» secondari: spettatori

Sostenitori del cyberbullo -spettatori attivi- (complici):

- possono conoscere direttamente la vittima anche se non necessariamente sono suoi amici
- possono temere anch'essi il bullo, fisicamente e/o socialmente, possono avere paura di ritorsioni e/o di diventare la sua futura vittima;
- a volte possono anche incolpare la vittima di avere provocato la situazione e di meritarsi ciò che gli sta accadendo;

Spettatori (bystander) -spettatori passivi-:

La loro indifferenza li rende responsabili come il bullo stesso e come i suoi diretti sostenitori, essi infatti non intervengono, mentre in realtà hanno la possibilità di fare qualcosa di positivo, non solo per la vittima, e potrebbero far cessare le vessazioni da lei subite.

Bystanders: attori secondari ma non troppo.

cyberbullismo: come riconoscerlo

cyberbullismo:

- Mortificazione, timore di rimproveri, paura a reagire a causa di ritorsioni
- Sensi di colpa, calo dell'autostima, senso di vergogna
- Calo del rendimento scolastico (anche per la difficoltà di concentrazione) fino all'abbandono
- Difficoltà comportamentali (rifiuto di uscire, di andare a scuola, di incontrare gli amici, di fare sport, ansia, fobie, manie di persecuzione, depressione, Introversione, silenzio, rifiuto di confidarsi)
- Disturbi del sonno, dell'appetito, sintomi psicosomatici
- Tendenza all'autolesionismo
- In casi estremi, suicidio

Possibili conseguenze cyberbullismo.

come difendersi

Tra le diverse cose che si possono fare, occorre:

- **«fare gruppo»** e …farsi dare una mano prima che il problema diventi troppo grave. Può apparire difficoltoso ma è il momento di fare vedere di cosa uno è capace e non vergognarsi di cosa le persone potrebbero pensare. È importante che la vittima trovi degli alleati in grado di difenderla dai soprusi di bullo/a e compagni. Del gruppo possono fare parte anche adulti e un importante aiuto può arrivare dai docenti che sono spesso abituati a trattare casi simili. Ovviamente si devono prendere le opportune misure perché, soprattutto il ricorso ai docenti non si riveli un'azione sconsiderata se loro non hanno una opportuna preparazione o sensibilità

- **«farsi furbi»** usando l'arma importante che il cyberbullismo mette a disposizione per difendersi: a differenza del bullismo che può essere più facilmente nascosto, del cyberbullismo rimangono le tracce, quindi **salvare tutto** e in particolare:
  - conversazioni sui social (foto, whatsapp, ask, kik, snapchat)
  - email
  - SMS, lista chiamate

  Ma come fare?

Soprattutto: salvare sempre tutto!

Windows: come salvare una schermata

Windows:

- Premere Alt-Stamp
- Aprire Paint o app simile
- Copiare («crtl+v») l'immagine e salvarla

https://upload.wikimedia.org/wikipedia/commons/4/49/Dell_Inspiron_One_23_Touch_AIO_Desktop_PC.png

macOS: come salvare una schermata

macOS:

- Premere Comando (⌘)-Maiuscole-3
- Aprire Anteprima
- Copiare («cmd+v») l'immagine e salvarla

https://static.pexels.com/photos/1185/apple-desk-office-technology.jpg

iOS/Android: salvare una schermata

https://upload.wikimedia.org/wikipedia/commons/f/fa/IPhone_5.png

https://upload.wikimedia.org/wikipedia/commons/e/ee/Samsung_Galaxy_S_Duos_3_Black.png

iOS:

Premi Standby/Riattiva e Home contemporaneamente

—

Android:

Premi Power e Home contemporaneamente

cyberbullismo: aspetti legali

Ingiuria :

In una chat (in una discussione on line con Giorgio):
«Giorgio sei un ….!. Anna, ma vacci piano con le parole»

- **Ingiuria** (art. 594 C.P.) chi offende l'onore o il decoro di una persona presente. Alla stessa pena soggiace chi commette il fatto mediante comunicazione telegrafica o telefonica, o con scritti o disegni, diretti alla persona offesa. Pena prevista:
  - l'**ingiuria** prevede ora una sanzione pecuniaria civile fino a 8.000 €
  - l'**ingiuria aggravata** (attribuzione di un fatto determinato o dalla sua commissione in presenza di più persone) prevede ora una sanzione pecuniaria civile fino a 12.000 €.

Diffamazione :

Su Facebook o altro social network/blog/ecc.:
«Claudia è una …!»

- **Diffamazione** (art. 595 C.P.) chi offende l'altrui reputazione in assenza della persona offesa. Pena prevista fino a 3 anni di carcere.

La diffamazione è un reato (l'ingiuria è stata depenalizzata) ma quante volte certe azioni vengono commesse online senza pensarci?

cyberbullismo: aspetti legali

Minaccia :

Su Whatsapp (in uno scambio di accuse):
«Paolo, giuro che ti uccido!»

- **Minaccia** (art. 612 C.P.), quando si scrivono delle minacce non solo si è perseguibili a querela di parte ma, nei casi più gravi, anche d'ufficio. Pena prevista fino a 1 anno di carcere

Sostituzione di persona :

Profilo «fake» su Facebook o altro social network/blog/ecc.:

Sostituzione di persona (art. 494 C.P.) l'atto di impersonare qualcun altro e diffamarla o tramite il suo account offendere altri. Pena prevista fino a 1 anno di carcere

Anche minacce e sostituzione di persona sono reati molto comuni online.

cyberbullismo: aspetti legali

Cyberstalking :

Persecuzione online di una persona.

- **Cyberstalking** (art. 612 bis C.P.), quando si minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura (casi gravi di cyberbullismo). Pena prevista fino a 4 anni di carcere e l'arresto immediato nel caso che il delinquente non si attenga alle misure restrittive previste (ad esempio se avvicina la vittima dopo avere ricevuto l'ingiunzione a rimanerle a non meno di una certa distanza)

Cyberstalking, uno tra i reati più odiosi.

grazie

Progetto:

- Stefano RAMACCIOTTI (CISSP)
  stefano.ramacciotti@isc2chapter-italy.it

Contributi:

- Luigi CRISTIANI
- Sylvio VERRECCHIA

Revisione:

- Ersilia MENESINI e Giovanna TAMBASCO (UNIFI)
- Giuseppe VACIAGO (UNINSUBRIA)