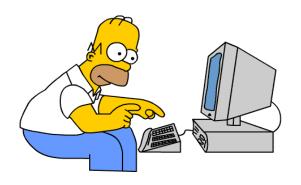
I MINORI E LE NOOVE TECNOLOGIE

GUIDA PRATICA PER GIOVANI NAVIGANTI



Quali sono queste nuove tecnologie?

1) IL COMPUTER



2) IL TELEFONINO



PER COSA USI IL COMPUTER?

- 1) fare i compiti
- 2) fare ricerche su internet
- 3) chattare con gli amici; visitare social network
 - 4) ascoltare musica
 - 5) ricevere e scrivere e-mail
- 6) guardare, modificare o pubblicare le foto ed filmati di amici

E PER COSA USI INVECE IL TELEFONINO?

- o 1) chiamare gli amici
 - o 2) chiamare a casa
- 3) mandare i messaggi (sms)
- 4) scambiare contenuti multimediali (filmati mp3..)
- o 5) produrre contenuti multimediali (foto, filmati)
 - o 6) collegarsi a internet col WAP

On line, come nella vita di tutti i giorni, abbiamo diritti e doveri ...

I NOSTRI DIRITTI NELLA RETE

- Hai il diritto di proteggere la tua identità online
- Hai il diritto di partecipare, divertirti e trovare tutte le informazioni adeguate alla tua età e personalità
- Hai il diritto di esprimerti liberamente quando sei online sempre nel rispetto degli altri
- Hai il diritto di essere ascoltato e trattato con rispetto

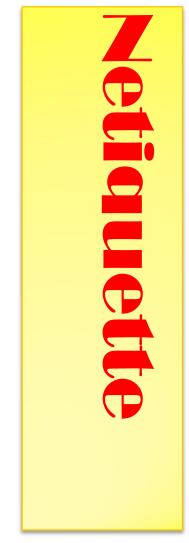
E ANCORA...

- Hai il diritto di proteggere tutto ciò che è frutto della tua creatività... ovunque, anche nel web!
- Hai il diritto di essere critico e di mettere in discussione tutto quello che leggi o che trovi quando sei online
- Hai il diritto di utilizzare le Nuove Tecnologie per sviluppare la tua personalità e le tue capacità
- o Hai il diritto di proteggerti da virus e spam

I DOVERI: NETIQUETTE

- o in un nuovo newsgroup o in una nuova lista di distribuzione via posta elettronica, è bene leggere i messaggi che vi circolano per almeno due settimane prima di inviare propri messaggi in giro per il mondo: in tale modo ci si rende conto dell'argomento e del metodo con cui lo si tratta in tale comunità;
- o non usare i caratteri tutti in maiuscolo nel titolo o nel testo dei tuoi messaggi, nella rete questo comportamento equivale ad "urlare" ed è altamente disdicevole;
- o non divagare rispetto all'argomento del newsgroup o della lista di distribuzione; anche se talvolta questo comportamento è accettato o almeno tollerato aggiungendo il tag [OT] (cioè Off Topic che significa "fuori argomento") nell'oggetto del proprio messaggio.

- Non pubblicare mai, senza l'esplicito permesso dell'autore, il contenuto di messaggi di posta elettronica o privati.
- Non pubblicare foto o filmati altrui;
- Non pubblicare messaggi stupidi o che semplicemente prendono le parti dell'uno o dell'altro fra i contendenti in una discussione..
- non inviare tramite posta elettronica messaggi pubblicitari o comunicazioni che non siano stati sollecitati in modo esplicito;
- o non essere intolleranti con chi commette errori sintattici o grammaticali, chi scrive, è comunque tenuto a migliorare il proprio linguaggio in modo da risultare comprensibile alla collettività;



violare la sicurezza di archivi e computer della rete; violare la privacy di altri utenti della rete, leggendo o intercettando la posta elettronica loro destinata o violando i loro account; compromettere il funzionamento della rete e degli apparecchi che la costituiscono con programmi (virus, trojan horses, ecc.) costruiti appositamente; costituiscono dei veri e propri crimini elettronici e come tali sono punibili dalla legge;

APPLICHIAMO IL DIRITTO...



Le chat...

Cosa significa chattare?

• Quando chattiamo?

o I pro e i contro delle chat



- Dalla wikipedia...
- o Il termine **chat** (in <u>inglese</u>, letteralmente, "chiacchierata"), si riferisce a un'ampia gamma di servizi sia <u>telefonici</u> che via <u>Internet</u>.
- Gli elementi della chat: il dialogo avviene in tempo reale; si possano mettere facilmente in contatto perfetti sconosciuti, generalmente in forma essenzialmente anonima.
- Il "luogo" (lo spazio virtuale) in cui la chat si svolge è chiamato solitamente *chatroom* (letteralmente "stanza delle chiacchierate"), detto anche *channel* (in italiano *canale*), spesso abbreviato *chan*.

IL NICKNAME...

è un soprannome che si usa online e che sostituisce il nome vero per proteggere la propria privacy. È meglio evitare di usare nick con riferimenti alla propria identità reale, come l'anno di nascita, la città di provenienza. Possiamo usarlo per nascondere la nostra identità. Non possiamo sapere chi c'è dall'altra parte...

es. consigliato: giusystar (senza riferimenti di età o luogo)

es. sconsigliato: gigetto98 (con riferimenti di età)

I TIPI DI CHAT ...

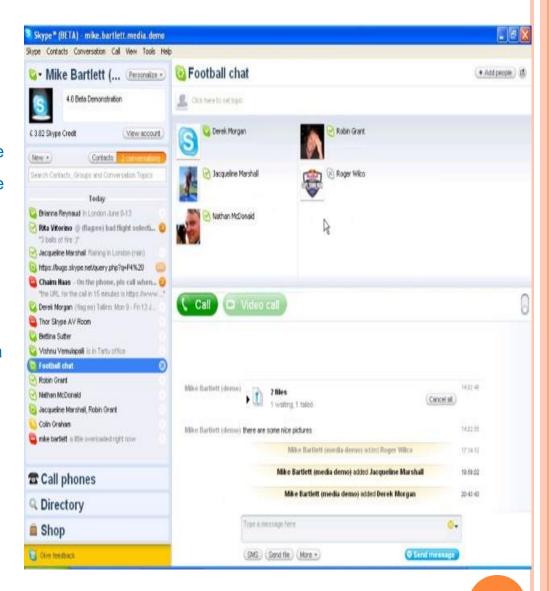
- Forum: è una pagina web nella quale si incontrano persone che hanno interessi simili per partecipare attivamente a discussioni inerenti la tematica del forum stesso. Le discussioni si sviluppano attraverso il succedersi dei commenti.
- o icq è uno dei primi sistemi di Instant Messaging, più diffuso in America che in Europa, con cui ogni utente registrato, tramite uno Universal Internet Number (UIN una sorta di codice di identificazione nel server ICQ), viene avvisato se qualcuno compreso nella sua contact list (una rubrica contatti di altri utenti ICQ) lo sta cercando per comunicare istantaneamente via internet.

E POI...

sistema Instant Messaging più diffuso tra i giovani, permette la comunicazione online via testo, via voce, o via web cam tra 2 persone o tra un gruppo di persone in tempo reale. Per poter entrare in contatto, le persone devono essere reciprocamente inserite nelle rispettive liste di contatti. Avere una lista contatti MSN molto folta è divenuto quasi una sorta di status symbol tra i giovani, una specie di riconoscimento della propria socialità.



- o **SKYPE**: è un programma sempre più diffuso con cui è possibile parlare via internet con chiunque in qualsiasi parte del mondo a costo zero. Se ambedue gli utenti hanno una webcam possono anche video chiamarsi online. Skype inoltre offre anche la possibilità di chattare con i propri contatti fino ad un massimo di 100 persone contemporaneamente.
- Con Skype si possono chiamare dal proprio pc anche telefoni fissi e cellulari a costi veramente vantaggiosi rispetto alla rete fissa.



I SOCIAL NETWORK

• Una rete sociale (in inglese social network) consiste di un qualsiasi gruppo di persone connesse tra loro da diversi legami sociali, che vanno dalla conoscenza casuale, ai rapporti di lavoro, ai vincoli familiari. (wikipedia)

I SOCIAL NETWORK PIÙ DIFFUSI...

OFacebook.

OTwitter.

OMsn.

• Myspace.

FACEBOOK

o Facebook è un sito web di reti sociali, di proprietà di Facebook, Inc., ad accesso gratuito. È il secondo sito più visitato al mondo, preceduto solo da Google. Il nome del sito si riferisce agli annuari con le foto di ogni singolo soggetto (facebook) che alcuni <u>college</u> e scuole preparatorie <u>statunitensi</u> pubblicano all'inizio dell'anno accademico e distribuiscono ai nuovi studenti ed al personale della facoltà come mezzo per conoscere le persone del campus. Secondo i dati forniti da Mark Zuckerberg stesso, nel luglio <u>2011</u> il numero degli utenti attivi ha raggiunto quota 750 milion

UN PO' DI STORIA..

- Facebook è stato fondato il <u>4</u> <u>febbraio</u> <u>2004</u> da <u>Mark Zuckerberg</u> all'epoca studente diciannovenne presso l'<u>università di Harvard</u>, con l'aiuto di Andrew McCollum e Eduardo Saverin.
- o Il sito è gratuito per gli utenti e trae guadagno dalla <u>pubblicità</u>, inclusi i <u>banner</u>.

FACEBOOK... LE PROBLEMATICHE.

• PRIVACY

• CYBER BULLISIMO

• PROPRIETA' INTELETTUALE E COPYRIGHT

PRIVACY

Quando pubblichiamo su Fb i nostri dati dobbiamo essere consapevoli che possono essere visibili e conoscibili da tutti informazioni personalissime che non dovrebbero essere conosciute da chicchessia: es. indirizzo, numeri di telefono, scuola... etc

 Non pubblicare MAI informazioni relative alla nostra città, abitazione e scuola:

- Non rendere visibili a tutti le nostre foto;
- Non accettare le richieste di amicizia di persone sconosciute;
- Bloccare e segnalare le persone che ci infastidiscono sulla rete.



SEMPRE SULLA PRIVACY....















Scrivi un commento...

Attività recenti



Laura ha cambiato la sua immagine del profilo.



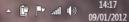
€ per i tuoi anni di specializzazione non riconosciuti. Aderisci anche tu alla causa collettiva con Consulcesi.

Tazza Obiettivo enjoymedia.ch

Se siete dei fotografi







14:17









Mary Raf

ForliCesena











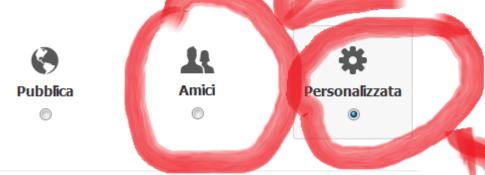
Controlla la privacy ogni volta che pubblichi qualcosa

Puoi gestire la privacy dei tuoi aggiornamenti di stato, foto e informazioni usando lo strumento di selezione del pubblico, quando li condividi o in un secondo momento. Ricorda: le persone con cui condividi possono sempre condividere le tue informazioni con altri, comprese le applicazioni. Provare a modificare il tuo profilo per vedere come funziona o maggiori informazioni.



Controlla la tua privacy predefinita

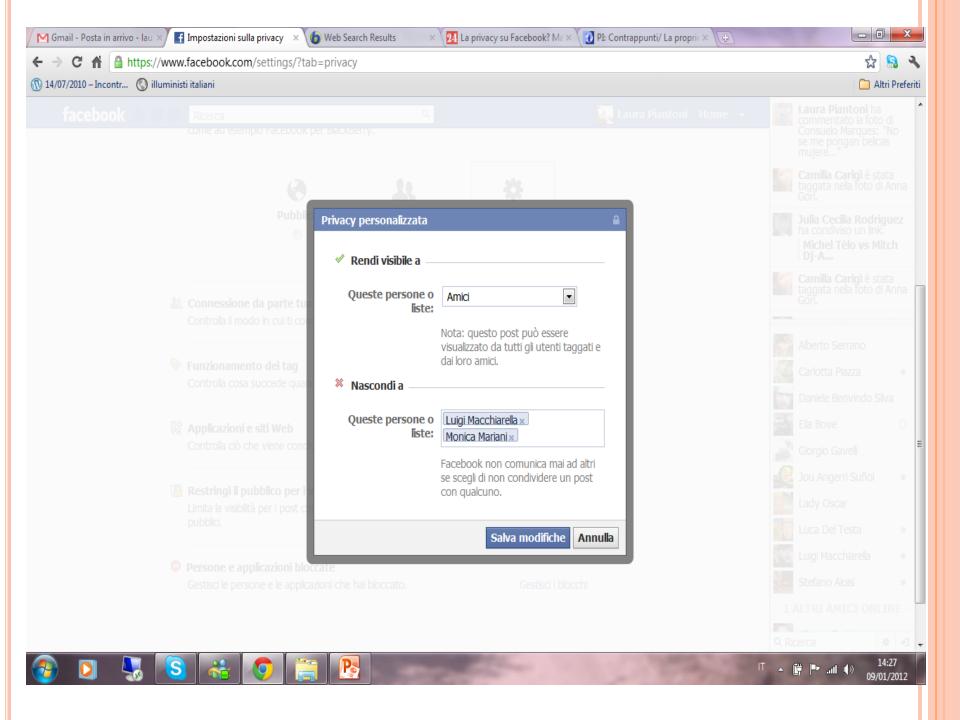
Questa impostazione viene applicata anche agli aggiornamenti di stato e alle foto che pubblichi sul tuo profilo da un'applicazione Facebook che non dispone dello strumento di selezione del pubblico in linea, come ad esempio Facebook per BlackBerry.

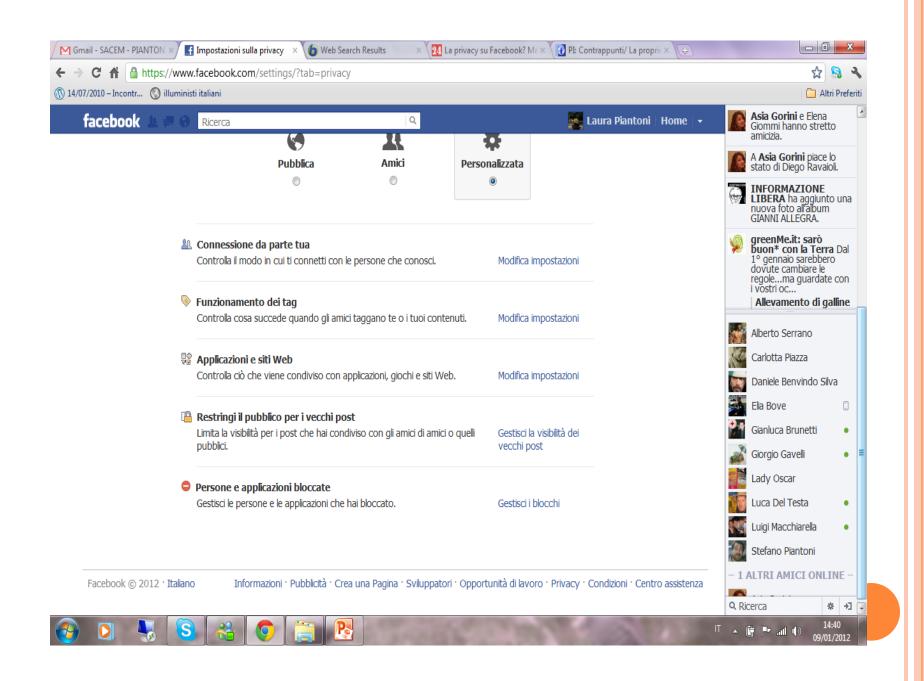


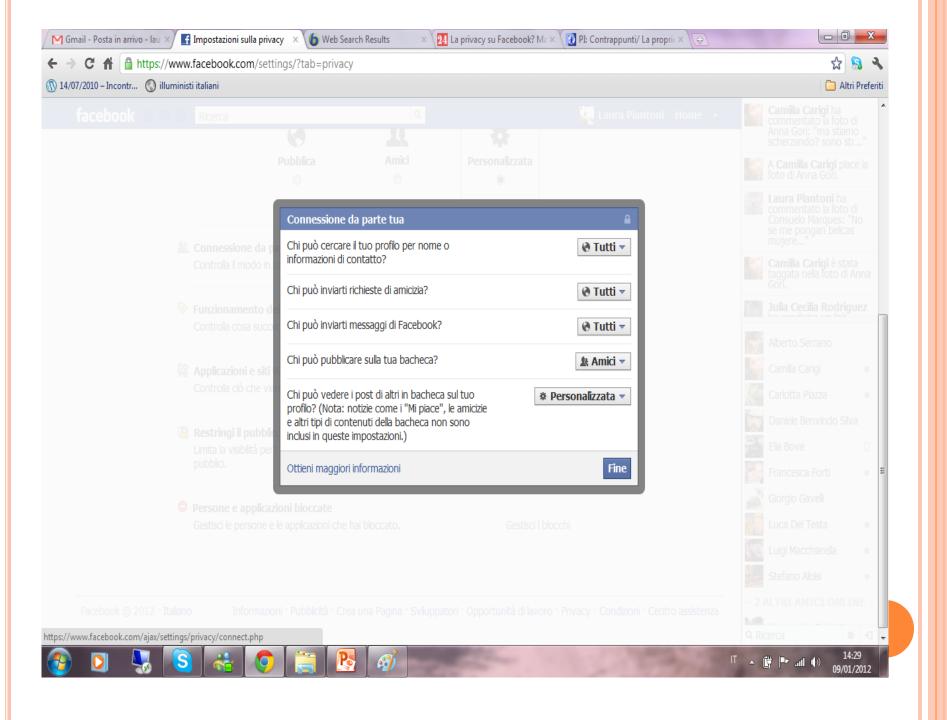
& Connessione da parte tua

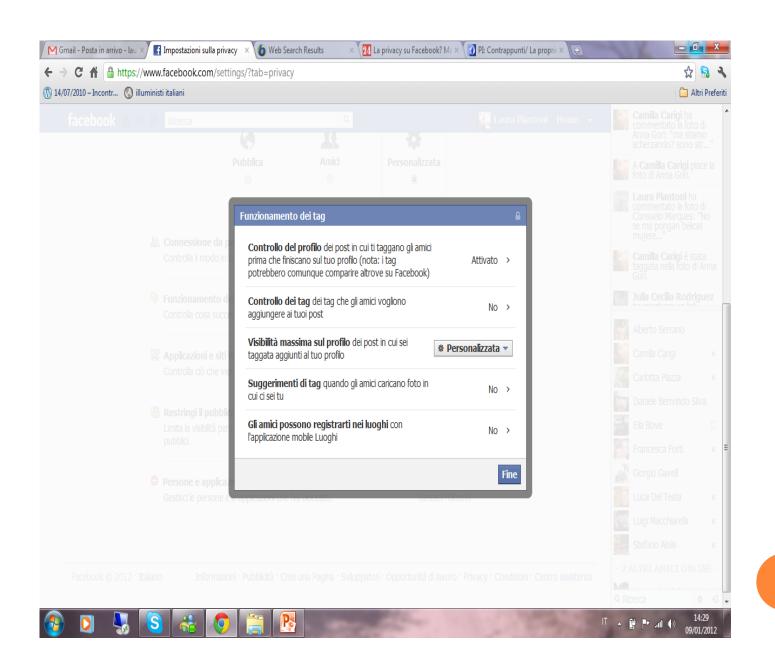
Controlla il modo in cui ti connetti con le persone che conosci.

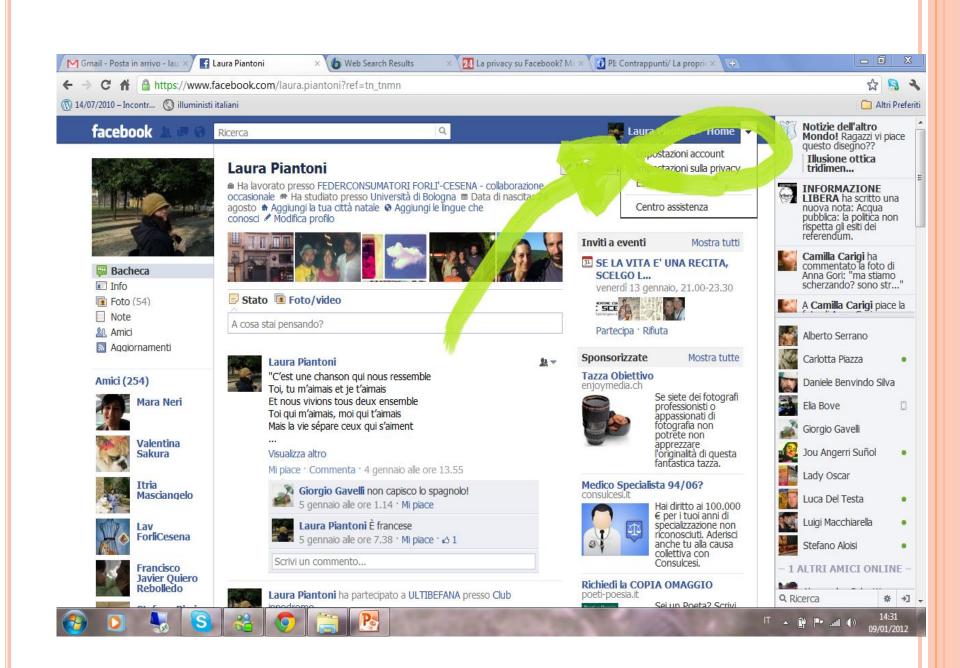
Modifica ir

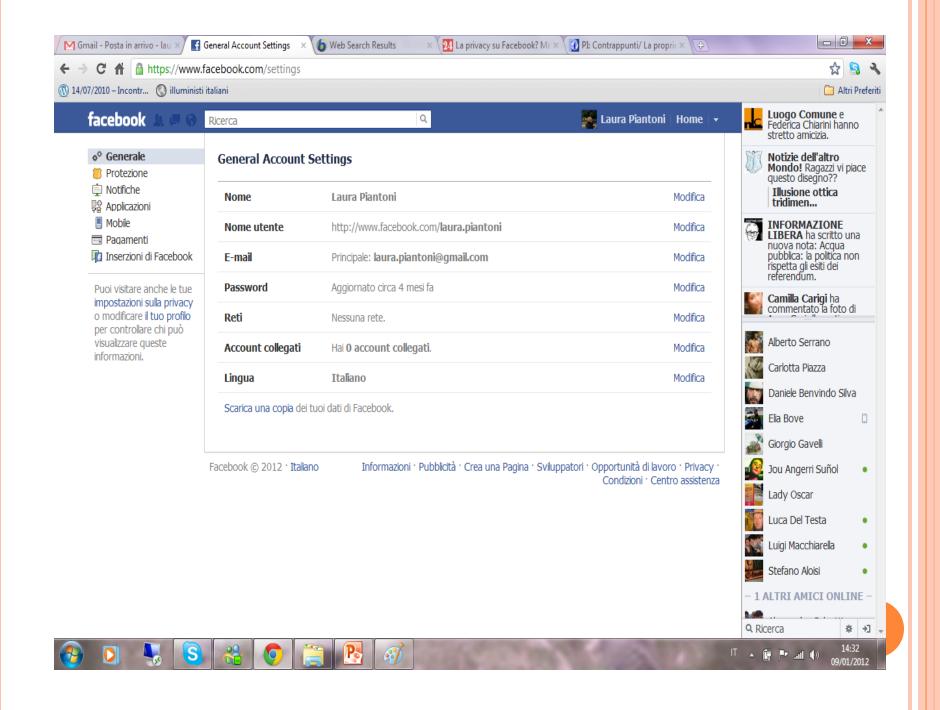


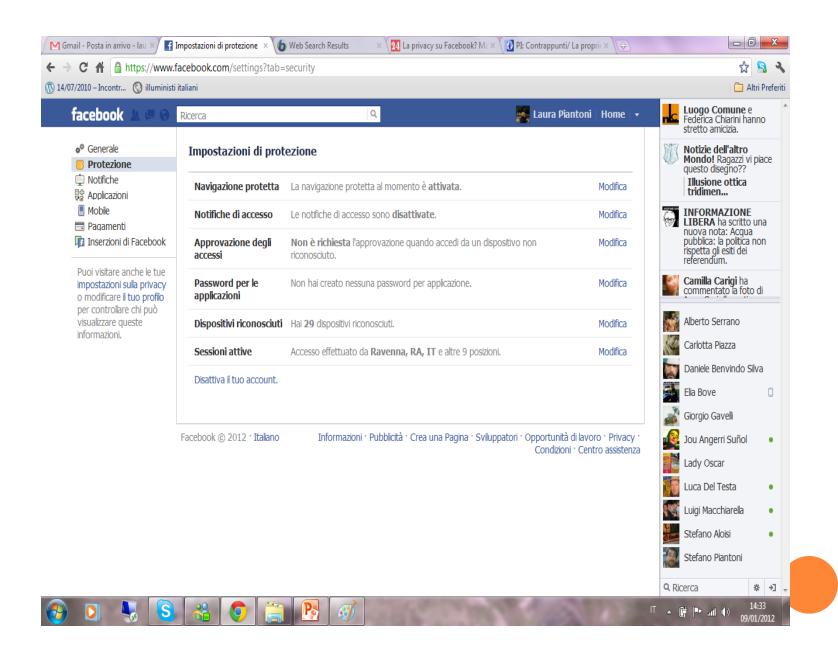


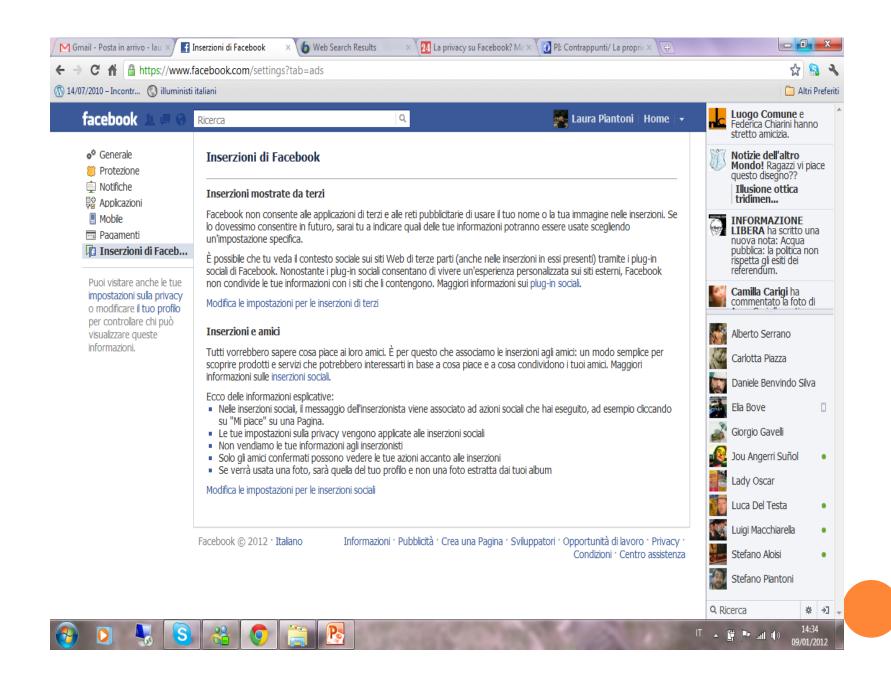


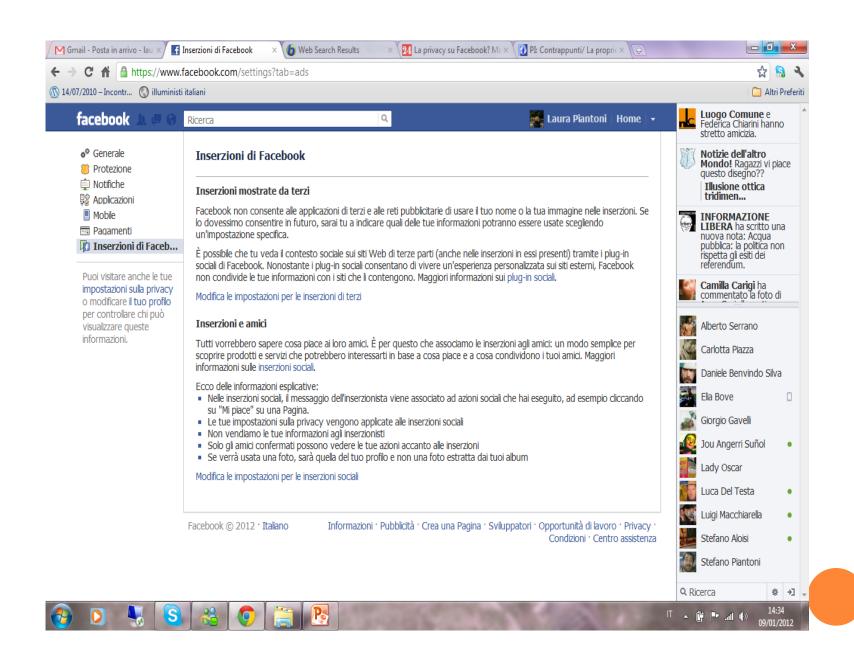


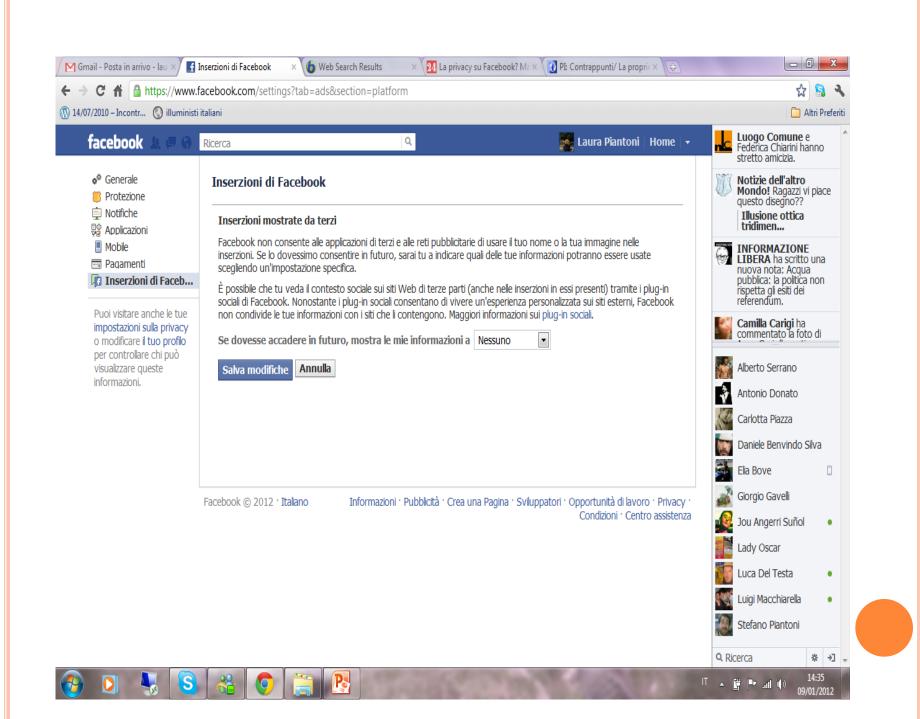


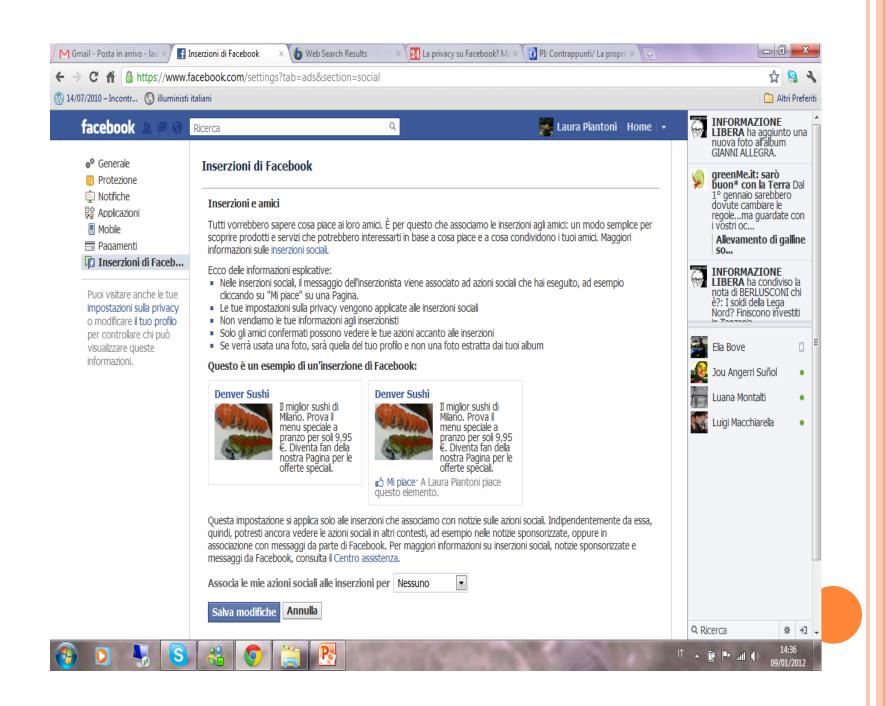














LE COSE DA EVITARE...

I rischi...

Furto dati personali e lesione della privacy;

Adescamenti e truffe

o Virus...

FURTO DI IDENTITÀ



- Nel momento in cui ci si registra in una Chat, vengono richieste numerosi dati personali che se si diffondono potrebbero essere usati in modo improprio Acquisti on line, diffamazione, ulteriori registrazioni etc.
- Non fornire mai i propri dati (o quelli di un amico) né in fase di registrazione né successivamente in chat room, né in privato né in pubblico.



PARLIAMO DEI MALWARE

Genericamente chiamati virus? Cosa sono? Quali sono i danni?

Un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito. Il termine deriva dalla contrazione delle parole inglesi malicious e software e ha dunque il significato letterale di "programma malvagio"; in italiano è detto anche codice maligno

SINTOMI...

- □ Il sistema operativo non viene avviato, sebbene non siano state apportate modifiche al sistema o non siano stati installati o rimossi dei programmi.
- È presente un'insolita attività del modem. Se si dispone di un modem esterno, si potrebbe notare il lampeggiamento continuo delle spie luminose, benché il modem non sia utilizzato in quel momento. È possibile che si stia inconsapevolmente trasmettendo software illegale.
- □ Il Sistema operativo non viene avviato, perché mancano alcuni importanti file di sistema. Inoltre, viene visualizzato un messaggio di errore che elenca i file mancanti.

□ Talvolta il computer viene avviato come previsto. Tuttavia, altre volte il computer si blocca prima che vengano visualizzate le icone del desktop e della barra delle applicazioni.

□ Le prestazioni del computer sono notevolmente rallentate. Inoltre, l'avvio del computer richiede più tempo del previsto.

□ Vengono visualizzati messaggi di errore che indicano "Memoria insufficiente", sebbene la quantità di RAM disponibile nel computer sia sufficiente.

- Nuovi programmi installati non correttamente.
- □ Si verifica il riavvio automatico di Windows in modo imprevisto.
- □ I programmi che in precedenza funzionavano correttamente si bloccano spesso. Anche se i programmi vengono rimossi e reinstallati, il problema persiste
- □ Si verifica il riavvio automatico del sistema operativo in modo imprevisto.
- □ I programmi che in precedenza funzionavano correttamente si bloccano spesso. Anche se i programmi vengono rimossi e reinstallati, il problema persiste.

□ Un'utilità per la manutenzione dei dischi, ad esempio ScanDisk, segnala diversi errori gravi del disco.

□ Scompare una partizione.

□ Il computer si blocca.

□ Non è possibile avviare Task Manager.

□ Il software antivirus segnala la presenza di un virus informatico



<u>Virus</u>: sono parti di un codice che si diffondono copiandosi all'interno di altri <u>programmi</u>, o in una particolare sezione del <u>disco fisso</u>, in modo da essere eseguiti ogni volta che il <u>file</u> infetto viene aperto. Si trasmettono da un <u>computer</u> a un altro tramite lo spostamento di file infetti ad opera degli utenti.

<u>Worm</u>: questi malware non hanno bisogno di infettare altri file per diffondersi, perché modificano il <u>sistema operativo</u> della macchina ospite in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo più <u>internet</u>. Per indurre gli utenti ad eseguirli utilizzano tecniche di <u>social anginaering</u>, oppure sfruttano dei difetti (<u>bug</u>) di alcuni <u>programmi</u> per diffondersi automaticamente

<u>Trojan horse</u>: software che oltre ad avere delle funzionalità "lecite", utili per indurre l'utente ad utilizzarli, contengono istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore. Non possiedono funzioni di auto-replicazione, quindi per diffondersi devono essere consapevolmente inviati alla vittima. Il nome deriva dal famoso cavallo di Troja.

<u>Backdoor:</u> letteralmente "porta sul retro". Sono dei <u>programmi</u> che consentono un accesso non autorizzato al sistema su cui sono in esecuzione. Tipicamente si diffondono in abbinamento ad un trojan o ad un worm, oppure costituiscono una forma di accesso di emergenza ad un sistema, inserita per permettere ad esempio il recupero di una password dimenticata.

<u>Spyware: software</u> che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato. Le informazioni carpite possono andare dalle abitudini di navigazione fino alle password e alle <u>chiavi crittografiche</u> di un utente.

<u>Olaler</u>: questi <u>programmi</u> si occupano di gestire la connessione ad <u>Internet</u> tramite la normale linea telefonica. Sono malware quando vengono utilizzati in modo truffaldino, modificando il numero telefonico chiamato dalla connessione predefinita con uno a tariffazione speciale, allo scopo di trarne illecito profitto all'insaputa dell'utente.

VIRUS POSSONO ESSERE O NON ESSERE DIRETTAMENTE DANNOSI PER IL SISTEMA OPERATIVO CHE LI OSPITA, MA ANCHE NEL CASO MIGLIORE COMPORTANO UN CERTO SPRECO DI RISORSE IN TERMINI DI RAM, CPU E SPAZIO SUL DISCO FISSO. POSSONO AVVENIRE PROBLEMI, ANCHE GRAVI, CON CONSEGUENZE NON SOLO PER IL SINGOLO UTENTE MA ANCHE PER I SUOI CONTATTI E PER IL SERVIZIO STESSO.



COME PROTEGGERE IL COMPUTER DAI VIRUS?

Per proteggere il computer dai virus, attenersi alla seguente procedura:

- 1. Attivare il firewall nel computer.
- 2. Mantenere aggiornato il sistema operativo del computer.
- 3. Utilizzare il software antivirus aggiornato nel computer.
- 4.Utilizzare il software antispyware aggiornato nel computer.

RIMOZIONE DI UN VIRUS INFORMATICO

Senza la guida degli strumenti di rimozione di virus informatici, la rimozione di un virus informatico potrebbe essere una difficile impresa anche per un esperto. Alcuni virus informatici e altri software indesiderati, ad esempio spyware, vengono reinstallati automaticamente persino dopo l'eliminazione e la rimozione dei virus. Fortunatamente, aggiornando il computer e utilizzando gli strumenti antivirus, è possibile rimuovere definitivamente il software indesiderato.

Per rimuovere un virus informatico,:

- 1. Installare gli aggiornamenti più recenti da Microsoft Update nel computer.
- 2. Aggiornare il software antivirus nel computer. Quindi, eseguire un'analisi approfondita del computer utilizzando il software antivirus.

ALCUNI ANTIVIRUS

- BitDefender Antivirus Pro 2011
- 2. Kaspersky Anti-Virus 2011
- 3. WebRoot Antiviurs 2011
- 4. Norton AntiVirus 2011
- Eset Nod32 AntiVirus 4
- 6. AVG Anti-Virus 2011
- 7. G Data Antivirus 2011
- 8. Avira Antivir Premium 2011
- 9. Vipre Antivirus 4

ANTIVIRUS FREEWARE

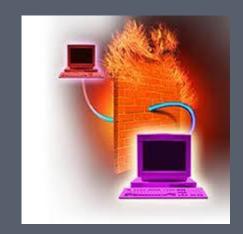
1. Avira AntiVir Personal.

2. Avast! Antivirus Home Edition.

3. AVG Antivirus Free Edition.

FIREWALL

COS'E'?



Letteralmente: Muro di fuoco (muro taglia fuoco)

Software usato per proteggere un server da attacchi pervenuti via rete locale o via Internet. Consente il passaggio solamente di determinati tipi di dati, da determinati terminali e determinati utenti.

ALCUNI FIREWALL

1. Comodo Internet Security

Offre sia un <u>antivirus</u> che un firewall ma è soprattutto il secondo a fare da padrone. Infine è molto conosciuto il suo sistema di protezione "Defense+".

2. Online Solutions Security Suite OSSS è un software di protezione complesso, diventato a pagamento, che include:

Proactive Defense (OSPD) – sistema di difesa proattiva di nuova generazione.

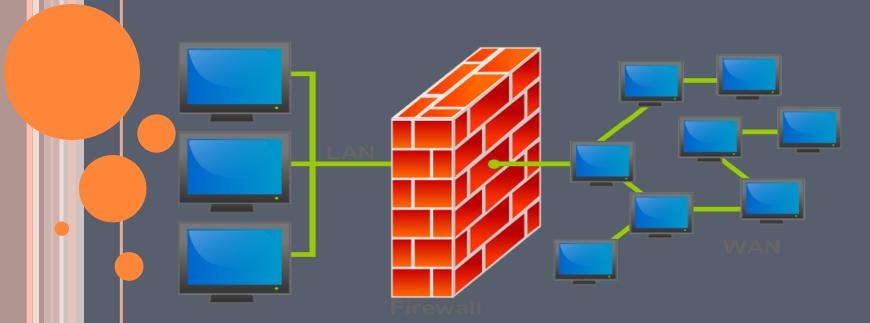
Personal Firewall (OSPF) – firewall personale estremamente potente.

Autorun Manager (OSAM) – modulo anti-<u>malware</u> e anti-<u>rootkit.</u>

ALTRI FIREWALL...

- 3-4. Outpost Security Suite free e a pagamento
- 5. Kaspersky Internet Security

Soluzione a pagamento del famoso antivirus che include tra le altre funzioni anche un firewall integrato, a quanto pare molto efficiente.



IN COSA CONSISTONO LE MOLESTIE?:

condotta penalmente perseguibile; punibile chiunque in ambito telematico rechi a taluno molestia o disturbo. Di solito si intende tra adulto e minore.

Non incontrare mai dal vivo persone conosciute esclusivamente su internet.

In caso di effettiva molestia: CONTATTARE IMMEDIATAMENTE UN ADULTO

è opportuno conservare una copia cartacea del messaggio (e-mail, chat o simile) facendo attenzione a non aprire allegati o eseguire file sospetti (potrebbero contenere malware); occorre poi segnare con cura data e ora in cui il fatto è avvenuto e, se possibile, annotare il nickname del molestatore e ogni altra informazione che potrebbe tornare utile ai fini dell'identificazione (qualsiasi cosa... un numero seriale, un identificativo, l'indirizzo IP, ecc.)

- RIVOLGERSI AL MODERATORE DELLA CHAT
- BLOCCARE L'UTENTE



Se la molestia è avvenuta tramite posta elettronica occorre stampare l'e-mail completa di header e non soltanto il testo del massaggio.

Una volta acquisito il suddetto materiale potrete portare il tutto alla <u>Polizia Postale</u>, oppure alla <u>più vicina stazione dei Carabinieri</u>, o chiamare il 114 (telefono azzurro) e presentare così una denuncia o una querela

IL DOWNLOAD

1. Cosa significa?



2. È sempre legale?

3. I rischi del download.....

IL DOWNLOAD: È L'AZIONE DI *SCARICARE* O *PRELEVARE* DALLA RETE UN <u>FILE</u>, TRASFERENDOLO SULL' HARD DISK DEL COMPUTER O SU ALTRA <u>PERIFERICA</u> DELL'UTENTE. NELLA MAGGIOR PARTE DEI CASI IL DOWNLOAD DI UN FILE È LA CONSEGUENZA DI UNA RICHIESTA, PIÙ O MENO TRASPARENTE ALL'UTENTE DEL SISTEMA.

Che cosa scarichiamo?

- omusica o filmati
- osuonerie per cellulari
- oprogrammi e giochi

Quali sono i rischi?

- Internet non è la terra di nessuno e molto di ciò che trovi nella rete è protetto dalla legge sul diritto d'autore: non puoi scaricarlo legalmente e gratuitamente.
- Alcuni programmi sono freeware ovvero di libero utilizzo, non paghi la licenza d'uso ma che non puoi modificare, oppure software shareware che sono gratuiti solo per un periodo di tempo limitato.
- Infine vi sono software liberi o free software che possono essere copiati, modificati e distribuiti da tutti, a patto che siano redistribuiti sempre sotto un regime di copyleft, ossia che rimangano sempre liberi da diritti di autore.

SE SI SCARICA UN FILE CL COMPUTER O COL TELEFONINO....



Ricordiamoci che:

- Potremmo violare il diritto d'autore... ex art. 171 bis I.d.a...
- Potremmo involontariamente scaricare dei virus e danneggiare i nostri computer...
- 3) Potremmo essere vittime di truffe! O comunque ritrovarci a pagare cose in più non volute..

LA POSTA ELETTRONICA



I rischi possono esserci anche nell' e-mail...

- 1) <u>Via posta possono arrivare virus dagli utenti</u> sconosciuti...
- 2) Posso chiederci dati personale nostri, dei nostri amici, o dei nostri genitotori...

IL CYBERBULLISMO E LA DIFFUSIONE DI CONTENUTI DIGITALI ON LINE...

- Il bullismo cybertico è la diffusione on line, via sms, via posta...
- o di insulti e minacce: ad esempio si fa riferimento all' aspetto fisico, voti a scuola, al 'indice' di popolarità o al fatto di portare gli occhiali o l'apparecchio ai denti...
- o di materiale digitale riguardanti fatti privati, di immagini violente o rubate a persone inconsapevoli...

o Il bullo online può offendere o ferire altri utenti senza avere necessariamente un contatto fisico ma ciò non toglie che le sue azioni possano essere altrettanto efficaci e dolorose. L'apparente anonimato dietro cui può nascondersi può infatti far pensare all'altra persona che sia quasi impossibile sottrarsi.

L'ANONIMATO E' SOLO APPARENTE PERO'....



Caratteristiche

- •Anonimato del molestatore: in realtà, questo anonimato è illusorio: ogni comunicazione elettronica lascia delle tracce. Però per la vittima è difficile risalire da sola al molestatore.
- •Difficile reperibilità: se il cyberbullismo avviene via <u>SMS</u>, <u>messaggeria</u> <u>instantanea</u> o <u>chat</u>, o in un forum online privato, ad esempio, è più difficile reperirlo e rimediarvi.
- •Indebolimento delle remore etiche: le due caratteristiche precedenti, abbinate con la possibilità di essere "un'altra persona" online (vedi i giochi di ruolo), possono indebolire le remore etiche: spesso la gente fa e dice online cose che non farebbe o direbbe nella vita reale.
- •Assenza di limiti spaziotemporali: mentre il bullismo tradizionale avviene di solito in luoghi e momenti specifici (ad esempio in contesto scolastico), il cyberbullismo investe la vittima ogni volta che si collega al mezzo elettronico utilizzato dal cyberbullo.

LA PRIVACY

- Per privacy si intendono tutte quelle informazioni che fanno strettamente parte della tua sfera privata: dati anagrafici (nome, cognome, data di nascita, ecc.), opinioni politiche, convinzioni religiose, stato di salute, ecc.
- La conoscenza di queste informazioni è permessa ad altri solo se la persona interessata dà il proprio consenso

QUALI POTREBBERO ESSERE LE CONSEGUENZE?

- Inviare agli amici con il tuo cellulare o con una e-mail una foto che trovi spiritosa, magari scattata di nascosto al tuo migliore amico... sei proprio sicuro che gli farà piacere? Lo sai che tutto questo non è permesso dalla legge che tutela la privacy senza chiedere il consenso della persona interessata?
- Può accadere che qualcuno faccia girare una tua e-mail contro la tua volontà, o che riveli ad altri cose che ti riguardano e che non volevi si sapessero in giro, che qualcuno, un po' troppo curioso, possa mettere il naso nel tuo pc o nei tuoi cassetti, leggere il tuo diario o gli SMS sul tuo cellulare...
- O può accadere che comunque i tuoi dati personali o quelli dei tuoi amici vengano diffusi...

..QUANTI PROBLEMI!!!



Proviamo insieme ad elaborare una mini guida da seguire per non cadere nelle rete!