Igiene Informatica

Da Wikipedia, l'enciclopedia libera.

Contents

Elementi di Igiene Informatica

Questo che stai leggendo è un maldestro tentativo di dare unità a tante semplici (ma importanti) attività informatiche. Sono appunti raccolti nel corso degli anni su diversi temi legati all'informatica e agli utenti meno esperti. L'unità si è cercato di darla non soltanto scrivendo tutto in una sola pagina, ma anche proponendo un nome e delle regole per questa nuova "materia": l'Igiene Informatica («**Computer Hygiene**» in inglese).

Adesso è disponibile anche una piattaforma di **e-learning** per organizzare **corsi di formazione** sull'Igiene Informatica (http://www.igieneinformatica.it/) , che viene utilizzata anche per i corsi del GOLEM. Tramite tale sito viene fornito anche supporto professionale sui temi trattati qua di seguito.

Queste sono le **linee guida** seguite nella redazione:

1. Non serve scrivere **tutto**. Basta scrivere le cose strettamente **necessarie**
2. Chiarezza e completezza **non** sono conciliabili. Preferiamo la **chiarezza**
3. Ci rivolgiamo a degli **inesperti**, non a degli **stupidi**
4. Sintesi!

Il dettaglio delle linee guida può essere letto nella pagina della discussione di questo articolo.

Torna a Visioni

Siti che ci «linkano»

- IgieneInformatica.it (http://www.igieneinformatica.it/)
- Lele Rozza blog (http://lelerozza.org/?p=216)
- Ingegneria Senza Frontiere (http://tic.isf-italia.org/ConsigliPerIndirizziEmail)
- Tuttoscript (http://www.tuttoscript.net/articoli.php?id=46)
- AgriModena (http://www.agrimodena.it/varie/Elementi%20di%20Igiene%20Informatica.htm)
- Zeus News (http://zeusnews.it/index.php3?ar=stampa&cod=2945&numero=389)
- Noema Labs (http://www.noemalab.org/sections/news_detail.php?IDNews=1316)
- Hacker Kulture (http://www.dvara.net/HK/infoetica.asp)
- Veglie News (http://www.veglienews.it/magazine/notizievarie/igiene_informatica.htm)

- X Style Script (http://xstylescript.interfree.it/igiene.htm)
- Free Software User Group di Padova (http://lists.fsugpadova.org/pipermail/fsug-pd/2007-February/000408.html)
- PerUnMondoMigliore (http://www.perunmondomigliore.net/os_igiene_informatica.php)
- Luigi Irace (http://luigi-irace.spaces.live.com/blog/cns!1DCB4B2F0258D323!920.entry)

Introduzione

L'utilizzo **etico** di ogni tipo di risorsa consiste nella fruizione, con **spreco minimo** possibile, della risorsa stessa. Utilizzare: si. Sprecare: no. Questo non dipende dalla quantità di risorse a disposizione.

L'Igiene Informatica (per brevità potremo chiamarla **IgInfo**) si occupa dell'utilizzo di risorse informatiche **senza spreco**. L'igiene informatica si occupa dell'utilizzo **malizioso** delle risorse informatiche fatto **a discapito dell'utente**. Si occupa anche di minimizzare il rischio a cui sono sottoposti i dati e le risorse degli utenti.

Non è ciò che viene generalmente detto «alfabetizzazione informatica». Chi è interessato all'Igiene Informatica, deve essere già un utente di programmi applicativi o posta elettronica o navigazione Internet.

Sarebbe importante che chi si interessa a questo «Elementi di Igiene Informatica» sappia spedire e ricevere posta elettronica e navigare su Internet. Si da per scontato che chi legge conosca il significato di alcuni termini tecnici (peraltro molto semplici: file, directory, backup).

l'IgInfo si occupa di **etichetta in Rete**, ma **non è** propriamente quella che viene definita «netiquette». Non riguarda solo la forma del rapporto fra persone, fa considerazioni anche tecniche (lavarsi le mani prima di andare a tavola non ha solo funzioni di etichetta). Si affrontano temi legati alla netiquette, ma non è netiquette.

L'IgInfo si occupa di **sicurezza informatica**. Promuove **comportamenti** dell'utente che migliorano tanti aspetti di sicurezza informatica (imparare ad attraversare la strada aumenta la sicurezza generale della rete stradale), ma decisamente **non è** «sicurezza informatica» così come viene comunemente intesa, è molto meno, anzi: è molto diversa. Si affrontano temi legati alla sicurezza informatica ma non è sicurezza informatica.

Si affrontano temi legati alla **privacy**, alla riservatezza dell'utente; temi legati ai diritti degli utenti in Rete; temi legati all'utilizzo «pieno» del web, saper trovare informazioni e farsi trovare; temi legati al rispetto del prossimo.

Sono state aggiunte le sezioni in cui si accennano i problemi legati al cosiddetto **tecnocontrollo**. Si danno dei piccoli consigli di **autodifesa digitale** per far faticare almeno un po' gli addetti al controllo sistematico e "incontrollato" dei cittadini della Rete.

Si affrontano temi importanti per **utenti** informatici **consapevoli**, maturi. Insomma: l'Igiene Informatica è decisamente una materia «**per adulti**», per utenti che usano in modo consapevole e pieno le risorse informatiche. L'utente interessato a questa

materia non deve essere un esperto informatico, ma non deve essere nemmeno un idiota: non ci piace l'informatica per idioti (che, del resto, non si rivolge a noi).

Questa è informatica **per utenti inesperti**, non per utenti stupidi!

La materia è **indipendente dalla piattaforma** tecnologica. Purtroppo alcune piattaforme (processore + sistema operativo) avranno il monopolio della materia, in quanto sono le piattaforme intrinsecamente meno sicure che richiedono il comportamento più attento e meticoloso.

Ancora è esclusa la parte relativa alla **salute**: posizione e tempi di lavoro, monitor, emissioni elettromagnetiche, muscoli oculari, effetti neurofisiologici.

Prima di questo scritto (nato nella sua versione 0.1.0 a **fine del 2001**) non si hanno notizie che attestino l'esistenza di una materia di studio denominata «Igiene Informatica».

Il primo **corso** di Igiene Informatica di cui si ha notizia è stato tenuto a Empoli (FI) dal GOLEM - Gruppo Operativo Linux Empoli, nell'Officina Informatica, il 21 maggio 2002. Dopocena.

Navigazione Internet

I più diffusi problemi di sicurezza legati a Internet (adesso parliamo del web) vengono **risolti** utilizzando **Linux**. Si consiglia la migrazione immediata a tale sistema. Questo capitolo potrebbe concludersi qua.

Se proprio vogliamo continuare (perché nostalgici o per scelta di fede) a usare «l'unico sistema operativo sensibile ai virus(TM)», allora è bene cercare di migliorarne la sicurezza, magari utilizzando Software Libero. Un buon articolo (http://www.dbazine.com/ofinterest/oi-articles/fosdick12) e una divertente presentazione (http://uniforumchicago.org/slides/FOSS4WindowsSecurity.ppt) di Howard Fosdick (purtroppo in formato non standard).

Una frase di Fosdick: «Molti sostengono che windows sia il bersaglio preferito di molti attacchi perché è il sistema **più diffuso**. Questo spiega il **motivo** per cui windows è soggetto ad attacchi… ma **non giustifica** perché debba **soccombervi**!».

Un altro passo obbligato è scaricare e installare Firefox (http://www.mozillaitalia.it /archive/index.html#p1) . **Subito!** È un ottimo browser, con molte opzioni di sicurezza e di tutela della privacy dell'utente. Un indispensabile strumento di **autodifesa** che sostituisce nella navigazione il vecchio e insicuro Explorer.

Una volta aperto Firefox premere [Ctrl] + [k], scrivere un criterio di ricerca e premere invio. Si vedrà che inizia subito la ricerca sul web utilizzando i maggiori motori di ricerca, indipendentemente dalla pagina che stavamo navigando.

Navigazione: uso delle **schede**. Prova a **cliccare** un link usando il **tasto centrale** del mouse (si, sulla rotellina).

Quasi tutti i siti di informazione e tutti i blog fanno (per fortuna) largo uso dei cosiddetti RSS o **segnalibri live**. Quando è possibile memorizzare un segnalibro live nella barra degli indirizzi di Firefox compare un quadratino **arancione**.

Firefox ha anche alcune **indispensabili** «estensioni». Riteniamo che chiunque debba installare Adblock Plus (https://addons.mozilla.org/it/firefox/addon/1865) , che blocca tantissima pubblicità che infesta i siti commerciali. C'è da considerare che la pubblicità, oltre a rendere più **faticosa** la lettura del web, **rallenta** la navigazione e fa aumentare il **costo** delle connessioni «a consumo» o «pay per use». Tocca anche pagare per vedere della fastidiosa pubblicità che rallenta pure la connessione: **pazzia totale**.

Per i più **spericolati** può servire anche NoScript (https://addons.mozilla.org /it/firefox/addon/722) . NoScript blocca l'esecuzione di tutti gli script (programmi che i siti fanno eseguire al nostro computer durante la navigazione), per cui molti siti potrebbero non funzionare pienamente se non vengono autorizzati. Però NoScript è indispensabile per navigare i siti super-commerciali che eseguono mille statistiche sulle pagine da noi navigate. Se si usa NoScript c'è da ricordarsi sempre di attivare l'esecuzione degli script per i domini «fidati». Nello stesso sito spesso ci sono script provenienti da molti domini diversi fra loro. NoScript è selettivo. Indispensabile per chi frequenta i bassifondi del web. (Se non hai capito questo paragrafo, non importa, passa oltre).

Opzioni di sicurezza dei browsers

ActiveX, cookies, Java, javascript e altre supposte. Molti siti web fanno largo uso di programmi che, veicolati dalle pagine web, possono **eseguire codice** sul computer dell'ignaro navigatore. La domanda fondamentale da fare è questa: «Di chi è il **tuo** computer?». Se il computer è tuo dovresti poterci fare quello che vuoi **tu** e non quello che vogliono **loro**, a meno che tu non li autorizzi. **Firefox è tuo amico**. Abbandona Explorer e **installa subito** Firefox (http://www.mozillaitalia.it/archive /index.html#p1) .

È vietato consultare la presente pagina web oltre questo limite usando Explorer.

```
Limite invalicabile
```

Disattiviamo e attiviamo **consapevolmente** ActiveX, Java, javascript, nel nostro browser.

Molti siti web **non usano tecnologie standard** ma utilizzano strumenti, come i cosiddetti «ActiveX (http://it.wikipedia.org /wiki/ActiveX#ActiveX_e_Internet_Explorer) », che funzionano soltanto con un browser (Explorer) e soltanto se sufficientemente nuovo. Tali siti **non** devono essere navigati, perché **portano sfortuna** a chi li visita. Se proprio si è costretti a visitarli conviene **disattivare** l'installazione degli ActiveX o -al limite- abilitarne l'installazione solo da siti web fidati.

Con Firefox i siti non possono installare ActiveX sul nostro computer.

Si accede alla finestra da cui modificare le impostazioni di Firefox in due modi (che variano col sistema su cui è installato)

Firefox su **Linux**: Menù **Modifica** --> **Preferenze** Firefox su sistemi operativi alternativi: Menù **Strumenti** --> **Opzioni**

Firefox ha un buon trattamento dati. Usiamo sempre Firefox. Aprire la finestra di dialogo delle **Preferenze** di Firefox e indagare a lungo dentro ciascuna scheda.

La finestra di dialogo che si apre «Preferenze di Firefox» andrebbe indagata a fondo. Lo faremo soltanto un po', ma merita investirci più tempo di quello che gli dedicheremo qua.

Java e Javascript possono essere attivati o disattivati (o attivati in modo parziale) dalla scheda **Contenuti**.

cookies

memorizzazione **password** e **dati personali**.

Iniziare con pagina vuota (il browser parte velocemente ed è subito pronto a navigare)

Eliminare i files. Non fidiamoci della «pulizia disco». Alcuni sistemi operativi necessitano di appositi programmi per cancellare i dati personali. Per esempio Disk Cleaner (http://www.diskcleaner.nl/download.php) .

Impostazioni cache: pochi mega

Cronologia: pochi giorni

Cancellare cronologia se non ci interessa

Cosa sono i web bugs?

I web bugs sono delle **immagini** inserite in una pagina web e servono a monitorare il traffico su quella pagina (ovvero quanto e da chi è richiesta la pagina). La caratteristica però più **insidiosa** è che tali immagini sono praticamente **invisibili**, perché di dimensione **1-per-1 pixel** e di solito appartengono a server diversi da quello su cui si trova il sito che state visitando.Per il tipo di lavoro che svolgono sono chiamate anche «microspie del web».

Dalla definizione si può quindi capire che solitamente sono **tre** i computer coinvolti in questo tipo di monitoraggio: quello dell'utente, quello del server dove si trova il sito da visitare ed il server dove si trova il web bug. Naturalmente il web bug viene messo in accordo con la società o la proprietà del sito da visitare e questo la dice lunga sull'onestà di certe società.

I web bugs raccolgono le seguenti informazioni:

1. il tipo di browser utilizzato dal visitatore della pagina web
2. il tempo che l'utente resta a visitare la pagina web
3. l'indirizzo ip del computer che sta visitando la pagina web
4. l'url della pagina dove è collocato il web bug
5. l'url dell' immagine 1-per-1 pixel(il web bug) collocato nella nostra pagina web

Possiamo dire che le prime due voci sono informazioni piuttosto generiche, mentre le altre sono informazioni più importanti perché servono a tracciare un profilo più specifico di un utente.

Ma perché monitorare un visitatore del web?

Ecco una risorsa (http://www.eff.org/Privacy/Marketing/web_bug.html) autorevole.

Naturalmente per raccogliere quante più informazioni su un visitatore circa le sue preferenze commerciali, affiliazioni politiche, gusti sessuali, informazioni personali come nome, indirizzo, e-mail,informazioni economiche e quante piu' informazioni possibile.

I web bugs secondo Punto Informatico (http://punto-informatico.it/p.aspx?i=1448845)

Come possiamo **difenderci** dai web bug?

Diciamo che non esistono veri e propri mezzi per evitare di essere spiati dalle web bugs, se utilizziamo Explorer, possiamo installare un programma che possiamo scaricare dal sito bugnosis.org (http://www.bugnosis.org/download.html) che dà la possibilita' di monitorare le pagine web e che ci avverte della presenza, o della sospetta presenza, di web bugs su quella pagina.

Chi usa Firefox, può scegliere di accettare **soltanto** le immagini che arrivano dal sito che stiamo navigando, rifiutando quelle da terze parti (cioè altri siti). Lo si fa dal «Preferenze di Firefox».

Per maggiori informazioni (http://www.bugnosis.org/faq.html) .

Bug-gnosis (conoscenza dei bugs, delle cimici che ti spiano). Molti gestori di siti mettono nelle loro pagine immagini che contengono programmi eseguibili che raccolgono dati sulla navigazione e li trasmettono a un sito centrale. Le immagini sono file binari, possono contenere piccoli programmi invisibili.

Con Bugnosis si ha un'idea di quanto queste cimici-spia sono comuni.

Se credi che i web bugs si trovino raramente o si trovino su siti particolari o «pericolosi» ti stai sbagliando perche' sono molto, molto, molto piu' frequenti di quello che si pensa: prova a installare bugnosis e a fare un po' di normale navigazione: ci saranno belle(?) sorprese.

Il tuo browser è una spia

Il browser si ricorda tutti i tuoi dati inseriti nei moduli, le password, i siti visitati. Potremmo anche fidarci, ma non lo faremo. Rimendio: impostare di NON memorizzare dati e password (possiamo farlo dalla finestra di dialogo "Preferenze" di Firefox).

I motori di ricerca, questi sconosciuti

links (modello "Google")

categorizzazione (modello "Yahoo")

indicizzazione (modello "Altavista")

directory http://dmoz.org/ http://dmoz.org/World/Italiano/about.html

altre directory (http://chefmoz.org/ http://musicmoz.org/)

consistenza del dato su Internet

Top ranking

problematica opposta alla consistenza del dato

Sintassi di ricerca (cenni validi per google)

Operatori booleani

Studiare: http://www.google.com/ http://www.yahoo.com/

Elencare e classificare i motori

Perché essere preoccupati di Google: Google-watch (http://www.google-watch.org/) .

Dimmi dove sei e ti tirò cosa **puoi** sapere oy-oy (http://oy-oy.eu/google/world/)

E perché essere preoccupati di Yahoo!: Yahoo-watch (http://www.yahoo-watch.org/) e Yahoo-watch proxy (http://www.yahoo-watch.org/cgi-bin/proxy.htm) .

Metamotori e cluster: Clusty (http://clusty.com/)

http://www.scroogle.org/

Ixquick (http://eu.ixquick.com/eng/privacy-policy.html) è il motore di ricerca che difende la nostra privacy?

Difesa personale on-line (personal firewalls)

Un firewall serve a prevenire gli **accessi indesiderati** al nostro computer fatti **via Rete**. Il firewall è utile solo se si è connessi. **Linux** ha un ottimo firewall interno. Chi usa Linux può saltare questo capitolo.

Ma, ricordando che lo scopo dell'Igiene Informatica, non è strettamente la sicurezza, dobbiamo notare che un buon firewall non deve controllare soltanto «**chi entra**», ma anche «**chi esce**» dal nostro pc.

Dalla versione XP service pack 2 anche windows ha un firewall integrato che dovrebbe funzionare bene. Dico «dovrebbe» perché non è software Open Source, non conosciamo il codice sorgente e quindi dobbiamo fidarci della parola del produttore. Speriamo bene.

Facciamo un po' di chiarezza: il firewall **non** protegge dai virus, **non** protegge la navigazione web, **non** controlla la posta elettronica. Il suo lavoro è quello di **prevenire gli accessi indesiderati** al nostro computer.

Un **buon** firewall deve monitorare sia le connessioni **in ingresso** sia le connessioni **in uscita**. Il firewall integrato nei nuovi windows **non avverte** quando i programmi, a nostra insaputa, si connettono a server remoti.

Ecco un firewall Libero (licenza GPL): iSafer (https://sourceforge.net/projects/isafer/) e uno **non-Libero**, ma gratuito: Comodo Free Firewall (http://www.personalfirewall.comodo.com/) . iSafer è un programma molto più scarno e meno aggiornato di Comodo. In attesa di un ottimo firewall Libero si

consiglia Comodo Free Firewall.

Prima di connettere il vostro nuovissimo «unico sistema operativo sensibile ai virus(TM)» installa il firewall, lascia gli avvisi attivi, e naviga per vedere quanti impiccioni ci sono.

Avvia il media player e vedi che cerca di uscire sul web (per fare cosa??) a tua insaputa. Ma il firewall ti avviserà e potrà impedire che il media player vada a giro a raccontare non si sa cosa su di te a non si sa chi.

Raccolta di firewalls (http://www.thefreecountry.com/security/firewalls.shtml) (molti non-Liberi).

Posta: come e perché (formati, netiquette, sicurezza)

La posta elettronica è senza dubbio l'anello più debole della sicurezza informatica:

1. è un canale per ricevere e diffondere virus
2. è utilizzata impropriamente da quasi tutti
3. è facilmente intercettabile da terzi

Installare e provare Thunderbird (http://www.mozillaitalia.it/archive/index.html#p2) . **Subito!**

Posta elettronica e virus

Microsoft Outlook è il programma più attaccabile e attaccato dai virus informatici. L'utilizzo sconsiderato degli allegati lo rende ancora più rischioso. I **virus** informatici non sono altro che **programmi**: sono pericolosi solo se qualcuno li esegue. I virus si possono eseguire solo se si utilizza il formato HTML per visualizzare i messaggi o se si utilizzano allegati.

Problema 1: Nel paragrafo "browsers" vediamo come il formato HTML può contenere piccoli programmi Java o Javascript auto-eseguibili. Appena leggiamo un messaggio, bello e colorato, possiamo inconsapevolmente scatenare un virus sul nostro pc e diffonderlo a tutte le persone che abbiamo memorizzato in rubrica.

Rimedio 1: Se invece del "formato HTML" utilizziamo il "formato Testo", non si trasmettono i virus inclusi nell'HTML. Il formato testo è meno carino (è come scrivere sul programma "Blocco note" o "Notepad"), ma molto più sicuro. Il "formato Testo" non diffonde virus. Col "formato testo" non si può colorare il testo, non si può cambiare il tipo di carattere, non si può inserire lo sfondo, ma permette di eludere molte insidie provenienti dalla Rete.

Problema 2: I messaggi si aprono in automatico (e quindi eseguono in automatico eventuali virus!).

Rimedio 2: Disattivare "anteprima automatica" e "riquadro anteprima". Questo ci permette di vedere il mittente e l'oggetto del messaggio, prima di decidere se

aprirlo. Con Outlook express Visualizza -> layout... -> Visualizza riquadro anteprima (disattivare).

Problema 3: Con gli allegati di Microsoft Office (Word, Excel, Power Point, Access, Project) e con allegati eseguibili si possono trasmettere i virus. Questo tipo di documenti si riconosce dall'estensione alla fine del nome: .doc, .xls, .ppt, .mdb, .mpp i documenti Office e .exe gli eseguibili. Tali documenti possono trasmettere virus perché hanno la capacità di eseguire "macro", cioè piccoli programmi in Visual Basic.

Rimedio 3a: Non utilizzare allegati quando possibile, in particolare quelli menzionati. Spesso pochi secondi di copia-incolla dal documento al messaggio in formato testo evitano danni catastrofici.

Rimedio 3b: Se proprio non è possibile evitare l'allegato, almeno si eviti che sia uno di quelli citati: utilizzare il formato .pdf. Il formato pdf deriva dall'elaborazione di un file di stampa "post script", che non riesce a trasmettere virus perché non esegue programmi. Il documento pdf è difficilmente modificabile dal destinatario; quindi è da preferire ai formati di Microsoft Office, facilmente modificabili, in tutti i casi di comunicazioni definitive che non debbano essere "corrette a piacere" dal destinatario. In tutti i casi di comunicazione verso l'esterno, si consiglia l'uso del formato pdf. Il formato pdf è leggibile da chiunque indipendentemente dai programmi installati. Chiunque può scaricare gratuitamente il lettore pdf da Internet.

Rimedio 3c: Se proprio non è possibile evitare formati "a rischio", almeno disattiviamo, e chiediamo ai nostri interlocutori di disattivare le macro. Se un documento contiene macro, all'apertura, ci viene chiesto se vogliamo attivarle: scegliamo sempre no. Poi, successivamente alla verifica del funzionamento del file, o dopo una scansione con antivirus, potremmo attivarle.

Problema 4: Alcuni virus, se contenuti in documenti compressi, o "zippati" (.zip), non vengono riconosciuti dagli antivirus.

Rimedio 4a: Mantenere al minimo la dimensione dei documenti in modo da poterli inviare non zippati. Ma non è un gran rimedio.

Rimedio 4b: Poiché è buona norma ridurre sempre al minimo il traffico di rete, spesso non si può rinunciare alla compressione dei file. Quindi non accontentiamoci della scansione automatica del file .zip ma eseguiamo su tali documenti una nuova scansione antivirus SUBITO DOPO averli scompattati. In generale, per la sicurezza, inviamo e chiediamo a tutti i nostri interlocutori esterni di inviarci messaggi di posta elettronica (nell'ordine):

1. in formato testo (64 caratteri non proporzionali, o 72) 2. senza allegati 3. con allegati ".pdf" 4. con allegati che non contengano macro

Altrimenti non ci resta che vivere sperando.

Posta elettronica e riservatezza

La posta elettronica **non** è un mezzo di comunicazione riservato. La posta elettronica è facilmente **intercettabile**. Inviare un messaggio di posta elettronica non equivale a inviare una lettera chiusa ma equivale a inviare una cartolina: molti

possono leggerne il contenuto senza che né il mittente né il destinatario se ne accorgano.

Per avere la certezza che il messaggio (o un documento) non venga **letto** da nessuno che non sia il destinatario è necessaria la **crittografia**.

Per avere la certezza che il messaggio (o un documento) **provenga** esattamente dal **mittente** dichiarato è necessaria la **firma digitale**.

Per avere la certezza che il contenuto del messaggio (o di un documento) non sia stato **alterato** è necessaria la firma digitale.

Quindi, in assenza di opportuni strumenti, la posta elettronica è da considerarsi un mezzo di comunicazione **non sicuro**, da non utilizzare per comunicare informazioni che si vogliono mantenere riservate.

Dimensione dei messaggi e prestazioni

Le prestazioni della rete dipendono dal carico di informazioni che la percorrono: per la posta elettronica, in particolare, dipendono dal numero di messaggi per la grandezza di ciascun messaggio. Un messaggio enorme (1 Mb) inviato a molti utenti (10-20 o più) può sovraccaricare la rete in modo rilevante.

Il problema del sovraccarico non è solo dinamico (la consegna), ma anche di archivio.

È necessario ridurre al minimo la dimensione e il numero di destinatari di ciascun messaggio.

È necessario cancellare dalla casella di posta ogni messaggio inutile.

I messaggi di posta elettronica scritti in formato testo e senza allegati occupano pochissimo spazio.

Ecco un elenco di **buone norme** di uso della posta:

1. Non propagare messaggi del tipo "catene di Sant'Antonio". Ogni messaggio reinoltrato a più utenti si propaga in modo esponenziale, ingolfando preziose risorse di rete. La sfortuna ci assale se si lasciano circolare certi messaggi, non se si interrompe la loro azione di inutile sovraccarico.
2. Non fare il "reinoltro selvaggio" di un messaggio carino a tutti i contatti della rubrica. È meglio fare selezione.
3. Non mandare messaggi di auguri generalizzati allegando foto (in genere molto pesanti) o addirittura programmi eseguibili con animazioni: si possono diffondere virus! Negli auguri fa piacere il pensiero e che siano indirizzati personalmente e direttamente. "Auguri a tutto il mondo" è come dire "Auguri a nessuno".
4. Gli auguri e i saluti devono essere inviati, agli amici, in formato testo (quindi senza virus e con poco affaticamento delle risorse).
5. Non propagare appelli umanitari. Sono sempre falsi. Chi non crede al fatto che siano SEMPRE falsi può di volta in volta cercarne conferma su Snopes (http://www.snopes.com/) e sul servizio antibufala (http://antibufala.info/) di Attivissimo. L'unico caso noto di messaggio umanitario vero è il caso di Safia,

donna nigeriana condannata alla lapidazione. Il caso, poiché vero, è stato ampiamente promosso da TUTTI i mezzi di comunicazione.
6. Fare la manutenzione continua dei propri messaggi: cancellare i messaggi inutili.

Regole riassuntive

1. La posta **non** deve essere utilizzata come un archivio
2. Preferire il formato **testo**
3. Ridurre al minimo la **dimensione** dei messaggi
4. Fare la **manutenzione** continua della propria casella di posta: cancellare i messaggi ormai inutili.
5. **Non propagare** messaggi del tipo "catene di Sant'Antonio" o messaggi umanitari.
6. **Non** inviare messaggi **generalizzati** di auguri, soprattutto se con foto o programmi eseguibili (animazioni).

Netiquette

Etichetta in rete, documento "ufficiale" in italiano: (http://www.ietf.org/rfc/rfc1855.txt) RFC 1855

Pubblicità: un ottimo libro sulla posta elettronica: "Posta Tosta" (http://www.google.it/search?hl=it&q=posta+tosta+gianni+lombardi) di Gianni Lombardi

Le lunghe liste di **destinatari** vanno messe in **bcc**

Non si scrive TUTTO MAIUSCOLO: È COME GRIDARE IN FACCIA AL DESTINATARIO!

Non rispondere d'impulso: rileggere e riflettere

Come quotare

tanto per cominciare (http://www.krisopea.it/mvp/Quoting.htm)

Spam

Con la parola «spam» si intendono messaggi di posta elettronica non desiderati, che ci vengono inviati con insistenza. Il termine spam è stato associato a qualcosa di indesiderato e che ci viene proposto con insistenza a causa di una famosa scenetta dei Monty Python (http://www.youtube.com/watch?v=cFrtpT1mKy8) , risalente al 1970. Nello sketch, per spam intendono una famosa marca di carne in scatola (http://www.cusd.claremont.edu/~mrosenbl/spam.html) .

Le prime vittime dell'insistenza con cui arrivano i messaggi di posta indesiderata avevano bene in mente i Monty Python e hanno iniziato a chiamare spam tali messaggi.

Risorse in italiano anti-spam:

- Colinelli (http://www.collinelli.net/antispam/)
- MaxKava (http://www.maxkava.com/spam/)
- Computerville (http://www.computerville.it/spam.htm)

Si accettano consigli di risorse più aggiornate.

- Postini (http://www.postini.com/stats/) . Ottimo sito, purtroppo spaccia dosi massicce di flash.

Ordine nel computer

Metti in ordine il tuo disco!

Mantenere in ordine i propri documenti ne facilita il salvataggio periodico. Mantenere in ordine il disco velocizza il computer.

Conservazione documenti personali

È opportuno che i documenti **personali** rimangano **separati** da tutti gli altri file "di sistema". Il modo migliore è conservare tutti i nostri documenti in una sola directory (e nelle sottodirectory necessarie). In qualsiasi momento si deve poter facilmente salvare o spostare tutti i documenti personali (il sistema operativo e i programmi si potranno comunque ripristinare con una nuova installazione). La situazione ottimale è che alla directory dei documenti sia dedicata una **partizione** o unità specifica, in modo da poter sostituire o ripristinare il sistema senza intaccare i dati personali. Quanto detto è importante per l'integrità dei dati.

Per la conservazione dei dati (**backup** periodico) è importante suddividere la directory contenente i documenti personali in due sotto directory dedicate ai **"documenti non ritrovabili"** e ai "documenti ritrovabili".

I documenti **ritrovabili** (non ci si pone qua il problema della recuperabilità di un documento cancellato ma della sua reperibilità in altri luoghi, per esempio su Internet) in genere occupano molto spazio, sono però sacrificabili. Si pensi ai files audio, video e alle fotografie scaricate, ai manuali, ai documenti scaricati da applicazioni specifiche - enciclopedie, libri, riviste.

I documenti **non ritrovabili** sono quelli autoprodotti, che occupano poco spazio ma sono, in genere, **preziosissimi**.

Forse la divisione migliore è avere la directory "documenti preziosi" a sua volta sotto la directory "documenti" (o "home", come è chiamata su Linux)

Questo permette di fare agevolmente backup periodici della sola home-directory "documenti preziosi", che sarà molto piccola.

Tutto il resto può perdersi senza danno (se non il tempo perduto a ripristinare il sistema o a ri-scaricare quanto disponibile.

È inoltre opportuno situare "home" o "documenti" in una partizione (o unità) dedicata, quindi separata da tutto il resto.

I "documenti preziosi" devono essere tutti raccolti sotto la stessa directory (con eventuali subdirectory) per agevolare il rapido backup completo di tutti i dati importanti.

Anche la memoria virtuale (file di swap) memorizza dati sul disco. La situazione ottimale è dedicare una partizione (o unità) completamente al file di swap. Linux lo fa predefinito. Windows purtroppo no.

Lo spazio dedicato a eventuali cestini deve essere limitato alle reali esigenze di conservazione temporanea dei files cancellati (meno del 10 % dello spazio totale).

Ogni volta che viene spento il pc ci si deve chiedere se si è pronti a perdere tutto il contenuto dei dischi fissi. Se si è tranquilli (o perché non ci sono dati importanti o perché si hanno i backup), allora ci si è avvicinati allo scopo dell'igiene informatica.

Lo spazio su pc deve essere ottimizzato (cioè non sprecato, l'obiettivo è "spreco = 0"), ovvero ciascun documento deve essere ridotto al minimo possibile.

Diventa essenziale scrivere dei buoni documenti: di piccole dimensioni, senza includere materiale inutile, con il numero minore possibile di documenti inclusi. Utilizzare il numero minimo possibile di caratteri diversi. Evitare le immagini inessenziali.

Una parte sostanziale nella dimensione dei documenti la hanno le immagini: vanno bene le immagini .jpg, ben ottimizzate, aiutano molto il risultato finale, in termini di dimensioni.

È importante controllare ogni volta le dimensioni dei singoli file e del disco in generale.

Per Windows è necessario eseguire ogni settimana la deframmentazione del disco. Avvio -> Programmi -> Accessori -> Utilità di sistema -> Utilità di deframmentazione dischi. La prima volta può richiedere anche alcune ore. Quando il disco è in buone condizioni sono sufficienti pochi minuti.

Linux non supera quasi mai le poche frazioni percento di deframmentazione.

Per Windows è necessario eseguire ogni mese il controllo degli errori disco (in modalità standard) è ogni sei mesi il controllo approfondito (che è molto lento perché fa l'analisi fisica completa del disco.

Avvio -> Programmi -> Accessori -> Utilità di sistema -> ScanDisk

Il consiglio è di mettere le icone di questi programmi sul desktop. Basta cliccare con il destro sul menù del programma, creare un collegamento e poi trascinarlo sul desktop.

Sul desktop NON si devono memorizzare file veri e propri. Sul desktop devono esserci soltanto **collegamenti** a file memorizzati nelle directory opportune.

Pulire il pc dai files spazzatura (è priiimaveraaa...)

Il cestino deve essere svuotato periodicamente. Si può sfruttare lo svuotamento automatico completo oppure fare uno svuotamento a mano, selettivo.

La directory dei files temporanei deve essere svuotata periodicamente.

La directory dei files temporanei di Internet deve essere svuotata periodicamente.

Avvio --> Programmi --> Accessori --> Utilità di sistema --> Pulitura disco

è un programma che cancella i files superflui, come l'estetista. Purtroppo non è un nostro amico ma è al servizio dei nostri nemici: Pulitura disco dichiara di cancellare tutti i files dalla directory dei files temporanei di Internet, ma in realtà mantiene inalterati tutti i files inseriti per spiarci. Provare per credere: dopo pulitura disco, andare a vedere C:\Windows\Temporary Internet Files e vedere cosa è rimasto. Poi cancellare tutto a mano.

Sul desktop devono essere tenuti i collegamenti alla cartella detta e alla cartella C:\Windows\Temp. Entrambe devono essere spesso aperte e cancellate.

Risorse del computer Visualizza --> Dettagli Visualizza --> opzioni cartella --> Visualizza File nascosti: mostra tutti i file Non memorizzare le impostazioni di visualizzazione di ogni cartella Non nascondere le estensioni dei files Visualizzare il percorso completo Tutte come cartella corrente

Programmi per la pulizia del sistema:

1. DiskCleaner (http://www.diskcleaner.nl/) per i file sul disco e per molti file creati dal normale funzionamento dei programmi;
2. Ccleaner (http://www.ccleaner.com/) pulisce e ottimizza file e registro di windows;
3. Eraser (http://www.heidi.ie/eraser/) è utile per ripulire realmente lo spazio vuoto del disco da frammenti di file e informazioni che potrebbero essere rimaste dopo la normale cancellazione e lo svuotamento del cestino.

Autoplay

Autoplay: "Sul mio pc comando io! E tu, sporco browser, fai quello che dico io. Non fare MAI l'autoplay". Msie si preoccupa di lanciare qualsiasi nefandezza senza chiedere il permesso. Per disattivare l'autoplay…

Programmi per l'altro sistema operativo

Questo è un semplice appunto, messo qua per non dimenticare una pagina web utile: http://tech-tonic.net/microsoft/25-essential-open-source-software-for-windows.html

Cacciare le spie dal proprio pc (spyware e cookies)

Due ottimi programmi purtroppo non-Liberi, Ad-aware (http://www.google.it /search?&q=+Ad-Aware+Lavasoft+site:download.com) e Spybot - S&D (http://www.safer-networking.org/it/download/index.html) .

Installare i programmi e lanciarli spesso.

Cancellare immediatamente Gator e simili "utilità"

MSN Passport e MSN .net sono lo strumento principe per attentare alla privacy

dell'utilizzatore di Internet.

Aiuto, un virus!

Chi ha scritto finora gli appunti di Igiene Informatica non è molto esperto di antivirus e **di sistemi operativi che ne hanno bisogno**. Si cercano consigli su quali antivirus installare. Chiediamo esperienza diretta e personale.

- antivirus Libero, GPL: clamwin (http://www.clamwin.net/) basato su ClamAV
- integrazione per rendere ClamWin un antivirus real-time: winpooch (http://winpooch.free.fr/)
- antivirus Libero on-line (ancora clamAV (http://it.clamwin.com/content/view/85/82/))
- antivirus portabile (su cd o chiave usb) per controllare pc già infetti (ancora Clamwin Clamwin (http://portableapps.com/apps/utilities/clamwin_portable))

Ormai **non ha più nessun senso** utilizzare antivirus non-Libero, anche se gratuito.

L'antivirus è la più importante difesa contro le vulnerabilità di windows.

Linux non necessita di antivirus: **non sono noti** virus informatici per Linux effettivamente funzionanti.

È necessario impostare l'aggiornamento automatico dell'antivirus almeno una volta a settimana.

È necessario eseguire la scansione di tutti i documenti di tipo "Office", di tutti i dischetti e di tutti i cdrom che provengono dall'esterno.

BIOS: le parti intime del computer

Metafore a parte, è importante conoscere anche il minimo della identita del nostro pc.

BIOS: Basic Input-Output Sistem (sistema basilare di ingresso e uscita di informazioni).

È l'identità del pc perché esiste comunque, anche se togliamo i programmi, anche se togliamo il sistema operativo, anche se togliamo i dischi - tutti.

Il BIOS risiede in una piccola memoria permanente sulla scheda madre.

All'accensione, prima di avviare il sistema operatvo, i PC visualizzano una serie di informazioni, generalmente scritte bianche su sfondo nero, tra queste c'è un avviso che spiega come accedere alle impostazioni del BIOS.

Bisogna agire in fretta:

- capire quale tasto (o combinazione) premere
- premerlo **subito**

I tasti variano a seconda dei casi, di solito è sufficiente premere il tasto "Del"

("Canc", sulle tastiere italiane), oppure "F1".

A volte sono richiesti altri tasti o combinazioni di tasti: "F2", "F8", "Ctrl"+"F1", "Ctrl"+"F2"

In casi rari si deve premere la barra spaziatrice o il tasto "tab" o il tasto "Esc". Raramente però.

Entrare, leggere le opzioni per la navigazione e uscire **SENZA** salvare eventuali modifiche.

Imparare soltanto a cambiare l'ordine dei dispositivi di avvio!

Sicurezza informatica e test d'ignoranza

Se non fai parte della soluzione fai parte del problema

Contributo degli utenti comuni alla sicurezza di un sistema informatico complesso

Password

Le caratteristiche fondamentali delle parole chiave o password informatiche sono: la complessità e la segretezza.

I migliori sistemi sono organizzati in modo tale che neppure l'amministratore può conoscere le password dei singoli utenti. Può cancellarle, può sostituirle ma non può conoscerle. La password, se non rivelata a nessuno, rende univoco il riconoscimento dell'utente: nessuno può fare errori a nome di un altro se non gli è stata rivelata la password.

La password NON deve essere rivelata a nessuno.

Se la password dovesse essere scoperta da altri, deve essere sostituita immediatamente.

La componente principale della sicurezza di una password è la sua COMPLESSITÀ. Ci sono programmi per scoprire le password informatiche, ecco per esempio una prova fatta dal Nucleo di Polizia Postale Italiana (2001).

Su un computer ordinario (Pentium II, 450 MHz, che permette 98.000 tentativi al secondo) il tempo necessario per scoprire una password con un attacco del tipo "a tentativi" è:

2 minuti per una password di 5 lettere tutte minuscole;

fino a 2000 anni per una password di 8 caratteri scelti tra lettere, numeri e alcuni simboli.

Per prevenire accessi, anche casuali, di non incaricati tramite il nostro computer è opportuno impostare la password del salvaschermo e impostare un ritardo prima dell'attivazione non superiore a 3 minuti.

Riassumendo: La password deve essere SEGRETA La password deve essere CAMBIATA frequentemente La password, se scoperta, deve essere CAMBIATA immediatamente La password deve essere COMPLESSA (otto o più caratteri misti) Il SALVASCHERMO deve essere protetto da password Il bios deve essere protetto da password Il pc deve avere l'avvio bloccato da password

Provare john the ripper

Ignoranza

Inizialmente si è sempre consapevoli che non conosciamo quasi niente della nuova materia che stiamo affrontando. Dopo poco si comincia ad avere la sensazione di orientarsi benino nel nuovo mondo. Appena si conoscono tutti i segreti dell'ambiente che ci circonda, e ci consideriamo esperti, …è solo arrivato il momento di uscire dal giardino di casa e esplorare il mondo.

Per sapere se stiamo ancora esplorando il giardino basta fare il seguente **test**

Test

Elenco delle piattaforme esistenti

Proviamo a misurare misurare la propria conoscenza della ricca molteplicità presente nel mondo informatico. Prima di procedere si devono elencare qua sotto: tre marche di processori, tre sistemi operativi (OS), tre client di posta, tre elaboratori di testi, tre fogli di calcolo.

- Processori Sistemi operativi Client di posta Elaboratori di testi Fogli di calcolo

1) ……. ……. ……. ……. …….

2) ……. ……. ……. ……. …….

3) ……. ……. ……. ……. …….

A esempio della vasta (e spesso sconosciuta) biodiversità informatica si elencano un po' di programmi e di hardware

Processori: Intel, AMD, Sparc, Risc,

Sistemi operativi: Linux (rpm), Linux (apt), Linux (slack), OpenBSD, FreeBSD, BeOS, FreeDOS, Solaris, Mac OS, Mac OS X, OS/2, OS/400, Aix, HP…, SCO Unix, …, …, …, MSDOS, Windows NT/2k, Windows 9x/ME/XP.

Interfacce grafiche: KDE, Gnome, Altri WM, …, …,

Client di posta: Kmail, Mozilla, Mutt, Pine, Netscape, Eudora, Opera, Sylpheed, Evolution, Lotus Notes, Star Office 5.x, …, …, …, Microsoft Outlook, Outlook Express.

Elaborazione testi: OpenOffice Write, Star Office Write, Kword, Abiword, …, …, …, …, …, Microsoft Word

Fogli di calcolo: OpenOffice Calc, Star Office Calc, Kspread, Gnumeric, …, …, Microsoft Excel.

Diritti digitali

Accesso ai mezzi di comunicazione

Diritto all'accesso alla comunicazione

Diritto all'accesso alle informazioni

Qua si ritiene che le informazioni e la possibilità di comunicare **non** siano delle **merci**, ma siano dei **diritti**.

Tecnocontrollo

```
Cosa e' il tecnocontrollo
"Roba da paranoici"
Dai Faldoni a Echelon
Database
Telecamere
Internet
Gli oggetti intelligenti
Decoder e Box Interattivi
Trusted computing
Prospettive
```

«La Piccola Bottega degli Errori»

…NON è un musical ;-)

Presentato la prima volta al Convegno e-privacy 2003 (Firenze).

Poche illusioni: trattasi di «pannicelli caldi» ovvero poco efficaci. Le soluzioni reali ai problemi posti qua sono ben altre. La piena consapevolezza di quanto scritto di seguito potrebbe portare però l'utente a migliorare il suo comportamento in Rete e fare qualche passo ragionevole in direzione delle soluzioni «vere», che comunque riteniamo un po' più difficili.

Intanto…

Difendiamoci da noi stessi

La prima minaccia alla nostra riservatezza siamo noi stessi.

Spesso compromettiamo inconsapevolmente la riservatezza altrui.

Primo errore: pensare che agli altri non interessi quello che facciamo

La riservatezza degli altri

Tutelare la privacy degli altri (che é importante quanto la nostra).

Evitare tutte quelle azioni che, pur non mettendo direttamente a rischio la propria privacy, comportano pericoli per quella dei conoscenti (es: dare liberamente indirizzi mail di amici o iscriverli a mailing-list e servizi internet senza il loro consenso)

Errori al computer

1. Usare sistemi poco sicuri per navigare in internet pensando che gli altri non possano sapere quali siti andate a visitare (magari solo perché cancellate la history)
2. Usare la stessa password per servizi diversi su host diversi
3. usare strumenti come passport o gator
4. Mettere una password nel BIOS e, solo per questo, sentirsi al sicuro
5. Giocare online. Che dettaglio psicologico si può tirare fuori da una persona osservandola mentre gioca (tra le altre cose pensando di non essere vista)?
6. Controllare che documenti tipo MS-Office non contengano dati personali, che di solito sono automaticamente inseriti nelle proprieta' del documento
7. Lasciare condivisioni aperte a tutto il mondo con netbios

Crittografia debole

1. Errore: usare sistemi di crittografia debole tra cui:

- Salvare le proprie password nel registro di windows pensando che siano al sicuro
- Proteggere con password i profili di programmi di posta che usano crittografia debole (outlook?)

Fidarsi del proprio amministratore di sistema Navigare su internet o inviare email dal computer dell'azienda pensando che nessuno sappia o legga

gestione utenti

Entrando come utente su un sistema informatico il nome utente deve avere meno informazioni possibile sulla identità' che voglio proteggere i cookies si chiamano mariorossi@ads.wanadooregie:mariorossi@ads.wanadooregie>[1].txt Quindi se mi sono loggato con "mariorossi" come utente e' inutile firmarsi "Zorro"

Posta

Non cliccare sui link che arrivano con gli spam (tanto cosa vuoi che succeda…) perché non sono link normali ma sono del tipo <http://bella.salamona.it /script.php?id=ASFRASE435waeaw43wa3> che passano un id allo script, e penso

proprio che sia unico per ogni email che inviano

Non inviare messaggi con molti destinatari in campo "A:" oppure "CC:", ma usare "BCC:": non difende la privacy del soggetto che scrive, ma quella del destinatario che altrettanto degna di essere difesa.

Non inserire i dati dei nostri conoscenti nella rubrica del proprio pc. Spesso si ha una pazienza infinita nel fare cose dannose per gli altri… Usiamo meglio la pazienza.

Ancora posta

Non cambiare il nome del destinatario nell'indirizzo di posta (esempio: il mio amico Mario usa gli indirizzi

1. <zorro@tin.it> e
2. <mario.rossi@libero.it>

non devo salvarli in rubrica come

1. Mario Rossi" <zorro@tin.it> e
2. "Zorro" <mario.rossi@libero.it>

ma come

1. "Zorro" <zorro@tin.it> e
2. "Mario Rossi" <mario.rossi@libero.it>

Se mi scrive Zorro, in pubblico (cioè su una lista di discussione), non lo saluterò dicendo "Ciao Mario" ma "Ciao Zorro". Si risponde come l'altro si firma.

Browser

Convincere il proprio browser/gestore di posta a non caricare immagini che non arrivino dal dominio che si sta visitando o dall'email aperta per evitare web-bugs.

Non fidarsi di quei siti che hanno una fase di autenticazione cifrata con https e poi rimandano ad una connessione in chiaro per lo scambio vero dei dati(?)

Attenti ai link su cui si clicca. La gente normalmente non distingue tra quello che c'è' scritto nel link e il link vero a cui si riferisce la scritta. Disabilitare il javascript che cambia il testo nella barra di stato.

Quindi mai andare sul sito della propria banca passando da un link trovato su un altro sito,

attenzione a link del tipo www.miabanca.com@216.217.21.13 <>, oppure al cross-site-scripting.

un'altra cosa che abbiamo accennato ma di cui non so dare riferimenti precisi sono gli header che il browser invia quando ci si connette ad una pagina indicando la pagina da cui si proviene (referer:). Sono quelli che permettono di scrivere nei contatori il sito di provenienza. La conseguenza più semplice è che si invia una traccia di dove si è stati, quella più complicata (e che forse riguarda più i

programmatori) è che si rischia che l'ultimo link visitato fosse qualcosa del tipo: http://www.banca.com/index.php?userid=ciccio&passwd=franco che è peggio

File sharing

Fare sempre molta attenzione ai programmi di sharing files: spesso richiedono la mail del soggetto, inutile dire che non è il caso di fornirla.

Non mettere mai in condivisione cartelle senza aver ben chiaro il loro contenuto e spostare i files scaricati ritenuti di interesse strettamente personale: da una visione anche sommaria dei files presenti su un hard disk si ottiene subito un quadro chiarissimo del profilo della persona che sta dall'altra parte del monitor.

Firma di documenti

Attenzione ai documenti che firmiamo i seguenti due link sono particolarmente esplicativi: <http://www.interlex.it/testi/dm030320.htm> e <http://www.sikurezza.org/ml/09_02/msg00054.html> il primo e' il testo della legge sulla firma digitale, che dice: «I documenti digitali conformi devono essere prodotti con procedimento tecnico che dia garanzia della riproduzione fedele e duratura del contenuto dei documenti originali; tale procedimento potrà consistere sia nella memorizzazione digitale dell'immagine del documento analogico originale, sia nella riproduzione su file (in formato "PDF" o "TIF")»

il secondo è un thread su sikurezza.org dove si parla del pericolo di firmare documenti con campi variabili (che, secondo il thread, possono essere inseriti anche nei PDF). Indipendentemente dal valore legale firmare un oggetto strano, per esempio un binario, non lega la propria firma a quello che viene visualizzato.

Tecniche avanzate

La materia «Igiene Informatica» non è, non vuole essere e non sarà una materia «per esperti» informatici. Ma non è nemmeno una materia per **stupidi**!

Ovvero parleremo, in maniera **tecnicamente semplice** e descrittiva, di temi complessi, culturalmente, eticamente e socialmente complessi. Non riteniamo che sia un compito facile.

L'Igiene Informatica è decisamente un tema «per adulti», nel senso di maturità e di pienezza che questo termine può evocare.

Crittografia

```
Scrittura segreta e scrittura nascosta
cenni di steganografia e perche serve a poco
cenni storici sulla crittografia
algoritmi crittografici ed hash
crittografia a chiave privata
crittografia a chiave pubblica
firma elettronica
cenni su valore legale e dispositivi di firma
certificati digitali
PKI e certificatori
Web-of-trust
Pgp, fondamenti
Uso di GPG
```

Introduzione a Privacy ed Anonimato elettronico

```
perche' l'anonimato
anonimato, diritti civili e liberta' di espressione
"non siamo la Banda Bassotti"
"ma tanto io non ho niente da nascondere"
"io ho il coraggio delle mie azioni"
Sistemi per l'anonimato informatico
anonymous remailer
pseudonym server
sistemi di pubblicazione anonima
proxy anonimizzatori: da Crowds a Tor e Privoxy
```

proxy anonimizzatori: da Crowds a Tor e Privoxy

Ecco un primo assaggio su come attivare la navigazione anonima sul nostro computer. Teniamo i consigli di Marco nella **massima** considerazione: è una risorsa preziosissima.

Usare TOR: prima lezione (http://punto-informatico.it/p.aspx?i=2070093) .

Remailer Anonimi

```
Penet, Cypherpunks, Mixmaster, Mixminion
Interfacce: Mixmaster, Quicksilver, Jack B. Nymble
Uso di Mixmaster
Uso di Mixminion
Pseudonym server: Penet, Newnym, Nymbaron
Uso di NewNym con JBN
Cenni su Nymbaron
```

Sistemi di pubblicazione anonima

```
Sistemi di pubblicazione anonima e diritti civili
Publius
Ethernity
Freenet
Ants
Entropy

Cenni sulle darknet
```