

## Relazione del Sovrintendente Santin dr. Roberto e del Sovrintendente Lamberti Luigi (Esperti della Polizia di Stato – Sezione Polizia Postale e della Comunicazione di Bolzano)

### “NAVIGARE IN INTERNET SENZA PERDERE LA BUSSOLA”

Martedì 23 novembre 2010



La conferenza di oggi toccherà con mano quelli che sono i reati che si verificano nell'ambito dell'uso di Internet e di quelle che sono le varie interfacce con cui Internet si mostra.

La Polizia Postale è una delle quattro specialità della Polizia di Stato (le altre sono la Polizia Ferroviaria, la Stradale e la Polizia di frontiera) cui fa riferimento un nutrito gruppo di ingegneri e tecnici specializzati in queste materie. È la specializzazione più recente in quanto è stata riorganizzata nei

compiti e nelle competenze nel 1999 ed è attualmente il reparto specializzato della Polizia di Stato in materia di prevenzione e repressione di quelli che sono gli illeciti penali e amministrativi nel settore delle telecomunicazioni o, altrimenti dette, comunicazioni via Internet. La Polizia Postale è presente sull'intero territorio nazionale con un ufficio compartimentale che normalmente è presso il capoluogo di regione e gli uffici sezionali che sono più o meno in tutte le province d'Italia. Per quanto riguarda l'Alto Adige c'è una sezione a Bolzano composta da circa 15-20 dipendenti, metà dei quali hanno compiti operativi.

Le attività di cui si occupa la Polizia Postale spaziano dal contrasto della pedopornografia online, competenza primaria che si sviluppa attraverso attività investigativa anche su segnalazione da parte dei cittadini o da parte di enti e strutture che si occupano della tutela dei minori, all'e-commerce con indagine relative a tutti quei reati attinenti al commercio elettronico (truffe e frodi online) e l'hacking, termine col quale si designa l'intrusione nei sistemi informatici privati o pubblici, fenomeno in continuo aumento.

Altre attività riguardano la struttura centrale della Polizia Postale dove è presente una squadra che si occupa di monitorare la rete in materia di terrorismo, quindi di tutti quei siti legati in qualche modo al terrorismo. Un'altra squadra si occupa di monitorare le infrastrutture critiche del paese e cioè tutti quei siti e quelle strutture che riguardano i servizi essenziali del paese (erogazione dell'acqua, del gas, dell'energia elettrica, la sicurezza), quei servizi che in caso di attacco metterebbero in ginocchio il paese.

Ognuno di noi cerca di proteggere i propri figli dalle minacce e dai pericoli della vita reale però non li si protegge a sufficienza nella navigazione in Internet. Spesso li si lascia ore e ore al computer senza una dovuta assistenza. Secondo un recente sondaggio il 20% (1 su 5) circa dei minori ammette di aver subito delle molestie indesiderate su Internet. Cosa occorre dunque fare? Occorre che anche nel nostro Paese cresca la consapevolezza della necessità di sensibilizzare tutta la società verso un corretto approccio alla rete da parte dei minori.

Sono molte le iniziative e i progetti lodevoli già messi in atto per arrivare a questo obiettivo, tra cui un'iniziativa nata su volontà del Ministero dell'Interno in collaborazione con il Ministero dell'Istruzione e Youtube che si chiama "Non perdere la bussola". Si tratta di un progetto che vede coinvolti, tra l'altro, in prima persona gli uomini e le donne della Polizia Postale che su richiesta degli istituti scolastici sono disponibili ad effettuare incontri con gli alunni, con i genitori e gli insegnanti per parlare insieme ed effettuare dei colloqui in tema di sicurezza in rete. La speranza è che queste iniziative siano sempre più diffuse e che anche i pericoli e i rischi della rete non vengano mai a limitare quello che è lo sviluppo della comunicazione sul web.

La criminalità informatica è un fenomeno crescente in tutto il mondo e naturalmente anche l'Italia non è immune da questo fenomeno: i pedofili trovano nuove strade per sviluppare le proprie perversioni sessuali e anche il file-sharing, la condivisione cioè di file con contenuti tutelati dal diritto d'autore, è in costante aumento.

I circuiti di condivisione dei file consentono la diffusione di materiale protetto dal diritto d'autore (immagini, filmati, film e musica). Molte persone ritengono che ciò non sia un reato, ma in realtà la duplicazione abusiva di tali contenuti è un reato tutelato da una legge risalente al 1941.

Internet è un insieme di computer collegati fra di loro cui possono accedere milioni di utenti in tutto il mondo per usufruire dei servizi messi a disposizione dove però si può incappare e anche commettere reati e illeciti di ogni tipo.

L'utilizzo di Internet è intergenerazionale nel senso che vi si possono trovare i bambini di 6 anni (circa il 30% di bambini di età compresa tra i 6 e i 10 anni nell'ultimo anno ha utilizzato la rete Internet, il 70% dagli 11 ai 17 anni con poca distinzione tra ragazze e ragazzi) così come i sessantenni ed è utilizzata per i più svariati motivi che vanno dalla messaggistica, agli acquisti online, dai giochi all'utilizzo dei social network.

L'utilizzo di Internet è in continuo aumento così come i siti in esso contenuti. Si stima che il 37% di tutti i contenuti della rete sia di natura pornografica; nell'ultimo trimestre del 2010 si è verificato un aumento esponenziale dei siti legati ai giochi e soprattutto dei giochi di ruolo che sono cresciuti del 211%, mentre i siti che contengono materiale violento sono cresciuti del 10%, quelli legati al terrorismo dell'8% e quelli legati al commercio di farmaci illegali del 6,8%. Questi dati fanno capire come sia necessario da parte dei genitori e degli adulti in generale di occuparsi del computer di casa per proteggere i propri ragazzi.

Spesso si associa Internet ad attacchi alla propria privacy. Il termine è un concetto di origine anglosassone ed inizialmente era riferito alla sfera privata delle persone. I primi a teorizzare la privacy furono due giuristi inglesi che alla fine dell'Ottocento scrissero un saggio in cui parlavano della privacy come diritto della persona di essere lasciata da sola "Right to be let alone". Nel corso del tempo, con lo sviluppo soprattutto delle nuove tecnologie, anche il significato di privacy si è evoluto e adesso è in qualche modo legato proprio al diritto di ognuno di controllare i propri dati personali e soprattutto il diritto di scegliere l'uso che gli altri possono fare degli stessi. Queste facoltà sono sancite dal Decreto Legislativo 196 del 2003 "Codice in materia di protezione dei dati personali". Il legislatore ha così voluto riconoscere dei diritti a tutti i cittadini, in primo luogo il diritto di disporre dei dati propri e soprattutto ha posto degli obblighi nei confronti di coloro che vogliono trattare i dati personali altrui. Obblighi che sono in sostanza l'informazione nei confronti degli interessati e il consenso. Il consenso diventa pertanto un requisito fondamentale nella trattazione dei dati personali.

Le riprese o le fotografie fatte, ad esempio, a scuola in occasione di una gita, per essere pubblicate necessitano dell'autorizzazione e del consenso esplicito dei diretti interessati.

### **Cosa può accadere in Internet in questo senso?**

> Perdere il controllo dei propri dati personali: tutti i contenuti che vengono immessi in Internet, una volta caricati, sono persi. Tutte le informazioni personali, numeri di telefono, indirizzo di casa, dati sulla professione, fotografie e filmati, possono essere viste, modificate, diffuse e riutilizzate da altri utenti. Se ne perde dunque il controllo e anche la proprietà. All'atto dell'iscrizione ad un social network, ad esempio Facebook, viene concessa - nella maggior parte dei casi in modo inconsapevole perché non si leggono i termini e le condizioni d'uso - la licenza di utilizzare in eterno tutti i contenuti pubblicati dall'utente. Da non sottovalutare è il fatto che tutto ciò che viene pubblicato in Internet rende l'utente rintracciabile dai malintenzionati. Meno informazioni sono presenti e meglio è. La creazione, soprattutto da parte dei ragazzi, di profili aperti a tutti e non solo agli amici, li rende vittime di contatti indesiderati.

> Subire un furto d'identità. Il furto d'identità è quella condotta relativa all'impossessamento di credenziali di accesso solitamente attraverso l'invio di mail truffaldine con scopi criminali.

> Essere vittime di cyberbullismo. Il bullismo tradizionale, consistente in atti di molestie e diffamazione compiuti normalmente a scuola da coetanei verso coetanei, si sta trasformando sempre più in cyberbullismo tant'è che si stima che il 34% del bullismo sia ora passato sulla rete con l'invio di e-mail diffamatorie e di fotografie con contenuti ingiuriosi.

Il bullo prova solitamente piacere a dominare un altro coetaneo non provando generalmente compassione per tutte le molestie e le ingiurie che arreca. Il bullismo è spesso caratterizzato dalla lunga durata, è un comportamento che dura a volte anche per mesi; altra caratteristica è la scelta della vittima perché nel bullismo la ricerca della vittima non è mai casuale, vengono solitamente scelte le persone che sono più inclini alla vittimizzazione, persone deboli che non reagiscono e che subiscono passivamente questi atti. La vittima si sente naturalmente isolata ed esposta agli attacchi, rifiutandosi anche di parlarne.

Il credere di restare nell'anonimato porta il soggetto bullo ad essere un se stesso diverso dalla realtà, ha bisogno di riempire il suo spazio e Internet gli dà una possibilità in più proprio

perché il cyberbullo non è visibile, non si ha un raffronto diretto con lui. Per cui per scoprire chi è il bullo, devo attendere l'intervento della Polizia Postale a seguito di formale denuncia. La soluzione migliore per affrontare il cyberbullo è innanzitutto non reagire alle provocazioni, ma conservare il materiale ed eventualmente passarlo alle autorità competenti.

### **Cosa fanno i ragazzi in rete?**

Scaricano video, spesso protetti da diritto d'autore, chattano, navigano su Youtube, usano la web cam, hanno un blog personale. Mettono quindi le loro informazioni sui servizi resi disponibili da Internet, condividendo messaggi e immagini con altre persone. La caratteristica che accomuna questi servizi è innanzitutto la loro gratuità, oltre cioè la connessione non si paga una vera e propria iscrizione e ciò porta ad iscriversi a più servizi con conseguente rischio di essere più esposti. Altra caratteristica è l'intergenerazionalità e l'internazionalità dei servizi offerti: Facebook ad esempio ha sede in California mentre Netlog è in Belgio. Se succede un reato la Polizia Postale si può dunque trovare in difficoltà a causa della diversa legislazione dei paesi stranieri perché la legge ha una propria territorialità e servono accordi diretti tra stati (le cosiddette trattative) per intervenire e indagare i siti esteri.

Per di più spesso non si sa da chi questi servizi siano gestiti perché le società vengono vendute o spezzettate e i servizi integrati gestiti da altre società diverse dalla titolare.

L'avvento di Internet ha abbattuto i limiti temporali e spaziali portando le persone ad avere un bisogno di usare questi servizi e a crearsi un falso senso di sicurezza. L'uso superficiale di questi servizi (perché non si leggono le condizioni d'utilizzo) porta, nei casi più gravi, ad essere vittime di furti d'identità, al bullismo e all'adescamento.

### **Alcuni consigli**

Utilizzare preferibilmente gestori e-mail e servizi italiani, utilizzare nick name e password diversi per ogni servizio; comporre password di difficile decifrazione e contenenti lettere minuscole, maiuscole, numeri e caratteri speciali quali i trattini. Sono da evitare totalmente nomi di genitori, amici, sorelle, animali domestici e date di nascita. Fare attenzione alla webcam: alcuni servizi parzialmente illegali, come le chat erotiche, la attivano senza il consenso dell'utente registrando ciò che si sta facendo. I contenuti vengono immessi in chat e se ne perdono le tracce. Meglio dunque attaccare alla webcam un pezzettino di scotch per oscurarla.

### **Facebook**

Il popolare social network conta 500 milioni di utenti; è il secondo sito al mondo con più traffico. In Italia conta 19 milioni di profili attivi, tanto da risultare la sesta nazione che ne fruisce. Facebook è sì un servizio gratuito per gli utenti ma produce per i titolari un sacco di soldi. La società è stimata in 11 miliardi di dollari e ben presto verrà quotata in borsa. Oltre un milione di sviluppatori scrivono codici per il social network.

Nel contratto di licenza, che spesso però l'utente non legge, Facebook dichiara che i contenuti immessi dall'utente (informazioni personali, fotografie, video) possono essere condivisi con altre società: possono dunque essere rivenduti con diritti in tutto il mondo e ceduti. Tale "licenza" termina quando l'utente chiude il proprio profilo ma in realtà non vi è alcuna garanzia di impossessarsi nuovamente dei contenuti se questi sono già stati venduti a terzi. Vi è la rimozione dei contenuti all'atto di chiusura del profilo ma Facebook si riserva di conservarli per un tempo non precisato. Esiste ovviamente la possibilità attraverso l'impostazione del livello di privacy di proteggere i contenuti in modo tale da renderli visibili ai soli "amici", ma si tratta di impostazioni complicate che quasi nessuno applica.

Le società che acquistano contenuti da Facebook e dai social network in generale fondano la propria attività e il proprio business analizzando in tempo reale tutto ciò che viene scritto in Internet dagli utenti: non solo gusti e preferenze ma anche emozioni e sentimenti e, in base a questi dati, inviano pubblicità mirate per canalizzare gli utenti verso una particolare tipologia di prodotto.

### **La pedofilia online**

La pedofilia è considerata dalla letteratura medico-scientifica una manifestazione psicopatologica ed è inserita infatti tra le alterazioni a carico della sfera sessuale. È considerato un crimine poiché il pedofilo è estremamente lucido nelle scelte delle sue vittime.

In Italia le principali ipotesi di reato in materia di pedopornografia online sono contenute in due articoli del codice penale e sono l'articolo 600ter e l'articolo 600 quater che sono relativi alla produzione, alla divulgazione e diffusione di materiale pedopornografico e alla detenzione dello stesso. Questi due articoli sono stati inseriti dal Legislatore nel 1998 dalla legge 269. Si tratta di un riferimento legislativo molto importante perché ha consentito all'ordinamento italiano di adeguarsi a quelle che erano i recenti accordi europei. Ha introdotto una serie di reati di condotte gravi quali la prostituzione e lo sfruttamento minorile, la diffusione e la detenzione di materiale pedopornografico e ha previsto anche una serie di strumenti molto importanti per la polizia giudiziaria, strumenti in materia di repressione di questi reati, quali, ad esempio la possibilità di operare sotto copertura anche attraverso la creazione di siti per scambiare materiale a contenuto pedopornografico (sempre dietro autorizzazione dell'autorità giudiziaria) per avere maggiori elementi probatori.

Nel 2006 un ulteriore provvedimento normativo, la legge 38, ha portato ulteriori novità: per quanto attiene alla prostituzione minorile l'età è stata estesa fino ai 18 anni, prima erano puniti gli atteggiamenti sessuali rivolti a coloro che avevano meno di 16 anni; è stata prevista l'interdizione dai pubblici uffici, dalle strutture che si occupano di minori per coloro che vengono condannati per questo tipo di reati. La legge 38 ha previsto inoltre l'istituzione del Centro Nazionale di Contrasto alla Pedopornografia online presso il servizio della Polizia Postale di Roma, che ha il compito di raccogliere le segnalazioni e di coordinare l'attività investigativa in materia di pedofilia, ha introdotto inasprimenti di pena per la produzione, la diffusione e la detenzione di materiale pornografico di ingente quantità e introdotto anche il concetto di pedofilia virtuale. Si tratta di quell'insieme di tecniche di elaborazione grafica che consentono di far apparire come reali delle cose che in realtà reali non lo sono, quali ad esempio la sovrapposizione del viso di un bambino ad un corpo di un adulto.

Normalmente i pedofili scelgono le loro vittime sulle chat o sui social network, la prima cosa che fanno è instaurare un clima di fiducia con la vittima, spesso si fingono dei coetanei utilizzando lo stesso gergo, dopodiché introducono contenuti di natura sessuale, fino a quando ricercano un effettivo incontro fisico. Diventa dunque importantissimo parlare con i bambini e ragazzi, comunicare con loro, chiarire i rischi connessi all'utilizzo di certi servizi. Diventa fondamentale rispettare i limiti d'età (su Facebook ad esempio il limite d'utilizzo è di 14 anni), è necessario fare attenzione a certe tipologie di chat, perché quelle non sorvegliate possono anche avere delle "stanze" private dove il pedofilo chiede di chattare a livello privato esponendo i ragazzi ad un rischio elevatissimo. Importante è anche la posizione corretta del computer domestico: meglio in un punto dove è possibile di tanto in tanto dare un'occhiata a ciò che viene fatto, piuttosto che in camera dei ragazzi con lo schermo rivolto verso il ragazzo stesso. Si rammenta che esistono anche dei software ad uso parentale utili per bloccare la navigazione su alcuni siti.

## **Phishing**

Si tratta di una frode sia facile da commettere sia facile da cascarci: vengono inviate sulla casella di posta elettronica mail provenienti da banche o dalle società titolari di carte di credito con loghi veri ma link fasulli dove chiedono di inserire i dati personali. Il linguaggio è quello tipico bancario e legale, offrono soluzioni immediate e gratuite a problemi che in realtà una persona non ha puntando su fasulli problemi di sicurezza e sistemi antifrode. Una volta inserite le credenziali del conto corrente i criminali informatici li carpiscono ed entrano nel nostro conto. Alcuni consigli: controllare che ci sia sempre la dicitura https anteposto all'indirizzo della pagina web che si visita, e che vi sia il lucchetto giallo a destra dell'indirizzo che indica una connessione sicura. Si ricorda inoltre che le banche, le poste e i circuiti di credito non inviano mai richieste di conferma dati via posta elettronica.

*Altre informazioni relative alla conferenza si trovano sul sito [www.tangram.it](http://www.tangram.it)*