ORDINE
DEI GIORNALISTI
D'ABRUZZO

La riservatezza, la sicurezza e l'anonimato delle fonti sul web

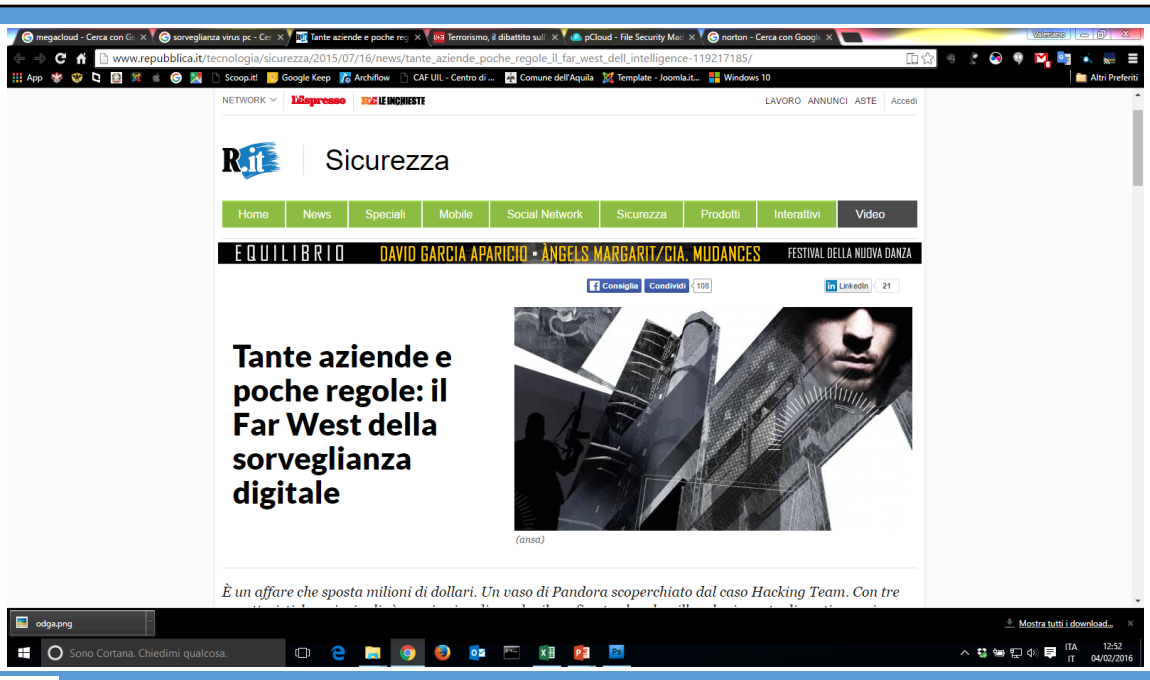
Teramo, 15 febbraio 2016

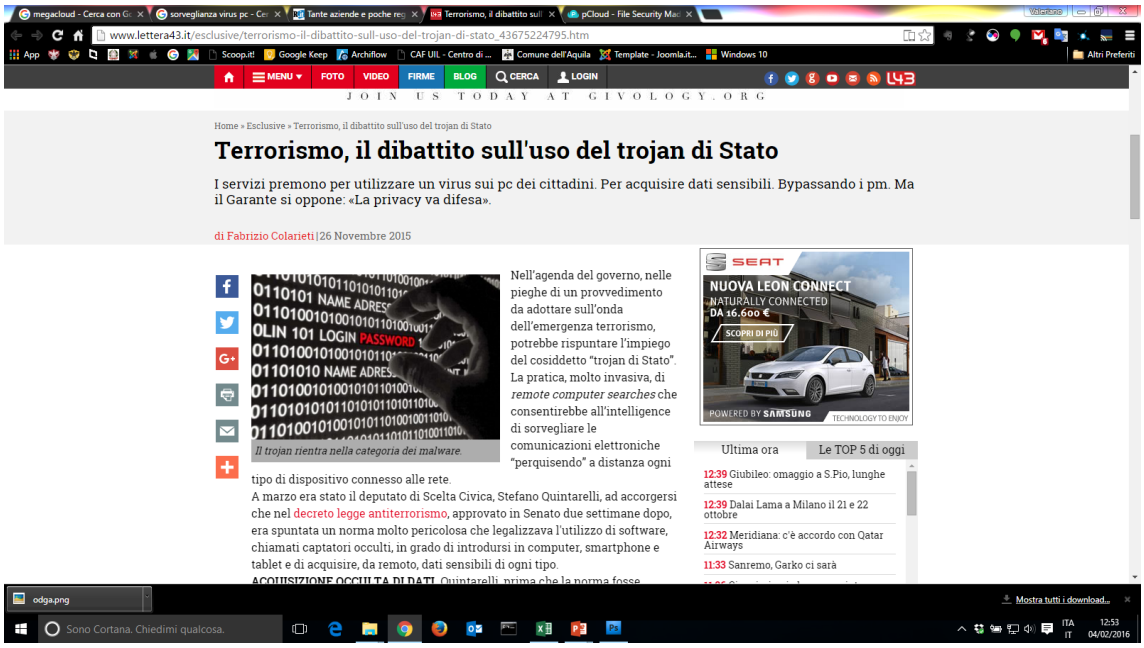
Valeriano Salve

Gli argomenti di oggi

- La privacy durante la navigazione
- La sicurezza dei dispositivi utilizzati (PC, tablet e smartphone)
- Manuale di autodifesa
- Consigli finali


www.ilsole24ore.com/art/notizie/2013-07-11/servizi-segreti-russi-tornano-115340.shtml?uuid=AbQeGJDI
ITALIA & MONDO
I servizi segreti russi tornano alle macchine da scrivere: «Più sicure dei computer»
di Antonella Scott 11 luglio 2013 Commenta
IN QUESTO ARTICOLO
I servizi segreti russi, che di sicurezza se ne intendono, hanno imparato la lezione: in tema di informazioni riservate, mai più fidarsi dei computer. Li hanno convinti le rivelazioni di Edward Snowden sulle possibilità di controllo che le nuove tecnologie hanno regalato agli Stati Uniti, poi l'annuncio online - rivelatosi un falso - delle dimissioni di Vladimir Yakunin, il capo delle Ferrovie di Stato, o le presunte incursioni dei servizi britannici nella posta elettronica dei
CONTATTA UN FAMILY BANKER
SCOPRI TUTTA LA NOSTRA OFFERTA MUTUI


www.repubblica.it/tecnologia/sicurezza/2015/07/16/news/tante_aziende_poche_regole_il_far_west_dell_intelligence-119217185/
Sicurezza
Tante aziende e poche regole: il Far West della sorveglianza digitale
(ansa)
È un affare che sposta milioni di dollari. Un vaso di Pandora scoperchiato dal caso Hacking Team. Con tre



E' possibile nascondersi in rete?

La struttura della rete è fatta in modo che tutti i dispositivi ad essa collegati siano identificabili.

Senza l'individuazione del dispositivo collegato la rete non potrebbe funzionare.

Per non essere tracciati o identificati abbiamo bisogno di ricorrere a strumenti appositi (software o hardware).

ORDINE DEI GIORNALISTI D'ABRUZZO

Identificazione dei dispositivi

- Ogni dispositivo connesso alla rete viene identificato tramite un numero detto "IP number" che può essere assegnato ad un solo dispositivo ogni volta. Uno stesso numero IP può anche essere assegnato a due dispositivi, ma MAI nello stesso momento. Un tipico indirizzo IP potrebbe essere 148.25.172.15

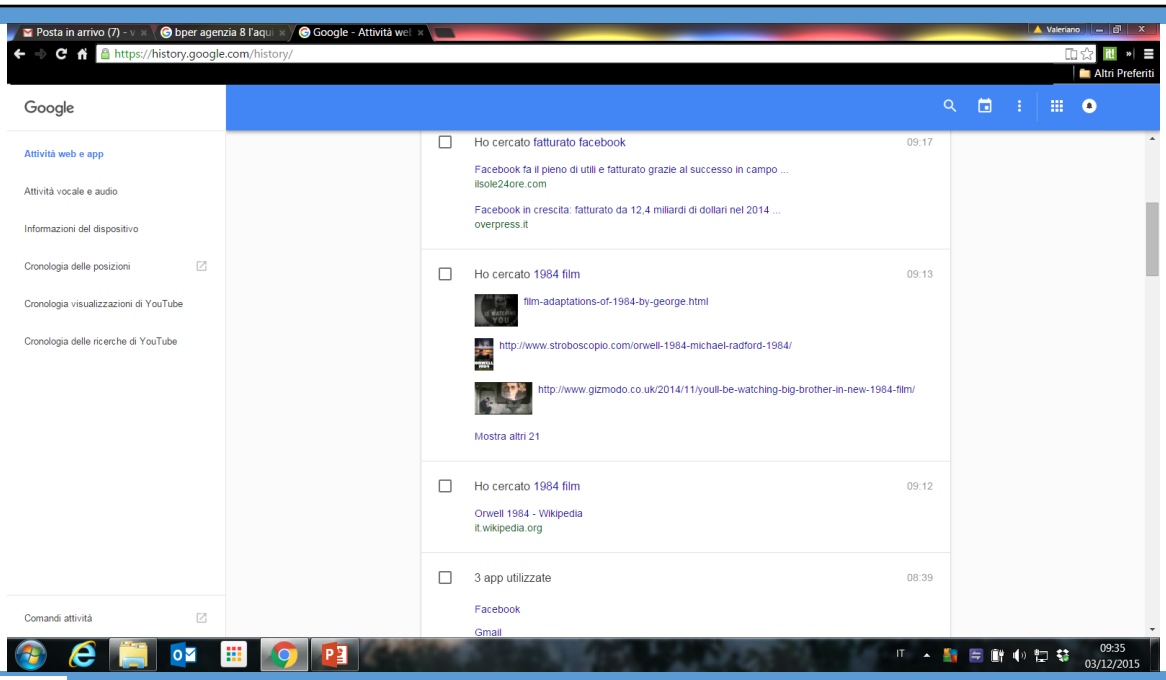
- Ogni scheda di rete (wireless, via cavo, o rete cellulare) dispone a sua volta di un identificativo, detto MAC Address, che è UNIVOCO ed è assegnato alla scheda di rete per sempre. Un esempio di indirizzo MAC address potrebbe essere: c8:f4:0B:d8:cb:d4

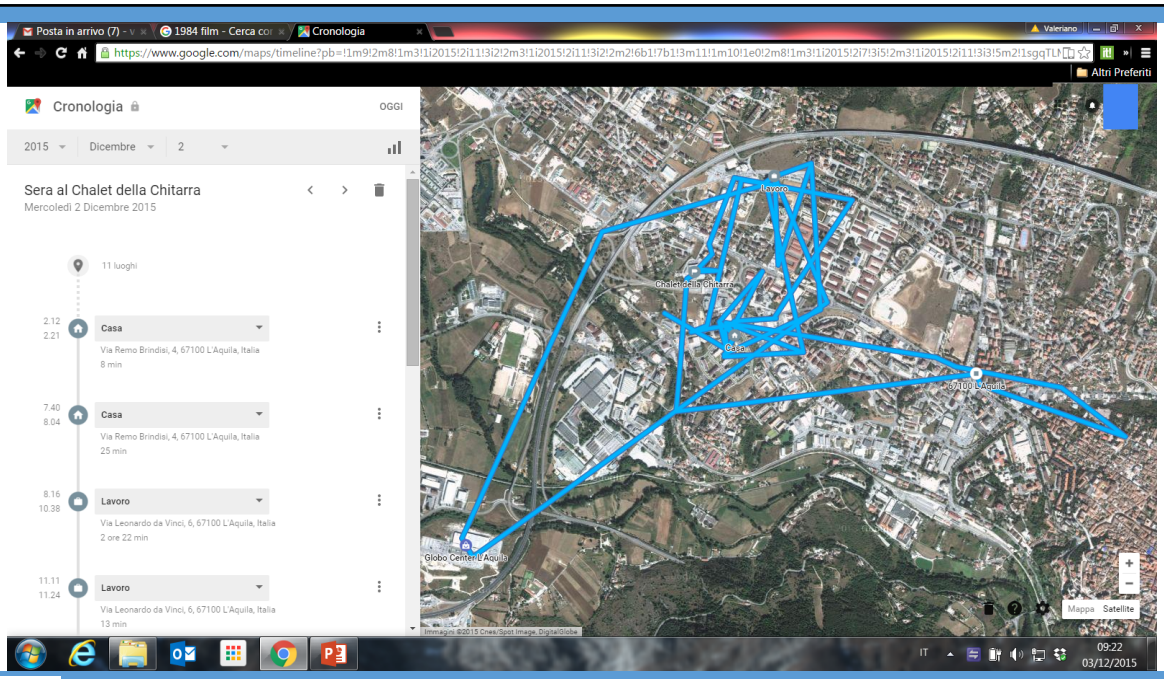
Coockie

- I cookie sono file memorizzati sui computer utilizzati per navigare in rete e utilizzati dai server per avere informazioni dal browser allo scopo di erogare servizi personalizzati per gli utenti (ad es.: meccanismi di autenticazione dell'utente, modalità di visualizzazione sul browser, carrello degli acquisti, sapere se si è già stati a visitare un sito, ecc…);
- Ne esistono di vari tipi:
  - cookie tecnici
  - cookie statistici o "analytics"
  - cookie per la memorizzazione delle preferenze
  - cookie pubblicitari
  - cookie di social network

Cosa conosce di noi Google?

- Le ricerche fatte
- Le pagine visitate
- I luoghi in cui siamo stati
- La nostra posta
- La nostra agenda
- I comandi vocali che abbiamo dato su Google Now
- Se utilizziamo uno smartphone o un tablet con Android Google sa quasi tutto quello che abbiamo fatto sul nostro dispositivo
- Se si dispone di un account gmail è possibile controllare parte di questi dati all'indirizzo: https://history.google.com

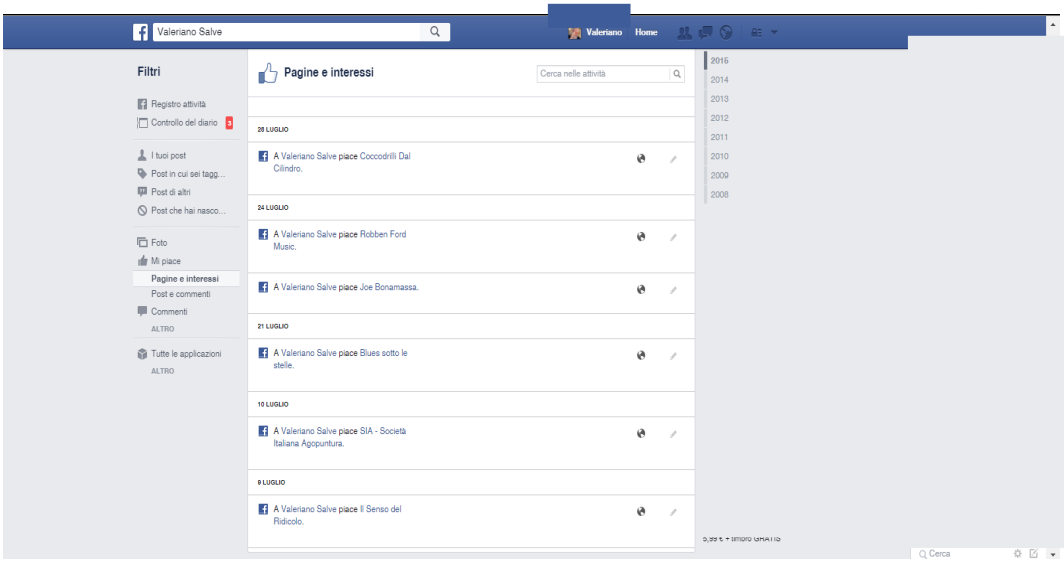




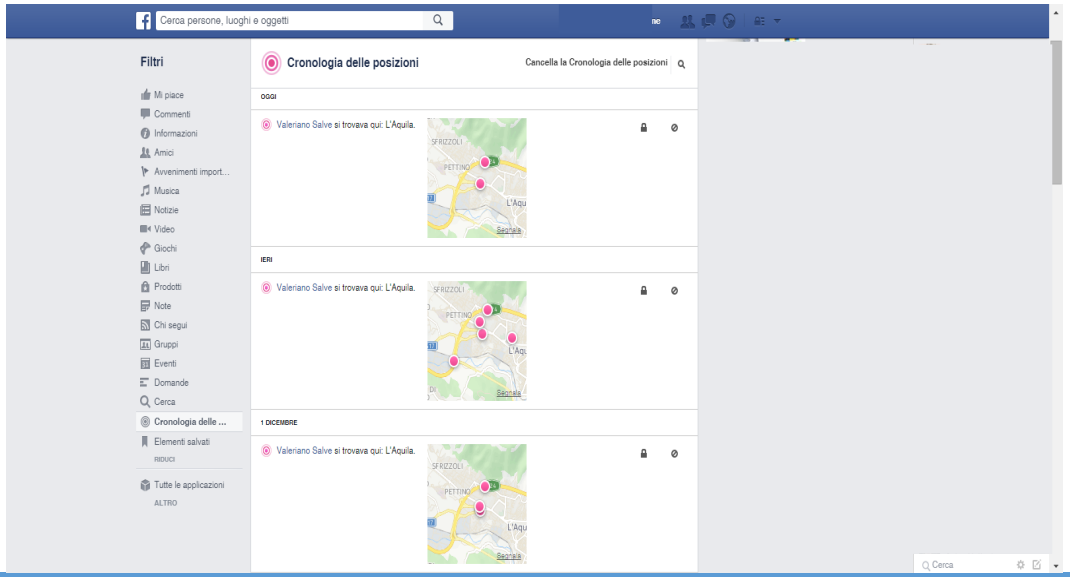
Cosa conosce di noi Facebook?

- Le tue preferenze in fatto di scelte sociali, politiche, religiose, sessuali…
- I tuoi amici
- I tuoi gusti culturali (cinema, libri, musica, ecc…)
- Dove ti trovi
- Come ti informi
- I gusti e le scelte dei tuoi amici
- …..

Facebook sa cosa ci piace



Facebook sa dove siamo stati



Facebook ti conosce meglio di chiunque altro?

- I ricercatori delle Università di Cambridge e di Stanford avrebbero dimostrato che tramite i «mi piace» Facebook ci conosce meglio dei nostri colleghi, amici o parenti
- Lo studio è stato pubblicato sulla rivista Proceedings of National Academy of Sciences, è diffuso anche dal Telegraph
- Il Sistema non è ancora completamente affidabile, ma è sicuramente un assaggio delle potenzialità future

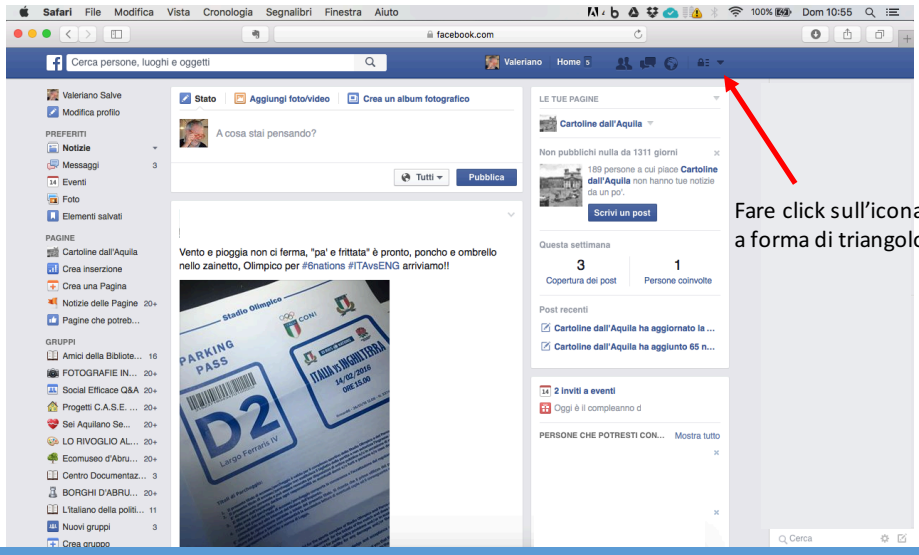
Vedi articolo su Wired: http://www.wired.it/internet/social-network/2015/01/13/facebook-like/
Vedi articolo su Repubblica: http://www.repubblica.it/tecnologia/social-network/2015/09/10/news/facebook_algoritmo_cosa_sa_di_noi-122531481

Facebook ci conosce bene

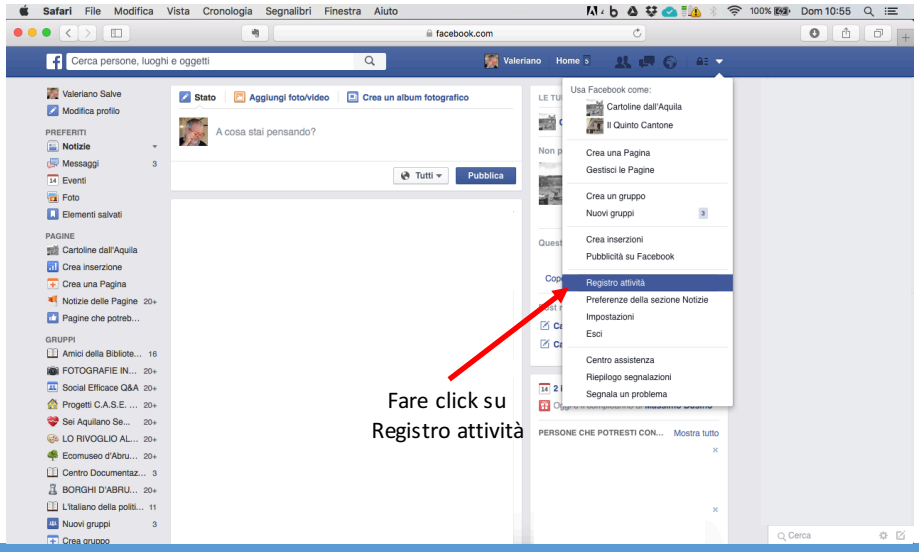
Secondo i risultati della ricerca il numero minimo di like necessari a Facebook per conoscere i nostri gusti e le nostre abitudini sono i seguenti:

- 10 like meglio di colleghi e conoscenti
- 70 like meglio di amici e coinquilini
- 150 like meglio di fratelli e parenti
- 300 like per «sfangarla» con coniugi e partner

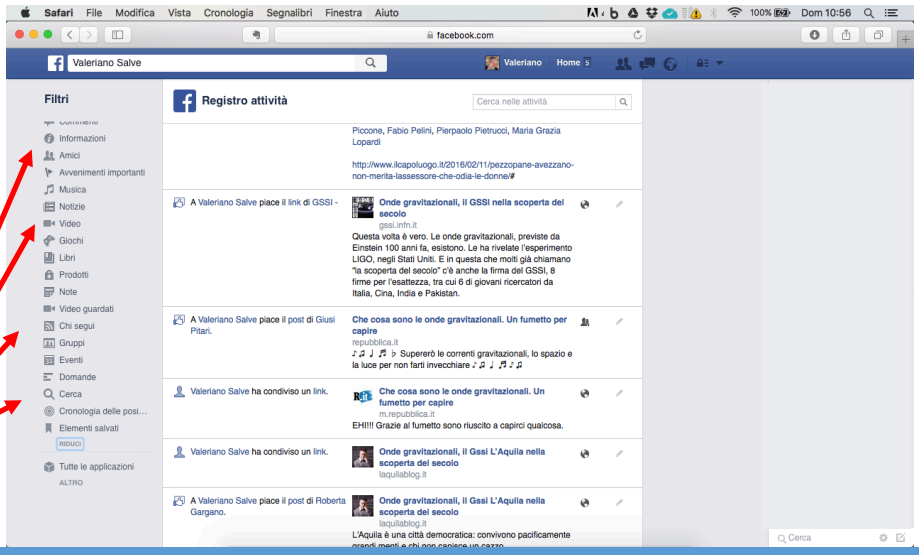
Controllare i nostri dati su Facebook



Controllare i nostri dati su Facebook



Controllare i nostri dati su Facebook



Accedere ai filtri

ORDINE DEI GIORNALISTI D'ABRUZZO

19

Come tanti Pollicino…

- Le tracce che lasciamo navigando sono migliaia;
- Oggi sono utilizzate soprattutto per vendere pubblicità verso un target individuato con precisione quasi chirurgica, ma non sappiamo cosa potrà succedere in futuro;
- Non possiamo delegare ad altri il controllo dei nostri dati e la legislazione, seppure molto stringente, non riesce a reagire alla velocità dei mutamenti tecnologici;

ORDINE DEI GIORNALISTI D'ABRUZZO

20

La nostra sicurezza, ma anche quella delle nostre fonti, dipende dalla sicurezza e dall'affidabilità dei dispositivi che utilizziamo.

Un malintenzionato potrebbe rendere impossibile il lavoro di un giornalista rendendogli inutilizzabile il personal computer. Come?

Ad esempio potrebbe essere sufficiente inviargli un virus tramite posta elettronica…

Proteggersi *dalla rete*

Negli ultimi anni, il maggiore dei pericoli per i dati è innescato dall'utilizzo dei servizi offerti dalla rete internet.

Sia la navigazione sul web che la posta elettronica possono diffondere programmi capaci di danneggiare o creare malfunzionamenti diversi ai sistemi informatici o rubare date ed informazioni.

Esistono varie tipologie di software maligni e anche le loro azioni dannose possono essere diverse, in funzione di una molteplicità di aspetti.

I VIRUS

Sono programmi (codice) che si diffondono copiandosi all'interno di altri programmi o in una particolare sezione delle memorie fisiche del personal computer, in modo da essere eseguiti ogni volta che il file infetto viene aperto;

Si trasmettono da un computer a un altro tramite lo spostamento di file infetti a opera degli utenti (soprattutto in presenza di reti).

BOMB

È un tipo di programma che consiste in una porzione di codice inserito in un programma "normale" generalmente utilizzato dall'operatore.

Una "bomba" è configurata per "esplodere" quando si verifichino determinate condizioni (per esempio, può attivarsi in concomitanza dell'esecuzione di determinati comandi o programmi oppure a una particolare ora o data ecc.).

Le azioni dannose sono riconducibili a modifiche, cancellazioni di file, blocchi di sistema ecc.

WORM

Sono software che si diffondono tramite modifiche effettuate sul sistema operativo utilizzato dal personal computer.

La diffusione del software avviene mediante un processo automatico di duplicazione, che si basa sull'utilizzo della rete (LAN o WAN).

Solitamente sfruttano i difetti (bug) di alcuni sistemi operativi e programmi specifici per diffondersi automaticamente.

TROJAN HORSE

E' un software che si annida all'interno di programmi "innocui" e che, al verificarsi di un determinato evento, attiva istruzioni dannose, che vengono eseguite all'insaputa dell'utilizzatore.

Non possiede funzioni di auto-replicazione e per diffondersi, quindi, deve essere consapevolmente inviato alla vittima.

BACKDOOR

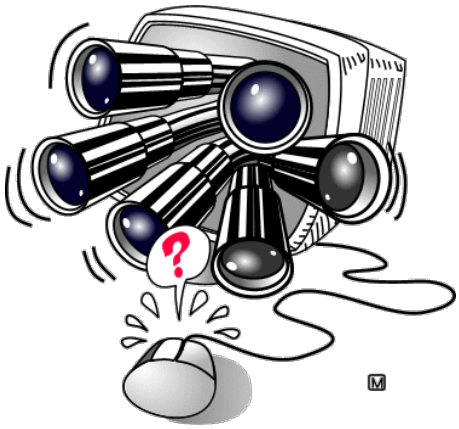
Sono programmi che consentono un accesso di tipo "non autorizzato" al sistema su cui sono in esecuzione.

Si diffondono sfruttando *bug* di sistema oppure si accompagnano a un *trojan horse* o a un *worm* oppure utilizzano un sistema di accesso di emergenza (di un sistema operativo) a un sistema informatico, che può essere utilizzato, per esempio, per consentire il recupero di una *password* dimenticata.

SPYWARE

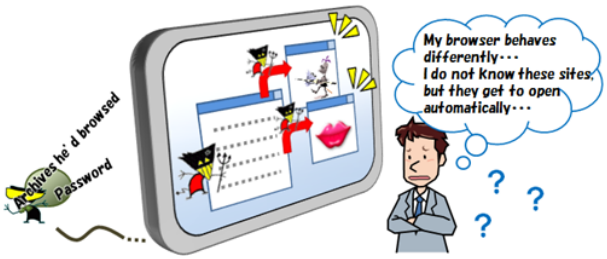
Sono software specifici che vengono utilizzati per la raccolta delle informazioni di un sistema solitamente collegato in rete.

Successivamente le informazioni raccolte vengono trasmesse a chi ha creato o immesso il virus: tali informazioni, così "catturate", possono essere di diverso tipo e possono essere utilizzate per scopi diversi (siti a cui ci si collega abitualmente, *password* per l'accesso a sistemi in rete, chiavi crittografiche dì un utente ecc.).



HIJACKER

Sono programmi che si impadroniscono delle funzionalità dei browser (i programmi per navigare in rete Explorer, Chrome, Firefox, Edge..) per causare l'apertura automatica di pagine web indesiderate.



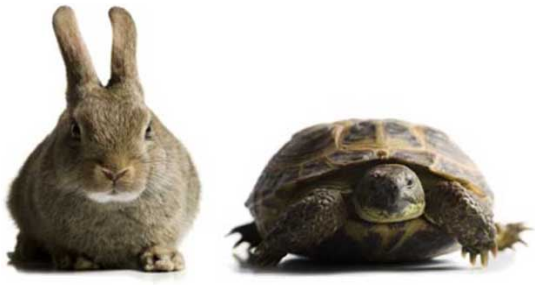
ROOTKIT

Sono composti da un *driver* e, solitamente, da copie modificate di programmi presenti nel computer.
Non sono particolarmente dannosi, ma possono nascondere, sia all'utente che a programmi *antivirus*, la presenza di particolari *file* o impostazioni del sistema.
Generalmente vengono utilizzati per mascherare *spyware* e *trojan.*

RABBIT

Sono programmi che basano la propria azione dannosa sull'esaurimento delle risorse del computer, creando copie di se stessi (in memoria o su disco) senza interruzione.

Solitamente generano la saturazione delle memorie di massa.



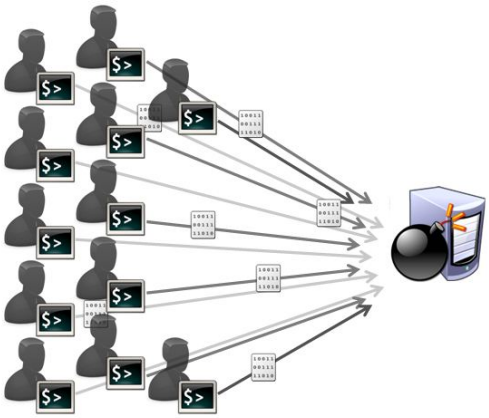
POSTA ELETTRONICA

Sono attacchi rivolti alla possibilità di accedere all'interno della rete di una organizzazione sfruttando i protocolli per la gestione delle posta elettronica (SMTP, POP3, IMAP4), che solitamente non prevedono misure per l'autenticazione affidabile integrate nel protocollo di base.

Proteggersi in rete: ATTACCHI INTRUSIVI E DI NEGAZIONE DI UN SERVIZIO

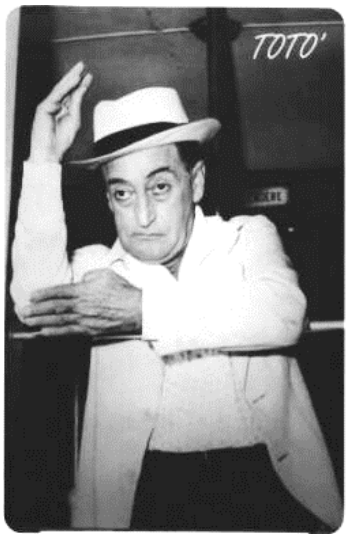
Sono tutte le metodologie "atte" a danneggiare un servizio offerto in rete (DOS, *denial of Service*), approfittando della vulnerabilità della rete stessa.

Esempi possono essere: saturazione delle risorse della rete, interruzione delle connessioni tra due computer, blocco delle comunicazioni tra i diversi servizi offerti, esclusione di un determinato utente dall'accesso a un servizio, interruzione dì servizi per un *client* o un sistema specifico ecc.



Proteggersi in rete: PHISHING

Corrisponde al tentativo degli *hacker* di indurre gli utenti di un sistema a rivelare (per imperizia, incuria o superficialità le credenziali dell'utente *(username* e *password*) o altre informazioni utili per l'accesso ad esempio, ad un conto corrente, ma anche dati di Facebook, Google o Amazon.
Sembra incredibile, ma secondo una ricerca della società produttrice dell'antivirus Kaspersky ogni giorno, nel mondo sono più di 100.000 le vittime della frodi.



Proteggersi in rete: SPAMMING

Lo ***spamming***, detto anche **fare spam** o **spammare**, è l'invio massivo di comunicazioni elettroniche indesiderate a fini commerciali. Può essere attuato attraverso qualunque sistema di comunicazione, ma il più usato è Internet, attraverso messaggi di posta elettronica, chat, tag board, forum, Facebook e altri servizi di rete sociale.

Cryptolocker e le sue varianti

Da qualche tempo si sta diffondendo il Cryptolocker. Un virus che cripta tutti i file presenti sul computer (Documenti Word, Excell, PDF, foto…) utilizzando una chiave RSA-2048 quasi inespugnabile.

Ci sono numerose varianti CryptoWall, CryptoLocker, CTB Locker, CryptorBit, KeyHolder, TELSA, Operation Global, TorrentLocker, CryptoDefense, ZeroLocker, che parteno tutte da Cryptoloker, ma che utilizzano chiavi sempre più complesse.

Ad oggi non esiste un modo per recuperare la chiave se non con tentativi "BruteForce", ma che sono fuori della portata degli utenti comuni.

Tra dicembre 2015 e gennaio 2016 la sua variante TELSA ha infettato decine di migliaia di macchine.

Come funziona il Cryptolocker

- Arriva tramite posta elettronica in forma di file .PDF o .ZIP e una volta avviato cripta tutti i file presenti sul computer e sui dispositivi ad esso collegati (Dischi di rete, chiavi USB, dischi esterni…)
- E' difficile riconoscerlo perchè può arrivare anche con la posta di mittenti che ci sono noti.
- Se si cancellano e-mail ed allegato non ci sono problemi.
- I malintenzionati generalmente chiedono denaro per inviare la chiave di decodifica, ma è raro che dopo aver pagato si risolva qalcosa.
- I metodi di pagamento sono difficilmente attuabili (Bitcoin o simili)
- Le uniche difese, ad oggi, sono backup costanti e attezione alle e-mail che si ricevono.

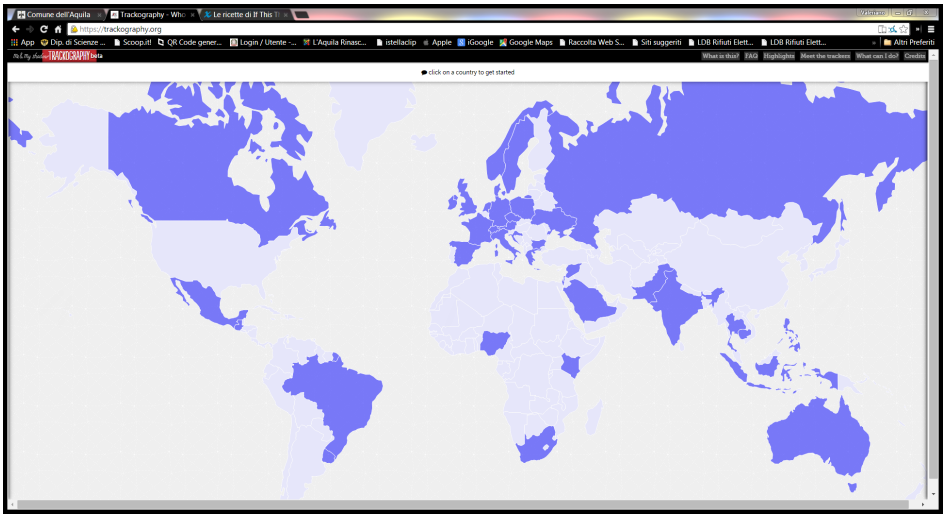
Importanza di un sistema aggiornato

A garanzia della nostra privacy e dell'integrità del nostro sistema oltre ad avere un buon antivirus è sempre necessario avere un sistema operativo aggiornato.

Molto spesso gli aggiornamenti dei sistemo operativi vengono sviluppati proprio per eliminare criticità ed aumentare la sicurezza e questo vale per PC, tablet e smartphone.

Manuale di autodifesa

Dove finiscono i nostri dati?



https://trackography.org/

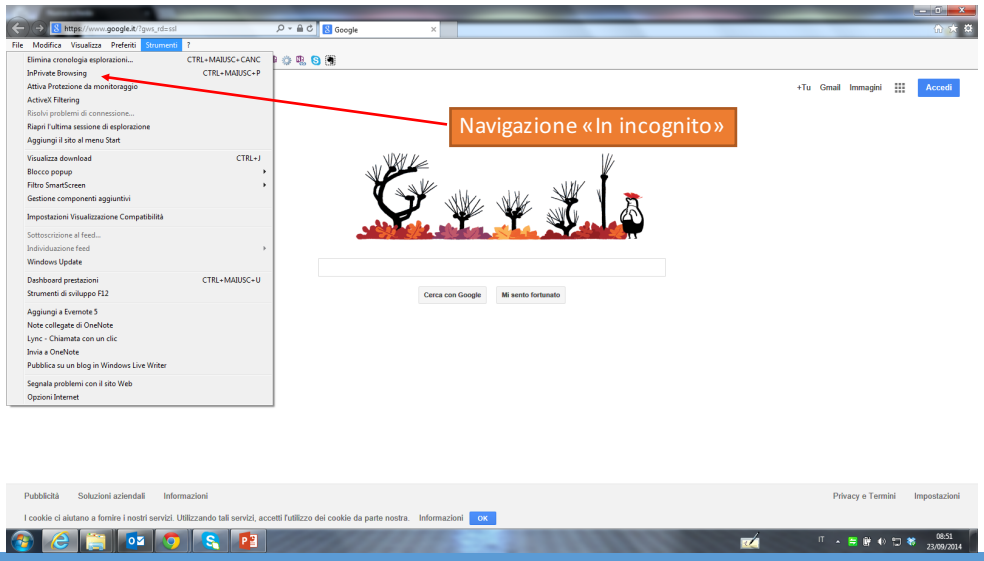
Mantenere un minimo di privacy

Al di la di voler giocare a fare l'hacker ci sono anche un minimo di regole da osservare per vedere tutelata la propria privacy quando occorre.

Tutti i browser più comuni mettono a disposizione strumenti che ci permettono di avere una garanzia «minima» quali la tutela dai coockies, il non mantenimento della cronologia dei siti visitati, l'impossibilità di memorizzare i dati che si inseriscono sui siti web (ad esempio nome utente e password)

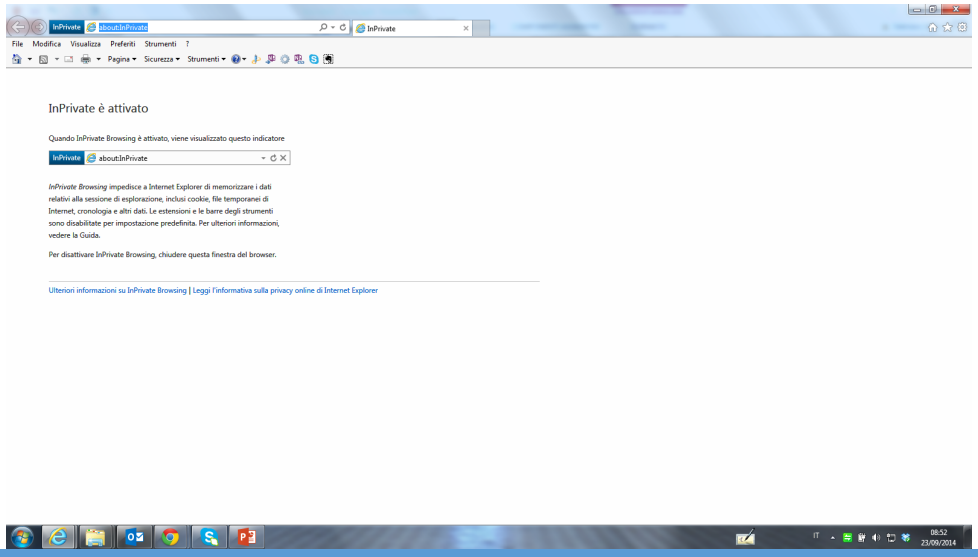
ORDINE DEI GIORNALISTI D'ABRUZZO

Navigazione in «incognito»: Internet Explorer

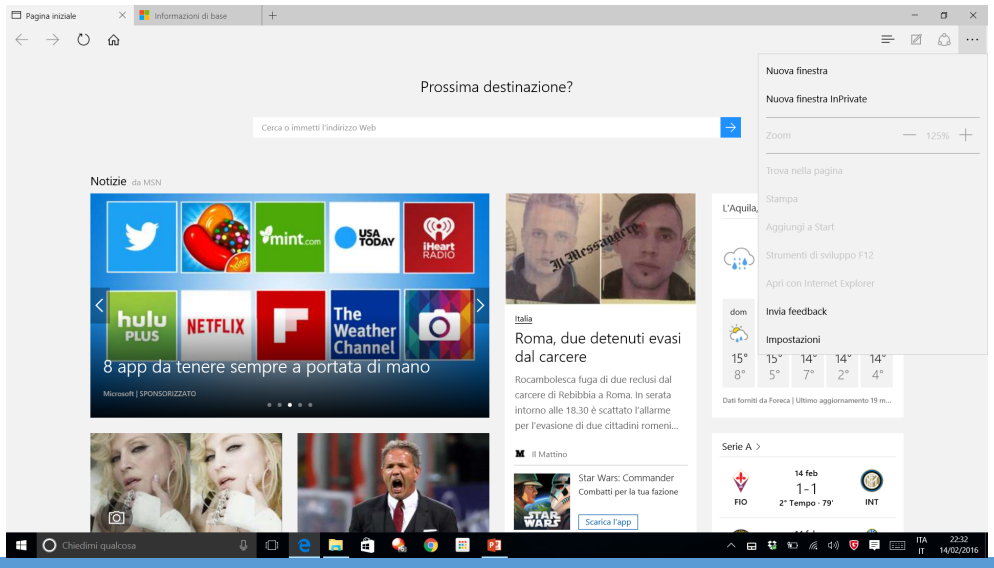


ORDINE DEI GIORNALISTI D'ABRUZZO

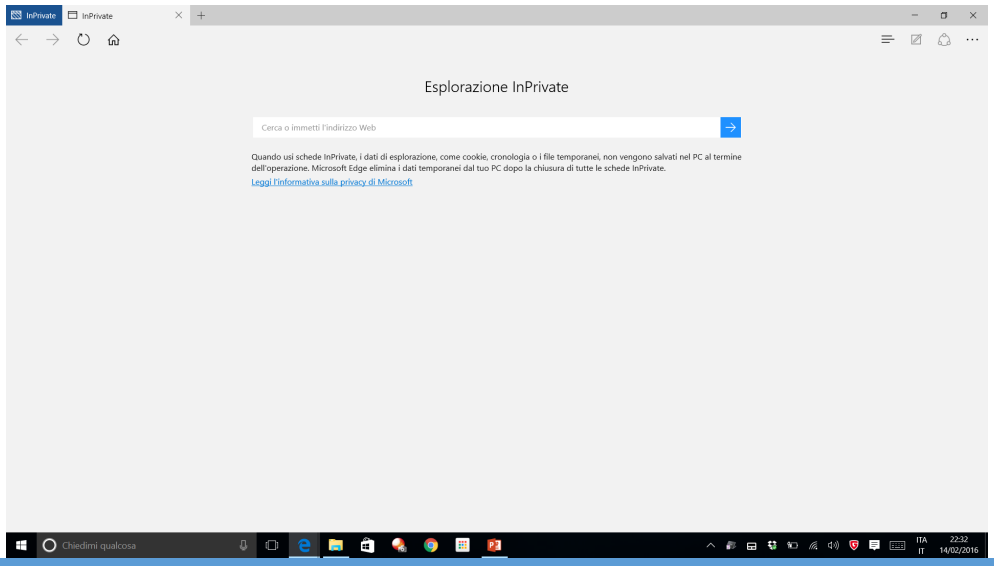
Navigazione in «incognito»: Internet Explorer



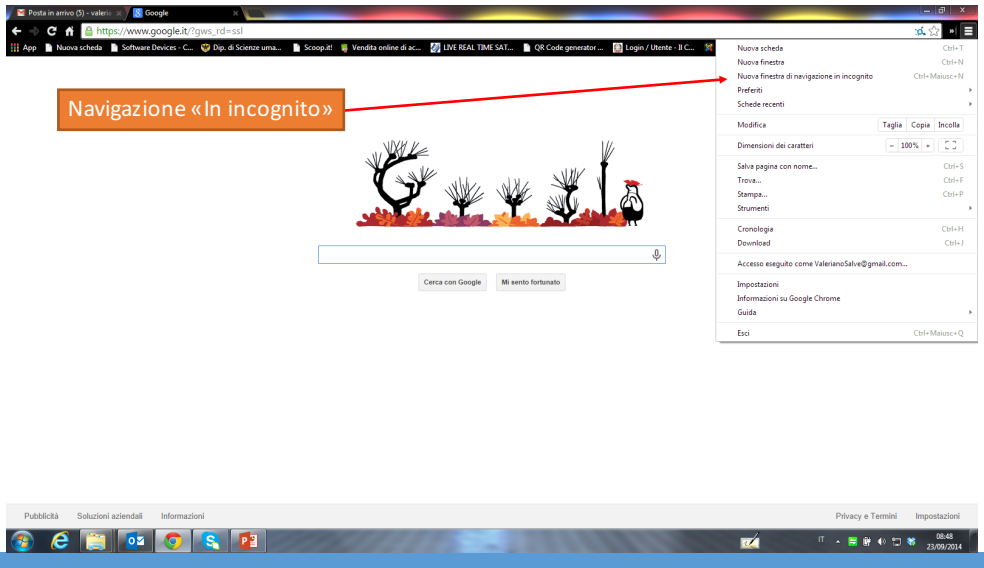
Navigazione in «incognito»: Microsoft EDGE



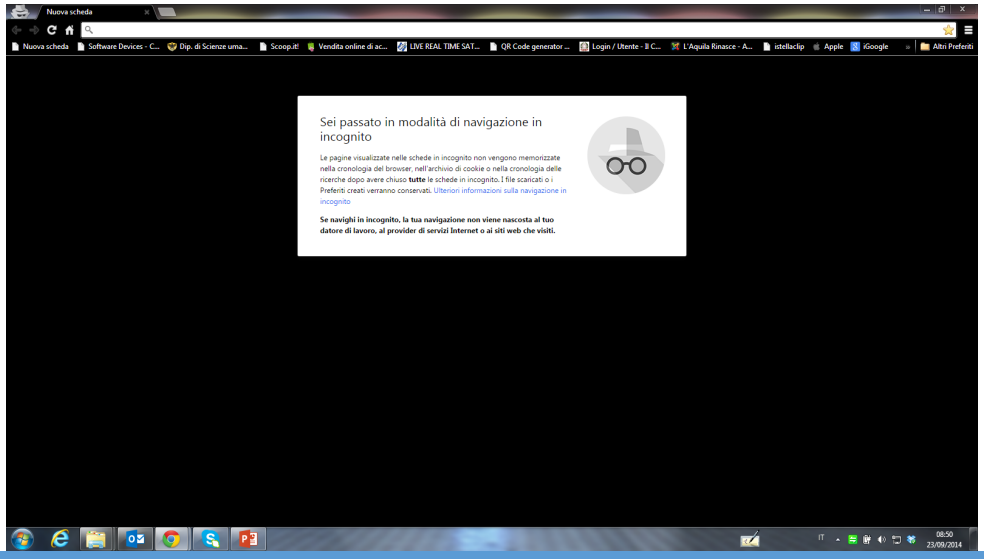
Navigazione in «incognito»: Microsoft EDGE



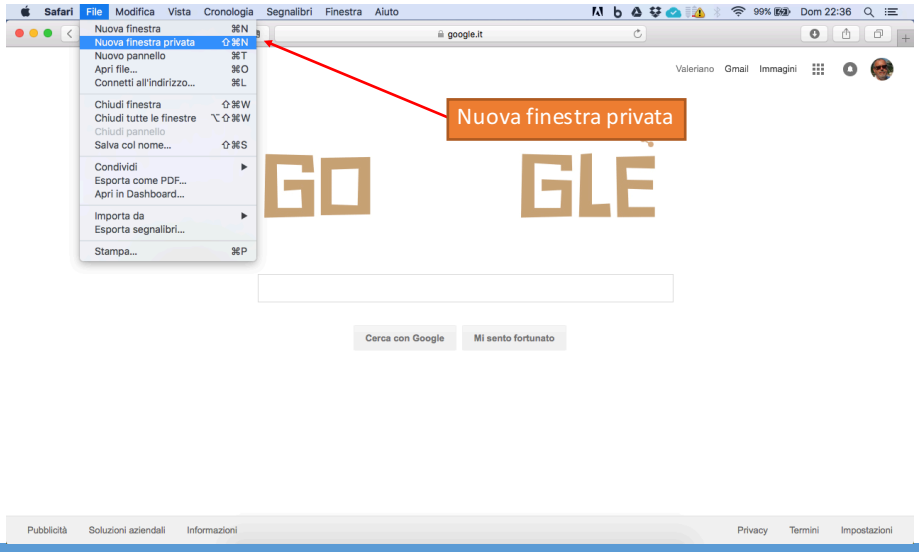
Navigazione in «incognito»: Chrome



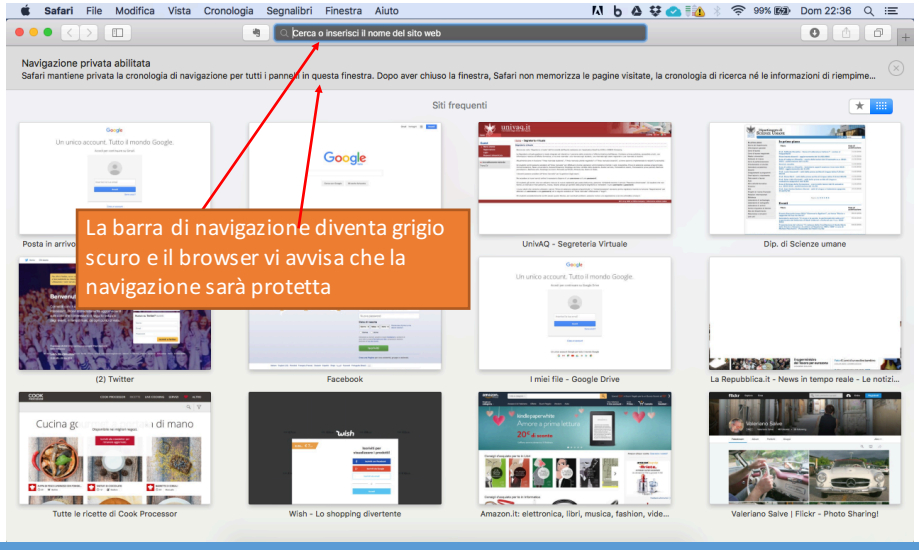
Navigazione in «incognito»: Chrome



Navigazione in «incognito»: Safari



Navigazione in «incognito»: Safari



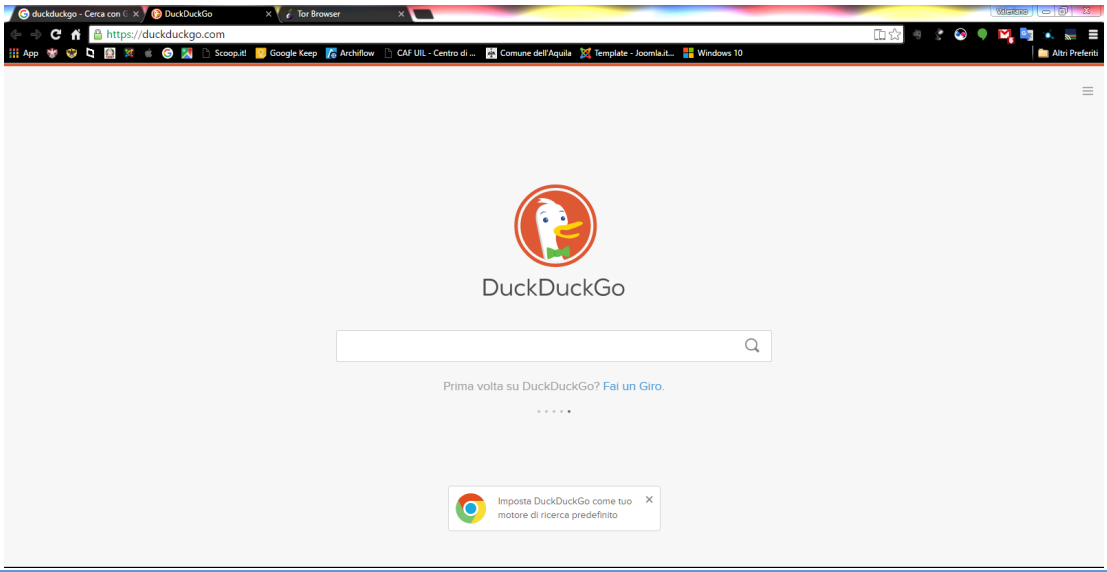
Ripulire i dati di navigazione

- Soprattutto se lavorate su computer e dispositivi condivisi con altri utenti sarebbe bene, quando necessario oppure dopo ogni utilizzo, ripulire il browser dai dati di navigazione e quindi:
- Cancellare i cookie
- Rimuovere la cronologia di navigazione
- Disabilitare il riempimento automatico
- Se si è fatto click su "SI" alla richiesta "Memorizza password" da parte del browser sarà opportuno cancellare anche i dati delle password

Altre misure minime per la sicurezza

- Se a casa avete una rete wi-fi accertatevi che il protocollo di cifratura sia almeno WPA2 (Wi-Fi Protected Access) e cambiate la password preimpostata con una personalizzata;
- Non utilizzate a casaccio le reti wi-fi libere e se lo fate siatene coscienti;
- Se fate transazioni on-line o fate viaggiare dati personali che non volete siano divulgati assicuratevi che il sito utilizzi il protocollo https (molti browser fanno vedere anche l'icona di un lucchetto)
- Non rivelate a nessuno e per nessun motivo le vostre password; se siete obbligati a fornirle ad un tecnico che vi cura la manutenzione ricordatevi di modificarla prima possibile;

DuckDuckGo: il motore che non ti traccia

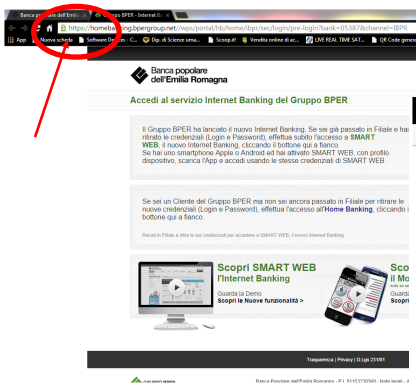


Proteggersi in rete: Scegliere una password

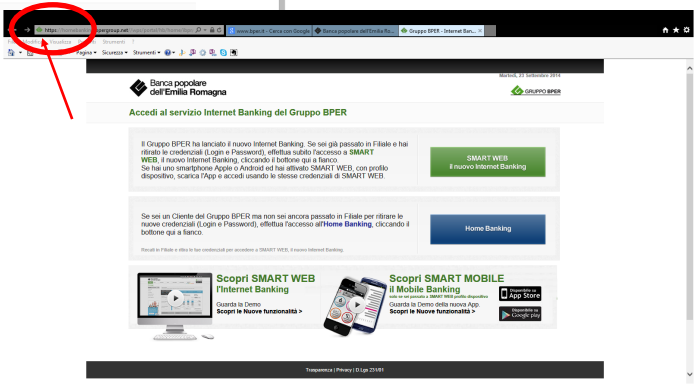
La normativa relativa alla privacy prevede che la password per l'accesso ai sistemi informatici abbia le seguenti caratteristiche:

- la lunghezza minima deve essere di otto caratteri
- deve contenere almeno un carattere numerico (0..9)
- deve contenere almeno un carattere alfabetico (a..z, a..Z)
- deve contenere almeno un carattere speciale tra i seguenti . (punto) ; (punto e virgola) $! @ - (meno)
- non devono essere ammessi caratteri diversi da quelli sopra elencati
- non devono essere ammessi spazi vuoti
- non devono essere ammessi più di due caratteri consecutivi uguali
- non deve essere uguale allo username
- non deve essere uguale ad una delle ultime quattro password utilizzate
- non può essere cambiata più di una volta nell'arco delle 24 ore

http o https?



Chrome



Internet Explorer

Come difendersi

- Crittografia
- Anonimato totale
- Cancellazione sicura dei file e distruzione dei supporti
- Ambiente (Sistema operativo ed applicazioni) anonimo
- Macchine virtuali
- Humanware

Crittografia

Scienza che studia gli algoritmi matematici idonei a trasformare **reversibilmente**, in funzione di una variabile detta **chiave**, il contenuto informativo di un documento o di un messaggio, in modo da nasconderne il significato.

Solo chi ha a disposizione la **chiave** sarà in grado di **decodificare** il messaggio e renderlo comprensibile.

Le prime forme di crittografia

Scitàla Lacedemonica

Messaggio = JULIS CAESAR
Cifratura M+K = MXOLXVFDHVDU

Codice di Cesare

Disco cifrante di Leon Battista Alberti

Macchina cifrante Enigma a quattro rotori

Crittografia

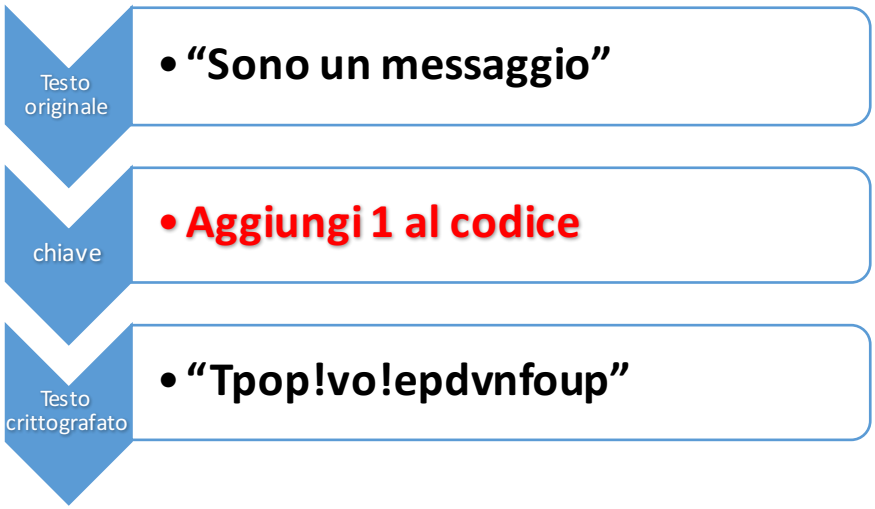
SIMMETRICA

ASIMMETRICA

Crittografia simmetrica: caratteristiche

- Unica chiave per codifica/decodifica
- Mittente e destinatario devono disporre di un canale "*sicuro*" con cui scambiarsi la chiave
- Chiave nota esclusivamente a mittente e destinatario (una chiave per ciascuna coppia di utenti)
- Per far comunicare n utenti tra di loro servono [n(n-1)/2] chiavi (es. 5 utenti e 10 chiavi; 100 utenti e 4.950 chiavi)
- Sostituzione delle chiavi solo se scoperte da terzi

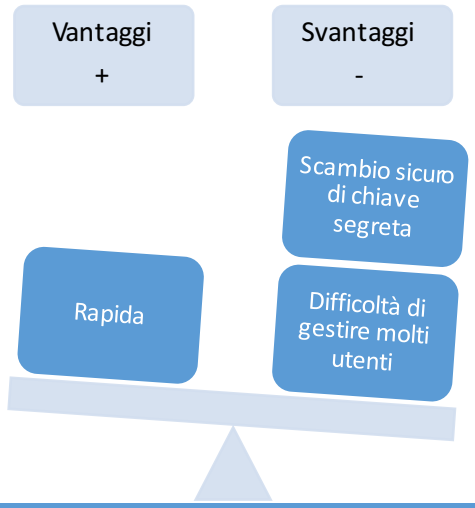
Crittografia simmetrica: esempio



Crittografia simmetrica: esempio

s	o	n	o		u	n		d	o	c	u	m	e	n	t	o
115	111	110	111	32	117	110	32	100	111	99	117	109	101	110	116	111
t	p	o	p	!	v	o	!	e	p	d	v	n	f	o	u	p
116	112	111	112	33	118	111	33	101	112	100	118	110	102	111	117	112

Crittografia simmetrica



Crittografia asimmetrica

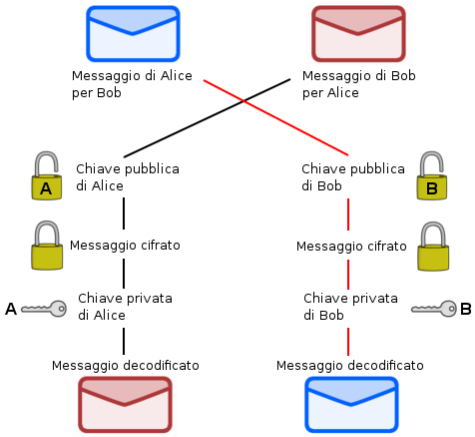
Prevede una coppia di chiavi crittografiche, una privata ed una pubblica, da utilizzarsi per la sottoscrizione dei documenti informatici. Pur essendo univocamente correlate, dalla chiave pubblica non è possibile risalire a quella privata che deve essere custodita dal titolare

Chiave privata
deve essere conosciuta solo dal titolare e viene utilizzata per apporre la firma sul documento

Chiave pubblica
Deve essere resa pubblica e viene utilizzata per verificare la firma digitale apposta sul documento informatico dal titolare della coppia di chiavi

Come funziona la crittografia a chiavi asimmetriche

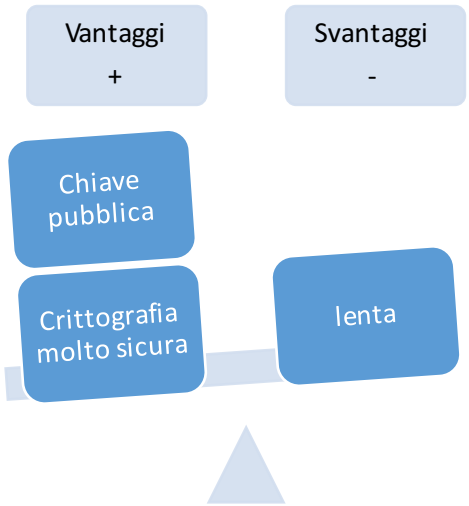
- Maria chiede a Luca di spedirle il suo lucchetto, già aperto. La chiave dello stesso verrà però gelosamente conservata da Luca.
- Maria riceve il lucchetto e, con esso, chiude il pacco e lo spedisce a Luca.
- Luca riceve il pacco e può aprirlo con la chiave di cui è l'unico proprietario.



Esempio tratto da Wikipedia

64

Crittografia asimmetrica



Crittografia dei propri dati

Nascondere i dati per renderli inutilizzabili in caso di furto o smarrimento di dispositivi o di attacco hacker o di virus, ma nasconderli anche per inviarli in modo sicuro.

- Software di criptazione:
  - **Veracrypt** (Software gratuito nato dalle ceneri di TrueCrypt)
  - **BitLocker** (Nativo in ambiente Windows)
  - **FileVault** (Nativo in ambiente MAC-OS)
- Assicurarsi di navigare in maniera cifrata (https) quando si trasmettono dati riservati

Tratto da: Il giornalista hacker, Giovanni Ziccardi, Marsilio Editori S.p.A., 2012 – ISBN: 978-88-317-3344-1

66

Protonmail: la posta criptata

Protonmail è un servizio nato in Svizzera per garantire la trasmissione di e-mail con un alto livello di sicurezza.

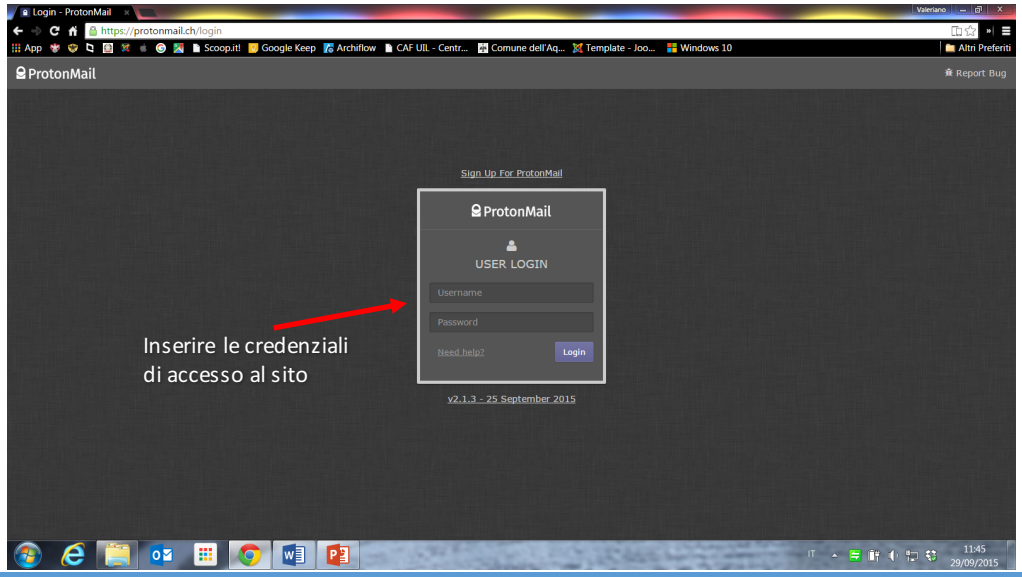
Il sistema si basa su algoritmi di criptazione molto robusti.

La comunicazione tra due utenti Protonmail è criptata con chiavi asimmetriche, ma anche la comunicazione con altri provider di posta (G-mail, Outlook, AOL, Yahoo!, ecc…) è protetta da una password.

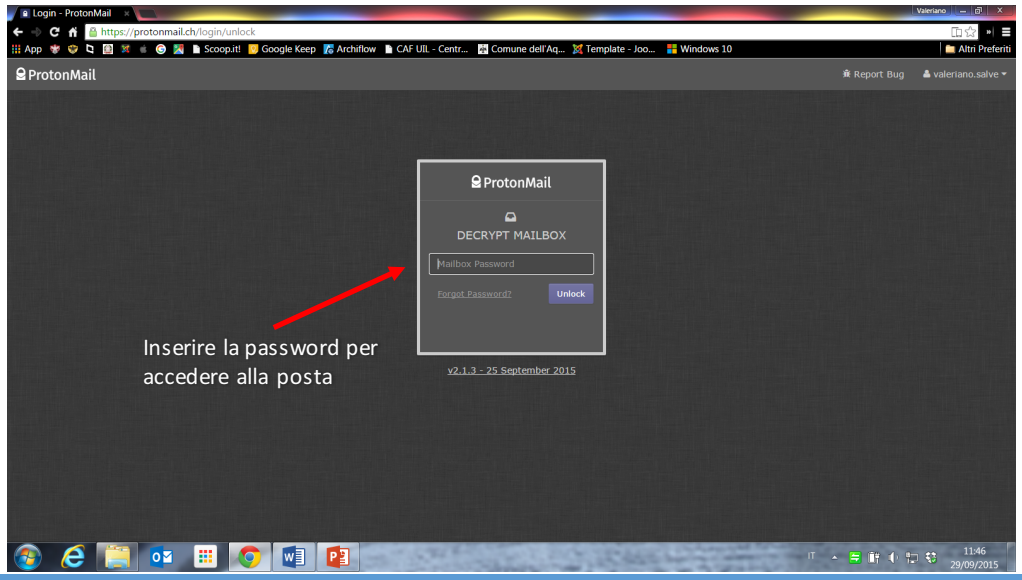
Il servizio è gratuito.

Sono state rilasciate le app per smartphone e tablet (Costo 25 euro), ma si può accedere comunque al servizio tramite il browser del dispositivo.

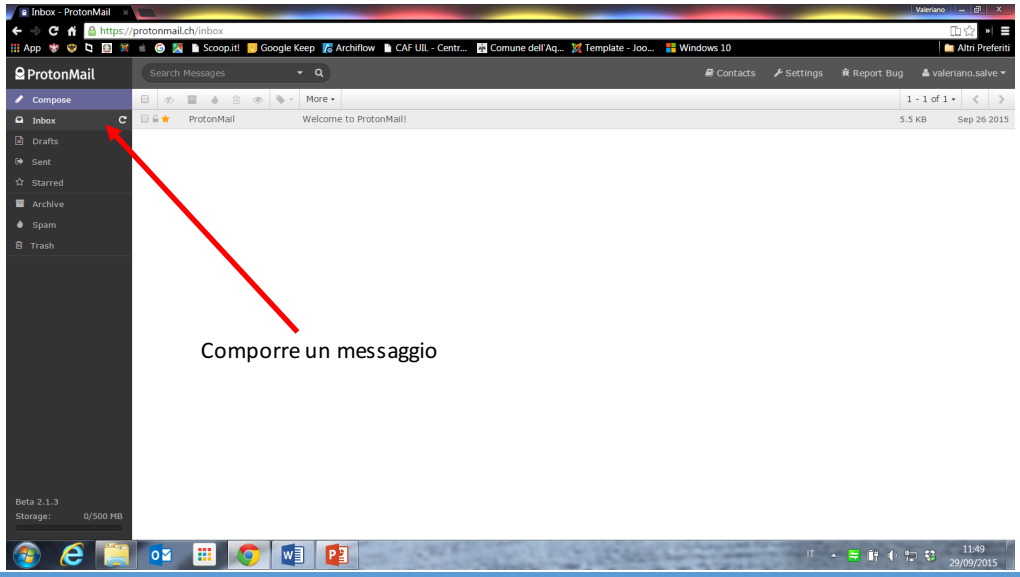
Protonmail: accesso



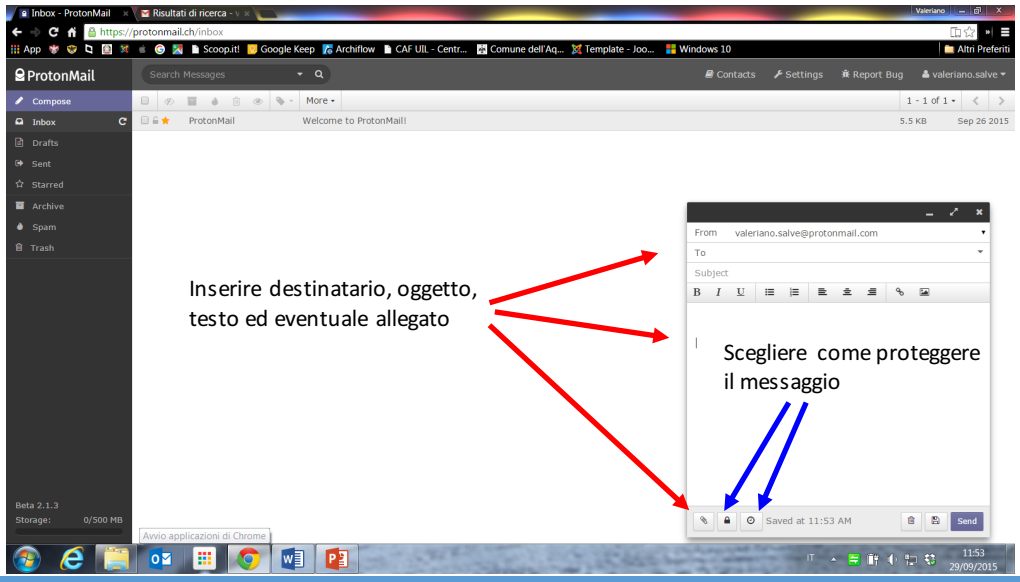
Protonmail: accesso



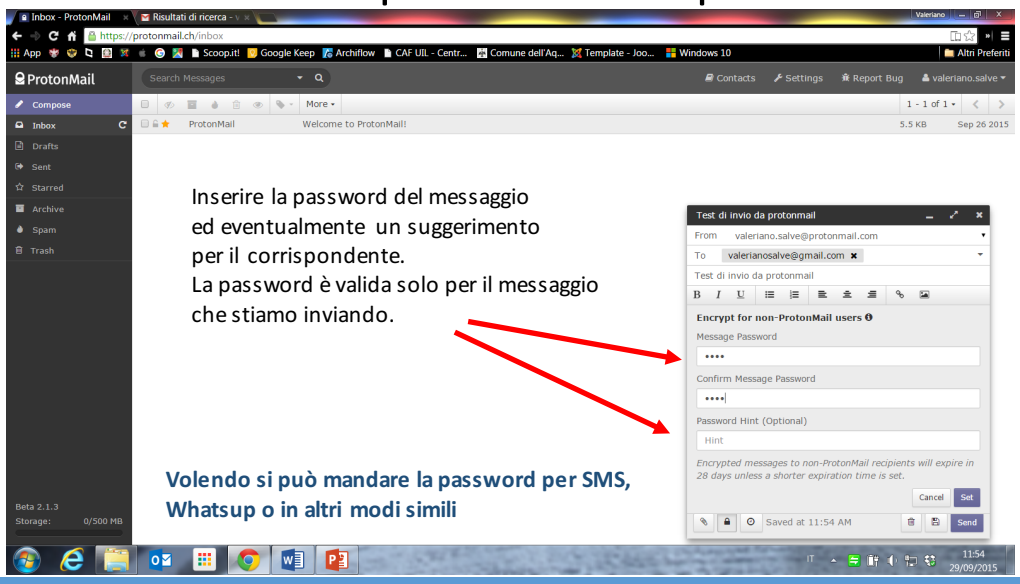
Protonmail: la dashboard



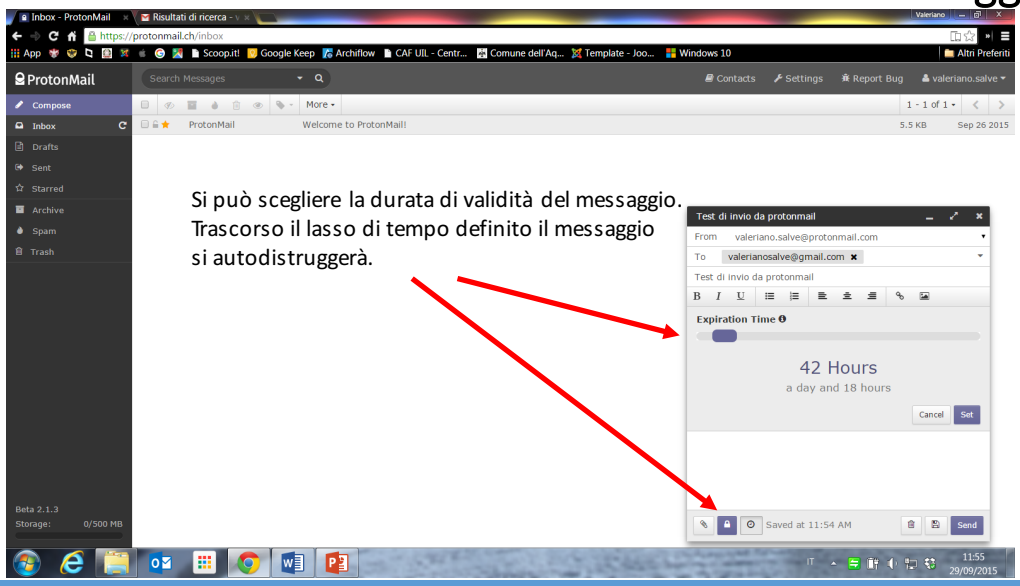
Protonmail: invio



Protonmail: protezione con password

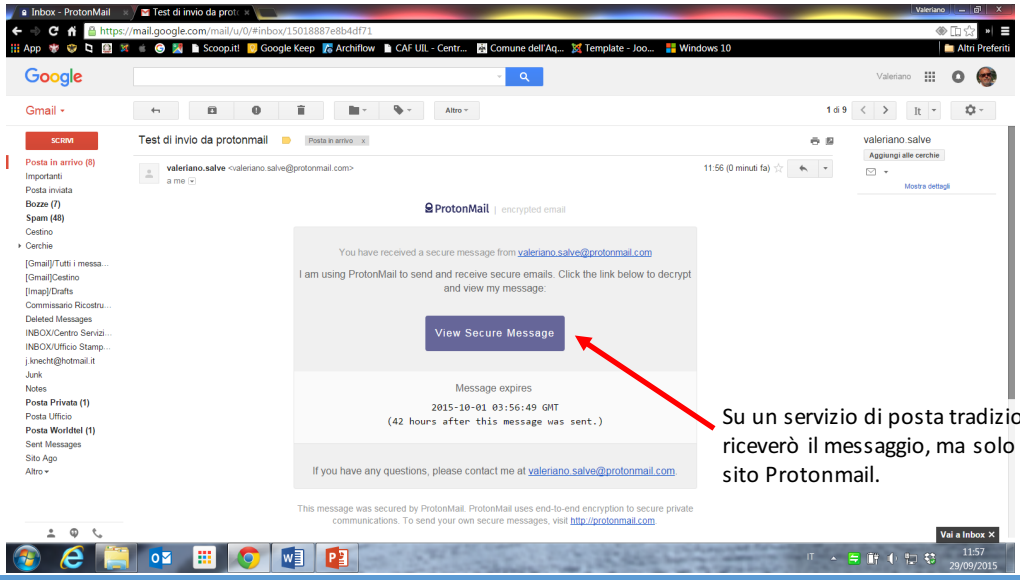


Protonmail: scadenza e autodistruzione del messaggio



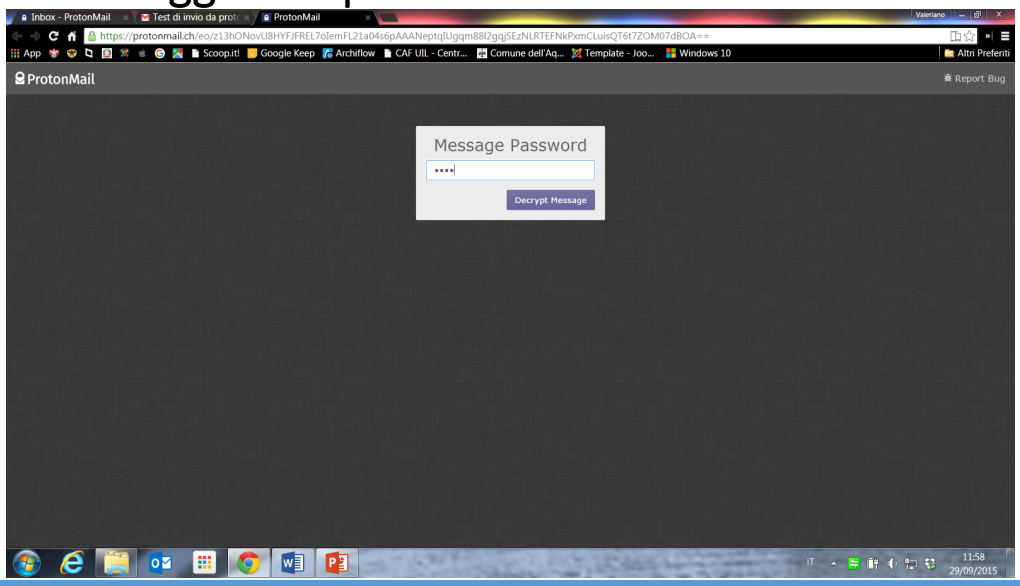
Si può scegliere la durata di validità del messaggio. Trascorso il lasso di tempo definito il messaggio si autodistruggerà.

Protonmail vista da Gmail

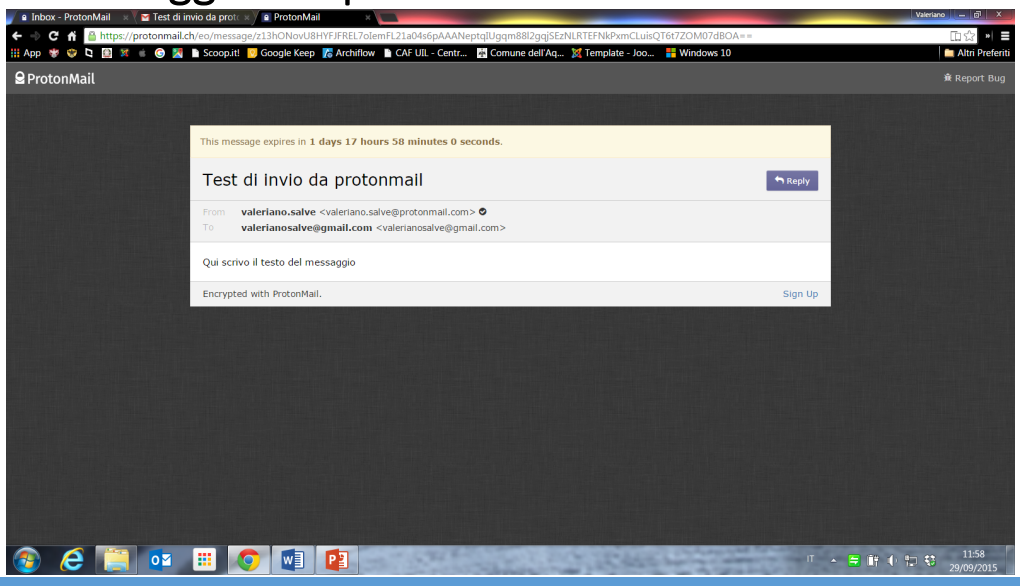


Su un servizio di posta tradizionale non riceverò il messaggio, ma solo il link al sito Protonmail.

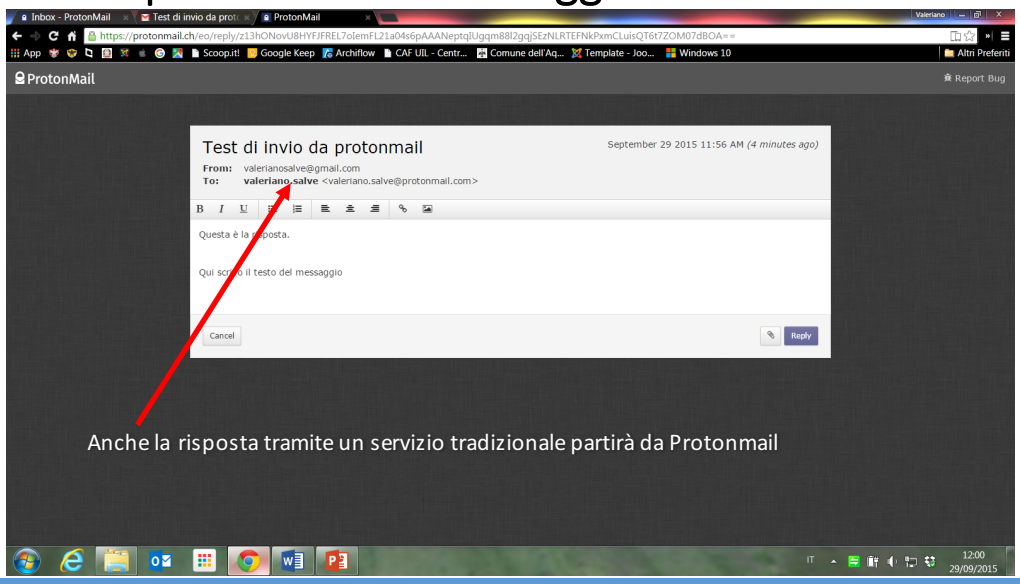
Leggere la posta inviata da Protonmail



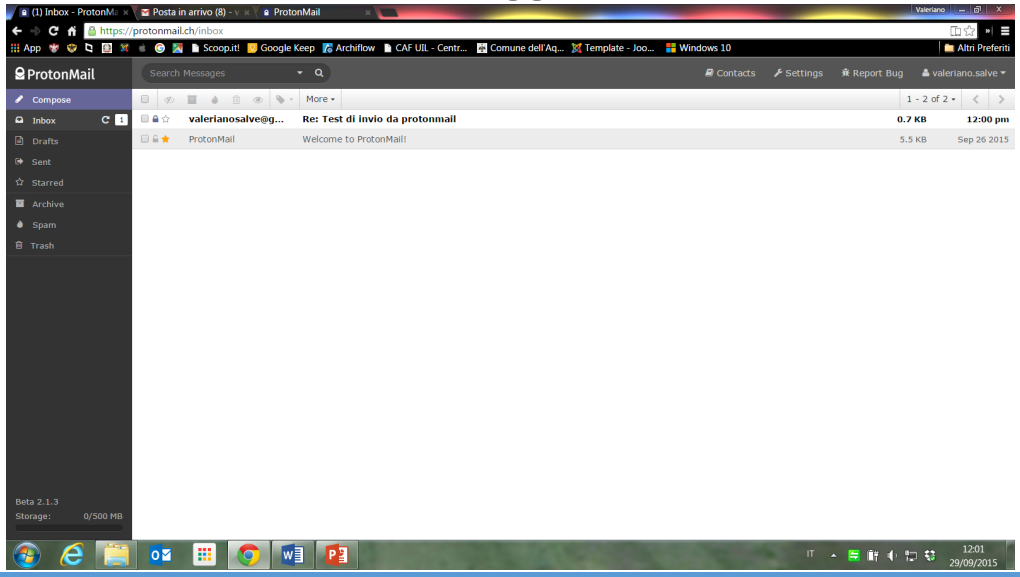
Leggere la posta inviata da Protonmail



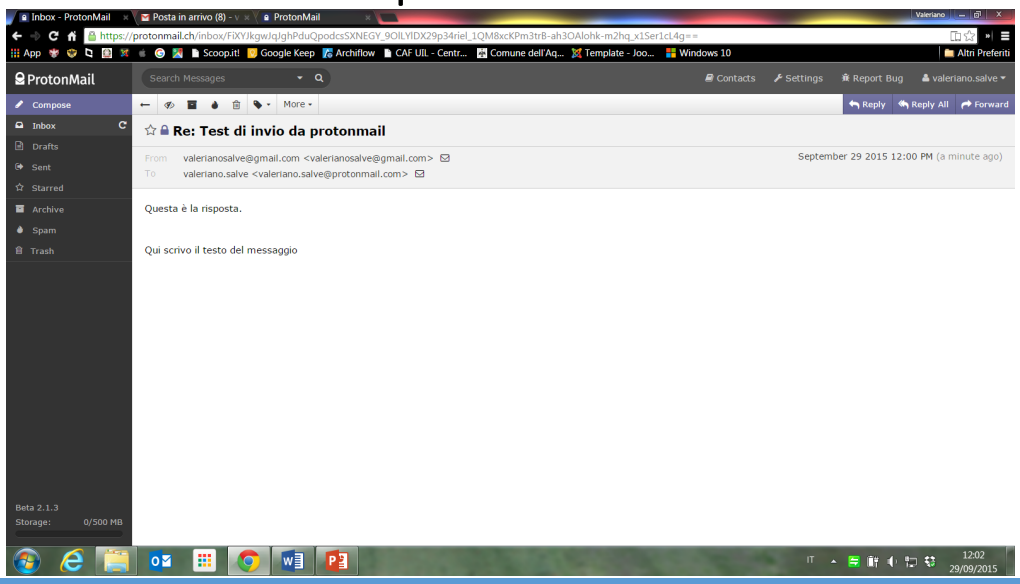
Rispondere a un messaggio di Protonmail



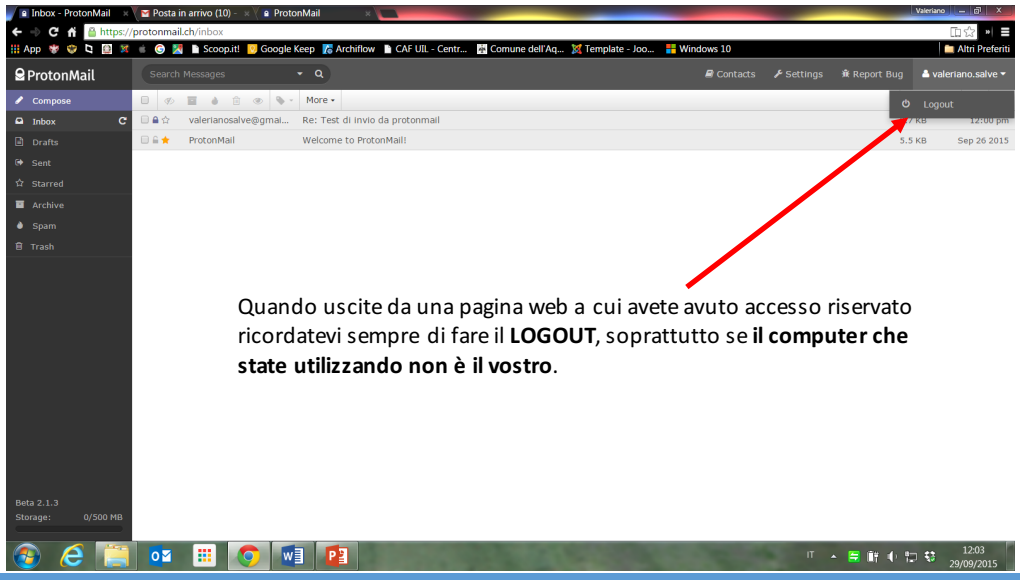
Ricevere un messaggio da Protonmail



Ricevere posta da Protonmail



Uscire da Protonmail



Quando uscite da una pagina web a cui avete avuto accesso riservato ricordatevi sempre di fare il **LOGOUT**, soprattutto se **il computer che state utilizzando non è il vostro**.

Anonimato in rete

Ci sono diversi sistemi per garantirsi l'anonimato in rete e garantire l'anonimato delle fonti.

Dal più banale che può essere farsi un indirizzo e-mail non intestato al proprio nome fino a servizi che assicurano l'anonimato più totale, dalla navigazione alla spedizione di e-mail, dalla creazione di blog o siti web anonimi alla creazione di pc virtuali e totalmente anonimi che spariscono dopo l'uso.

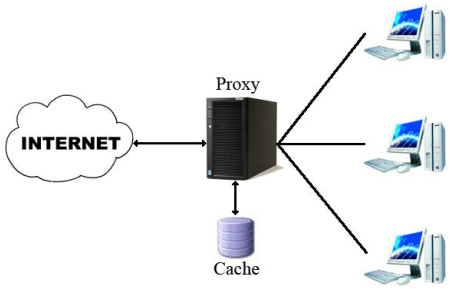
Di seguito vedremo le risorse e le tecniche principali.

Cos'è un proxy e quali sono i livelli di sicurezza

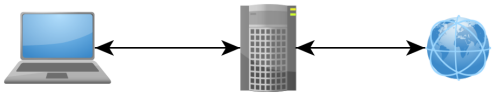
Un proxy è un server posizionato tra il dispositivo (PC, smartphone, tablet) e la rete internet. E' il proxy che visita i siti richiesti e che passa i risultati al dispositivo. Possiamo elencarne tre tipologie:

- **Transparent Proxy**: non sono anonimi, non mascherano il vostro indirizzo IP e non notificano ai siti visitati che state utilizzando un proxy (di solito si utilizzano in organizzazioni che hanno una rete interna)
- **Anonymous Proxy**: non mostrano l'indirizzo IP, ma indicano che si sta utilizzando un proxy;
- **High Anonymous Proxy**: non mostrano l'indirizzo IP e non indicano che si sta utilizzando un proxy

Proxy: schema di funzionamento



Proxy per grandi organizzazioni ed enti



Proxy per il singolo utente

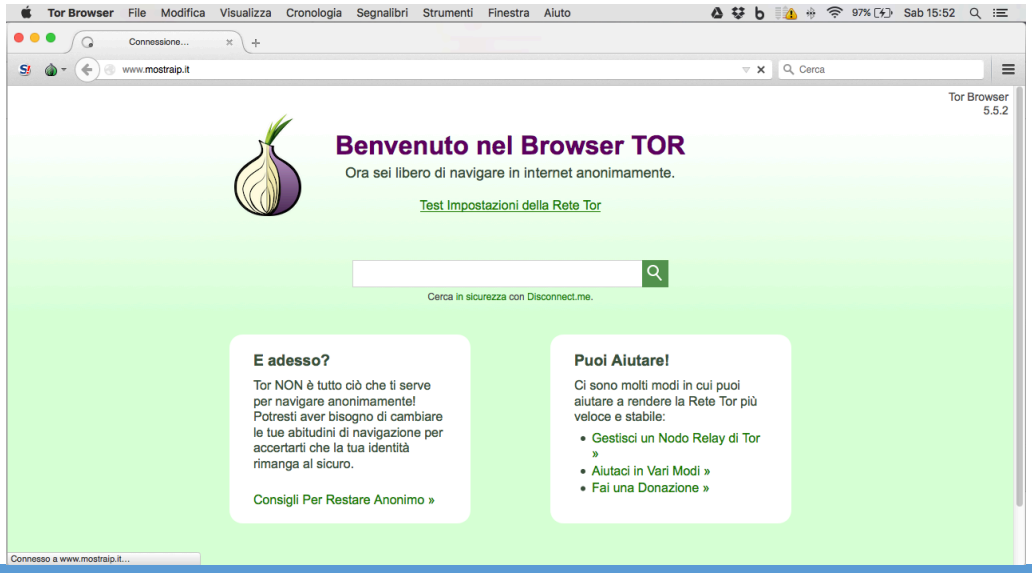
Proxy anonimi: dove trovarli

Ecco qualche risorsa su cui trovare elenchi di proxy anonimi e gratuiti, ma basta fare una ricerca su un qualsiasi motore per trovarne abbastanza. Possono cambiare o sparire, quindi ogni tanto è bene verificarne il funzionamento

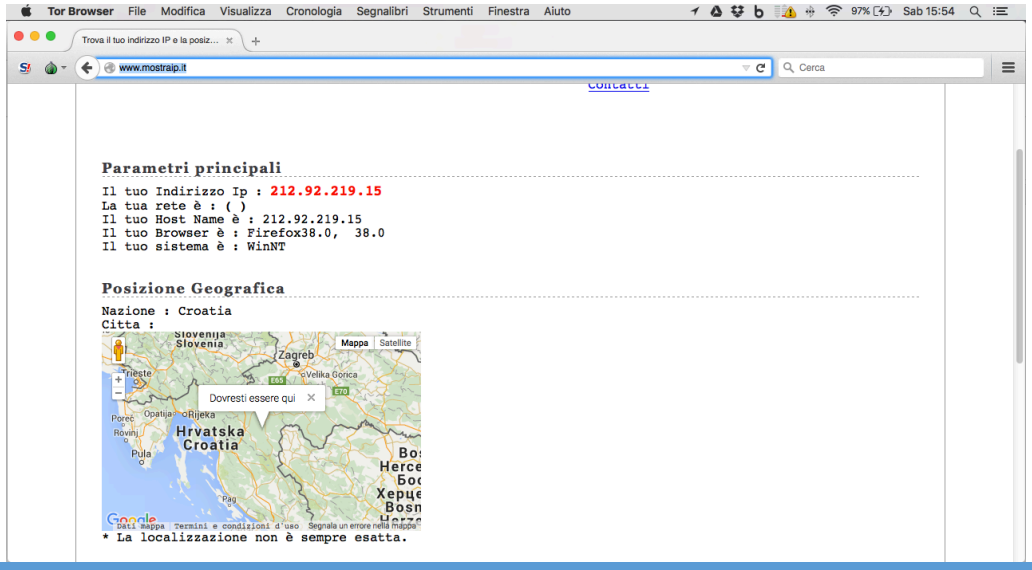
- http://proxoit.altervista.org/web-http-proxy.html
- http://www.aranzulla.it/server-proxy-63922.html
- http://anonymouse.org/anonwww.html

TOR: nascondersi (o quasi) al mondo

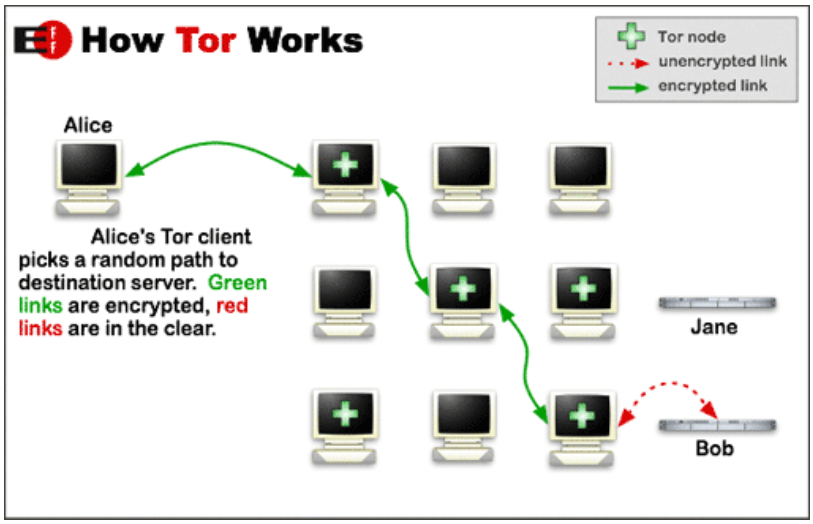
Il Browser TOR



Il Browser TOR



Come funziona TOR



Anonimato

Navigare anonimi aggirando anche filtri e blocchi

- Utilizzare Tor, un software libero, che garantisce un buon livello di anonimato. Il software può essere scaricato dal sito https://www.torproject.org ed è disponibile per qualsiasi piattaforma (Windows, Mac-OS, Linux e Android). Può essere installato anche su un dispositivo usb per averlo sempre a portata di mano.
- Tor provvede all'anonimato, ma non alla riservatezza della trasmissione. Il collegamento finale è «in chiaro» quindi attenzione ad inserire informazioni personali.

Tratto da: Il giornalista hacker, Giovanni Ziccardi, Marsilio Editori S.p.A., 2012 – ISBN: 978-88-317-3344-1

Senza attenzione Tor non basta

- **Want Tor to really work?**
- You need to change some of your habits, as some things won't work exactly as you are used to.
- **Use the Tor Browser** Tor does not protect all of your computer's Internet traffic when you run it. Tor only protects your applications that are properly configured to send their Internet traffic through Tor. To avoid problems with Tor configuration, we strongly recommend you use the Tor Browser. It is pre-configured to protect your privacy and anonymity on the web as long as you're browsing with the Tor Browser itself. Almost any other web browser configuration is likely to be unsafe to use with Tor.
- **Don't torrent over Tor** Torrent file-sharing applications have been observed to ignore proxy settings and make direct connections even when they are told to use Tor. Even if your torrent application connects only through Tor, you will often send out your real IP address in the tracker GET request, because that's how torrents work. Not only do you deanonymize your torrent traffic and your other simultaneous Tor web traffic this way, you also slow down the entire Tor network for everyone else.
- **Don't enable or install browser plugins** The Tor Browser will block browser plugins such as Flash, RealPlayer, Quicktime, and others: they can be manipulated into revealing your IP address. Similarly, we do not recommend installing additional addons or plugins into the Tor Browser, as these may bypass Tor or otherwise harm your anonymity and privacy.
- **Use HTTPS versions of websites** Tor will encrypt your traffic to and within the Tor network, but the encryption of your traffic to the final destination website depends upon on that website. To help ensure private encryption to websites, the Tor Browser includes HTTPS Everywhere to force the use of HTTPS encryption with major websites that support it. However, you should still watch the browser URL bar to ensure that websites you provide sensitive information to display a blue or green URL bar button, include **https://** in the URL, and display the proper expected name for the website. Also see EFF's interactive page explaining how Tor and HTTPS relate.
- **Don't open documents downloaded through Tor while online** The Tor Browser will warn you before automatically opening documents that are handled by external applications **DO NOT IGNORE THIS WARNING**. You should be very careful when downloading documents via Tor (especially DOC and PDF files) as these documents can contain Internet resources that will be downloaded outside of Tor by the application that opens them. This will reveal your non-Tor IP address. If you must work with DOC and/or PDF files, we strongly recommend either using a disconnected computer, downloading the free VirtualBox and using it with a virtual machine image with networking disabled, or using Tails. Under no circumstances is it safe to use BitTorrent and Tor together, however.
- **Use bridges and/or find company** Tor tries to prevent attackers from learning what destination websites you connect to. However, by default, it does not prevent somebody watching your Internet traffic from learning that you're using Tor. If this matters to you, you can reduce this risk by configuring Tor to use a Tor bridge relay rather than connecting directly to the public Tor network. Ultimately the best protection is a social approach: the more Tor users there are near you and the more diverse their interests, the less dangerous it will be that you are one of them. Convince other people to use Tor, too!
- Be smart and learn more. Understand what Tor does and does not offer. This list of pitfalls isn't complete, and we need your help identifying and documenting all the issues.

Senza attenzione TOR non basta

- Così come recita la home page del browser "***Tor NON è tutto ciò che ti serve per navigare anonimamente! Potresti aver bisogno di cambiare le tue abitudini di navigazione per accertarti che la tua identità rimanga al sicuro.***" Ecco qualche consiglio:
- TOR non protegge tutto il traffico internet generato dal tuo PC. Essendo una rete, essa protegge le applicazioni correttamente configurate per indirizzare il proprio traffico internet attraverso TOR.
- Per come è strutturato il file sharing su base torrent, anche se sei su rete TOR manderai sempre il tuo IP reale per la richiesta di GET al tracker. Dunque **è sconsigliato di usare torrent su rete TOR.**
- **Non installare plugin di terze parti.** Plugin come Flash, RealPlayer, Quicktime, sono facilmente programmabili per rivelare l'indirizzo IP del navigatore.
- **Naviga su siti col protocollo HTTPS.** Le connessioni da e per la rete TOR sono criptate, ma come sappiamo la sicurezza di non avere ascoltatori indesiderati ce la da solo il protocollo https.
- Si dovrebbe essere molto attenti quando si scaricano documenti via Tor (soprattutto DOC e PDF) in quanto questi documenti possono contenere link a risorse Internet che verranno scaricate o contattate al di fuori di Tor e che potrebbero compromettere l'anonimato. **Prima di aprire documenti scaricati da TOR è bene disconnettere il computer dalla rete.**

Utilizzare una e-mail temporanea

Ci sono servizi che permettono di crearsi una casella e-mail «temporanea», «anonima» che si autocancella dopo un certo periodo

- Di solito non consentono l'invio di e-mail, ma solo di riceverne
- Di solito non consentono l'invio di allegati
- I più noti e semplici da utilizzare sono:
  - YOPmail: www.yopmail.com
  - AirMail: it.getairmail.com
  - GuerrillaMail: https://www.guerrillamail.com/ (allegati fino a 150Mb)

Ne esistono anche altri, basta fare una ricerca in rete

Utilizzare una e-mail temporanea su smartphone

GuerrillaMail rende disponibile una applicazione per Android che crea una email temporanea che si cancella dopo un'ora. L'applicazone si scarica gratuitamente, ma per inviare messaggi da Guerrilla Mail ad un altro dominio (es. gmail) bisogna comprare del credito. 100 invii costano circa 2,60 euro.

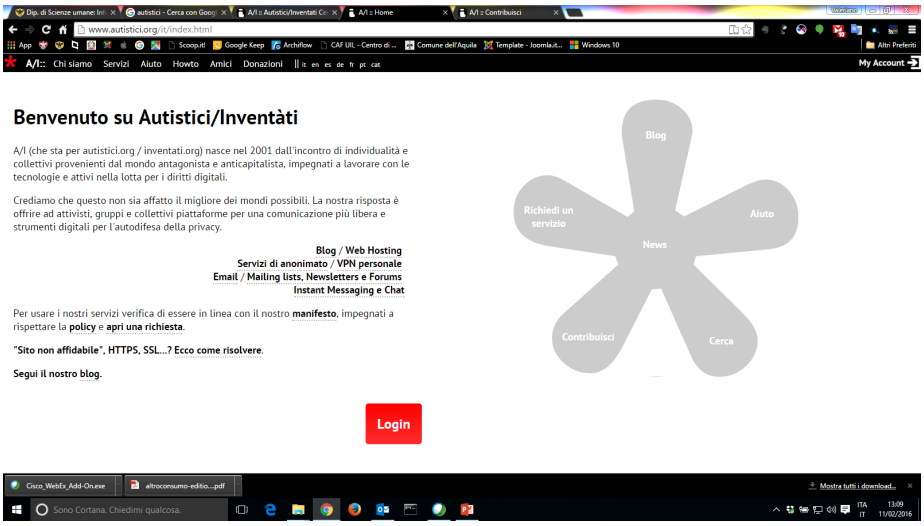
Può essere scaricata dal Google Play Store all'indirizzo:

https://play.google.com/store/apps/details?id=com.guerrillamail.app

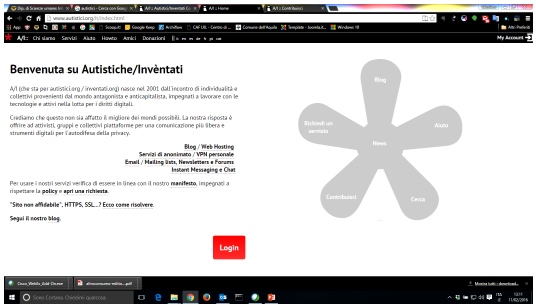
Per gli utenti iPhone possono rivolgersi al servizio Harakirimail https://harakirimail.com/ e scaricare l'app dall'Apple Store all'indirizzo:

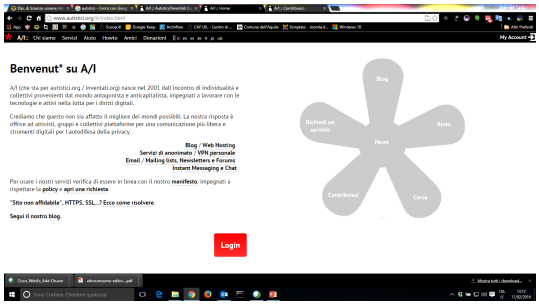
https://itunes.apple.com/it/app/harakirimail/id633675820?l=sv&ls=1&mt=8

Una piattaforma con molti servizi



http://www.autistici.org





Ambiente anonimo

Esistono applicazioni (scrivere, posta elettronica, cifratura dati, chat, navigare, cancellare) che sono portabili e cioè che non hanno bisogno di essere installate su un pc, ma possono funzionare anche su una chiave usb o un CD/DVD

- Non lasciano (quasi) tracce sul computer;
- Possono far partire un nuovo sistema operativo e possono essere utilizzati su computer di cui «non ci si fida» e in questo caso, una volta rimosse e riavviato il pc, non lasciano alcuna traccia.

Creare un ambiente anonimo con TAILS: https://tails.boum.org

Tratto da: Il giornalista hacker, Giovanni Ziccardi, Marsilio Editori S.p.A., 2012 – ISBN: 978-88-317-3344-1

Macchine virtuali

- Le macchine virtuali sono nate per far funzionare più sistemi operativi su un solo PC;
- E' possibile creare una macchina virtuale che non ha quasi nessun contatto con il sistema operativo che la ospita;
- Permette di usare ad esempio diverse versioni di Windows o una macchina Linux in un ambiente Windows o anche una macchina Windows in un Mac-OS;
- Se la macchina virtuale viene cancellata sparisce anche il suo contenuto.

- http://www.virtualbox.org
- http://www.vmware.com

Tratto da: Il giornalista hacker, Giovanni Ziccardi, Marsilio Editori S.p.A., 2012 – ISBN: 978-88-317-3344-1

Identità anonima

- Giocare con le false identità in internet è facile
- Difficile è non far risalire ai nostri dati
- Creare un account mantenendo anonimo il nostro numero IP
- Quello che si fa in rete non deve essere riferibile al soggetto e con un IP non riferibile

Il comportamento per rimanere anonimo deve essere mantenuto anche cercando di non incrociare dati che possano far risalire a riferimenti personale (caricare foto con i dati di una macchina fotografica o peggio le coordinate GPS, utilizzare IP che non siano stati preventivamente mascherati…)

Tratto da: Il giornalista hacker, Giovanni Ziccardi, Marsilio Editori S.p.A., 2012 – ISBN: 978-88-317-3344-1

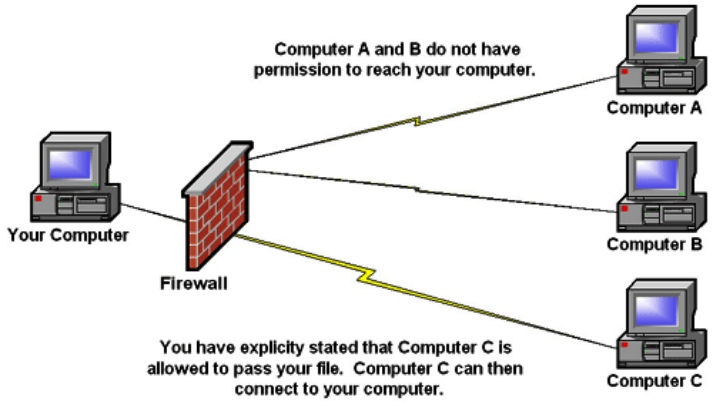
Il Firewall

- Un firewall controlla il traffico da e verso l'esterno della rete, in particolare con internet, bloccando quello indesiderato e potenzialmente pericoloso
- Possono essere utilizzati
  - Firewall software
  - Firewall hardware
- E' necessario un costante **aggiornamento** del firewall, che in caso contrario diventa velocemente vulnerabile
- In aggiunta al firewall, può essere opportuno utilizzare un IDS (Intrusion Detection System)

Il Firewall

- Il firewall analizza tutti i pacchetti che lo attraversano in modo da prendere una decisione conforme ad un set di regole definito dall'utente.
- In linea generale queste regole sono specificate in modo da comportare l'accettazione o il blocco dei pacchetti in transito sulla base di quelli che sono i loro elementi distintivi, vale a dire indirizzo IP e porta della sorgente nonché indirizzo IP e porta della destinazione.

Il Firewall



Il backup

Con il termine backup s'identifica una specifica operazione tesa a duplicare su differenti supporti di memorizzazione di massa {hard disk, pen drive, CD-DVD ecc.) tutti i dati e/o programmi contenuti nei sistemi informativi dell'azienda.

Questa operazione consente di recuperare il materiale nel caso in cui si verifichino guasti, manomissioni, alterazioni e danneggiamenti dei sistemi informatici primari, con conseguente possibile perdita dei dati contenuti.

Esistono due tipi di backup:

- ✓ ***salvataggio manuale*** *{backup* effettuato dal responsabile dell'operazione e gestito nei tempi e nelle modalità stabilite dall'operatore stesso)
- ✓ ***salvataggio automatico*** (procedura gestita automaticamente da appositi programmi dedicati alle operazioni di *backup)*

Il backup

Il Backup permette di realizzare delle COPIE DI SICUREZZA.

Secondo i dati forniti da BackBlaze nella sua inchiesta annuale, il **30% degli utenti non hai mai fatto copie di sicurezza** dei dati del suo computer, e solo un 10% fa copie di sicurezza quotidiane. Il 93% degli utenti fa solo copie in locale.

Il 46% degli utenti domestici perde dati ogni anno.

Fare un backup o copie di sicurezza è MOLTO importante soprattutto perché permette di salvaguardare l'integrità e la disponibilità dei dati.

Cancellazione sicura dei file

- Quando si cancella un file o una cartella spostandola nel cestino e svuotandolo il file non viene «cancellato», ma solo reso introvabile dal file system;
- Per cancellare completamente un file questo va «sovrascritto» con altri dati. Un programma che permette di farlo è Eraser (http://eraser.heidi.ie);
- Attenzione a quando si cede o vende un pc o un dispositivo: assicurarsi prima di avere completamente eliminato i propri dati;
- La formattazione veloce non cancella i dati, ma semplicemente azzera il file system

Tratto da: Il giornalista hacker, Giovanni Ziccardi, Marsilio Editori S.p.A., 2012 – ISBN: 978-88-317-3344-1

Humanware

Per garantirsi un sistema sicuro occorrono tre cose:

- Un hardware senza difetti
- Un software senza difetti
- **Un essere umano senza difetti (dal punto di vista informatico)**

Tutti e tre gli elementi hanno la stessa importanza, ma spesso tendiamo a sottovalutare i nostri comportamenti mentre utilizziamo un dispositivo connesso alla rete.

Tratto da: Il giornalista hacker, Giovanni Ziccardi, Marsilio Editori S.p.A., 2012 – ISBN: 978-88-317-3344-1

GRAZIE PER L'ATTENZIONE

valeriano@salve.ws
http://www.salve.ws