POLIZIA POSTALE E DELLE COMUNICAZIONI

Sommario

La capillare diffusione di sofisticati personal computer e di telefoni cellulari di ultima generazione consente connessioni ad Internet sempre più facili ed immediate.

Il numero di chi naviga in rete si amplia di giorno in giorno e ricomprende anche fasce di utenti di giovanissima età.

Le ***nuove frontiere della innovazione tecnologica*** consentono peraltro di fruire dei vari servizi della E-society anche all'interno di nuove forme di aggregazione virtuale, i social network, che comportano massive condivisioni di informazioni e dati personali.

Si tratta di evidenti occasioni di sviluppo e di progresso di cui occorre però garantire opportuna sicurezza di esercizio.

Di qui attuale ed impellente la necessità di assicurare la tutela dei diritti individuali dei cittadini-utenti, soprattutto di quelli più vulnerabili come i minori, con l'impegno quotidiano di strutture altamente specializzate quali la Polizia delle Comunicazioni.

.

Il Capo della Polizia
Direttore Generale della Pubblica Sicurezza
Antonio Manganelli

La vasta comunità degli utenti della società digitale è potenziale obiettivo di aggressioni criminali che, da ogni parte del mondo, mirano oltre che al patrimonio economico anche a fare incetta di preziosi dati personali.

La tutela della comunità e dei singoli utenti da nuove minacce criminali impone il ricorso a sofisticate tecniche di intervento specialistico e ad innovative forme di cooperazione tra partner pubblici e privati ed anche tra stati.

In Italia, la Polizia delle Comunicazioni è la componente di eccellenza della Polizia di Stato deputata al contrasto dei crimini commessi attraverso i mezzi di comunicazione ad alta tecnologia e alla tutela delle potenziali vittime ed al presidio delle condizioni di sicurezza dell'ambiente virtuale.

Si avvale di alcuni strumenti innovativi: il ***Centro Nazionale per il Contrasto della Pedopornografia On-line*** (CNCPO) per tutelare i minori dal crimine on-line; il ***Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche Informatizzate*** (CNAIPC) per proteggere i gangli vitali del Paese; il ***Commissariato On-Line*** per assicurare un facilitato e continuativo contatto con il cittadino.

Il Direttore Centrale
delle Specialità della Polizia di Stato
Santi Giuffrè

Il contrasto al crimine informatico è una sfida senza tregua e senza confini imprescindibilmente connessa con il vertiginoso sviluppo delle nuove tecnologie.

In uno scenario di comunicazioni globalizzate, diffuse ed interconnesse, preziose informazioni e dati sensibili degli utenti della rete sono oggetto di innovative forme di gestione che li vedono tra l'altro sempre più distribuiti e delocalizzati. Indicative in tal senso le nuove forme di trattamento indotte dal ***cloud computing*** e le massive forme di aggregazione sociale favorite dai ***social networks***.

Tali dati sono il patrimonio informativo più appetibile per i criminali informatici imponendo la più forte attenzione degli addetti al contrasto ai crimini del settore.

La Polizia delle Comunicazioni è chiamata a rispondere ogni giorno a sfide sempre più complesse utilizzando moderne attrezzature ed innovative tecniche investigative operando con professionalità in forte sinergia con partner pubblici e privati ed in sintonia con organismi internazionali.

Il Direttore del Servizio
Polizia Postale e delle Comunicazioni
Antonio Apruzzese

La Polizia postale e delle comunicazioni

La Polizia Postale e delle Comunicazioni nasce all'interno dello scenario che, grazie all'evoluzione tecnologica e alla crescita culturale del Paese, ha reso la rete Internet un mezzo indispensabile per lo scambio di informazioni, l'accesso alle grandi banche dati, l'esecuzione di transazioni e disposizioni finanziarie, l'ideazione e creazione di nuove attività professionali: la rapida diffusione dell'uso di questo nuovo strumento di comunicazione ha messo in evidenza i punti di debolezza della Rete, soprattutto riguardo alla sicurezza informatica; in questo campo la Polizia di Stato, attraverso il reparto specialistico della Polizia Postale e delle Comunicazioni – creato con la legge di riforma dell'Amministrazione della Pubblica Sicurezza –, è all'avanguardia nell'azione di prevenzione e contrasto della criminalità informatica, a garanzia dei valori costituzionali della segretezza della corrispondenza e della libertà di ogni forma di comunicazione.

Il principale sforzo operativo della Polizia Postale e delle Comunicazioni è nel trovare argini di controllo sempre più adeguati alle nuove frontiere tecnologiche utilizzate dalla delinquenza, in particolare occupandosi di:

- *Pedopornografia*: attraverso il Centro Nazionale per il contrasto della pedopornografia su Internet la Polizia Postale e delle comunicazioni raccoglie segnalazioni e coordina le indagini sulla diffusione, in Internet o



tramite altre reti di comunicazione, delle immagini di violenza sessuale sui minori.

- ***Cyberterrorismo***: una qualificata squadra di investigatori monitora costantemente la rete Internet e conduce indagini specialistiche sul sempre più diffuso utilizzo di nuove tecnologie di comunicazione da parte dei gruppi antagonisti ed eversivi nazionali e stranieri.
- ***Copyright***: i circuiti di condivisione di file (*file-sharing*) e i numerosi altri servizi Internet che consentono la circolazione di opere dell'ingegno hanno contribuito alla diffusione illegale di file e hanno imposto una costante attenzione operativa al fenomeno.
- ***Hacking***: tutti coloro che utilizzano la Rete Internet per danneggiare o per colpire obiettivi a essa correlati sono oggetto di attenzione da parte degli investigatori.
- ***Protezione delle Infrastrutture Critiche del Paese***: le aziende e gli enti che sostengono e garantiscono il funzionamento del Paese mediante reti e servizi informatici o telematici vengono monitorati e protetti da attacchi informatici attraverso l'azione di un'*équipe* di investigatoti specializzati.
- ***E-banking***: le nuove frontiere del commercio e della circolazione di denaro impongono un puntuale monitoraggio delle risorse tecnologiche correlate per garantirne la sicurezza.
- ***Analisi criminologica dei fenomeni emergenti***: una qualificata *équipe* di psicologi e investigatori analizza ed elabora dati relativi alle nuove frontiere del crimine informatico, ponendo il sapere clinico e criminologico delle scienze sociali al servizio di una più efficace azione di prevenzione e repressione dei reati informatici.
- ***Giochi e scommesse online***: attraverso il monitoraggio della Rete e un'attenta analisi dei siti dedicati si individuano le attività non autorizzate dal Ministero delle Finanze – Amministrazione autonoma monopoli di Stato.

Il Servizio Polizia delle Comunicazioni

Il Servizio Polizia delle Comunicazioni è stato istituito con decreto ministeriale del 1 marzo 1998 come organo del Ministero dell'Interno per la sicurezza e la regolarità dei servizi di telecomunicazione: oggi è il punto di riferimento nel coordinamento, nella programmazione e nella pianificazione operativa degli uffici periferici della specialità.

La sua organizzazione interna ricalca l'ampia tipologia dei fenomeni di criminalità informatica e garantisce, attraverso l'alta professionalità dell'*équipe* di coordinamento, un'efficace azione di raccordo tra i singoli operatori e i rispettivi uffici territoriali. Il Servizio, cui affluiscono tutte le informazioni rilevanti in materia di *cybercrime*, svolge inoltre azioni mirate:

- nell'analisi della sfera applicativa delle normative in materia di comunicazioni;
- nell'analisi criminologica dei fenomeni criminali legati all'utilizzo di strumenti *hi-tech* ("*High Tech Crime*");
- nell'individuazione delle strategie di contrasto ai fenomeni criminali generati da sistemi



telematici e di elaborazione computerizzata dei dati;
- nella partecipazione a gruppi di lavoro istituiti presso organismi nazionali e internazionali;
- nella selezione e formazione del personale;
- nella collaborazione con il mondo accademico e gli operatori del settore della "*New Economy*";
- nella cooperazione con organi di polizia di Paesi stranieri.

I compartimenti e le sezioni

La Polizia Postale e delle Comunicazioni è presente in modo capillare sul territorio nazionale attraverso ***20 Compartimenti e 80 Sezioni***, impegnati nella lotta contro le attività illecite. Dislocazione geografica e conoscenza del territorio sono caratteristiche fondamentali per un'azione investigativa efficace.
I compiti istituzionali comprendono:
- la prevenzione e repressione dei crimini postali e informatici;
- la tutela dei servizi postali, di bancoposta e di telecomunicazione;
- il controllo del corretto utilizzo delle licenze radio-amatoriali degli apparati, degli impianti, delle emittenti radio e televisive;
- il controllo degli esercizi che commercializzano materiali o apparecchiature di telecomunicazione soggette a marcatura e omologazione;
- il raccordo operativo con gli Ispettorati Territoriali del Ministero delle Comunicazioni nelle attività di controllo amministrativo di comune interesse;
- la prevenzione e repressione dei reati legati al commercio elettronico.

La cooperazione internazionale

La necessità di muoversi in un contesto globale per finalità investigative, ha portato la Polizia Postale e delle Comunicazioni ad intessere una fitta rete di indispensabili collegamenti internazionali con gli investigatori specializzati nella materia.
Ne sono un chiaro esempio il pieno coinvolgimento in organizzazioni di cooperazione internazionale specialistica quali l'European Electronic Crime Task Force (E-ECTF) per affrontare il crimine economico on line e la Virtual Global Task Force (VGT) per tutelare i minori dai fenomeni di sfruttamento ed abuso commessi attraverso le reti di comunicazione.
Nel contempo, sono favorite le occasioni di interscambio info-investigativo con alcune polizie straniere maggiormente interessate negli illeciti criminali quali, ad esempio, il FBI ed il Secret Service degli Stati Uniti, le polizie di Bulgaria, Romania e Spagna

Il Commissariato di P.S. online

Parallelamente all'incremento dell'uso di Internet sono cresciute le aspettative di sicurezza da parte del cittadino. Per questo lo Stato ha risposto prontamente con l'istituzione del primo Ufficio di Polizia online, reperibile all'indirizzo *www.commissariatodips.it*. Prima e unica esperienza in Europa, il portale del "Commissariato di P.S. online" è un punto di riferimento per chi cerca informazioni, consigli, suggerimenti di carattere generale, o vuole scaricare modulistica e presentare denunce.

I principali servizi offerti sono tre:

- *informazione*: passaporti, immigrazione, minori, concorsi e licenze;
- *prevenzione*: Internet, consigli, segnalazioni, forum telematico;
- *repressione*: denunce via web per furti, smarrimenti e reati informatici.

Nei sei anni di attività il sito ha ricevuto più di 3.440.600 visite con oltre 142.700 iscritti. Il progetto del "Commissariato di P.S. online" ha ricevuto il premio "Most Inspring Good Practice" all'European e-Government Awards 2007, organizzato dalla Commissione Europea a testimonianza dell'innovatività e l'efficacia dell'iniziativa. Il portale del "Commissariato di P.S. online" è attualmente in fase di ristrutturazione, per la realizzazione di nuovi servizi pensati per gli utenti della rete Internet.

ALCUNI NUMERI DELL'ATTIVITÀ DEL COMMISSARIATO ON-LINE

ATTIVITÀ COMMISSARIATO P.S. ON-LINE	
Richieste di informazioni	8.384
Segnalazioni ricevute	9.884
Denunce on-line	6.327

REATI CONTRO LA PERSONA	
Denunce ricevute	5.798
Persone denunciate	1.112
Perquisizioni	62
ATTIVITÀ CONNESSE AI CONTROLLI PRESSO PHONE CENTER E INTERNET POINT	
Denunciati	6
Controlli presso esercizi	114

REATI INERENTI AL SERVIZIO POSTALE	
Arrestati	31
Denunciati	236
Uffici postali controllati	174.456

C.N.C.P.O.

Centro nazionale per il contrasto alla pedopornografia on-line

Tutte le indagini in tema di pedopornografia online e tutte le iniziative correlate alla prevenzione e alla gestione delle fonti informative in materia sono coordinate dal "Centro nazionale per il contrasto alla pedopornografia sulla Rete Internet", istituito con la legge n. 38 del 6 febbraio 2006 presso il Servizio Polizia Postale e delle Comunicazioni.
Attraverso una capillare attività di monitoraggio dei siti pedopornografici, il Centro aggiorna costantemente una black list da trasmettere agli Internet Service Provider così che possano applicare filtri per impedire a chi naviga dall'Italia di imbattersi in tale tipologia di spazi illeciti della Rete Internet.
Le stesse attività di monitoraggio hanno consentito di acquisire una conoscenza sempre più approfondita dei fenomeni della Rete e, in primo luogo, hanno rivelato agli investigatori nuove modalità tecnologiche messe in atto da circuiti criminosi finanziari dediti alla commercializzazione della pedopornografia.
Il Centro nazionale antipedofilia pertanto ha indirizzato le proprie attività anche sul fronte del contrasto al mercato di questo materiale, avvalendosi del sostegno delle banche e delle aziende di credito con la mediazione della Banca d'Italia.
Quale organo di raccordo operativo in materia di lotta alla pedofilia in Rete, il Centro dialoga con l'Osservatorio per il contrasto della pedofilia presso la Presidenza del Consiglio dei Ministri-Dipartimento per le Pari Opportunità, al fine di contribuire all' analisi dei fenomeni e dei dati provenienti dalle attività di prevenzione e contra-

sto allo sfruttamento ed abuso sessuali di minori attraverso le nuove tecnologie.
Le attività del Centro si avvalgono altresì del confronto e della collaborazione di tutte le categorie istituzionali e sociali dedite all'educazione e alla tutela dei minori. In tal senso, anche nell'ambito di progetti europei , sono state avviate procedure di dialogo avanzato con Organizzazioni non Governative e mondo dell'Industria, per perseguire comuni strategie di contrasto ai fenomeni di rischio della Rete e per avanzare settori di ricerca e di produzione di nuove tecnologie utili alle investigazioni.
Anche nell'ultimo anno gli sforzi investigativi si sono concentrati in particolare sull'identificazione delle vittime di abuso sessuale ritratte nel materiale pedopornografico, attività particolarmente complessa e laboriosa che richiede la ricostruzione di una storia di abuso a partire da un volto, da uno sfondo, a volte da pochissimi dettagli significativi presenti nelle immagini. Grazie ai notevoli investimenti compiuti dalla Polizia di Stato in tale settore, il Centro si avvale oggi di collegamenti in tempo reale con la Banca dati delle immagini pedopornografiche dell'Interpol di Lione e con il "NCMEC" (National Center for Missing and Exploited Children), agenzia non governativa statunitense preposta al supporto delle Forze di Polizia per la gestione dei casi investigativi ed al coordinamento negli U.S.A. delle informazioni sulla circolazione di materiale pedopornografico via web provenienti dai Provider.
L'esplorazione degli ambienti della Rete frequentati da comunità virtuali ha puntato con successo investigativo verso spazi che si definiscono di pura "pedofilia ideologica" , ovvero siti che sostengono con motivazioni "pseudoculturali" la legittimazione della pedofilia. Ancora una volta indagini di carattere internazionale, condotte sotto il coordinamento di Europol, hanno rivelato che, anche nel nostro territorio, i frequentatori delle comunità "boylover", apparentemente innocui, non si limitavano allo scambio di sole opinioni , confermando in pieno i propri comportamenti criminosi di scambio di materiale pedopornografico e di abuso sessuale su minori.
È importante sottolineare che sono sempre più numerose le segnalazioni pervenute da parte di adolescenti, di familiari e di insegnanti in merito a casi di adescamento in Rete soprattutto riferite a profili sui social network; ciò ha quasi sempre consentito ai minori coinvolti di "evitare spiacevoli incontri".

ATTIVITÀ INVESTIGATIVA IN MATERIA DI PEDOPORNOGRAFIA

Arrestati	51
Denunciati	777
Perquisizioni	665
Siti monitorati	21.199

Unità di analisi del crimine informatico

In seno al C.N.C.P.O. opera l'Unità di Analisi dei crimini informatici, composta da un'*équipe* di psicologi della Polizia di Stato. Le attività del nucleo specialistico si prefiggono di integrare le competenze di natura socio-psicologica con i contributi provenienti dall'attività di contrasto al Cyber-Crime. Tale integrazione si sostanzia in un complessivo approfondimento della conoscenza dei fenomeni della devianza informatica, che diventa patrimonio conoscitivo a disposizione degli operatori della Specialità della

Polizia di Stato e del mondo civile. Il lavoro di studio e analisi condotto dall'U.A.C.I., dunque, supporta le attività investigative attraverso un costante e sistematico contributo psicologico e criminologico alle indagini stesse. Riguardo alla prevenzione del fenomeno pedofilia on-line vengono effettuate attività di formazione delle figure professionali impegnate sul campo e forniti contributi psico-educativi all'interno dei contesti preposti alle iniziative di contrasto. Nell'ultimo anno l'attività dell'Unità si è concentrata maggiormente su due progetti di ricerca-intervento:

- ***Digital-profiling***: attraverso un'analisi dettagliata dei comportamenti on-line, delle abitudini di navigazione, delle conversazioni in chat e nei socialnetwork tra autori dei reati di sfruttamento sessuale dei minori a mezzo Internet, si stanno costruendo modelli comportamentali e strumenti di valutazione della pericolosità calati sulla specificità della coniugazione italiana del fenomeno pedofilia on-line.

Le attività di *profiling* vengono integrate da un continuo e proficuo confronto con forze di Polizia straniere, in un'ottica di fruttuosa condivisione delle informazioni e dei dati di analisi criminologica.

- Il ***sostegno al personale***: dal 2010 si conduce un'attività di "ricerca-intervento" che prevede il coinvolgimento di circa 400 tra operatori, funzionari e dirigenti degli Uffici periferici, in attività di analisi e prevenzione dello stress lavorativo specifico. Attraverso la somministrazione di questionari, la realizzazione di colloqui individuali e la presentazione periodica dei risultati della ricerca, l'Unità sta studiando nel dettaglio gli effetti, le strategie percorse e percorribili, le procedure protettive necessarie alla tutela emotiva e psicologica del personale quotidianamente impegnato nel contrasto alla pedofilia on-line.

Progetti educativi

Navigazione sicura e consapevole dei minori sulla rete Internet

Negli ultimi anni si è verificato un vertiginoso aumento dell'utilizzo delle nuove tecnologie, soprattutto da parte dei minori, i cosiddetti "nativi digitali"; d'altra parte si risconta un altrettanto preoccupante aumento dei crimini informatici, di cui la pedopornografia è una delle più deprecabili espressioni.
Proprio perché l'unica arma veramente incisiva è la prevenzione, sono state realizzate numerose campagne di sensibilizzazione e prevenzione sui rischi e i pericoli per i minori sulla rete Internet, le cui più significative espressioni sono i ***progetti educativi*** attuati dalla Polizia delle Comunicazioni, supportati da numerose strutture che ne hanno reso possibile la concretizzazione all'interno delle scuole su tutto il territorio nazionale.

Tra i nuovi progetti attuati vi è in particolare ***Vodafone Smart Tutor***, un'applicazione per smartphone Android realizzata da Vodafone in collaborazione con la Polizia di Stato che consente di personalizzare le funzionalità del cellulare per un utilizzo sicuro e protetto da parte dei minori.
L'applicazione è scaricabile gratuitamente dal portale inFamiglia (*www.infamiglia.vodafone.it*) e su Google Play.

Particolare rilievo ha l'iniziativa ***Web in cattedra***, il cui fine è quello di "formare i docenti per proteggere gli studenti", cui viene data la possibilità di apprendere direttamente dagli specialisti della Polizia delle Comunicazioni, degli Uffici minori delle Questure, di Microsoft e dell'O.N.A.P., sia i rischi che i rimedi della navigazione sicura.
Nel corso vengono impartite nozioni specifiche, anche sui più diffusi programmi di protezione utilizzati sulla rete per salvaguardare il proprio PC da virus o da fenomeni di malware e spamming, e viene messo a disposizione il materiale informativo necessario. I docenti hanno il compito di istruire i colleghi all'interno dei singoli istituti, in modo da creare una rete di formatori, con competenze e strumenti adeguati, che possano sensibilizzare gli studenti

verso un uso consapevole e corretto del mezzo informatico, nel giusto equilibrio tra potenzialità e rischi.
Ha inoltre assunto grande rilevanza il progetto ***Non perdere la bussola***, frutto della collaborazione tra la Polizia Postale e delle Comunicazioni, Google e YouTube. L'iniziativa nasce per gli studenti delle scuole medie inferiori e superiori, ma con il tempo è stata estesa a un numero sempre più ampio di utenti, compresi genitori e insegnanti, fino a raggiungere 450.000 studenti e oltre 1.000 istituti scolastici su tutto il territorio nazionale.
La necessità di istituire un progetto rivolto direttamente ai giovani, utilizzatori assidui di internet e di social network, si è fatta sempre più pressante nel corso degli ultimi anni, a causa dei gravi e crescenti rischi connessi all'uso, spesso scorretto e indiscriminato, di strumenti che nascono per la comunicazione e la socializzazione.
"Non perdere la bussola" si è rivelato uno strumento fondamentale per aiutare i giovani studenti, le proprie famiglie e i loro insegnanti, a utilizzare in modo responsabile e sicuro lo strumento informatico.
Di particolare importanza infine il progetto ***In strada come in rete***, realizzato dalla Provincia di Roma con la Polizia Postale e delle Comunicazioni, Polizia Provinciale, Unicef, Microsoft, Unione Nazionale Consumatori, Google, YouTube e il portale Skuola.net.
L'iniziativa, rivolta ai ragazzi tra i 10 e i 14 anni, ai loro genitori e agli insegnanti delle scuole medie di primo grado della provincia di Roma, ha l'obiettivo di contrastare i rischi tipici dell'età adolescenziale relativi al comportamento degli stessi sia durante la navigazione in Rete che nella circolazione stradale.

La peculiarità del progetto si basa sul fatto che si muove in parallelo a quello realizzato dalla Polizia Provinciale sulla circolazione sicura in strada.
Al progetto si affianca inoltre un concorso, al termine del quale vengono premiati i migliori elaborati, (testi, filmati e altro) ispirati ai temi della circolazione sicura e consapevole su strada e della navigazione sicura in Internet.
L'intervento della Polizia delle Comunicazioni, grazie a queste iniziative, ha reso possibile aprire

un canale di dialogo preferenziale con i giovani, incrementando la consapevolezza di un agire cosciente e facilitando la comunicazione con le istituzioni. I risultati conseguiti fino a ora rappresentano solo il primo passo di un percorso mirato a rendere sempre più trasparente e sicura la navigazione informatica dei nostri ragazzi.

Consigli per un uso sicuro dei social network

È sconsigliato l'uso dei social network ai minori di 14 anni: la loro inesperienza, la loro tendenza a sottostimare i rischi della diffusione di immagini e informazioni riservate, la loro curiosità verso gli altri e verso le nuove tecnologie potrebbero esporre i ragazzi e le loro famiglie a vari rischi reali (es. adescamento,

PER I GENITORI

Consigli

Scegliete per i vostri figli un computer portatile e, se possibile, utilizzatelo per la sola navigazione in internet: posizionatelo 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".
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.
Per la navigazione dei più piccoli usate software "filtro" con un elenco predefinito di siti possibili, scegliete la lista di questi siti insieme ai vostri figli spiegandogli che è una misura di sicurezza indispensabile. È opportuno verificare periodicamente che i filtri funzionino in modo corretto e tenere segreta la parola chiave.
Insegnate ai vostri figli l'importanza di non rivelare in Rete dati personali come nome, cognome, età, indirizzo, numero di telefono, nome e orari della scuola, nome degli amici. Ricordategli inoltre che non è consigliabile pubblicare in internet foto di sé o degli altri, soprattutto se questi sono minorenni e inconsapevoli di apparire on-line.

PER I BAMBINI E I RAGAZZI

Consigli

Nelle chat, nei forum, nei blog e nei giochi di ruolo non dare mai il tuo nome, cognome, indirizzo, numero di cellulare o di casa. Lo schermo del computer nasconde le vere intenzioni di chi chatta con te.
Non scaricare programmi se non ne conosci bene la provenienza: potrebbero contenere virus che danneggiano il computer, spyware che violano la privacy e rendono accessibili informazioni riservate.
Non incontrare mai persone conosciute su Internet senza avvertire i tuoi genitori. Se proprio vuoi incontrare qualcuno conosciuto su Internet, prendi appuntamento in luoghi affollati e porta con te almeno due amici.
Ricorda che le tue immagini e quelle degli altri sono una cosa privata, da proteggere: non mettere foto o filmati fatti con il telefonino in community, chat o socialnetwork che siano aperti a tutti, grandi e piccini. Una volta immessi in rete, foto e filmati, possono continuare a girare anche se tu non vuoi.
La promessa di ricariche facili, di regali gratuiti, di vantaggi fantastici che arrivano via sms o nelle chat da adulti sconosciuti devono metterti in allerta: alcuni truffatori e criminali utilizzano questi mezzi per farti aderire a costosi abbonamenti a pagamento, o per carpire la tua fiducia e suggerirti di fare cose non adatte alla tua età.
Ricorda che se qualcuno vuole offrirti un vantaggio troppo facile, senza neanche conoscerti, probabilmente ti prende in giro!

violazione della privacy propria e altrui, commissione inconsapevole di reati, etc.).
Ricorda che un'immagine condivisa in un social network entra definitivamente nel web e che non sarà possibile controllarne mai più la diffusione, anche qualora fosse utilizzata in siti che non conosci, che non ti piacciono e/o che non condividi.
Ricorda che molte delle informazioni che posti nella bacheca del tuo profilo consentono di ricostruire la tua identità, le tue abitudini, i tuoi gusti e molto più di quel che immagini: sei sicuro di volere che molte persone, magari anche i tuoi genitori e/o i tuoi insegnanti e/o i tuoi futuri datori di lavoro sappiano quello che racconti?
Creare profili con nomi equivoci e/o postare messaggi allusivi di una disponibilità sentimentale e/o erotica ti espone al rischio di richiamare l'attenzione di malintenzionati della rete. Evita di proporti in un ruolo non adatto alla tua età o ai tuoi reali desideri se non sei pienamente consapevole, per età ed esperienza, delle conseguenze che tali dichiarazioni di disponibilità possono comportare (es. contatti

COME EQUIPAGGIARE IL COMPUTER E USARLO IN SICUREZZA

Consigli

- 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 dei dati più importanti.
- Tenete aggiornato un buon antivirus e un firewall che proteggano continuamente il vostro pc e chi lo utilizza. Vi metterete al sicuro dal rischio di malware e virus indesiderati e dai rischi per la vostra sicurezza personale che essi comportano. Aggiornate e scaricate le nuove versioni dei programmi per rendere permanente la protezione del computer.
- Usate un firewall come "gatekeeper" tra il vostro computer e Internet; i firewall sono essenziali per chi ha una connessione ADSL o via cavo ma sono preziosi anche per chi utilizza la connessione telefonica.
- Impostate la "cronologia" di navigazione in modo che mantenga traccia per qualche giorno dei siti visitati da vostro figlio.
- Controllare periodicamente il contenuto dell'hard disk del computer.
- Usare software "filtri" con un elenco predefinito di siti da evitare. Verificate periodicamente che funzionino in modo corretto e tenete segreta la parola chiave.
- Leggere le e-mail con i bambini più piccoli controllando ogni allegato al messaggio. Se non conoscete il mittente non aprite l'e-mail, né eventuali allegati: possono contenere virus o spyware in grado di alterare il funzionamento del computer. Date le stesse indicazioni ai ragazzi più grandi.
- Non tenete il computer allacciato alla Rete quando non lo usate: è consigliato piuttosto disconnettere il computer.
- 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'utilizzatore ne sia a conoscenza.
- Scaricate regolarmente le "security patches" (modifiche per incrementare la sicurezza dei software) dal vostro fornitore di software.

da sconosciuti, argomenti imbarazzanti, offerte e richieste oscene).
Ricorda che a disciplinare il comportamento in Rete c'è non solo una netiquette da rispettare ma anche leggi che definiscono chiaramente cosa costituisce reato e cosa no: comportati sempre correttamente nei confronti degli altri utenti dei social network, evita di creare gruppi che inneggiano a comportamenti indesiderabili e che ledono l'immagine e/o la credibilità di persone note e meno note.
Ricorda di tenere segreta la password di accesso al tuo profilo sul social network: compagni di classe e conoscenti potrebbero utilizzarla per sostituirti e commettere azioni scorrette a tuo nome, per diffondere informazioni riservate che ti riguardano, anche al solo scopo di fare uno scherzo. Non cercare di ottenere la password di accesso al profilo o alla casella di email di altri utenti poiché questo, seppur animato dalle più innocenti intenzioni, costituisce reato ed espone te al rischio di accuse molto serie.
Imposta il tuo profilo in modo da consentirne la visitabilità solo agli amici che avrai autorizzato tu previa richiesta: in questo modo selezionerai direttamente chi accede alla tua pagina e ti garantirai di essere contattato solo da persone conosciute e affidabili.

Il cyber-stalking: nuove strade per la persecuzione

La Legge n. 38/2009 introduce in Italia il reato di "Stalking" definendo in maniera chiara quali comportamenti persecutori siano da considerarsi reato e possano essere quindi oggetto di denuncia. La progressiva diffusione dei nuovi mezzi di comunicazione ha contribuito negli ultimi anni a modificare i luoghi e le modalità attraverso le quali un persecutore riesce a ingenerare uno stato permanente di preoccupazione, ansia e terrore nella vittima delle sue attenzioni deviate. Dall'emanazione della legge, molte denunce sono state sporte alla Polizia delle Comunicazioni, anche se esiste un "numero oscuro" di casi non denunciati a causa dei gravi risvolti psicologici che tale reato ha sulla vittima.
Sono i social network e le caselle di posta elettronica, i luoghi virtuali dove spesso si cerca visibilità per danneggiare qualcuno; anche il telefono cellulare è il mezzo che più frequentemente trasforma una delusione in assillo, in persecuzione. Trasversale a tutte le età e a tutte le condizioni socioculturali, il cyber-stalking, la coniugazione più moderna dell'incapacità di gestire una relazione sentimentale d'amore o d'amicizia, entra nella vita delle potenziali vittime da un monitor per rimanervi a lungo, a volte conducendo a epiloghi tragici. La sicurezza sul web dipende soprattutto da chi lo utilizza: le persecuzioni telematiche si possono prevenire attraverso l'uso di semplici accorgimenti tecnici e un adeguato utilizzo della navigazione nel mondo di internet.

Le regole d'oro anti-cyberstalking:

- quando apri un profilo sui social network limita al minimo le informazioni visibili a tutti che ti riguardano: non pubblicare il tuo indirizzo, il tuo luogo di lavoro, i luoghi di svago solitamente frequentati.
- Imposta le regole di tutela della tua privacy sui social network consentendo solo a persone da te autorizzate l'accesso ai contenuti della tua bacheca, alle immagini e ai video caricati sulla tua pagina.
- Se concedi la possibilità a sconosciuti di accedere alla tua casella di posta, al tuo blog, al tuo profilo di un social network segnala immediatamente agli amministratori dei vari servizi web eventuali comportamenti indesiderati.
- Dietro allo schermo di un computer si nascondono intenzioni anche molto diverse: le parole scritte, gli emoticons, le immagini che ricevi da uno sconosciuto possono far nascere in te sentimenti reali verso persone che non esistono.
- Se la tua relazione d'amore o amicizia virtuale ti fa sentire a disagio parlane con qualcuno di cui ti fidi: ricorda che un amore o un'amicizia autentica non generano, di solito, sensazioni così negative.
- Considera un gioco le relazioni sentimentali che nascono su internet: un incontro reale con qualcuno conosciuto nel mondo del virtuale ti espone sempre al rischio di trovare una persona molto diversa da quella che pensavi, magari anche pericolosa.
- Non rispondere mai a messaggi provocatori, offensivi e minacciosi pubblicati sugli spazi web personali: le tue risposte possono alimentare l'ossessione del potenziale stalker. Annota i tempi e i luoghi virtuali degli atti persecutori, i contenuti dei messaggi minatori e recati in un ufficio di Polizia Postale e delle Comunicazioni per effettuare una denuncia.
- Se le attenzioni virtuali di una persona conosciuta sul web si fanno costanti, minacciose, offensive, o comportano la rivelazione pubblica di immagini e contenuti personali

forse sei vittima di cyberstalking: segnala i comportamenti, la tempistica dei contatti, i contenuti diffusi senza il tuo consenso al sito *www.commissariatodips.it* in modo che esperti della materia possano aiutarti a capire cosa fare.

- Se sei oggetto di minacce, ingiurie e molestie sui tuoi spazi web sei vittima di un reato denunciabile in qualsiasi ufficio della Polizia delle Comunicazioni. Vedi indirizzi e numeri di telefono su www.commissariatodips.it.
- Se hai deciso di incontrare una persona conosciuta su internet dagli un appuntamento in un luogo frequentato, in orario diurno e, se possibile, in compagnia di altre persone.

I comportamenti allarme

Alcuni comportamenti dei vostri figli non vanno sempre ascritti a situazioni di abuso o molestie, soprattutto se stanno attraversando un momento evolutivo particolare (preadolescenza, adolescenza, separazioni o cambiamenti familiari). Tuttavia, se questi comportamenti riguardano l'uso del computer o del

NOVE REGOLE DA TENERE A MENTE

Abitudini in Rete

- TIENI IL TUO PC BEN PROTETTO
  Usa gli aggiornamenti automatici per avere sempre l'ultima versione del software, soprattutto quello per Internet. Usa firewall, antivirus e antispam.
- CUSTODISCI LE INFORMAZIONI PERSONALI
  Prima di inserire i tuoi dati personali su Internet controlla che siano presenti i segni che indicano la sicurezza della pagina: la scritta https nell'indirizzo e il segno del lucchetto.
- UTILIZZA PASSWORD SICURE E TIENILE RISERVATE
  Devono essere lunghe (almeno otto caratteri), contenere maiuscole e minuscole, numeri e simboli. Non usare la stessa password per siti diversi.
- PRIMA DI FARE CLIC, USA LA TESTA
  Quando ricevi un allegato sospetto, controlla bene prima di selezionarlo: potrebbe essere un trucco. Se conosci la persona che lo invia chiedi conferma che te lo abbia mandato veramente; se non la conosci, ignoralo.
- NON DARE INFORMAZIONI VIA E-MAIL
  Non dare mai informazioni personali in risposta a un messaggio e-mail o di Messenger (cognome, indirizzo, numero di telefono, foto, età e così via).
- ATTENZIONE AI FALSI
  Messaggi allarmistici, richieste disperate d'aiuto, segnalazioni di virus, offerte imperdibili, richieste di dati personali "per aggiornare il tuo account": diffida di tutti i messaggi di questo tono e attiva un sistema per individuarli, come il filtro SmartScreen® di Windows® Internet Explorer®.
- SUI SOCIAL NETWORK CON ALLEGRIA E PRUDENZA
  Su Facebook, Twitter, Windows Live™ e su tutti gli altri social network controlla bene le impostazioni. Chi può vedere il tuo profilo? Chi può fare ricerche su di te? Chi può fare commenti? Chi può esporti in situazioni che non controlli?
- PENSA A QUELLO CHE PUBBLICHI SU INTERNET
  Le tue foto, i tuoi messaggi e le tue conversazioni possono essere viste anche da sconosciuti. Non postare nulla che consideri personale o riservato e di cui potresti pentirti in futuro.
- RISPETTA LA NETIQUETTE
  La netiquette è un insieme di regole di buon comportamento da seguire sui social network, nei forum, nelle community: prima di seguire il tuo istinto, leggi il regolamento del sito in cui ti trovi; non insultare o mettere in cattiva luce nessuno; non pubblicare messaggi privati di altre persone.

Cellulare

L'USO SICURO DEL TELEFONINO PER I GENITORI

- Spiega a tuo figlio che il telefonino è un mezzo di comunicazione che impone una cautela analoga a quella che si ha nei confronti del computer. Scegli per i più piccoli modelli semplici, quelli con telecamere e fotocamere riservali a quando sapranno utilizzarli in modo sicuro e consapevole.
- Spiega a tuo figlio che foto e riprese effettuate con il telefonino sottostanno alla normativa italiana in materia di protezione dell'immagine e della privacy delle persone.
- Per i telefonini che consentono la navigazione in Internet o l'accesso a community e chat, spiega a tuo figlio che i rischi in termini di adescamento da parte di pedofili online sono i medesimi della Rete "tradizionale".
- Scegli per i tuoi figli SIM Card ricaricabili e ricarica sempre tu il credito in modo da poter monitorare la quantità di traffico telefonico effettuato.
- Al momento dell'attivazione della SIM Card fornisci ai tuoi figli il PIN ma non il PUK. Con il PUK infatti potrai accedere al telefono anche se il PIN è stato modificato.
- Spiega ai tuoi figli che sms o mms che promettono ricariche facili o altri vantaggi immotivati sono spesso il primo contatto effettuato da chi non ha buone intenzioni.
- Parla ai tuoi figli della potenziale pericolosità di richiamare col telefonino numeri sconosciuti da cui provengono squilli o chiamate mute. In passato si è trattato di una modalità con cui i pedofili adescavano i minori.
- Scoraggia tuo figlio dal diffondere foto o filmati fatti con il telefonino in community o chat telefoniche. Una volta immesse in Rete foto e filmati possono continuare a essere diffuse senza controllo per lungo tempo.

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.

Contrasto degli illeciti relativi al commercio elettronico

Anche l'acquisto di beni e servizi online è sempre più frequente mediante il pagamento con carte di credito, bancomat, moneta elettronica. Nell'ambito delle frodi online l'attività della Polizia Postale e delle Comunicazioni ha raggiunto eccellenti risultati, così come si può rilevare dai dati pubblicati in queste pagine.

Uso delle carte di credito

Le carte di credito garantiscono un sistema di pagamento comodo e relativamente sicuro, sia nell'utilizzo tradizionale che in Rete. Il verificarsi di alcune frodi implica però che l'utente ponga attenzione e cautela nel loro utilizzo. Uno dei sistemi più diffusi utilizzati dai truffatori per acquisire i codici è chiamato *skimming*. Consiste nella cattura dei dati della banda magnetica con la semplice "strisciata" della carta di credito su un apparecchio denominato, ap-

LA CARTA DI CREDITO NEI NEGOZI

Ecco una lista di cautele necessarie per l'utente di carta di credito dovrebbe adottare per ridurre le possibilità di clonazioni e di frodi:

1. Non cedere la carta ad altre persone.
2. Non perdere mai di vista la propria carta di credito al momento del pagamento.
3. Diffidare di un qualsiasi esercizio che afferma di non avere l'apparecchiatura P.O.S. in prossimità della cassa.
4. Controllare, al momento del recapito della carta di credito e del successivo codice PIN che la busta sia integra, che rechi l'intestazione della vostra banca, di chi emette la carta di credito oppure della società incaricata dei servizi di recapito postale.

PER GLI ESERCENTI

Anche i commercianti dovrebbero adottare alcune cautele, effettuando due semplici controlli per ridurre le possibilità di frodi:

1. In caso di sospetto di utilizzo fraudolento di carta di credito clonata, è utile confrontare se vi sono differenze tra il numero della carta di credito sul supporto plastico e il numero di carta di credito (15 o 16 cifre) che viene stampato dal P.O.S. sullo scontrino. Il numero è rilevabile subito sotto data e ora della transazione, a volte preceduto dalla lettera "C".
2. Controllate frequentemente il macchinario P.O.S., al fine di impedire la manomissione e la modifica dell'apparecchiatura.

punto, *Skimmer*. Lo Skimmer può essere grande quanto un pacchetto di sigarette e autoalimentato con batteria, ma anche più grande e può memorizzare fino a diverse decine di bande magnetiche. I dati illecitamente acquisiti vengono trascritti, attraverso un comune PC e un programma di gestione per bande magnetiche, su un supporto plastico, con le caratteristiche di una carta di credito/ bancomat. Lo skimmer è un'apparecchiatura diversa dal P.O.S.: per eseguire questo genere di frodi è necessario perciò che il malintenzionato entri in possesso della carta di credito del cliente senza essere visto.

COME BLOCCARE LA PROPRIA CARTA DI CREDITO

n. utili

Tutte le società emittenti delle carte di credito forniscono un numero telefonico gratuito da chiamare in caso di furto o smarrimento per bloccare immediatamente la carta. Di seguito si segnalano i numeri telefonici verdi delle carte più diffuse:

Servizi interbancari: 800.151616
American Express Italia: 06.72900347
American Express estero: 800.26392279
Top Card: 800.900910
Diner's: 800.864064
Agos Itafinco: 800.822056
Deutschebank: 800.207167
Setefi: 800.825099
Banca Sella: 800.663399
Findomestic: 800.866116
Citibank: 800.407704
Banca Fineco: 800.525252

Contrasto al crimine economico e finanziario on line e mezzi elettronici di pagamento

Le nuove frontiere dell'informatica consentono oggi di estendere al mondo virtuale ciò che in precedenza era peculiarità di quello reale. I pagamenti, il denaro o i titoli di credito virtuali sono oggi patrimonio corrente della società dell'informazione e sono diventati strumenti di larghissimo uso per gran parte della popolazione. Ma l'applicazione dell'informatica ai sistemi di pagamento è diventato anche una nuova e redditizia frontiera per le organizzazioni criminali. La Polizia Postale e delle Comunicazioni si frappone allo sfruttamento illecito di tali strumenti e conduce una lotta senza quartiere a quelle organizzazioni criminali generando sicurezza ed uso consapevole dei sistemi di pagamento e credito elettronici. Per il conseguimento di tale obiettivo il Servizio Polizia Postale e delle Comunicazioni ha instaurato un efficace rapporto di collaborazione con l'Associazione Bancaria Italiana – ABI, i principali istituti di credito ed i fornitori dei sistemi di pagamento elettronico, formalizzato con la stipula di accordi convenzionali mirati alla condivisione dei dati e delle informazioni utili alla prevenzione e al contrasto dei fenomeni di aggressione criminale alla clientela dei sistemi e servizi di home banking e monetica.

Utilizzo consapevole del sistema di home banking e delle carte elettroniche di pagamento

È opportuno effettuare gli acquisti su siti web conosciuti in modo da limitare la possibilità di fornire informazioni personali a terzi; per il perfezionamento dell'acquisto on line è infatti necessario inserire il numero della carta di credito, la relativa scadenza ed il codice di sicurezza posto sul retro della stessa (CVV); recentemente le società emittenti le carte utilizzano ulteriori sistemi di autenticazione attraverso l'inserimento di un codice o una password che conclude la transazione; è consigliabile non fornire troppe

ATTIVITÀ DI CONTRASTO ALLE TRUFFE ON LINE

COMPUTER CRIME (Phishing, Furto identità personale, Attacchi Informatici, diffusione malware)	
Arrestati	6
Denunciati	975
Controlli effettuati	19.929

MONETICA	
Arrestati	77
Denunciati	1.264
Controlli effettuati	968

COMMERCIO ELETTRONICO	
Arrestati	15
Denunciati	3.022
Controlli effettuati	2.008

informazioni personali: le transazioni per andare a buon fine necessitano dei soli dati riportati sulla carta di credito.
I siti dedicati al commercio elettronico utilizzano protocolli di sicurezza che permettono di identificare l'utente (uno tra i più diffusi è Secure Socket Layer – SSL), e impediscono l'accesso, casuale e non, ad altri utenti. Si può verificare se durante la transazione in basso a destra della finestra compare un'icona con un lucchetto, ciò sta a significare che in quel momento la connessione è sicura; è opportuno non accedere ai siti di commercio elettronico attraverso link all'interno di e-mail; con questa tecnica truffaldina, denominata "phishing" (abboccamento), il collegamento nel messaggio non vi farà andare sul sito ufficiale del vostro negozio virtuale, bensì su un clone, creato per carpire i dati della vostra carta di credito. I negozi online, le banche e le società emittenti le carte di credito non inviano messaggi e-mail contenenti collegamenti diretti al sito web ufficiale.

Il computer utilizzato per gli acquisti e le operazioni bancarie on-line deve essere sempre aggiornato, sia per quanto riguarda il sistema operativo, sia il browser di navigazione. È necessario inoltre installare un sistema antivirus. Sulla rete internet sono presenti, infatti, particolari "malware", programmi dannosi, in grado di carpire i dati immessi sulla rete dal proprio computer.

Carte di debito (bancomat)

Ecco cosa fare invece prima di eseguire una qualsiasi operazione presso uno sportello Bancomat:

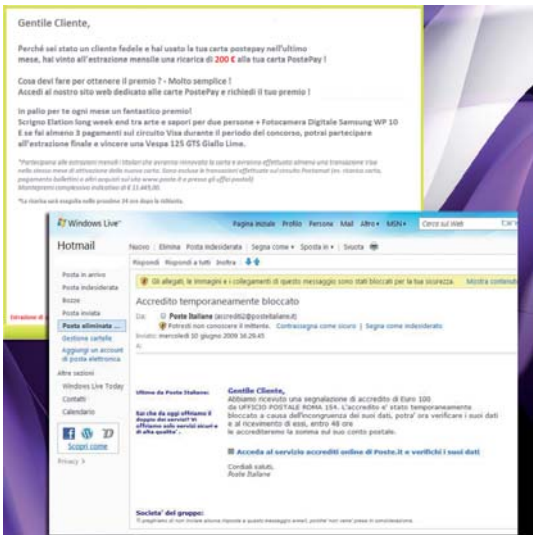
1. Accertarsi delle "condizioni" dello sportello alla ricerca di anomalie e modifiche come, per esempio, microtelecamere posizionate sulla verticale o diagonale rispetto alla tastiera che riprendano quanto viene digitato.
2. Controllare se la bocca della fessura dove si inserisce la tessera Bancomat è fissa sullo sportello. Se si muove o addirittura si stacca significa che è stata coperta da uno Skimmer.

3. Verificare se anche la tastiera è ben fissa. Se si osserva un gradino di un paio di millimetri, allora è probabile che i malfattori abbiano sovrapposto una "loro" tastiera per catturare il codice PIN.
4. Digitare il codice PIN avendo cura di nasconderlo con il palmo della mano.
5. Nel caso di dubbi non introdurre la tessera e non inserire il codice Pin, allontanarsi dalla banca e poi chiamare le forze dell'ordine. Generalmente i malfattori sono appostati nei dintorni, quel tanto che basta per essere in contatto visivo e "tenere" d'occhio la situazione. In auto hanno un computer portatile con tecnologia "senza fili" che riceve informazioni e immagini dalla telecamera.

Le truffe via e-mail

L'attività di pubblicizzazione di merci e business e il commercio elettronico su Internet offrono possibilità di sviluppo notevoli per molte aziende oltre a costituire una effettiva comodità per i consumatori. Ma al moltiplicarsi delle opportunità aumenta il rischio delle truffe ai danni degli utenti attuate attraverso i messaggi di posta elettronica.
Di seguito si indicano alcune delle principali truffe telematiche perpetrate soprattutto via e-mail:

- *finte vendite all'asta sul web* con prezzi gonfiati e merci offerte e mai inviate ai clienti;
- *vendite di merci generiche* su catalogo online, con merci mai inviate o diverse rispetto a quanto pubblicizzato;
- *offerta di servizi gratuiti* su Internet che poi si rivelano a pagamento o mancata fornitura di servizi pagati o fornitura di servizi diversi da quelli pubblicizzati;



- *vendite di hardware o software su catalogo online*, con merci mai inviate o diverse rispetto a quanto pubblicizzato;
- *schemi di investimento a piramide* e multilevel business;
- opportunità di *affari e franchising*;
- *offerte di lavoro a casa* con acquisto anticipato di materiale necessario all'esecuzione di tale lavoro;
- *prestiti di denaro* (che non vengono poi concessi) con richiesta anticipata di commissione;
- *false promesse di rimuovere informazioni negative* per l'ottenimento di crediti (es. rimozione di nominativi da black list); false promesse di concessione (con richiesta di commissione) di carte di credito a soggetti con precedenti negativi;
- *numeri a pagamento* (tipo 899) da chiamare per scoprire un ammiratore segreto o una fantomatica vincita (di vacanze, di oggetti).

Quasi sempre il tentativo di truffa inizia con l'*invio di una e-mail* alla potenziale vittima. In caso di sospetto è opportuno salvare l'e-mail e informare immediatamente la Polizia delle Comunicazioni.

Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche

Con decreto del Ministro dell'Interno del 9 gennaio 2008 è stato istituito il "Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche – C.N.A.I.P.I.C.". Tale provvedimento ha dato attuazione a quanto previsto dall'art. 7 bis, comma 1°, della legge 31 luglio 2005 n. 155, che affida al Servizio Polizia Postale e delle Comunicazioni (nella sua qualità di organo centrale del Ministero dell'Interno per la sicurezza e la regolarità dei servizi delle telecomunicazioni), la competenza esclusiva per l'erogazione dei servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale (I.C.). Con lo stesso decreto, sono stati individuati come I.C. i sistemi e i servizi informatici di supporto alle funzioni di istituzioni e amministrazioni pubbliche, enti con personalità giuridica pubblica o privata e aziende, operanti nei settori dei rapporti internazionali, della sicurezza, della giustizia, della difesa, della finanza, delle comunicazioni, dei trasporti, dell'energia, dell'ambiente, della salute e delle acque, ovvero la cui attività, per ragioni di tutela dell'ordine e della sicurezza pubblica, sia riconosciuta di interesse nazionale dal Ministro dell'Interno, anche su proposta dei Prefetti – Autorità provinciali di pubblica sicurezza. I servizi di protezione informatica sono erogati attraverso collegamenti telematici dedicati tra il C.N.A.I.P.I.C. e le singole I.C., realizzati sulla base di convenzioni stipulate con il Dipartimento della

Pubblica Sicurezza e, in sostanza, in un contesto di collaborazione sinergica pubblico-privato.

Funzioni del C.N.A.I.P.I.C.

Avvalendosi delle tecnologie di elevato livello e del personale altamente qualificato del Servizio Polizia Postale e delle Comunicazioni, in cui è inserito, il C.N.A.I.P.I.C. è incaricato della prevenzione e del contrasto della minaccia informatica di matrice terroristica o criminale, che ha per obiettivo le I.C., e opera attraverso l'esercizio delle funzioni di:

- Sala operativa – Punto di contatto univoco, disponibile 24 ore su 24 e 7 giorni su 7, dedicato all'interscambio informativo con le I.C.
- Intelligence – Raccolta dei dati e delle informazioni utili ai fini di prevenzione, attraverso il costante monitoraggio Internet e i consolidati rapporti di collaborazione operativa e condivisione informativa con gli altri organismi di polizia, gli enti e le aziende impegnati nei settori dell'ICT Security, sia a livello nazionale che internazionale.
- Analisi – Approfondimento in chiave comparativa dei dati e delle informazioni raccolte; predisposizione di rapporti previsionali sull'evoluzione della minaccia e delle vulnerabilità informatiche, delle tecniche e delle iniziative criminali.
- Investigazione – Erogazione della risposta operativa al verificarsi di un evento criminale in danno delle I.C., anche attraverso la collaborazione dei 20 Compartimenti e delle 80 Sezioni che rappresentano l'articolazione periferica della Polizia Postale e delle Comunicazioni e di organismi di polizia stranieri ed internazionali, come Interpol, Europol, Sottogruppo G8 High Tech Crime.

Tutela della Rete e delle aziende e protezione delle infrastrutture critiche

Nella società attuale, le "informazioni" rappresentano il patrimonio di maggior valore in qualsiasi ambito: per la collettività, le imprese e le istituzioni. Basti pensare, per quanto riguarda i privati cittadini, ai dati personali e alle comunicazioni (la cui integrità e riservatezza è costituzionalmente garantita); o al know how aziendale (quale patrimonio di informazioni ed esperienze che caratterizzano processi produttivi e commerciali esclusivi); infine, alle banche dati attraverso le quali la Pubblica Amministrazione eroga i servizi di pubblica utilità. Il valore delle informazioni dipende non solo dal loro contenuto ma anche dal possesso dei requisiti di accessibilità, integrità, disponibilità e riservatezza: in sintesi, dal livello di sicurezza che le caratterizza. Al giorno d'oggi i processi di archiviazione, elaborazione e trasmissione delle informazioni sono affidati – quasi esclusivamente – a reti, sistemi e servizi di comunicazione elettronica. La dematerializzazione delle informazioni e la loro trasmissione per via telematica garantiscono, da un lato, economie di scala e rapidità di gestione dei suddetti processi ma, al contempo, ampliano sensibilmente (rispetto alle tradizionali procedure di trattamento delle informazioni) l'ambiente e le possibilità tecniche di aggressione criminale. Fronteggiare la minaccia proveniente dallo spazio cibernetico (convenzionalmente declinata in cyber crime, cyber terrorism e cyber espionage) rappresenta pertanto l'impegno principale delle istituzioni preposte alla tutela della pubblica sicurezza. Ma si tratta di una sfida che richiede un approccio sinergico, multidisciplinare e che presuppone forme concrete di collaborazione pubblico-privato oltre che la sensibilizzazione della collettività ai temi della sicurezza delle informazioni e del corretto utilizzo delle risorse telematiche.

Prevenzione e contrasto delle attività terroristiche, degli atti discriminatori e di turbativa dell'ordine e della sicurezza pubblica, rilevati sulla Rete

La Specialità collabora alla conduzione di indagini di particolare complessità sui fenomeni di eversione e terrorismo, a livello nazionale e internazionale, qualora caratterizzati dall'utilizzo di strumenti informatici e di comunicazione telematica. Con l'obiettivo di prevenire turbative e pericoli per l'ordine e la sicurezza pubblica, la Polizia Postale e delle Comunicazioni provvede anche al sistematico e costante monitoraggio della Rete, in particolare degli spazi web e dei servizi di comunicazione online utilizzati dai militanti e dalle organizzazioni o gruppi con finalità di propaganda, proselitismo e pianificazione di manifestazioni e altre iniziative e azioni di carattere dimostrativo e violento. Allo stesso scopo, gli Uffici della Specialità svolgono indagini sugli atti discriminatori, rilevabili on-line, con particolare riferimento a quelli delle associazioni e dei gruppi di ispirazione razzista e xenofoba. Sottopongono inoltre a costante monitoraggio le iniziative delle frange estreme delle tifoserie sportive, così come l'organizzazione di "rave party".

La lotta alla contraffazione

L'uso dilagante dell'informatica e più in particolare della rete internet in ogni settore della vita sociale, ha agevolato la consumazione di numerosi reati, sia contro la persona che contro il patrimonio, e da ultimo anche contro la proprietà intellettuale.
Ciò ha determinato il diretto coinvolgimento della Polizia Postale e delle Comunicazioni anche nella prevenzione e repressione dei reati in violazione del diritto d'autore, qualora consumati con l'utilizzo della rete Internet.
In particolare, la Polizia Postale e delle Comunicazioni svolge attività di repressione sulle seguenti attività illecite:

- La vendita o diffusione non autorizzata online di opere protette dal diritto d'autore senza il legittimo consenso di chi ne ha diritto, con particolare riferimento a chi, a qualunque scopo ed in qualunque forma mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa;
- La fabbricazione, importazione distribuzione, vendita, noleggio e cessione di attrezzature, prodotti o componenti ovvero la prestazione di servizi che abbiano la prevalente finalità di eludere misure tecnologiche apposte dal titolare del diritto d'autore o di diritti connessi sulle opere o sui materiali protetti, al fine di impedire o limitare atti non autorizzati;
- La duplicazione abusiva, per fini di profitto, di programmi per elaboratore;
- La detenzione per la vendita o la distribuzione, la distribuzione, la vendita, il noleggio, la cessione e l'installazione di dispositivi o elementi di decodificazione speciale che consentono

ATTIVITÀ DI CONTRASTO ALLA CONTRAFFAZIONE

DIRITTO D'AUTORE	
Denunciati	30
Controlli effettuati	160

l'accesso ad un servizio criptato, e in particolare di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale senza il pagamento del canone dovuto.

L'attività condotta dalla Polizia Postale e delle Comunicazioni ha permesso di riscontrare che tutti i servizi della Rete, di volta in volta, sono stati coinvolti nel mercato parallelo ed abusivo di opere intellettuali e artistiche: software, opere cinematografiche e musicali sono state oggetto di una divulgazione massiccia nella Rete, una volta dietro corrispettivi irrisori, oggi addirittura gratuitamente. In particolare, il fenomeno si è sviluppato dalla contraffazione di copie all'utilizzo domestico della Rete che, attraverso

chat, community, file-sharing, siti web, offre gratuitamente opere tutelate dal diritto d'autore appena presentate al mercato, con notevole danno per il mercato legittimo e per le industrie che vi operano.
Ultima frontiera, in ordine di tempo, di tali reati è rappresentata dal fenomeno del "card-sharing", consistente nella violazione dei sistemi di sicurezza o accesso condizionato preposti alla distribuzione di contenuti televisivi a pagamento, al fine di consentirne la illecita visione a soggetti non abilitati che utilizzano il segnale originariamente destinato ad un solo utente.
Tali attività integrano il reato di frode informatica e di accesso abusivo al sistema informatico e prima ancora della violazione del copyright, con grave danno delle aziende che producono e diffondono programmi televisivi e di quelle che forniscono sistemi di sicurezza digitale.
La competenza acquisita nel settore del contrasto ai delitti consumati on-line relativamente al diritto d'autore, il costante monitoraggio della Rete e gli ormai solidi rapporti di collaborazione intrecciati con la SIAE, la Federazione Anti-pirateria Audio Visiva (FAPAV) e la Motion Picture Association (MPA), consentono oggi alla Polizia Postale e delle Comunicazioni di avere un quadro reale del fenomeno e di intervenire tempestivamente sulle nuove forme di aggressione, reprimendole efficacemente.
Oltre che sul fronte della repressione, la Polizia delle Comunicazioni è impegnata in un'intensa attività di prevenzione consistente nella sensibilizzazione dell'utenza sulla gravità delle condotte integranti la violazione della normativa a tutela della proprietà intellettuale.

Glossario

Adware: Particolare versione di spyware atto a monitorare informazioni personali o sensibili a fini pubblicitari.

Antispam: Programma o tecnologia che impedisce, o quantomeno limita, la ricezione di posta indesiderata nella propria casella di posta in antrata.

Antispyware: Il software antispyware protegge il computer da popup pubblicitari, lentezza e minacce alla sicurezza dovute a spyware e altro software indesiderato.

Antivirus: Programma che individua, previene e rimuove programmi dannosi, come virus e worm. Affinchè sia efficace deve essere costantemente aggiornato.

Attivazione: Procedura indispensabile, connessa all'installazione di molti software per attestarne la genuinità.

Backdoor: Accesso abusivo a un sistema informatico. Di solito una backdoor viene inserita dagli stessi programmatori del sistema per poter effettuari accessi di emergenza, ma a volte gli hacker riescono a individuarle sfruttandole a proprio vantaggio.

Backup: Operazione che consiste nel salvare periodicamente i dati memorizzati sul disco fisso del PC. È indispensabile fare backup frequenti perché un virus, un guasto dell'hardware, un incendio o anche un'operazione sbagliata possono causare la perdita dei dati.

Bot: Il termine bot è un'abbreviazione di "robot". I pirati informatici li usano per trasformare il tuo computer in un dispositivo in grado di effettuare automaticamente operazioni su Internet a tua insaputa.

Chat: Significa "chiacchierare" e indica le conversazioni scritte in tempo reale che si possono fare in rete con altri utenti tramite appositi programmi, per esempio Messenger e Skype. Nelle versioni più evolute le Chat prevedono la possibilità di parlare sfruttando microfono e casse del PC o addirittura di effettuare videoconversazioni.

Cloud: Il termine inglese cloud computing indica un insieme di tecnologie che permettono di memorizzare ed elaborare dati grazie all'utilizzo di risorse hardware e software distribuite e virtualizzate in Rete. SkyDrive e le Office Web Apps sono un esempio di servizio cloud offerto gratuitamente da Microsoft.

Controllo ActiveX: I controlli ActiveX sono piccoli programmi che vengono utilizzati su Internet. Nella maggior parte dei casi sono utili, per esempio per l'installazione di aggiornamenti di sicurezza, ma se usati illegalmente possono effettuare attività senza il tuo controllo.

Cookie: I Cookie sono piccoli file che i siti web salvano sul tuo disco rigido alla tua prima visita. Il loro compito è quello di ricordare i tuoi dati quando ritorni a visitare un sito.Generalmente i cookie non sono dannosi, ma se usati in maniera fraudolenta possono sottrarre informazioni a tua insaputa.

Copyright: È il diritto d'autore che stabilisce la proprietà intellettuale di un'opera.

Craccare: Neologismo gergale da "to crack", "spezzare". Si intende il superamento delle protezioni di un programma o di un sistema informatico.

Crack: Un sistema, generalmente software, in grado di eliminare le protezioni che vengono normalmente applicate ai programmi per evitare che vengano duplicati e installati illecitamente. L'utilizzo dei crack è illegale.

Cracker: Declinazione negativa dell'hacker. Quest'ultimo generalmente viola i sistemi informatici solo per metterli alla prova, mentre il Cracker lo fa con l'obiettivo di sottrarre i dati, danneggiare i sistemi o sottrarre denaro, per esempio da un conto corrente online.

Cyberbullismo: Termine che identifica attività di bullismo perpetrate tramite internet. Segnala l'episodio di bullismo al sito Web in cui è avvenuto. Molti servizi si avvalgono di moderatori e di luoghi in cui segnalare gli abusi, ad esempio abuse@microsoft.com

Cyberpedofilia: Il pedofilo telematico è un individuo estremamente pericoloso perché spesso è difficile da individuare. Tipicamente cerca di instaurare un clima di fiducia e di amicizia fingendosi coetaneo dei bambini e cercando di agire quando il minore non è controllato da persone adulte.

Dialer: è uno speciale programma auto-eseguibile che altera i parametri della connessione a internet impostati sul computer dell'utente, agendo sul numero telefonico del collegamento e sostituendolo con un numero a pagamento maggiorato su prefissi internazionali satellitari o speciali

Disclaimer: Significa "Esonero di responsabilità". L'insieme dei diritti e doveri dell'utente e limitazioni di responsabilità del produttore, relative a un software, da accettare al momento dell'installazione.

DRM: Acronimo di Digital Right Management, standard ideato da Microsoft sulla gestione dei diritti relativo alle opere digitali protette da copyright.

Fake: Identifica un falso. Su Internet usato spesso per identificare l'utilizzo di un'identità falsa o altrui, un file fasullo o un allarme relativo a un virus inesistente.

File sharing: Scambio di file solitamente attraverso reti paritarie (p2p), ma anche attraverso apposite piattaforme. Può essere illegale.

Filtro Smart Screen: Il filtro SmartScreen è una funzionalità di Internet Explorer 9 e 8 che ti aiuta a evitare le minacce di ingegneria sociale, sotto forma di malware e phishing, e le truffe online quando navighi sul web.

Firewall: Un firewall è un programma software o un componente hardware che permette di respingere gli attacchi di hacker, virus e worm che cercano di raggiungere il computer attraverso Internet.

Firma digitale: Procedura che garantisce l'integrità e l'autenticità di un documento informatico, in analogia con la firma autografata.

Flame: Il termine significa "fiammata" ed è tipico dei newsgroup. Identifica un attacco o reazione aggressiva verbale nei confronti di un utente.

Furto di identità: Il furto di identità è un qualsiasi tipo di frode che porta alla perdita di dati personali, come password, nomi

utente, dati bancari o numeri di carte di credito. La forma più diffusa è il phishing, ovvero la frode perpetrata tramite mail.

HACKER: Nella sua forma più pura si può considerare una sorta di studioso dei sistemi informatici, che tenta di violare per saggiarne i limiti e la sicurezza senza provocare danni. Purtorppo sempre più spesso gli hacker diventano cracker, ovvero persone che lo fanno a scopo di lucro, per sottrarre dati o per mettere fuori uso i sistemi informatici.

HOAX (FINTE MAIL): Un fenomeno legato al Phishing e al furto dì identità. Si tratta di finte mail, per esempio provenienti da istituti bancari o altri organismi, il cui unico scopo è sottrarre informazioni personali.

HTTPS: L'utilizzo del protocollo HTTPS (Hypertext Transfer Protocol Secure) consente di proteggere le informazioni inviate in Internet. In Hotmail viene per esempio utilizzato il protocollo HTTPS per la crittografia delle informazioni di accesso.

ICRA: Internet Contant Rating Association. Un'associazione internazionale senza fini di lucro nata per difendere e aiutare la navigazione dei minori in Rete.

INPRIVATE BROWSING: Tecnologia che consente di evitare che la cronologia delle esplorazioni, i file internet temporanei, i dati dei moduli, i cookie nonché i nomi utente e le password vengano mantenuti nel browser. In questo modo non lascerai traccia della tua navigazione.

LOGIN: Procedura di accesso a un computer, a un programma o a un servizio, generalmente legata all'inserimento di un username e di una password.È fondamentale scegliere password sicure per evitare che altri possano accedere senza il nostro consenso.

LURKER: Chi sta in agguato. Nelle attività in rete indica chi osserva senza prendere parte attiva.

MALWARE: Malware è l'abbreviazione di "malicious software", ovvero software dannoso. Con questo termine si identifica un software che viene installato senza il tuo consenso, per esempio mentre scarichi un programma gratutito o un file da una rete peer to peer.

MICROSOFT SECURITY ESSENTIALS: Microsoft Security Essentials è un software antimalware gratuito per il tuo computer. Ti protegge da virus, spyware e altro malware. È scaricabile gratuitamente per Windows 7, Windows Vista e Windows XP SP2 e superiori.

NETIQUETTE: Contrazione di Net Etiquette, ovvero "etichetta di rete". Insieme di regole che disciplinano il comportamento di un utente in internet. Il rispetto della netiquette non è imposto da alcuna legge, ma è prassi comune attenervisi.

NETIZEN: Il termine significa "cittadino della Rete". Neologismo abbastanza usato derivato da network e citizen.

NEWBIE: Neologismo gergale che indica un nuovo utente della rete, un navigatore alle prime armi.

NICKNAME: Quando non si vuole usare il proprio nome in rete, si può scegliersi un soprannome, detto appunto nickname. Non è possibile sapere chi si nasconde dietro a un nickname, per questo occorre fare molta attenzione quando si naviga in rete e ci si raffronta con altri utenti.

PEER-TO-PEER: Architettura di rete nella quale tutti i computer funzionano sia come client sia come server. Tutti i computer sono quindi uguali e di pari livello. Un esempio di rete peer-to-peer è Emule. Spesso questo tipo di reti vengono utilizzate per scambiare file illegalmente.

PHARMING: Tecnica che permette di sfruttare a proprio vantaggio le vulnerabilità di server controllando il dominio di un sito e utilizzandolo per redirigere il traffico su un altro sito.

PARENTAL CONTROL: Un filtro che permette di bloccare la visione dei contenuti non adatti ai bambini o a persone particolarmente sensibili.

PHISHING: Il phishing è un furto di identità online. Si basa su email, notifiche e siti web fraudolenti progettati per rubare dati personali o informazioni riservate, come dati account, numeri di carte di credito, password o altro.

POP-UP: "Il termine significa "saltar su" e indica le finestre che si aprono nel browser in modo automatico, di solito a scopi pubblicitari.

PROXY SERVER: Un server che si interpone tra i computer di chi naviga e il Web. Il suo scopo è sia quello di incrementare le prestazioni di navigazione, verificando se la pagina richiesta è già disponibile in memoria, sia di filtrare la navigazione, per esempio per impedire ai dipendenti di visitare siti vietati o aree particolari.

RIPPER: Letteralmente "squartatore". È così definito un programma che acquisisce i dati da CD musicale o DVD video e li importa sul disco fisso, per un'eventuale conversione e modifica. Questo genere di azioni è quasi sempre illegale.

SPAM: Lo spam è qualsiasi tipo di comunicazione online indesiderata. Attualmente la forma più comune di spam è la posta elettronica, per questo sono nate tecnologie, come il filtro SmartScreen di Microsoft, che riduce drasticamente la posta indesiderata in grado di raggiungere la nostra casella di posta.

SPYWARE: Spyware è un termine che descrive un software che si installa sul computer senza il tuo consenso. Uno spyware può fare pubblicità, raccogliere informazioni personali e addirittura arrivare a modificare la configurazione del tuo computer.

SSL: Acronimo di "Secure Sockets Layer", un protocollo che rende sicure le transazioni commerciali in rete, per esempio con carte di credito, grazie alla trasmissione dei dati cifrata.

TRACKING PROTECTION LIST: La TPL o Protezione da monitoraggio, permette di scegliere i siti autorizzati a ricevere le informazioni che riguardano la navigazione da parte dell'utente e di controllare la propria privacy durante la navigazione.

TROJAN: è un software che nasconde al suo interno un virus. Installando ed eseguendo il programma che contiene il Trojan, l'utente innesca il virus.

VIRUS: I virus informatici sono software progettati per diffondersi da un computer all'altro e interferire con il funzionamento della macchina. Un virus può cancellare dati, carpire informazioni, usare il programma di posta per diffondersi ad altre macchine e addirittura rendere il PC inutilizzabile.

WAREZ: Neologismo usato per individuare software scaricabili abusivamente e illegalmente dalla rete.

WEP: Acronimo di Wired Equivalent Privacy, un sistema di crittografia che si basa su una chiave pubblica. Serve per rendere più sicure le comunicazioni wireless. Fa parte dei protocolli di sicurezza wireless anche l'algoritmo di crittografia AES, sigla di Advance Encryption Standard.

WORM: Un worm è un particolare virus informatico in grado di propagarsi senza la necessità che l'utente inneschi il suo funzionamento compiendo un'operazione, per esempio installando un software.

Contatti

Compartimento Polizia Postale e delle Comunicazioni per l'Abruzzo
Pescara, Via Ravenna n. 8, cap 65100, centralino: tel. 085.4279750,
fax 085.4212317, e-mail: poltel.pe@poliziadistato.it
Sezioni
- Chieti: tel. 0871.584447, fax 0871.565283
- L'Aquila: tel. 0862.579091, fax 0862.579081
- Teramo: Via San Benedetto in Chartulis n. 4, cap 64100, Teramo Presso, CPO Poste, tel. 0861.439044, fax 0861.439022

Compartimento Polizia Postale e delle Comunicazioni per la Basilicata
Potenza, Via Pasquale Grippo 27/29, cap 85100,
centralino: tel. 0971.327364, fax 0971.327229,
e-mail: poltel.pz@poliziadistato.it
Sezioni
- Matera: tel. 0835.331028, 0835.332722, fax 0835.331028

Compartimento Polizia Postale e delle Comunicazioni per la Calabria
Reggio Calabria, Via S. Anna, 2° tronco, cap 89100,
centralino: tel. 0965.309011-49, fax 0965.309051,
e-mail: poltel.rc@poliziadistato.it
Sezioni
- Catanzaro: tel. 0961.743923, fax 0961.747519
- Cosenza: tel. 0984.687411, fax 0984.687418

Compartimento Polizia Postale e delle Comunicazioni per la Campania
Napoli, Via delle Repubbliche Marinare n. 495, cap 80146,
centralino: tel. 081.2433001, fax 081.2433397,
e-mail: poltel.na@poliziadistato.it
Sezioni
- Avellino: tel. 0825.34103, 0825.21074, fax 0825.34103
- Benevento: tel. 0824.50407, fax 0824.28192
- Caserta: tel. 0823.527294-6-3, fax 0823.527290
- Salerno: tel. 089.224097, fax 089.2572017

Compartimento Polizia Postale e delle Comunicazioni per l'Emilia Romagna
Bologna, Via Zanardi n. 28, cap 40132,
centralino: tel. 051.6352611, fax 051.6352612,
e-mail: poltel.bo@poliziadistato.it
Sezioni
- Ferrara: tel. 0532.978348, 0532.294520, fax 0532.978406
- Forlì: tel. 0543.373304, 0543.373360, fax 0543.373316
- Modena: tel. 059.243064, 059.220068, fax 059.225315
- Parma: tel. 0521.219550, 0521.933251, fax 0521.933253
- Piacenza: tel. 0523.322857, fax 0523.316442
- Ravenna: tel. 0544.243320-1, 0544.243314, fax 0544.243321
- Reggio E.: tel. 0522.498531-2-3, fax 0522.498519
- Rimini: tel. 0541.634296-7-8, fax 0541.634296

Compartimento Polizia Postale e delle Comunicazioni per il Friuli Venezia Giulia
Trieste, Piazza Vittorio Veneto n. 1, cap 34100,
centralino: tel. 040.6764589, 040.6764588, fax 040.6764246,
e-mail: poltel.ts@poliziadistato.it
Sezioni
- Gorizia: tel. 0481.590257, fax 0481.590314
- Pordenone: tel. 0434.222360, fax 0434.21331
- Udine: tel. 0432.223248-49-50, fax 0432.223220

Compartimento Polizia Postale e delle Comunicazioni per il Lazio
Roma, Viale Trastevere n. 191, cap 00153,
centralino: tel. 06.588831, 06.5813429, 5813608, fax 06.5814225,
e-mail: poltel.rm@poliziadistato.it
Sezioni
- Frosinone: tel. 0775.218532-3, fax 0775.218534
- Latina: tel. 0773.449214-0, fax 0773.449219
- Rieti: tel. 0746.270114, fax 0746.201484
- Viterbo: tel. 0761.335458-335561, fax 0761.335499

Compartimento Polizia Postale e delle Comunicazioni per la Liguria
Genova, Via Dante n. 4, cap 16100,
centralino: tel. 010.5366550, 010.540135, fax 010.593756,
e-mail: poltel.ge@poliziadistato.it
Sezioni
- Imperia: tel. 0183.795502, 0183.710619, fax 0183.294623
- La Spezia: tel. 0187.734074, fax 0187.734074
- Savona: tel. 019.8414537, fax 019.8414415

Compartimento Polizia Postale e delle Comunicazioni – Lombardia
Milano, Via Moisè Loria n. 74, cap 20144,
centralino: tel. 02.43333011, fax 02.43333066-67,
e-mail: poltel.mi@poliziadistato.it
Sezioni
- Bergamo: tel. 035.4532208, fax 035.4532208
- Brescia: tel. 030.3750385, fax 030.3757952
- Como: tel. 031.2763036-7, fax 031.2763004
- Cremona: tel. 0372.593588, fax 0372.593630
- Mantova: tel. 0376.327022, fax 0376.327022
- Pavia: tel. 0382.33950, 0382.392228, fax 0382.27081
- Sondrio: tel. 0342.545529, fax 0342.212471
- Varese: tel. 0332.281402, fax 0332.245507

Compartimento Polizia Postale e delle Comunicazioni – Marche
Ancona, Via Marconi n. 56, cap 60100,
centralino: Tel. 071.4190330, Fax 071.4190327,
e-mail: poltel.an@poliziadistato.it
Sezioni
- Ascoli Piceno: tel. 0736.242317, 0736.242306-09, fax 0736.263341-242229
- Macerata: tel. 0733.254615-6, 0733.273036-7, fax 0733.273002-273012
- Pesaro: tel. 0721.549718-19-20-21, fax 0721.549704

Compartimento Polizia Postale e delle Comunicazioni – Molise
Campobasso, Via S. Giovanni n. 55, cap 86100,
centralino: tel. 0874.64321, 0874.482100, fax 0874.63041,
e-mail: poltel.cb@poliziadistato.it
Sezioni
- Isernia: tel. 0865.504324, fax 0865.504435

Compartimento Polizia Postale e delle Comunicazioni – Piemonte
Torino, Corso Tazzoli n. 235, cap 10100,
centralino: tel. 011.3014611, fax 011.3014670,
e-mail: compartimento.polposta.to@pecps.interno.it
Sezioni
- Alessandria: tel. 0131.302252-50, fax 0131.302208
- Aosta: tel. 0165.44038, fax 0165.276207
- Asti: tel. 0141.357270, fax 0141.357209
- Biella: tel. 015.3590685, fax 015.3590685
- Cuneo: tel. 0171.443558, fax 0171.67532
- Novara: tel. 0321.335257-8, fax 0321.335230
- Vercelli: tel. 0161.264112, fax 0161.264019

Compartimento Polizia Postale e delle Comunicazioni per la Puglia
Bari, Via Amendola n. 116, cap 70100,
centralino: tel. 080.5920611, fax 080.5507058,
e-mail: poltel.ba@poliziadistato.it
Sezioni
- Brindisi: tel. 0831.523185, fax 0831.523185
- Foggia: tel. 0881.722100, fax 0881.708243, e-mail: poltel.fg@poliziadistato.it
- Lecce: tel. 0832.244150, fax 0832.249877
- Taranto: tel. 099.4554265, fax 099.4554235

Compartimento Polizia Postale e delle Comunicazioni per la Sardegna
Cagliari, Via Simeto n. 38, cap 09100,
centralino: tel. 070.27665, fax 070.2766505,
e-mail: poltel.ca@poliziadistato.it
Sezioni
- Nuoro: tel. 0784.214266, fax 0784.31019
- Oristano: tel. 0783.322274, fax 0783.322234
- Sassari: tel. 079.232217, fax 079.232217

Compartimento Polizia Postale e delle Comunicazioni per la Sicilia Occidentale
Palermo, Via Roma n. 320, cap 90146,
centralino: tel. 091.323403, 091.580375, fax 091.7535437,
e-mail: poltel.pa@poliziadistato.it
Sezioni
- Agrigento: tel. 0922.551593, fax 0922.551537
- Caltanissetta: tel. 0934.562153, fax 0934.562049
- Enna: tel. 0935.562331, fax 0935.562252
- Trapani: tel. 0923.434389, 0923.434391, fax 0923.434253

Compartimento Polizia Postale e delle Comunicazioni per la Sicilia Orientale
Catania, Via San Euplio n. 74, cap 95124,
centralino: tel. 095.7155225, fax 095.7155221,
e-mail: poltel.ct@poliziadistato.it
Sezioni
- Messina: tel. 090.6257295, 090.6527452, fax 090.6257203
- Ragusa: tel. 0932.235683, 0932.235665, fax 0932.235615
- Siracusa: tel. 0931.498263, fax 0931.498217

Compartimento Polizia Postale e delle Comunicazioni per la Toscana
Firenze, Via della Casella n. 19, cap 50100,
centralino: tel. 055.7876711, 055.784863, fax 055.7876709,
e-mail: poltel.fi@poliziadistato.it
Sezioni
- Arezzo: tel. 0575.400518-332431-2, fax 0575.318518
- Grosseto: tel. 0564.448443, fax 0564.448536
- Livorno: tel. 0586.276468, fax 0586.276417
- Lucca: tel. 0583.467807, fax 0583.467807
- Massa C.: tel. 0585.255491, 0585.259252, fax 0585.259212
- Pisa: tel. 050.3162431, fax 050.3162440
- Pistoia: tel. 0573.970726, fax 0573.504865
- Prato: tel. 0574.614540, fax 0574.614525
- Siena: tel. 0577.276645, fax 0577.276653

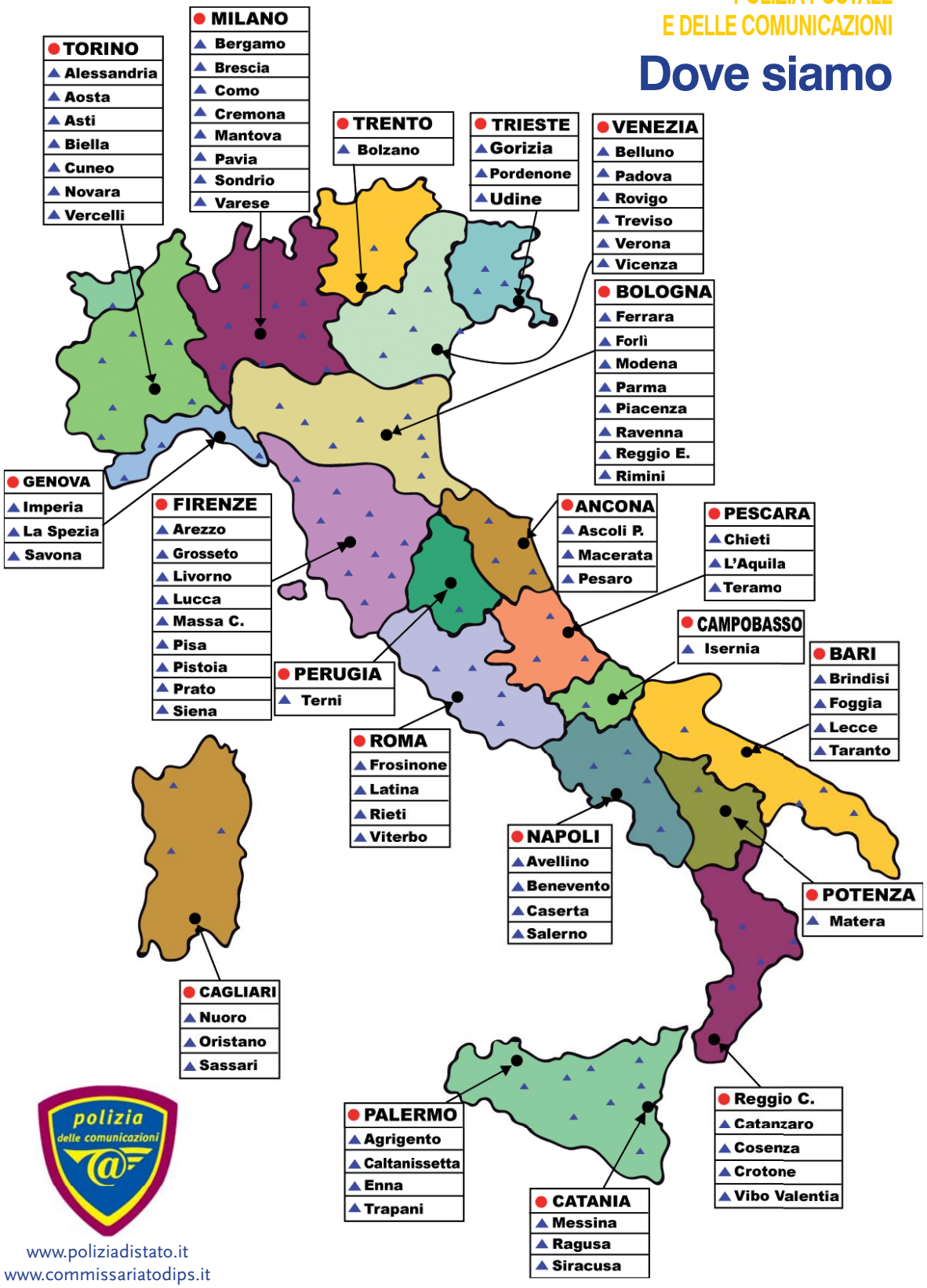
Compartimento Polizia Postale e delle Comunicazioni per il Trentino Alto Adige
Trento, Via Vannetti n. 15, cap 38100,
centralino: tel. 0461.232462, 0461.987138, fax 0461.263401,
e-mail: poltel.tn@poliziadistato.it
Sezioni
- Bolzano: tel. 0471.531413, fax 0471.531415

Compartimento Polizia Postale e delle Comunicazioni per l'Umbria
Perugia, Via Mario Angeloni n. 72, cap 06124,
centralino: tel. 075.5001703, 5009734, 5011967, 5062646, 5000747, fax 075.5000655, e-mail: poltel.pg@poliziadistato.it
Sezioni
- Terni: tel. 0744.201390, 0744.201396, 0744.480658, fax 0744.401784

Compartimento Polizia Postale e delle Comunicazioni per il Veneto
Venezia, Via Cappelletto n. 11, Venezia Mestre, cap 30174,
centralino: tel. 041.2907311, 041.2907349, fax 041.5310438,
e-mail: poltel.ve@poliziadistato.it
Sezioni
- Belluno: tel. 0437.931776, 0437.932129, fax 0437.939886
- Padova: tel. 049.656456, 049.666038, fax 049.8772004
- Rovigo: tel. 0425.202521, 0425.420330, fax 0425.460168
- Treviso: tel. 0422.653301-2, fax 0422.653244
- Verona: tel. 045.8059386, 045.8059309, fax 045.8059446
- Vicenza: tel. 0444.507070, 0444.338558, 0444.338584, fax 0444.322554

POLIZIA POSTALE
E DELLE COMUNICAZIONI

Dove siamo



polizia delle comunicazioni

www.poliziadistato.it
www.commissariatodips.it

L'impegno di Vodafone Italia per la sicurezza e per la tutela dei minori

La Sostenibilità e la Sicurezza in Vodafone Italia

Vodafone Italia ha scelto un approccio alla sostenibilità di lungo periodo, di integrazione con il business, con il territorio e il tessuto sociale nel quale l'azienda opera, con l'obiettivo di creare un progetto di impresa sostenibile.
L'approccio alla sicurezza che Vodafone Italia persegue è improntato a una cultura di trasparenza, responsabilità e collaborazione con tutti gli stakeholder interni ed esterni, in un'ottica di "sicurezza partecipata" per un migliore Sistema Paese. L'accordo siglato con il C.N.A.I.P.I.C. (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche) della Polizia Postale e delle Comunicazioni, il contributo quotidiano alle attività di pubblico soccorso, il contrasto alla pedopornografia, sono solo alcuni esempi di questa strategia.
Sul fronte della privacy e tutela dei dati e delle informazioni dei clienti, Vodafone Italia ha effettuato nel tempo investimenti per circa 20 milioni di euro, individuando soluzioni innovative anche in attuazione alle normative nazionali e comunitarie in materia. La compliance su una materia delicata come quella della privacy e della protezione dei dati rappresenta sempre più un elemento differenziante del brand Vodafone e dunque della reputation dell'azienda, impegnata a custodire e proteggere i dati personali e di traffico della propria clientela.

Le nuove tecnologie il divario generazionale e la tutela dei minori

Con l'obiettivo di favorire un uso consapevole, responsabile, sicuro e critico di internet, del telefono cellulare e delle nuove tecnologie è nato il progetto inFamiglia per genitori, nonni e figli.
Il portale www.infamiglia.vodafone.it è stato pensato come uno spazio di discussione e approfondimento aperto in cui potersi confrontare e condividere esperienze tramite un forum, un blog e un team di esperti che si occupa di temi legati alla genitorialità, alla tecnologia e all'uso dei nuovi media.
L'impegno di Vodafone Italia prosegue anche nell'ambito della tutela dei minori attraverso l'accesso ai servizi di telefonia mobile a contenuto sensibile, garantendo un sistema di Parental Control denominato Filtro Famiglia attivabile mediante chiamata al 190 che consente di inibire l'accesso a chat, forum di discussione e servizi a contenuto sensibile.
Vodafone Italia e Polizia di Stato hanno inoltre realizzato una nuova applicazione per smartphone Android denominata "Vodafone Smart Tutor", che consente di personalizzare le funzionalità del cellulare per un utilizzo sicuro e protetto da parte dei minori.
L'applicazione è scaricabile gratuitamente dal portale inFamiglia e dall'Android Market.

vodafone

Stampa: LITOGRAFIA SOLARI S.r.l. Peschiera Borromeo (Milano), maggio 2012 | Redazione e Grafica: Officinaventuno, Milano.