



Commissione Nazionale
per la Prevenzione
del Disagio e del Bullismo

Milano



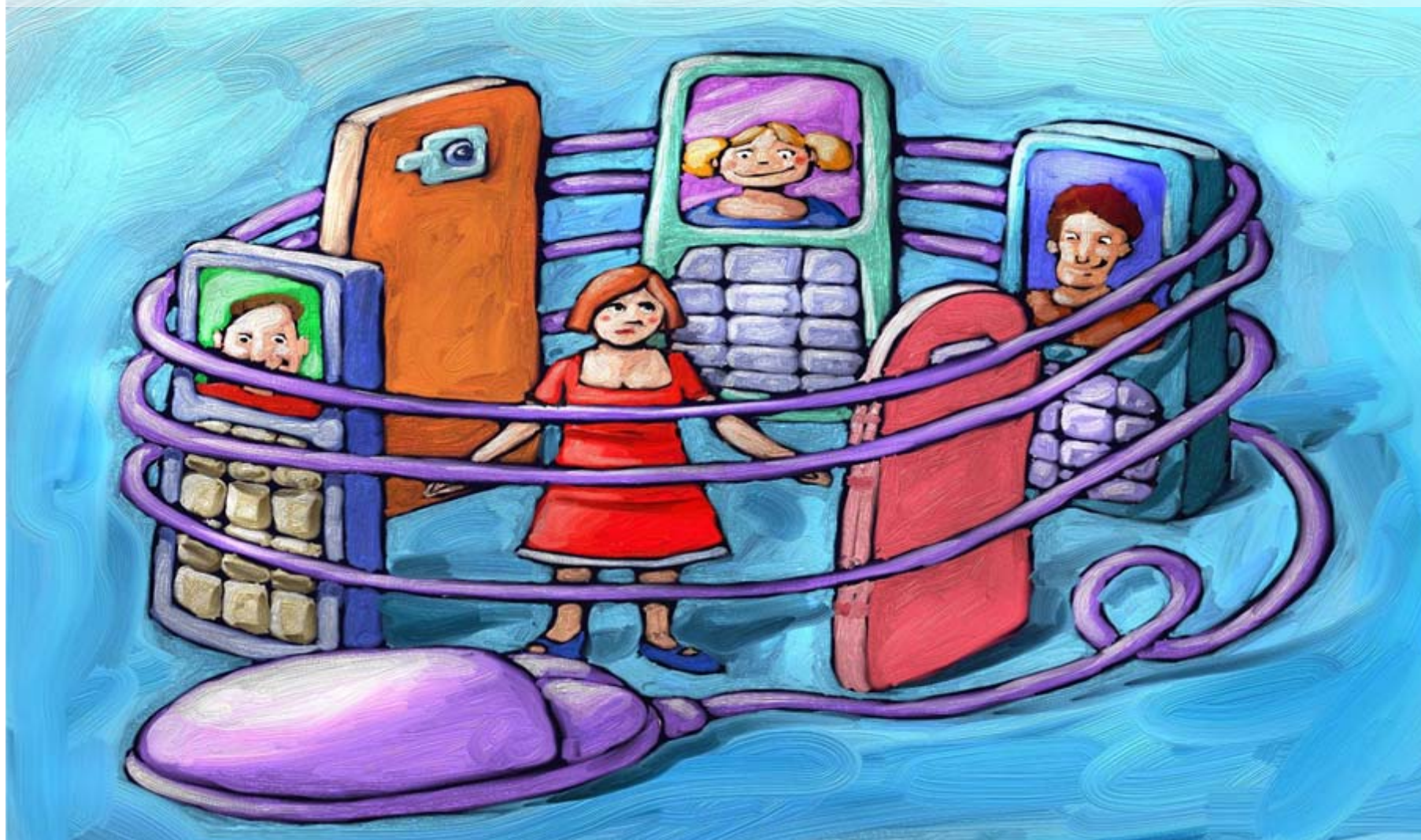
Comune
di Milano

Famiglia, Scuola
e Politiche Sociali



Stop al Cyberbullismo

8 giugno 2010 – Istituto Carlo Porta - Milano





POLIZIA DI STATO

COMPARTIMENTO POLIZIA POSTALE E DELLE COMUNICAZIONI PER LA LOMBARDIA
MILANO

*I rischi nell'uso dei nuovi mezzi di
comunicazione*

La Polizia Postale

La Specialità può contare su una presenza capillare sul territorio garantita dai **20 Compartimenti** e dalle **75 Sezioni** presenti nei principali capoluoghi di provincia



Potenziali insidie per gli utenti

● Malware

- Virus
- Worm
- Dialer
- Spyware



● Truffe

- Phishing
- Pharming



● Hacking

● Spam

- Hoax
- Catene di S. Antonio



Potenziali pericoli per i più piccoli

- **Contenuti inadeguati**
 - Violenza
 - Fanatismo
 - Pornografia
 - ecc.
- **Contatti con malintenzionati**
- **Istintiva fiducia nel mezzo e negli interlocutori**



Le insidie di Internet: pedofilia

Il fenomeno della pedofilia è sempre esistito, ma si è accentuato con l'avvento di Internet grazie alla facilità con cui è ora possibile reperire materiale video o fotografico ritraente minori.

Siti web, forum, programmi di filesharing e social network sono solo alcuni dei mezzi più usati per reperire materiale o individuare minori al fine di prestazioni sessuali.

Social Network

I mezzi attraverso i quali l'uomo socializza nella rete sono vari, ad ognuno corrisponde un livello di complessità, di interazione e di evoluzione differente

Social Network

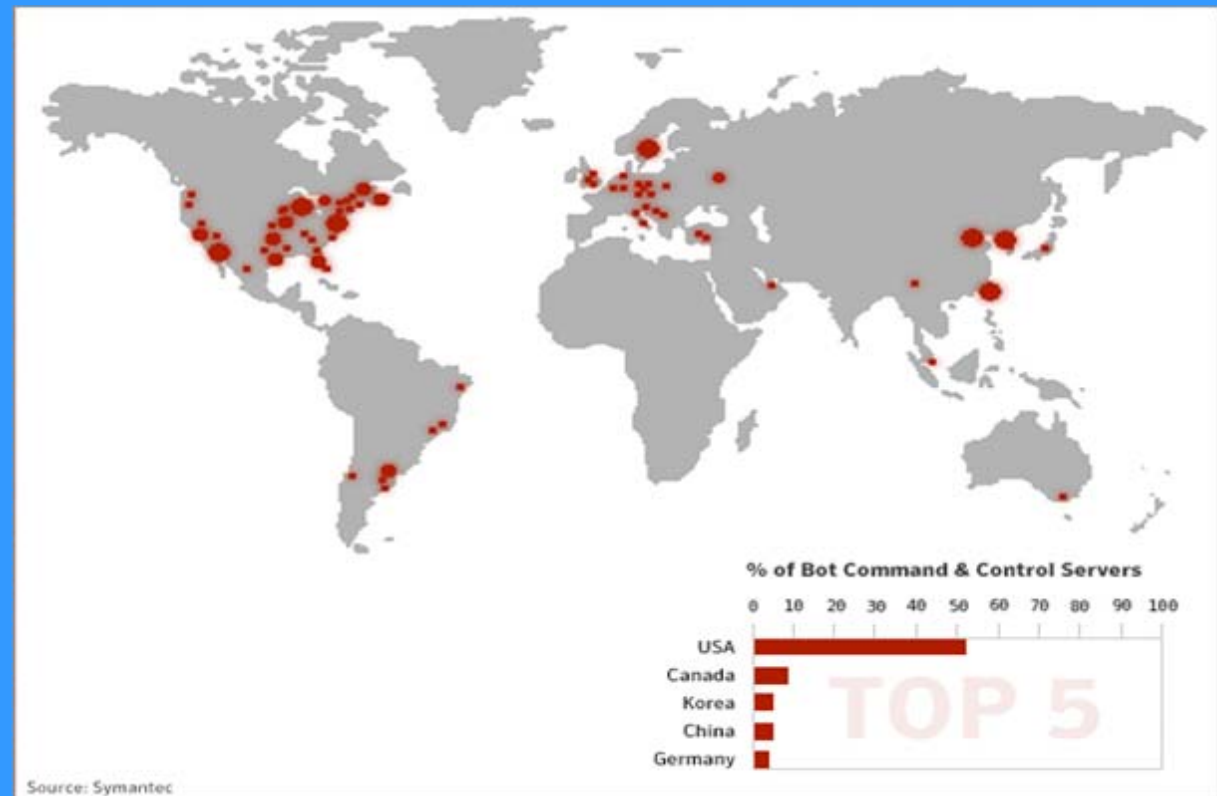
Forum

IM=Istant Messanging

Blog

Chat

Community



Social Network

Una rete sociale è formata da un gruppo di persone connesse tra loro da diversi legami sociali, che vanno dalla conoscenza casuale ai vincoli familiari

La versione Internet delle reti sociali è una delle forme più evolute di comunicazione in rete e in pratica utilizza la Computer Mediated Communication come infrastruttura di un Social Network.

L'utente struttura una mappa della propria rete di contatti personali e/o professionali, gestibile ed espandibile tramite la CMC.

Il Social Network diventa quindi un luogo virtuale di relazioni attive con le persone che già si conoscono, ma anche un database ricercabile e organizzato di nuovi contatti.

In un'era di convergenza digitale (stampa, tv, radio, affissioni) anche l'uomo si sta digitalizzando, creando parte dei suoi legami sociali su Internet.

Social Network

Sebbene le caratteristiche di questi siti siano differenti, tutti consentono di accedere alle proprie informazioni personali e offrono vari meccanismi di comunicazione (forum, chat room, e-mail, instant messenger) che consentono di connettere gli utenti tra loro. In alcuni siti è possibile ricercare persone anche secondo alcuni criteri. Alcuni altri siti, invece, hanno comunità o sottogruppi che sono basati su particolari interessi comuni.

Quali sono i rischi di questi siti?

I social network sites si basano sullo scambio di informazioni tra i partecipanti, così incoraggiano gli utenti a mettere a disposizione una certa quantità di informazioni personali. La particolare tipologia di questi siti, il desiderio di incrementare le proprie conoscenze ed il falso senso di sicurezza ingenerato dalla rete sono i fattori che spingono gli utenti a fornire una notevole mole di informazioni personali, non tenendo conto che queste possono cadere in mano a malintenzionati.

Social Network

I dati inseriti, che possono subire rielaborazioni e diffusioni anche a distanza di anni, possono essere registrati da tutti i contatti e dai componenti dei gruppi a cui si aderisce.

Talvolta le condizioni di utilizzo prevedono la licenza di usare i dati inseriti senza limiti di tempo.

OGGETTIVA DIFFICOLTA' DI APPLICAZIONE DELLA LEGGE ITALIANA

La maggior parte dei siti dei S.N. ha sede all'estero.

In caso di disputa legale non sempre si è tutelati dalle leggi italiane ed europee.

La forma più efficace di tutela è sempre l'autotutela ovvero la gestione oculata dei propri dati personali.

In soccorso degli utilizzatori concorrono le forze di polizia (in primis la Polizia Postale e delle Comunicazioni) ed il Garante per la protezione dei dati personali.



Compartimento Polizia Postale di Milano



Social Network

Attacchi conseguenti allo sfruttamento di informazioni personali raccolte in Internet

▶ **Identity Theft/
uso indebito dei dati personali**

▶ **Usò indebito
coordinate di home banking/
numero di carta di credito**

▶ **Spamming**

▶ **Virus/ worm**

▶ **Accesso abusivo
a sistema informatico**



Social Network

Attacchi conseguenti allo sfruttamento di informazioni personali raccolte in Internet

- ▶ **Diffamazione**
- ▶ **Minaccia**
- ▶ **Adescamento minori**
- ▶ **Cyber stalking**
- ▶ **Cyber bullismo**



Le tecniche di indagine

Acquisizione dei file di log

Intercettazione di comunicazioni in uscita da un computer e/o telefoniche

Duplicazione del contenuto delle caselle di posta elettronica

“Perquisizione” di un computer

Sequestro del contenuto con efficacia probatoria

Problematiche investigative

- ▶ Anonimato / Cammuffamento del luogo di commissione.
- ▶ Necessaria collaborazione dei provider, anche esteri.
- ▶ Collaborazione internazionale tra Forze di Polizia.
- ▶ Armonizzazione delle legislazioni.
- ▶ Data retention.
- ▶ Procedure uniformi per la registrazione e per il trattamento delle evidenze informatiche.
- ▶ Corretta conservazione della documentazione elettronica.
- ▶ Approccio ancora troppo legato al cartaceo.

Cosa si può fare per favorire le indagini:

PAGINE WEB

- Indicazione esatta e completa dell'indirizzo del sito illecito

NEWSGROUP

- Messaggio con contenuto illegale presente nel newsgroup o nella community e indicazioni esatte per reperirlo

E-MAIL

- Testo, eventuale allegato e header del messaggio di posta elettronica con contenuti illeciti

CHAT

- Testo della conversazione con riferimenti illegali avuta in chat (se conservato), indicazioni precise di data e ora, del nickname dell'utente, delle caratteristiche della chat usata, dei log delle conversazioni, ecc.

SOCIAL NETWORK

- Indicazione esatta del social network adoperato, profilo utente, messaggio/fotografia con contenuto illecito, dati di inserimento, log delle conversazioni, ecc.

Risultati attività anno 2009

Persone arrestate	233
Persone denunciate in stato di libertà:	8620
Perquisizioni:	1731
Siti web monitorati:	56505
Siti web oscurati:	127

Pedofilia - Risultati attività anno 2009

Persone arrestate	53
Persone denunciate in stato di libertà:	1186
Perquisizioni:	1.224
Denunce-quererele-segnalazioni:	2133
Siti web monitorati:	26.910

Pedofilia - Risultati attività anno 2008

Persone arrestate	39
Persone denunciate in stato di libertà:	1167
Perquisizioni:	559
Siti web monitorati:	23.281



Truffe telefoniche e on line- Risultati anno 2009

Persone arrestate:	1
Persone denunciate in stato di libertà:	1099
Perquisizioni:	97
Siti web monitorati:	433

Truffe telefoniche e on line- Risultati anno 2008

Persone arrestate:	5
Persone denunciate in stato di libertà:	1341
Perquisizioni:	193
Siti web monitorati:	582

Hacking- Risultati attività anno 2009

Persone denunciate in stato di libertà:	687
Indagini avviate:	2068
Perquisizioni:	67
Denunce-querele-segnalazioni:	3723
Siti web monitorati:	4540



E-commerce- Risultati attività anno 2009

Persone arrestate:	118
Persone denunciate in stato di libertà:	4582
Perquisizioni:	207
Denunce-quererele:	17007
Siti web monitorati:	16011

E-commerce- Risultati attività anno 2008

Persone arrestate:	102
Persone denunciate in stato di libertà:	4115
Perquisizioni:	253
Siti web monitorati:	12462

Commissariato on line - Risultati anno 2009

Richieste informazioni: nr. maggiore per e-commerce e phishing	9156
Segnalazioni: nr. maggiore per phishing e pedopornografia	11203
Denunce: Nr. maggiore per e-commerce e phishing	5239

Precauzioni e contromisure: cosa fare

Utilizzare software specifici:

▶ **Antivirus**

da mantenere costantemente aggiornati

▶ **Antispyware e HIPS**

in grado di rilevare altri malware o modifiche alla configurazione

▶ **Personal Firewall**

che controlli anche le connessioni in uscita e che escluda alcuni protocolli di comunicazione, se necessario

Toolbar per i browser

(Netcraft, Google Toolbar ecc.)

▶ **Client di posta evoluti**

e soprattutto ben configurati

▶ **Filtri anti-spam**

▶ **Costante aggiornamento del S.O. e dei software applicativi**



Precauzioni e contromisure: cosa NON fare

▶ Cliccare sui link nelle e-mail

Sempre meglio digitare l'indirizzo personalmente

▶ Fornire dati sensibili

Nessun istituto di credito vi chiederà mai la password o altre informazioni riservate per e-mail

▶ Fornire dati personali

Anche informazioni apparentemente insignificanti potrebbero essere vantaggiose per l'attaccante.

Le immagini e le informazioni personali possono riemergere a distanza di anni grazie all'indicizzazione nei motori di ricerca

Non è consentito pubblicare fotografie relative ad altre persone senza aver ottenuto il loro consenso.

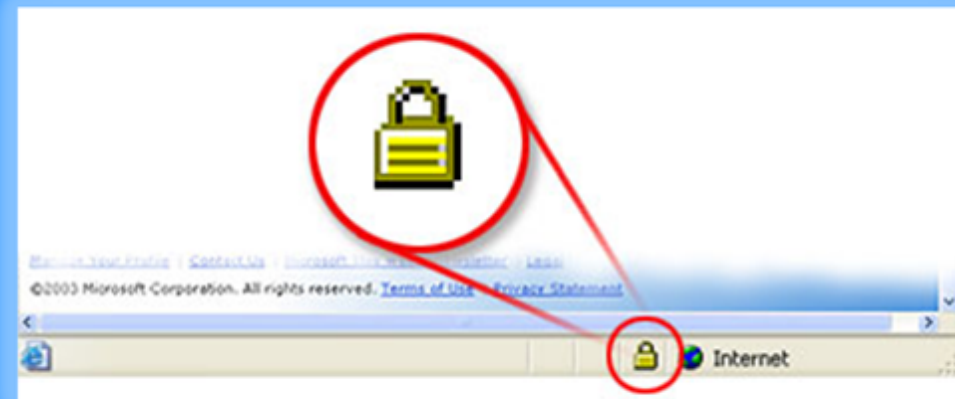
▶ Rispondere alle e-mail

Nemmeno per insultare o minacciare denunce



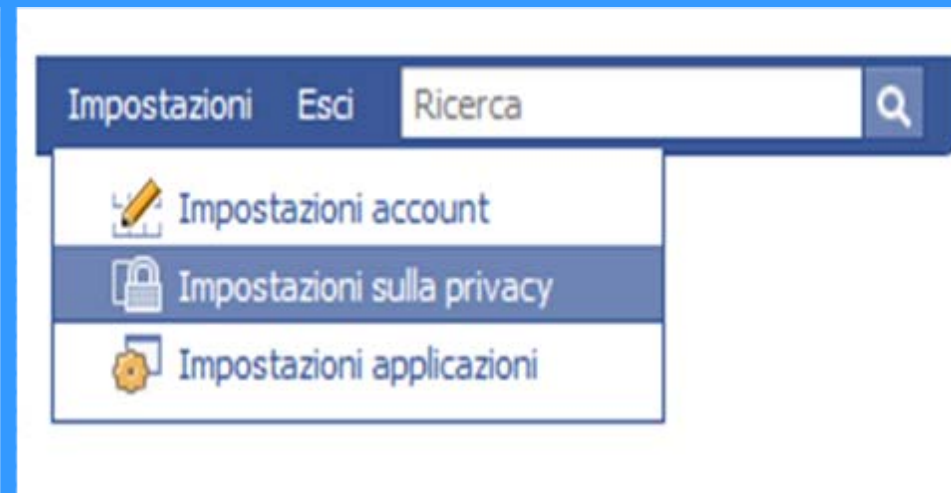
Precauzioni e contromisure: cosa fare

- ▶ **Generale diffidenza**, anche nell'accettazione di proposte di amicizia
- ▶ **Usare password robuste**, alfanumeriche, lunghe almeno 8 caratteri e provvedere alla loro sostituzione con regolarità
- ▶ **Attenzione agli errori di grammatica**
 - o alla presenza di caratteri anomali; p.e. l'alfabeto cirillico in una mail di Poste Italiane...
- ▶ **Attenzione alle richieste di informazioni**
non è credibile che la banca vi richieda informazioni che già possiede
- ▶ **Verifica telefonica**
- ▶ **Verifica dei certificati nei collegamenti SSL**



Precauzioni e contromisure: cosa fare

- ▶ Valutare la rimozione dagli elenchi pubblici e dalle indicizzazioni dei motori di ricerca
- ▶ Creare liste di amici con diversi livelli di privacy
- ▶ Impostare il livello di visibilità degli album fotografici



● **Controllo parentale**

- **Privilegi limitati**
- **Software specifici**
 - **Browser**
 - **Filtri**
 - **Logger**
- **Abbonamenti appositi**
 - **Connettività**
 - **Caselle e-mail**



**Nessun software sostituirà mai
il controllo dei genitori!**

Punti di forza per il pedofilo/cyberstalker

**Controllo dei genitori
scarso o assente**



Insufficiente informazione sui pericoli

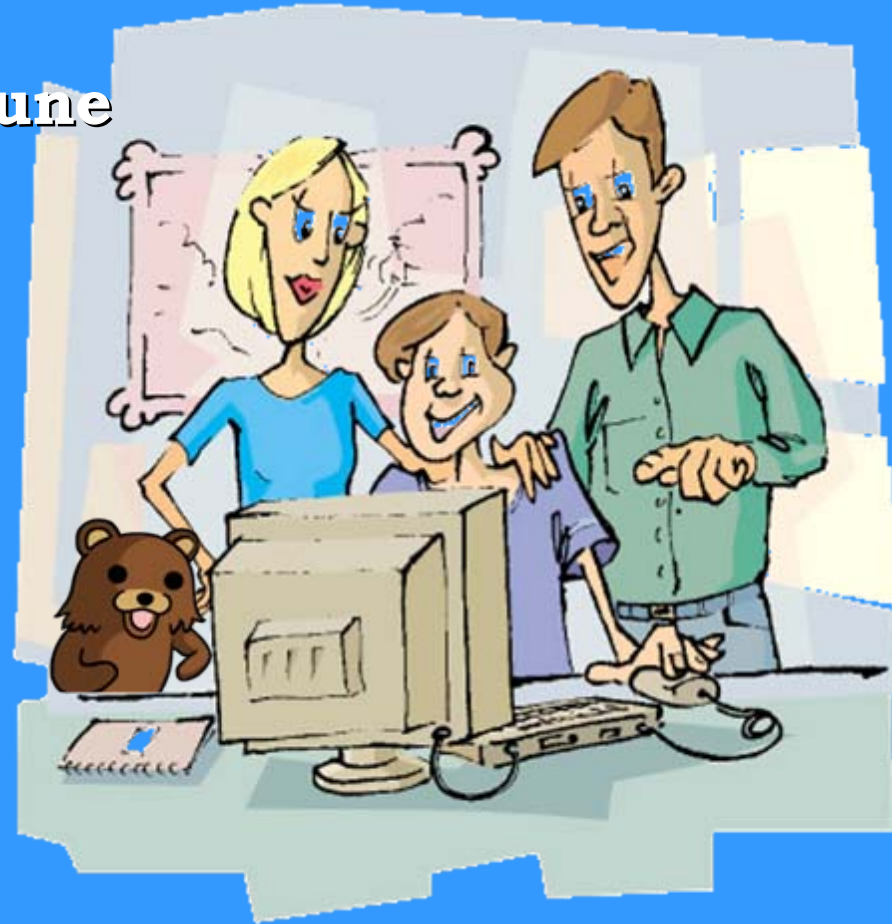
**Fisiologica curiosità dei minori
verso tematiche sessuali**

Assenza di comunicazione con i genitori

- vergogna, imbarazzo;
- sfiducia, timore di una punizione;
- percezione del rischio scarsa o nulla;
- curiosità, complicità.

● Regole familiari

- Internet come attività comune
- Collocazione del PC
- Controllo
- Educazione all'uso
- ecc.



Educazione all'uso

GUIDA ALLA SICUREZZA INFORMATICA

NET & WEBBY

IN VIAGGIO PER LA RETE

Protezione Civile
Ministero della Sanità
Ministero dell'Interno
Ministero della Giustizia
Ministero della Salute
Ministero dell'Istruzione, dell'Università e della Ricerca
Comitato Nazionale per la Sicurezza della Rete

I dialer illegali, che truffa!!

Controlla periodicamente le impostazioni della tua connessione ad internet, disabilita i codici 709, 809 e, se non ti servono, le chiamate internazionali!



Non fare la fine del pesce!

Valuta con attenzione le email che ricevi ogni giorno e non inviare mai a nessuno dati personali, codici segreti e soprattutto i riferimenti di una carta di credito.



www.guidaallasicurezza.it

Segnalazioni e informazioni utili

- www.poliziadistato.it
- www.commissariatodips.it
- www.interneteminori.it
- www.guidaallasicurezza.it
- www.hot144.it
- www.stop-it.org
- *Non perdere la bussola www.youtube.com/t/safety*

CONTATTI

Compartimento Polizia Postale e delle Comunicazioni per la Lombardia

Via Moisè Loria, 74 - 20144 - MILANO

Tel. 02.43333011 - Fax 02.43333067

E-mail: poltel.mi@poliziadistato.it

Dirigente VQA dott. Salvatore La Barbera

Funzionario VQA dott.ssa Treffiletti Fabiola

www.poliziadistato.it

www.commissariatodips.it
