

Spett.le ISTITUZIONE SCOLASTICA

in contratto con lo Studio Ing. PIERI - Torino

c.a.: Dirigente Scolastico

**Oggetto:** Circolare Sicurezza Studio Ing. PIERI Paolo - Consigli per i giovani che usano il WEB

**Messaggio:** La sicurezza informatica non è una competenza del RSPP; tuttavia può comportare situazioni di disagio psicologico che potrebbero riflettersi anche sulla valutazione del Rischio Stress Lavoro Correlato.

Pertanto il sottoscritto ritiene che la Direzione di ogni Istituzione scolastica possa acquisire alcuni utili consigli dalla presente circolare e, di conseguenza, ritenere ragionevole di divulgarli sia al proprio personale dipendente e sia agli studenti e alle loro famiglie.

Torino, 8 gennaio 2017

Con i migliori saluti.

**Ing. Paolo Pieri**

### [Consigli per i giovani \(dal sito della Polizia di Stato\)](#)

- Non date mai informazioni come il vostro nome e cognome, indirizzo, nome della scuola o numero di telefono a persone conosciute su Internet;
- non mandate mai vostre foto a qualcuno conosciuto via Internet senza il permesso dei vostri genitori;
- leggete le e-mail con i vostri genitori, controllando con loro ogni allegato al messaggio;
- dite subito ai vostri genitori o ai vostri insegnanti se leggete o vedete qualcosa su Internet che vi fa sentire a disagio o vi spaventa, per esempio fotografie di persone adulte o di bambini nudi;
- non fissate incontri con persone conosciute via Internet senza il permesso dei vostri genitori;
- ricordatevi che on line le persone possono non essere quello che dicono di essere. La bambina con cui credete di chattare potrebbe essere un uomo adulto!

### [Comportamenti da seguire](#)

I genitori possono trovare in rete molti consigli per la protezione dei minori sul sito dell'[Arma dei carabinieri](#) e della [Polizia di Stato](#).

## Consigli per i genitori (dal sito della Polizia Postale)

Insegnate ai bambini più piccoli l'importanza di non rivelare in Rete la loro identità.

- Spiegate loro che è importante per la loro sicurezza e per quella di tutta la famiglia non fornire dati personali (nome, cognome, età, indirizzo, numero di telefono, nome e orari della scuola, nome degli amici).
- Controllate i più piccoli affiancandoli nella navigazione in modo da capire quali sono i loro interessi e dando consigli sui siti da evitare e su quelli da visitare.
- Collocate il computer in una stanza centrale della casa piuttosto che nella camera dei ragazzi. Vi consentirà di dare anche solo una fugace occhiata ai siti visitati senza che vostro figlio si senta "sotto controllo".
- Impostate la "cronologia" in modo che mantenga traccia per qualche giorno dei siti visitati. Controllate periodicamente il contenuto dell'hard disk del computer.
- Insegnate ai vostri figli preadolescenti e adolescenti a non accettare mai di incontrarsi personalmente, magari di nascosto, con chi hanno conosciuto in Rete. Spiegate come un computer collegato a Internet sia per alcune persone male intenzionate il modo migliore per nascondere propositi criminali dietro bugie e false identità, a volte molto attraenti.
- Leggete le e-mail con i bambini controllando ogni allegato al messaggio. Se non conoscete il mittente non aprite l'e-mail, né eventuali allegati: possono contenere virus, trojan o spyware in grado di alterare il funzionamento del vostro computer.
- Tenete aggiornato un buon antivirus e un firewall che proteggano continuamente il vostro pc e chi lo utilizza.
- Dite ai bambini di non rispondere quando ricevono messaggi di posta elettronica di tipo volgare, offensivo e, allo stesso tempo, invitarli a non usare un linguaggio scurrile o inappropriato e a comportarsi correttamente in rete.
- Spiegate ai bambini che può essere pericoloso compilare moduli on line e dite loro di farlo solo dopo avervi consultato.
- Cercate di stare vicino ai bambini quando creano profili legati ad un nickname (pseudonimo) per usare programmi di chat.
- Non lasciate troppe ore i bambini e i ragazzi da soli in Rete. Stabilite quanto tempo possono passare navigando su Internet: limitare il tempo che possono trascorrere on-line significa limitare di fatto l'esposizione ai rischi della Rete.
- Usate software "filtri" con un elenco predefinito di siti da evitare.
- La migliore garanzia di tutela per i minori, in generale, è non lasciarli soli in un ambiente popolato da adulti come la Rete.

1. Un virus informatico è un file che infetta altri file del pc e che si trasmette come allegato nelle email o tramite dispositivi di memorizzazione (es. pendrive). Il trojan si presenta come software legittimo; una volta convinto l'utente ad eseguirlo apre un passaggio nascosto sul sistema che può essere utilizzato per eseguire qualunque tipo di operazione sul computer infettato. Lo spyware spia la vostra attività al computer. Esistono diversi tipi di spyware, da "keylogger" che registrano i tasti premuti sulla tastiera per rubare i dati della carta di credito e le password di online banking, a programmi che monitorano l'attività di navigazione web per poi inviarla su server remoti per scopi pubblicitari.

## I comportamenti allarme

Potrebbe essere tutt'altra l'origine del turbamento di vostro figlio, alcuni comportamenti non vanno sempre ascritti a situazioni di abuso o molestie, soprattutto se sta attraversando un momento evolutivo particolare (preadolescenza, adolescenza, separazioni o cambiamenti familiari). Tuttavia,

se questi comportamenti riguardano l'uso del computer o del telefonino, vale la pena cercare di comprendere cosa sta realmente accadendo.

### **Ecco i casi in cui prestare attenzione:**

- se tuo figlio modifica improvvisamente l'uso del telefonino o del computer e passa molto tempo a scrivere sms, a effettuare o ricevere chiamate, anche in tarda serata, e rimane connesso per molte ore al PC;
- quando si allontana e si apparta ogni volta che riceve o effettua una chiamata con il telefonino o si connette a Internet;
- se mostra ansia o rifiuta categoricamente di farti vedere il suo telefonino o lo schermo del computer mentre naviga o è connesso;
- se consuma molto velocemente il credito telefonico e non ti dà spiegazioni circa i suoi consumi;
- se mostra ansia e preoccupazione quando squilla il telefonino o mentre è connesso senza spiegarne spontaneamente il perché;
- quando modifica i ritmi sonno-veglia (dorme troppo, dorme poco, ha incubi) o il comportamento alimentare e il rendimento scolastico.

## **Internet e minori**

Con la diffusione delle nuove tecnologie della comunicazione e il facile accesso, anche dei minori, ai contenuti della Rete, sorgono giustificati motivi di apprensione nei genitori. Se è sbagliato demonizzare Internet e tutte le risorse in essa contenute, è altrettanto errato sottovalutare il problema della tutela dei minori dati i rischi che la Rete stessa contiene. A protezione dei minori è possibile agire su due fronti, che possono coesistere:

1. porre alcune **limitazioni all'utilizzo del computer** (orari, durata, accesso ai siti...) mediante software specifici o a seguito di una apposita configurazione del computer stesso;
2. seguire comportamenti utili ad accompagnare il ragazzo verso un utilizzo sicuro, consapevole e proficuo della rete.

## **Limitazioni all'utilizzo del computer**



I sistemi operativi Windows possiedono sistemi di controllo della navigazione in internet e di programmazione degli orari di utilizzo delPC. Il [sito della Microsoft](#) o [altro sito](#) forniscono le indicazioni per operare con Windows 7 e Windows Vista. Esistono numerosi [programmi gratuiti](#) che filtrano la navigazione in rete. Anche la Microsoft ha prodotto un software a tutela della navigazione dei bambini e per il controllo della stessa da parte dei genitori: *Windows Family Safety*. Prima di scaricare il programma è utile leggere una guida introduttiva all'uso del programma dal [sito della Microsoft](#).

## **Come equipaggiare il proprio computer e usarlo in sicurezza (dal sito della Polizia Postale)**

- Garantitevi una preparazione informatica quantomeno analoga a quella dei vostri figli per rispondere alle loro domande e predisporre le opportune misure di protezione del computer.
- Fate regolari backup<sup>1</sup> dei dati più importanti.
- Installate un buon antivirus.
- Aggiornate e scaricate le nuove versioni dei programmi per rendere permanente la protezione del computer.
- Usate un firewall<sup>2</sup> per proteggere la vostra navigazione in Internet.
- Usare software “filtri” con un elenco predefinito di siti da evitare. Verificate periodicamente che funzionino in modo corretto e tenete segreta la parola chiave.
- Non aprite gli allegati delle e-mail provenienti da sconosciuti e verificate prima il nome dei mittenti e l’oggetto.
- Siate sospettosi anche di allegati inaspettati ricevuti da chi conoscete perché possono essere spediti da una macchina infettata senza che l’utente ne sia a conoscenza.
- Scaricate regolarmente le “security patches”<sup>3</sup>

1. Copia di sicurezza o copia di riserva, su un qualunque supporto di memorizzazione, di materiale informativo al fine di prevenire la perdita definitiva dei dati in caso di eventi malevoli accidentali o intenzionali.
2. Il firewall è una risorsa software o hardware che controlla le informazioni provenienti da Internet o da un altro tipo di rete, bloccandole o consentendone l'accesso al computer, a seconda delle opzioni impostate. Windows Firewall è attivato per impostazione predefinita in Windows 7, quindi non occorre configurarlo.
3. Aggiornamenti dei programmi per incrementarne la sicurezza.

---

Torino, 8 gennaio 2017

RSPP

Ing. Paolo Pieri

Tratto da:

**Associazione "Pensiamo al Futuro"**

**c.f. 97452470582**

**Piazza Filattiera 84, 00139 Roma**

**Cell: 3385253415 - 3382046227**