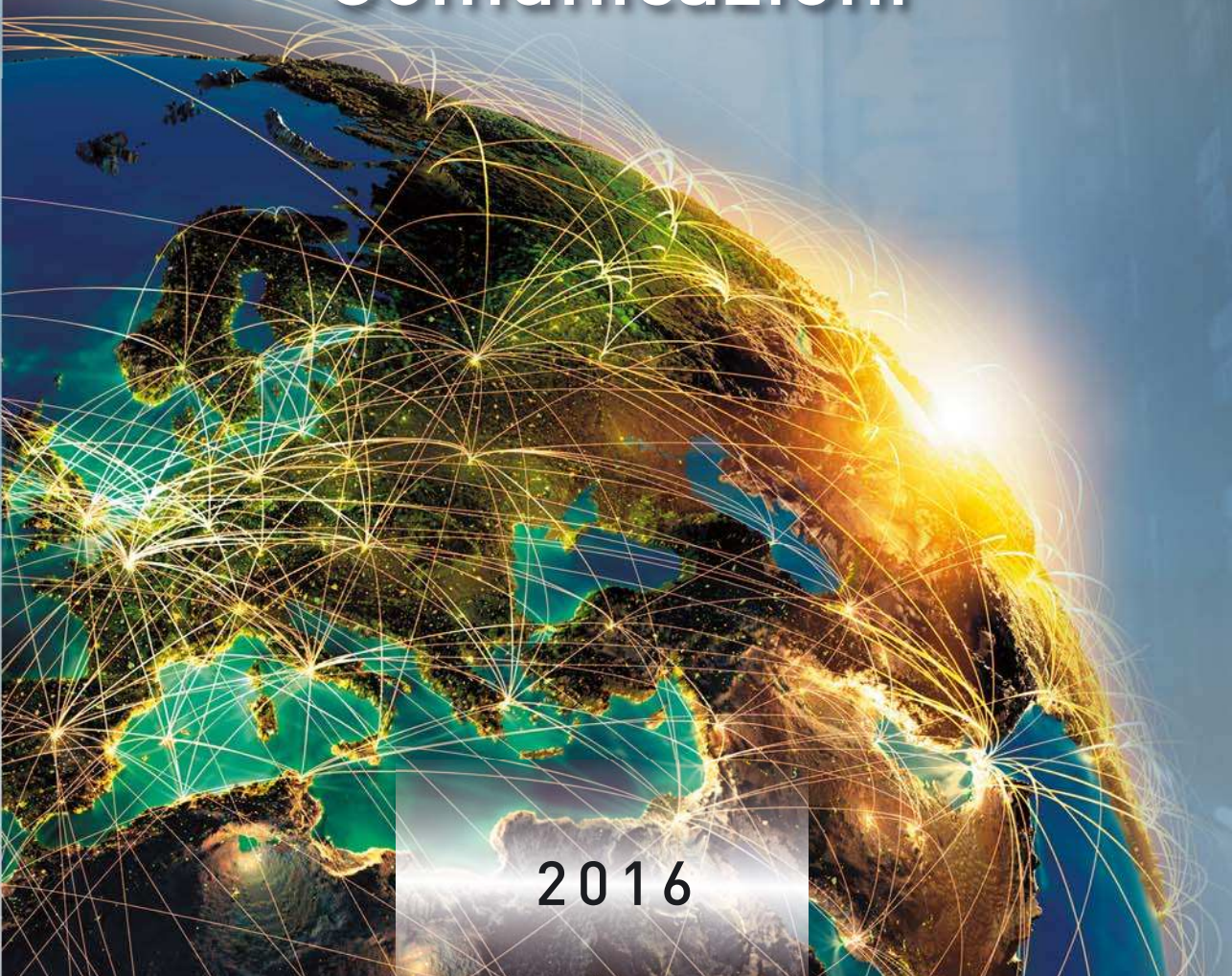
Polizia di Stato

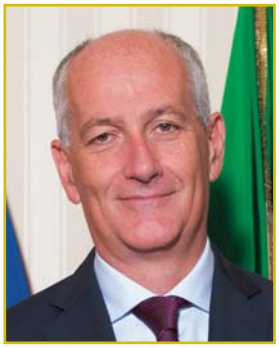
Polizia Postale
e delle
Comunicazioni



2016

Sommario

Prefazione



Credo che il Servizio di Polizia Postale e delle Comunicazioni del Dipartimento della Pubblica Sicurezza possa costituire un interessante oggetto di approfondimento per gli studiosi dei modelli di organizzazione del lavoro, poiché è riuscito, lì dove molti hanno fallito, a trasformare una criticità in una opportunità di crescita.

I processi di privatizzazione che hanno interessato il nostro sistema postale, hanno, infatti, fortemente ridimensionato le originarie competenze del Servizio che ha, tuttavia, trovato nuova linfa dirottando risorse umane e strumentali su una funzione che inizialmente era solo residuale, quella della sicurezza delle telecomunicazioni.

Il passaggio da quest'ultima alla sicurezza del web è stato breve.

Nel giro di pochi anni il Servizio ha sviluppato una straordinaria competenza e professionalità nel settore della lotta ai crimini informatici, riconosciuta anche sul piano internazionale.

Nella perenne corsa ad anticipare le mosse dell'avversario, che è propria dei navigatori del web, il Servizio, da qualche tempo, ha intrapreso un nuovo ambizioso progetto: affrontare l'arena cyber giocando non solo in difesa, quale mero fruitore di tools elaborati da altri, ma partecipando attivamente alla progettazione e realizzazione di strategie e strumenti efficaci per la prevenzione e repressione dei reati informatici.

Il Servizio di Polizia Postale, in questo senso, si è trasformato in un laboratorio che attraverso una stretta interconnessione con il mondo accademico, i settori più avanzati della ricerca e gli omologhi organismi internazionali si sta preparando ad affrontare una criminalità sempre più "attrezzata" ed aggressiva.

Dal cyber crime al terrorismo informatico, dalla lotta al cyber bullismo al furto di identità molteplici sono i campi di azione del Servizio di Polizia Postale.

Alcuni di questi li troverete sintetizzati in questa agile pubblicazione che contribuisce a fornire un quadro della varietà delle attività compiute e dei risultati conseguiti.

Il Capo della Polizia
Direttore Generale della Pubblica Sicurezza
Franco Gabrielli

La vasta comunità degli utenti digitali rappresenta un potenziale obiettivo per i *cyber criminali* che, da ogni parte del mondo, mirano a colpire non solo il patrimonio economico dei singoli e delle società, ma anche ad appropriarsi dei loro dati personali.

La Polizia Postale e delle Comunicazioni, componente di eccellenza della Polizia di Stato, è deputata proprio alla tutela delle comunità digitali e al presidio delle condizioni di sicurezza dell'ambiente virtuale.

Per fare ciò, la Specialità si avvale anche del partenariato pubblico-privato di settore, non disgiunto dal sistematico coinvolgimento del mondo accademico e degli organismi di cooperazione internazionale. Ed in tal senso sono già state formalizzate in vari ambiti specifiche convenzioni finalizzate a mettere in sicurezza interi settori che operano nel mondo della rete.

Si tratta di significative partnership che hanno lo scopo, da un lato, di fornire un innovativo contributo nel campo della sicurezza online, dall'altro di promuovere attività di formazione, specializzazione e perfezionamento del personale della Polizia di Stato con particolare riguardo a quello della Polizia Postale e delle Comunicazioni, impegnato in prima linea nella prevenzione e nel contrasto al *cybercrime*, fornendo altresì impulso ad attività di ricerca di strumenti tecnologicamente più avanzati per essere al passo delle nuove frontiere della criminalità informatica.

Il Direttore Centrale
delle Specialità della Polizia di Stato
Roberto Sgalla

Nuove forme di comunicazione e la disponibilità di tecnologie in costante evoluzione ci permettono di disporre di vantaggi ed opportunità senza precedenti.

Ne consegue tuttavia che accanto alla globalizzazione delle comunicazioni si affianchi una maggiore vulnerabilità delle reti informatiche che necessita di una risposta tempestiva e specializzata.

La Polizia Postale e delle Comunicazioni è dunque chiamata ogni giorno a sfide sempre più complesse, attraverso l'utilizzo di strumentazioni moderne e di innovative tecniche investigative in sinergia con organismi di polizia internazionali.

Le attività messe in campo dalla Specialità, in termini di prevenzione e di contrasto delle nuove forme di criminalità informatica, hanno raggiunto un elevatissimo livello di specializzazione riconosciuto a livello mondiale.

Per rendere più incisiva la presenza degli operatori di polizia in Rete la Specialità si avvale dei suoi Centri di eccellenza, il C.N.A.I.P.I.C. (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche Informatizzate), il C.N.C.P.O. (Centro Nazionale per il Contrasto della Pedopornografia Online) ed il Commissariato di P.S. online, il quale fornisce la possibilità di interagire per via diretta con gli utenti digitali.

Nel settore della prevenzione spicca l'impegno della Polizia Postale e delle Comunicazioni in campagne di sensibilizzazione rivolte soprattutto alle giovani generazioni sui temi della sicurezza in Rete.

Tra queste *"Una Vita da Social"*, in collaborazione con il Ministero dell'Istruzione, dell'Università e della Ricerca e con il Patrocinio dell'Autorità Garante per l'Infanzia e l'Adolescenza; senza dimenticare la collaborazione con i principali *"web actors"*, selezionata dalla Commissione Europea tra le migliori pratiche di sicurezza internazionale.

Il Direttore del Servizio
Polizia Postale e delle Comunicazioni
Nunzia Ciardi

La Polizia Postale e delle Comunicazioni

La Polizia Postale e delle Comunicazioni, istituita con la legge di riforma dell'Amministrazione della Pubblica Sicurezza, rappresenta il settore specialistico della Polizia di Stato atto a prevenire e contrastare la criminalità informatica.

Nell'attuale processo di digitalizzazione della moderna società, in cui assistiamo ad una continua e rapida evoluzione tecnologica che influenza ogni azione del vivere quotidiano, Internet rappresenta da un lato, il mezzo fondamentale per lo scambio di informazioni, per l'accesso alle grandi banche dati, per l'esecuzione di transazioni finanziarie, dall'altro un mondo insidioso e pieno di pericoli.

In questo settore nevralgico la Specialità si inserisce con un'azione costante volta ad eliminare i punti di debolezza della Rete, con particolare riguardo alle problematiche di sicurezza, rappresentando un punto di riferimento a garanzia di un corretto uso del mondo virtuale.

IL SERVIZIO POLIZIA POSTALE E DELLE COMUNICAZIONI

Il Servizio Centrale, vertice della struttura, è stato istituito con decreto ministeriale dell'1 marzo 1998 come organo del Ministero dell'Interno per la sicurezza e la regolarità dei servizi di telecomunicazione e punto di riferimento nel coordinamento, nella programmazione e nella pianificazione operativa degli uffici periferici della specialità. Grazie all'alta professionalità dello staff e dei suoi tre Centri di eccellenza, (Centro Nazionale per il Contrasto della Pedopornografia Online – C.N.C.P.O., Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche – C.N.A.I.P.I.C., Commissariato di P.S. on line), il Servizio assicura un'efficace azione di raccordo operativo con gli Uffici territoriali nelle attività di competenza della Specialità e, in particolare, nelle quattro macro aree criminali di

interesse prioritario per la Polizia Postale e delle Comunicazioni:

- Pedopornografia on line;
- Hacking e crimini informatici;
- Financial Cyber crime;
- Cyberterrorismo.

Il Servizio, cui affluiscono tutte le informazioni rilevanti in materia di cybercrime, svolge inoltre azioni mirate nei seguenti campi:

- cooperazione con gli omologhi organi di polizia stranieri;
- individuazione delle strategie di contrasto ai fenomeni criminali generati da sistemi telematici e di elaborazione computerizzata dei dati;
- selezione e formazione del personale;
- collaborazione con il mondo accademico e quello privato di settore;
- analisi della sfera applicativa delle normative in materia di comunicazioni;
- partecipazione a gruppi di lavoro istituiti presso organismi nazionali ed internazionali.

LE DIRAMAZIONI TERRITORIALI DELLA SPECIALITÀ

La Polizia Postale e delle Comunicazioni è presente in modo capillare sul territorio nazionale attraverso 20 Compartimenti e 80 Sezioni, le cui attività di competenza comprendono, oltre alle quattro macro aree criminali (pedopornografia online, hacking e crimini informatici, crimine finanziario cibernetico e cyberterrorismo), anche:

- la prevenzione e repressione dei crimini informatici;
- la tutela dei servizi postali, di bancoposta e di telecomunicazione;
- la prevenzione e repressione dei reati legati al commercio elettronico;
- il raccordo operativo con gli ispettori territoriali del Ministero delle Comunicazioni nelle attività di controllo amministrativo di comune interesse;
- il concorso nel contrasto delle violazioni del diritto d'autore per quanto attiene agli aspetti telematici.

Pedopornografia online

Il contrasto e la prevenzione della pedopornografia in Rete e delle connesse forme di devianza e di rischio per i minorenni sono demandati al Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O), istituito con la legge 6 febbraio 2006 n. 38, nell'ambito del Servizio Polizia Postale e delle Comunicazioni, preposto al coordinamento delle investigazioni e alla predisposizione della "Black List" dei siti pedopornografici per il relativo filtraggio da parte degli Internet Service Provider italiani.

Il C.N.C.P.O. coordina le indagini condotte su tutto il territorio nazionale dai Compartimenti della Specialità e, avvalendosi dei migliori investigatori attivi sottocopertura online, sperimenta nuove tecniche investigative e strumenti tecnologici d'avanguardia, quali i sistemi di raccolta e di analisi dei dati investigativi ed i sistemi di analisi forense delle immagini digitali.

L'orientamento investigativo si concentra principalmente sulle piattaforme di navigazione maggiormente a rischio per le vittime quali quelle dei *social network*, ove emergono costantemente modalità di adescamento di minori e di cyberbullismo, nonché nelle reti "darknet", aree profonde e nascoste del web, prescelte dalle comunità pedofile, ove l'utilizzo di tecnologie sofisticate rende inefficaci i tradizionali mezzi di accertamento delle identità online.

Misure di contrasto vengono messe in campo anche con riferimento a minori autori di reato, dalla contraffazione delle identità online per finalità ludiche o di aggressione telematica, al furto di identità e immagini sui social network e la creazione di profili a nome di altri, comportamenti questi che costituiscono spesso solo il punto di partenza per la commissione di fattispecie più gravi, quali la produzione di materiale pedopornografico, frequentemente nell'assoluta inconsapevolezza degli effetti concreti che possono produrre sulle vittime.

Sin dal 2012, con l'entrata in vigore della legge n.172, le indagini su casi di adescamento online continuano a registrare un progressivo aumento (da 234 nel 2015 a 322 nel 2016).

Sempre più spesso adescatori e abusanti contattano minori sui socialnetwork e attraverso la messaggistica istantanea cercando di indurli al sexting,ad azioni sessuali,alla produzione di immagini e video privatissimi. Tutto questo contribuisce ad incrementare l'immissione in rete di nuove immagini pedopornografiche, che entrano nei circuiti di condivisione più comuni fino ad arrivare alle comunità pedofile nascoste nel web.

Inseguendo le diversificate dinamiche che presiedono l'utilizzo dei vari servizi

web, le investigazioni più sofisticate sono state ancora una volta indirizzate verso le reti darknet contribuendo ad affinare modalità e strumenti condivisi nell'ambito della collaborazione internazionale di polizia da parte delle varie Agenzie investigative estere ed avvalendosi del coordinamento dell'EC3 di Europol.

Le fruttuose sinergie attivate nell'ambito di tale settore investigativo hanno consentito di smantellare una comunità virtuale pedofila composta da 45.000 iscritti, nell'ambito di un'operazione che ha portato all'arresto degli amministratori di nazionalità australiana e canadese della stessa comunità, di identificare diverse centinaia di utenti di varie nazionalità, molti dei quali si sono rivelati abusanti di minori e produttori di materiale illecito

In particolare, in Italia le investigazioni condotte nell'operazione "*Deep web*", sotto la direzione della Procura di Roma, hanno consentito di ricostruire a livello probatorio la struttura criminale dell'organizzazione, inquadrandola in un'associazione per delinquere transnazionale finalizzata alla commissione dei reati afferenti alla pedopornografia e pedofilia.

La complessiva attività di contrasto svolta dalla Polizia Postale e delle Comunicazioni, nell'anno in disamina, ha consentito di raggiungere i seguenti risultati:

QUADRO DI SINTESI DELL' ATTIVITA' INVESTIGATIVA 2016	
Persone denunciate	**467**
Persone denunciate sottoposte a provvedimenti restrittivi	**52**
Perquisizioni	**434**
Minori vittime di adescamento	**322**

QUADRO DI SINTESI DELL' ATTIVITA' DI PREVENZIONE 2016	
Siti monitorati in black list	**22.398**
Nuovi siti inseriti in black list	**151**
Totale siti in black list	**1.972**

Unità di Analisi dei Crimini Informatici

L'*Unità di Analisi dei crimini informatici* è un'*équipe* composta da psicologi della Polizia di Stato che integra le competenze di natura socio-psicologica con l'attività di contrasto al cybercrime.

Il lavoro di profiling criminologico svolto dagli psicologi provvede alla ricostruzione dei diversi profili di abusanti che utilizzano la rete per scambiare e condividere immagini di abuso sui bambini: usando il **deepweb e le darknet,** i pedofili online diventano sempre più diffidenti e tecnologicamente preparati, si nascondono convinti di essere anonimi, si affiliano in community chiuse e segrete nelle quali gli agenti undercover sanno inserirsi ed espugnare il muro di bieca omertà dietro il quale questo tipo di criminali pensano di rimanere impuniti.

Il team è impegnato in un progetto di formazione assistita**,** avviato nel 2009, finalizzato alla protezione psicologica degli operatori della Specialità attraverso l'ascolto e il sostegno.

Fenomeni recenti e preoccupanti come quelli della delinquenza giovanile in rete, realtà borderline tra devianza giovanile e psicologia dei gruppi, hanno visto nel cyberbullismo e nel sexting, gli esempi più eclatanti dell'attuale criticità dei rapporti tra nuove generazioni e tecnologia.

Secondo le analisi criminologiche della casistica trattata dalla Specialità, alla base della commissione di reati contro la persona, posti in essere da minori contro minori su internet, c'è spesso una *conoscenza reale,* nata dalla condivisione della realtà scolastica, sportiva o ricreativa in genere.

I dati dell'ultimo anno testimoniano una lieve flessione nel numero delle denunce e un dimezzamento dei minori incriminati per reati legati a sexting e cyberbullismo, individuando nel progressivo impegno a promuovere nei giovani, nei genitori e negli insegnanti una maggiore consapevolezza sui pericoli della rete, una strategia promettente per ridurre la pericolosità di certe "cattive abitudini tecnologiche".

2016	Stalking	Diffamazione online	Ingiurie Minacce Molestie	Furto di identità su social network	Divulgazione e diffusione materiale pedopornografico	Totale
Denunce	8	42	88	71	27	236
Minori *	1	11	6	3	10	31

* denunciati all'Autorità Giudiziaria

Il contrasto dei crimini informatici

HACKING

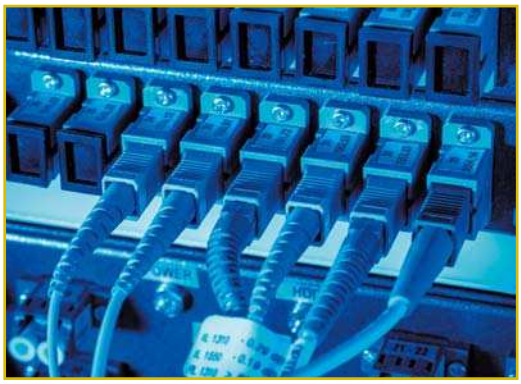
La società dell'informazione in cui oggi viviamo, trova nell'informatica il suo elemento essenziale. Purtroppo accanto a questo rapido sviluppo della tecnologia si è assistito ad un altrettanto rapido aumento del rischio dovuto all'uso illecito degli strumenti informatici.

Internet per le enormi potenzialità che può esprimere nel campo della comunicazione, intesa nel più ampio senso del termine, è considerato come un vero e proprio catalizzatore dei traffici illegali e di strumenti per lo scambio di informazioni, oltretutto facilmente fruibili grazie all'ampia diffusione di apparati mobili. In tale quadro appare fin troppo scontato come la criminalità organizzata attinga da tale generosa fonte per poter trafficare, riciclare ovvero delinquere direttamente, garantendosi oltretutto un sostanziale anonimato grazie alla sempre più ampia disponibilità di sistemi di "anonimizzazione", ovvero di vere e proprie piazze virtuali di scambio allocate nel c.d. dark web. È in tali ambiti, soprattutto, che si accede, spesso solo tramite conoscenze dirette o "passaparola virtuali", a veri e propri suk in cui l'offerta di dati e immagini di provenienza illecita ovvero malware programmati ad hoc per compiere attacchi informatici, incontra la sempre crescente domanda di vere e proprie organizzazioni criminali, alla ricerca di "merce digitale illegale" così come di vere e proprie "armi virtuali".

Nel settore dei cd cyber attacks, si è passati da fenomeni criminali a matrice politica, meglio hacktivista, con attacchi informatici ad alta valenza dimostrativa (DDOS, violazione di sistemi informatici e successiva pubblicazione di documenti riservati) alla vera e propria realizzazione di

campagne mirate verso interi settori dell'economia ed amministrazioni pubbliche, finalizzate alla sottrazione di informazioni, know how industriale, al danneggiamento dei sistemi bersaglio. Gruppi criminali con risorse tecnologiche importanti, spesso supportati più o meno apertamente da governi ostili, sono all'origine di diffusi attacchi cyber, connotati dalla customizzazione dei malware impiegati, dalla scientifica selezione dei target, che lasciano intendere la presenza di un vero e proprio salto di qualità nelle strategie di attacco e nel livello delle organizzazioni criminali coinvolte. L'attuale tendenza criminale vede quindi la proliferazione di ben definite campagne di APT (advanced persistent threat), generate con librerie complesse, veicolate attraverso dedicate mail di spear phishing, spesso dirette verso i vertici delle organizzazioni bersaglio.

Tali attacchi su larga scala, difficilmente individuabili nell'immediato, sfruttando bug di sistema non conosciuti (cd 0 days), spesso finiscono per determinare vere e proprie scalate di privilegi all'interno di complessi sistemi di rete, fino al controllo totale delle comunicazioni e quindi dell'organizzazione colpita.



Alla complessità sopraccennata si aggiunga la dimensione internazionale che assume la problematica allorquando una forza di polizia si trovi a dover svolgere indagini che spesso finiscono per arenarsi sui banchi di legislazioni nazionali diverse in termini di data retention, sui diversi livelli di competenza delle forze di polizia di altri paesi chiamate a collaborare in caso di richieste di cooperazione internazionale.

In questo contesto si colloca il C.N.A.I.P.I.C. che, ai sensi della legge 155/2005 e del decreto 9 gennaio 2008 del Ministro dell'Interno, ha la competenza della protezione informatica delle infrastrutture critiche.

Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.)

I servizi di protezione informatica sono erogati sulla base di apposite convenzioni, previste dalla stessa legge istitutiva, stipulate tra il Dipartimento della Pubblica Sicurezza e le singole infrastrutture critiche, con le quali si realizza in tale particolare settore un rapporto di partnership pubblico-privato.

In tale ambito, nell'ultimo anno il C.N.A.I.P.I.C. ha sottoscritto 2 nuove convenzioni con ACEA S.p.A. e il Dipartimento della Protezione Civile, nonché 3 protocolli d'intesa con Assicurazioni Generali, Unieuro-SGM e Salini-Impregilo.

E' stata inoltre rinnovata la convenzione già in essere con ACI.

FUNZIONI DEL C.N.A.I.P.I.C.

Avvalendosi di tecnologie di elevato livello e di 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 infrastrutture critiche, 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 G7 High Tech Crime;
- ***Unità tecnica*** - l'Unità tecnica è invece deputata alla gestione e all'esercizio dell'infrastruttura tecnologica del C.N.A.I.P.I.C., nonché ai processi di individuazione, testing ed acquisizione di risorse strumentali e alla pianificazione di cicli di formazione/aggiornamento del personale.

TABELLA STATISTICHE GENERALI 2016	
Attacchi rilevati	**844**
Alert diramati per attacchi, vulnerabilità e minacce	**6.721**
Indagini avviate	**70**
Persone denunciate	**26**
Richieste di cooperazione Punto di Contatto rete 24/7 High Tech Crime G7	**85**

LA COOPERAZIONE INTERNAZIONALE C.N.A.I.P.I.C. PER IL GIUBILEO

Nel corso dell'anno, in concomitanza con lo svolgimento del Giubileo Straordinario della Misericordia, il Centro ha posto in essere un dedicato dispositivo di sicurezza volto alla prevenzione di eventi cyber critici o di veri e propri attacchi informatici in danno di infrastrutture informatizzate impegnate per l'evento in questione. Si tratta anche in questo caso del complesso sistema di servizi ed infrastrutture più o meno interconnesse tra loro che di fatto hanno erogato i servizi essenziali per la città e per i pellegrini in particolare (trasporti, energia, telecomunicazioni, ecc.).

La suddetta attività ha generato 40 segnalazioni riguardanti attacchi informatici in atto, minacce e vulnerabilità.

OPERAZIONI DI RILIEVO

Nel mese di gennaio 2016, è stato denunciato un membro di spicco di Anonymous Italia conosciuto all'interno del movimento come "X".

Su un quotidiano italiano on line, il 28 dicembre 2015, "X" aveva rilasciato un'intervista millantando di avere sventato un attentato che l'ISIS avrebbe portato a termine in Italia, creando un notevole allarme proprio nel periodo delle festività natalizie.

Nel successivo mese di luglio il C.N.A.I.P.I.C., finalizzava l'operazione "Hackinitaly" denunciando i responsabili dei reati di accesso abusivo a sistemi informatici, diffusione di malware e frode informatica.

I provvedimenti hanno costituito il frutto di laboriose indagini condotte in collaborazione con il Federal Bureau of Investigation statunitense, che hanno portato ad accertare come gli indagati avessero compromesso migliaia di dispositivi informatici connessi in rete, mediante i quali simulavano visite a spazi pubblicitari inseriti in siti Internet di loro proprietà, al fine di frodare società pubblicitarie che offrono servizi di pay per click.

Sempre in tema di collaborazione internazionale, il Centro ha partecipato allo smantellamento di una vasta e pericolosa botnet unitamente all'FBI statunitense e alle polizie e magistrature di 30 Paesi dei 5 continenti, nell'ambito dell'operazione internazionale "Avalanche", coordinata da Europol e Interpol. L'operazione ha consentito, su scala globale, di arrestare 5 persone, eseguire 37 perquisizioni, sequestrare 39 server, mentre altri 221 sono stati inibiti, e bloccare ben 800.000 domini infetti.

PUNTO DI CONTATTO DELLA RETE 24/7 HIGH TECH CRIME DEL G7

Presso il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche è inserito il Punto di Contatto italiano per le emergenze tecnico-operative connesse al verificarsi di episodi di criminalità transnazionale, secondo quanto stabilito dalla Convenzione sul Cybercrime sottoscritta a Budapest il 23 novembre 2001.

Il Punto di Contatto opera 24 ore su 24 e 7 giorni su 7 all'interno della rete High Tech Crime costituita in ambito G7 e successivamente estesa al Consiglio d'Europa.

La rete, che attualmente collega ben 71 Paesi, è finalizzata a realizzare sollecite forme di ausilio nelle investigazioni ed in particolare ad ottenere il "congelamento" dei dati informatici utili alle inchieste, nelle more della loro formale acquisizione.

Financial Cybercrime

La Polizia Postale e delle Comunicazioni è da sempre in prima linea sul fronte della lotta al "Financial Cybercrime", l'ambito criminale che con l'avvento della new economy, in un mondo sempre più globalizzato, è divenuto più pericoloso e subdolo che mai.

Tutte le persone, giuridiche o fisiche, appartenenti al settore pubblico o privato, erogatrici di servizi o semplici fruitori, fanno ormai parte di questo nuovo mondo digitale senza confini, aperto a un'infinità di migliorie, innovazioni e rivoluzioni.

In questa nuova realtà sono nati nuovi modi di comunicare.

I soggetti che ne fanno parte sempre più spesso si riuniscono in gruppi creando delle vere e proprie reti sociali ove, al contrario di come avveniva nelle interazioni fisiche di una volta, lo scambio di informazioni tra i consociati, è immediato e l'informazione è fruibile a tutti secondo le norme e gli statuti che regolano quel determinato contesto.

Con tali presupposti anche il settore economico - finanziario ne è entrato a far parte, dettando di fatto nuove regole commerciali e semplificando al massimo il trasferimento di capitali da una parte all'altra del pianeta riducendo tale attività a un semplice click sulla tastiera.

La velocità e la semplicità degli scambi e l'utilizzo sempre più diffuso dei servizi di home banking contribuisce ad innalzare vertiginosamente il volume globale dei traffici. Se da un lato l'incremento del mercato digitale ha segnato una grossa opportunità per gli operatori economici, dall'altro ha attratto gli interessi soprattutto della criminalità organizzata transnazionale che ha rivolto da subito la propria attenzione ai servizi bancari online ed alle nuove transazioni mediante moneta elettronica.

Il phishing o la clonazione logica di carte di credito/debito, realizzati tramite furti massivi d'identità digitali, e aggressioni su larga scala, pur continuando a costituire una grossa problematica nel settore eco-

nomico è stata soppiantata dalle più moderne tecniche di attacco denominate CEO fraud o BEC fraud.

Le aziende, con disponibilità economiche ben più ingenti rispetto a un privato cittadino, sono oggi soggette ad attacchi specificatamente mirati, che attraverso la sostituzione di persona e il social engineering consente ai delinquenti la disposizione di ingenti somme di denaro verso conti correnti appositamente creati.

Nel primo caso il malfattore si sostituisce all'amministratore delegato dell'azienda, nel secondo caso si pone in mezzo alla transazione commerciale. In entrambi i casi vengono forniti IBAN di destinazione delle somme diversi da quelli genuini. Questa nuova metodica criminale costituisce, sempre più, la nuova frontiera degli attacchi informatici che oltre a minare in radice il sistema, rischiano di favorire l'insorgere di diffuse e incontrollabili sensazioni di insicurezza.

L'esperienza operativa della Polizia Postale e delle Comunicazioni ha dimostrato che il mezzo per contrastare efficacemente tali reati, può essere solo la partnership pubblico-privato.

OF2CEN
UN NUOVO MODELLO DI COOPERAZIONE TRA PUBBLICO E PRIVATO

Solo lo scambio immediato di informazioni che avviene sulla piattaforma OF2CEN (On line Fraud Cyber Centre and Expert Network) appositamente creata per l'analisi e il contrasto avanzato delle frodi del settore, riesce a fare fronte e a bloccare la transazione in frode, grazie alla collaborazione con le principali realtà bancarie italiane rappresentate dall'ABI (Associazione Bancaria Italiana) nonché allo stesso gruppo Poste Italiane S.p.A.

EUOF2CEN
OBIETTIVI DEL PROGETTO

In considerazione degli ottimi risultati raggiunti durante il primo periodo di operatività, la piattaforma OF2CEN sta per essere esportata in Europa con il nome di EU OF2CEN. Il nuovo progetto europeo, che vede l'Italia come leading country e la Polizia Postale e delle Comunicazioni come driver, prevede l'installazione di un datacenter presso l'Europol, che veicolerà in tempo reale le informazioni provenienti dalle varie banche degli altri paesi dell'UE e dalle Forze di Polizia connesse alla piattaforma, creando una comune rete di information sharing europea per il contrasto del financial cybercrime.
Anche in ambito europeo si continuerà a lavorare sulla base dei presupposti della piattaforma italiana avviata già dal novembre 2013, con lo scopo di:

- raccogliere le segnalazioni di operazioni sospette inoltrate alla Polizia dagli istituti bancari attraverso un canale sicuro di comunicazione;
- analizzare ed elaborare le informazioni trasmesse attraverso metodi di correlazione informatici;
- mettere a fattor comune e informare in tempo reale tutti gli istituti bancari sui fenomeni fraudolenti in corso.

COOPERAZIONE INTERNAZIONALE

Quanto mai produttiva risulta essere la collaborazione in ambito internazionale con Europol e Interpol. Sotto l'egida dei citati Organismi internazionali di polizia, il Servizio Polizia Postale e delle Comunicazioni viene coinvolto periodicamente, in qualità di coordinatore per l'Italia, in operazioni ad alto impatto denominate "GAAD" (*Global Airport Action Day)* ed "EMMA" (European Money Mules Action).

Il **"GAAD"** si sviluppa in 129 aerostazioni del mondo ed è volto al controllo dei passeggeri muniti di titolo di viaggio acquistato in frode, attraverso l'indebito utilizzo di carte di pagamento. Partecipano 43 Stati e 71 Compagnie Aeree, tre centrali operative: una a Singapore presieduta da personale di INTERPOL; una a Bogotà, presieduta da personale di AMERIPOL; la terza presso il quartier generale di EUROPOL con il supporto in tempo reale dei responsabili del settore frode, in Europa, di Mastercard, Visa, American Express, IATA *(International Air Transport Association)* e Perseuss. L'operazione in Italia si articola su circa 20 aeroporti italiani prevedendo anche il coinvolgimento della Direzione Centrale dell'Immigrazione e della Polizia delle Frontiere italiana.

"EMMA" è invece incentrata sul contrasto al fenomeno dei "money mules", primi destinatari delle somme provenienti da frodi informatiche e campagne di phishing, che offrono la propria identità per l'apertura di conti correnti e/o carte di credito, sui quali vengono poi accreditate le somme frodate a ignari cittadini con varie tecniche fraudolente.

Nel corso del 2016 si sono registrati 221 arresti e l'individuazione di circa 1.200 "muli" in Europa, molti dei quali avevano collegamenti oltre oceano (Brasile, Nigeria, Qatar).

Sono state individuate, inoltre, più di 800 transazioni bancarie fraudolente e recuperate e sequestrate somme superiori agli 8 milioni di euro con il coinvolgimento delle polizie di 16 Paesi dell'Unione Europea sotto il coordinamento di Europol ed Eurojust e con il supporto della Federazione Bancaria Europea (EBF)**.**

In questo contesto sono state eseguite una serie di operazioni di polizia giudiziaria nei confronti di gruppi criminali di diverse nazionalità ed estrazione responsabili di financial cybercrime ai danni di singoli cittadini, piccole e medie imprese ed importanti gruppi bancari e di intermediazione finanziaria. Gli investigatori della Polizia Postale e delle Comunicazioni hanno condotto le operazioni avvalendosi della già citata piattaforma per la condivisione delle informazioni denominata "OF2CEN", realizzata appositamente al fine di prevenire e contrastare le aggressioni criminali ai servizi di home banking e monetica. In Italia sono stati identificati 65 *money mules* di cui 12 arrestati e 28 denunciati; 66 sono le transazioni fraudolente per un totale di circa 1 milione e mezzo di euro di cui 1 milione recuperato.

Contrasto al cyberterrorismo e ai reati di odio

Nel settore del cyberterrorismo gli investigatori della Polizia Postale e delle Comunicazioni concorrono con altri organi di Polizia e di intelligence alla prevenzione e al contrasto dei fenomeni di eversione e terrorismo, sia a livello nazionale che internazionale, posti in essere attraverso l'utilizzo di strumenti informatici e di comunicazione telematica.

Nell'ultimo anno, la strategia mediatica messa in campo dalle organizzazioni terroristiche di matrice religiosa islamista ha indotto la Specialità a effettuare un costante monitoraggio della Rete per individuare forme di proselitismo e segnali precoci di radicalizzazione in rete, ma anche segnali di natura razzista, xenofoba, sessuofobica o comunque ispirate a reati di odio.

Al fine di realizzare una efficace azione di contrasto al terrorismo che attraverso la rete fa opera di proselitismo, di indottrinamento e di addestramento, la Polizia Postale e delle Comunicazioni ha individuato nove Compartimenti pilota (Bologna, Catania, Genova, Milano, Napoli, Palermo, Perugia, Roma, Torino), che effettuano il monitoraggio della rete con l'ausilio di un mediatore culturale indispensabile per comprendere non solo la lingua ma anche l'ambito storico e formativo che caratterizza queste nuove forme di manifestazione del terrorismo di matrice islamica.

Il Servizio Polizia Postale e delle Comunicazioni costituisce, inoltre, *punto di contatto nazionale* per l'IRU (Internet Referral Unit), Unità di Riferimento Internet in ambito Europol, sviluppata sulla base del progetto *Check the Web*, con l'intento di condividere con altri Paesi informazioni di intelligence e per rispondere alla necessità di agire tempestivamente quando si presentino contenuti pericolosi che riguardano la nostra o altre Nazioni, mettendo a fattor comune notizie di interesse generale.

L'IRU, infatti, effettua una approfondita analisi dei contenuti emersi in rete che possano essere di interesse per la sicurezza nazionale, condividendoli con i Paesi UE e con gli altri Paesi interessati.

Riguardo l'attività di contrasto ai reati di antisemitismo, odio raziale o più in generale di discriminazione, la Polizia Postale e delle Comunicazioni lavora in costante raccordo con l'UNAR (Ufficio Nazionale Antidiscriminazioni Razziali) e l'OSCAD (Osservatorio per la Sicurezza contro gli Atti discriminatori), che trasmette le segnalazioni ritenute rilevanti.

In tale ambito si evidenzia anche la partecipazione dei cittadini che provvedono a segnalare alla Polizia Postale manifestazioni di hate speech.

L'analisi dell'attività investigativa, di iniziativa o delegata, appare quanto mai di fondamentale importanza nella comprensione dei fenomeni.

La valutazione dei dati, infatti, può fornire informazioni utili all'interpretazione degli stessi e sull'andamento e rapido mutamento che caratterizzano questi crimini.

ATTIVITÀ ANTITERRORISMO

Richieste di espulsione	1
Persone arrestate	2
Persone denunciate	9
Perquisizioni	5
Spazi web con contenuti illeciti	13.491
Spazi web monitorati	435.959
Accertamenti in cooperazione con altri enti	110
Contenuti web oscurati direttamente dal gestore del Servizio	510
Contenuti web oscurati su segnalazione di questa Specialità (profili Facebook, Twitter)	13

SEGNALAZIONI RICEVUTE DAI CITTADINI TRAMITE COMMISSARIATO DI PS ONLINE

Spazi web riconducibili alla xenofobia e al razzismo	106
Spazi web riconducibili al terrorismo	394

ATTI DISCRIMINATORI NEI CONFONTI DELLE MINORANZE, XENOFOBIA E RAZZISMO

Spazi web monitorati	1.120
Persone denunciate	8
Perquisizioni	1

Lotta alla contraffazione

Nella realtà odierna la rapida evoluzione tecnologica, che ha caratterizzato l'ultimo ventennio, tende a catalizzare in maniera esponenziale l'essere umano e nel complesso la sua vita sociale. Sebbene questo progresso accelerato costituisca un elemento peculiare in quanto esercita nell'essere umano il potenziamento di alcune caratteristiche, di contro può accadere che tale rapidità possa causare nell'uomo comportamenti irrazionali che provocano inevitabilmente forti lacerazioni del tessuto sociale. L'utilizzo di Internet, esploso grazie a nuovi sistemi di elaborazione, computer e reti, ha così procurato anche un parallelo processo evolutivo delle attività criminose a svantaggio dei membri della società e del loro patrimonio.

La Polizia Postale e delle Comunicazioni, impegnata costantemente nella prevenzione e contrasto del cybercrime, rappresenta oggi un punto di riferimento a garanzia di un corretto uso del mondo virtuale ed è fortemente sostenuta dalle innovazioni legislative in materia di crimini informatici.

La competenza acquisita nel settore del contrasto ai delitti consumati online 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 svolgere attività di repressione riguardo:

- 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 sevizi 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 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 e opere cinematografiche e musicali sono stati 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 di Internet 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.

La Polizia Postale e delle Comunicazioni collabora inoltre in sinergia con l'AGCOM, in relazione al nuovo regolamento, entrato in vigore il 31 marzo 2013, in materia di Tutela del Diritto d'Autore sulle Reti di Comunicazione Elettronica.

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 consentire la illecita visione a soggetti non abilitati che si servono del 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 la violazione del copyright, con grave danno alle aziende che producono e diffondono programmi televisivi e a quelle che forniscono sistemi di sicurezza digitale.

Il Commissariato di P.S. online

Dal febbraio del 2006 il portale del Commissariato di P.S. online, anche grazie alla nuova implementazione avvenuta nel 2013, continua ad essere una risposta alle aspettative di sicurezza da parte dei cittadini che sempre più utilizzano la Rete quale mezzo di scambio di informazioni, di transazioni finanziarie, di accesso alle grandi banche dati o per la creazione e l'implemento di svariate attività professionali. In considerazione dell'incremento dell'uso del mezzo telematico e della naturale crescita di aspettative di sicurezza da parte del cittadino, il portale del Commissariato di P.S. on-line, con la sua primaria funzione di prevenzione dei crimini informatici, si riconferma un punto di riferimento specializzato di chi cerca informazioni, consigli, suggerimenti a carattere generale o per scaricare modulistica e presentare denunce. Il portale con i suoi innovativi sistemi di interattività con l'utente della Rete attraverso apposite "finestre dialogo" è direttamente collegato con il mondo dei social network e vede tra i suoi interlocutori privilegiati i più giovani, nonché utenti che spesso versano in condizioni di emarginazione e vulnerabilità. La ratio è rendere sempre più fruibile e semplice la possibilità per il cittadino di interagire con la Polizia, senza la necessità di uscire di casa per raggiungere l'Ufficio di Polizia più vicino. Prima esperienza in Europa, in tal senso il portale del Commissariato di P.S. online (www.commissariatodips.it), inserito all'interno del Servizio della Polizia Postale e delle Comunicazioni, è suddiviso in tre macro aree di intervento di facile e rapida consultazione denominate:

- Informati - contenitore di informazioni, notizie, approfondimenti e consigli utili;
- Domanda - canale per contattare gli esperti a cui rivolgere quesiti, richiedere informazioni e consigli;
- Collabora - spazio ove è possibile trasmettere segnalazioni, sporgere denunce online relative a reati telematici.

Il Commissariato, tra l'altro, offre il servizio news. Queste ultime sono costantemente aggiornate e permettono di conoscere in tempo reale le nuove tipologie di truffe operate in Rete nonché di essere preventivamente aggiornati sulla divulgazione di software malevoli diffusi attraverso la stessa. In considerazione della sorprendente evoluzione della comunicazione la cui massima espressione è rappresentata oggi dalle "piazze virtuali" dei social network, il sito del Commissariato non poteva non essere presente, con la sua attività di informazione, sulla community più diffusa ed utilizzata del momento:FACEBOOK. Dal portale è possibile, inoltre, accedere ad ulteriori servizi di approfondimento che riguardano altre tematiche come: passaporti, armi, immigrazione, minori, nonché scaricare moduli per autorizzazioni e licenze.

Piace ricordare che il progetto del "Commissariato di P.S. online" ha ricevuto il premio "Most Inspring Good Practice" all'European e-Government Awards 2007, lanciato dalla Commissione Europea a testimonianza dell'innovatività e dell'efficacia dell'iniziativa.

APP DEL COMMISSARIATO DI PS ONLINE

Rappresenta uno strumento agevole che consente al cittadino di entrare nel portale del Commissariato Virtuale, da casa, dal posto di lavoro o da qualsiasi luogo si desideri, usufruendo dei medesimi servizi di segnalazione, informazione e collaborazione che la Polizia Postale e delle Comunicazioni quotidianamente ed ininterrottamente offre agli utenti del web nell'arco delle 24h, per dare maggiore sicurezza in rete, fornendo anche tutte quelle notizie di interesse a tutela dei dati personali, della protezione da frodi e rischi sui temi "caldi" particolarmente sentiti da chi utilizza Internet. L'applicazione, che integra i servizi già offerti al cittadino dal portale del Commissariato di PS online, è scaricabile gratuitamente sul proprio smartphone o su tablet, sia per il mondo Apple che Android. E' uno strumento di semplice consultazione che consente non solo di venire incontro alle

POLIZI@

crescenti richieste di assistenza e di aiuto degli utenti della Rete, in tempo reale, ma permette altresì di conoscere sempre di più il mondo del web anche con un pizzico di divertimento. E' infatti possibile cimentarsi da soli o in compagnia in un gioco a quiz di venti domande, attinenti alla sicurezza informatica in genere, dal titolo "A CHE ER@ APPARTIENI", il cui risultato potrà essere condiviso con i propri amici anche sulla piattaforma Facebook, dove è presente la nostra pagina istituzionale.

DATI STATISTICI COMMISSARIATO VIRTUALE

SERVIZI OFFERTI	
Informazioni:	**17.374**
Segnalazioni:	**19.492**
Denunce:	**8.355**
Visite al portale totali	**1.241.498**
Iscritti al portale	**60.057**

STATISTICHE DOWNLOAD APP (dalla nascita luglio 2015 al 30 giugno 2016)

Play Store	**7.221 download**
iOS	**4.823 download**

Le campagne educative della Polizia Postale e delle Comunicazioni

La Polizia Postale e delle Comunicazioni svolge ormai da tempo un ruolo di primo piano nel campo della sensibilizzazione e della prevenzione sui rischi e pericoli connessi all'uso della rete, mediante una serie di iniziative rivolte soprattutto alle giovani generazioni.

Lo scopo di queste campagne è quello di far pervenire ai giovani messaggi concreti in tema di rispetto delle regole ed educazione alla legalità.

Ha compiuto 3 anni la più importante e imponente campagna educativa itinerante al fianco delle nuove generazioni, "Una Vita da Social", realizzata dalla Polizia di Stato in collaborazione con il Ministero dell'Istruzione, dell'Università e della Ricerca e cofinanziata per l'edizione 2016 dalla Comunità Europea.

La preziosa esperienza maturata nel corso dei tre anni ha consentito di perfezionare e proporre un progetto al passo con i tempi dei nativi digitali e non solo, che nel corso delle tre edizioni ha raccolto grandi consensi: gli operatori della Polizia Postale e delle Comunicazioni hanno incontrato oltre 1 milione di studenti sia nelle piazze che nelle scuole, 106.125 genitori, 59.451 insegnanti per un totale di 8.548 istituti scolastici, 30.000 km percorsi e 150 città raggiunte sul territorio e una pagina Facebook con 98.000 like e 12 milioni di utenti mensili sui temi della sicurezza online. "Una Vita da Social" rappresenta un progetto dinamico, innovativo, che si avvicina alle nuove generazioni attraverso i social network, evidenziando sia le opportunità del web, sia i rischi di cadere nelle tante trappole dei predatori della rete, confezionando un vero e proprio "manuale d'uso", affinché "i gravissimi episodi di cronaca, culminati con il suicidio di alcuni adolescenti e il dilagante fenomeno del cyberbullismo e di tutte le varie forme di prevaricazione connesse ad un uso distorto delle tecnologie, non abbiano più a verificarsi". Ed in effetti, i primi tre anni di vita della campagna hanno esaltato la evidente bontà dell'iniziativa, che ha avuto un alto impatto sociale ed è stata

altamente apprezzata da studenti, insegnanti e genitori di tutta Italia e che ha permesso alla Polizia Italiana di raggiungere risultati elevati nell'attività di prevenzione su problematiche di grande attualità in collaborazione con le varie aziende private, dimostrando l'importanza di fare sistema in favore di una idea di sicurezza partecipata in cui pubblico e privato superano antiche logiche di pedanti consuetudini o di mercato, per dare spazio ad iniziative sinergiche di grande efficacia ed impatto.

Utilizzando un truck multimediale allestito come un'aula didattica, gli operatori della Polizia Postale e delle Comunicazioni e i rappresentanti delle aziende, hanno incontrato studenti, genitori e insegnanti sui temi della sicurezza online con un linguaggio semplice ma esplicito adatto a tutte le fasce di età che ha permesso di far emergere tutte quelle situazioni di grave disagio da parte degli adolescenti, in termini di molestie, diffamazione, furti di identità online e adescamenti in rete prima sopite all'interno delle mura scolastiche.

L'iniziativa è stata anche supportata da numerosi testimonial del mondo della cultura, dello spettacolo, della musica e dello sport, che hanno sostenuto l'evento attraverso messaggi di legalità e di rispetto delle regole, e ha anche visto la presenza delle più alte Cariche dello Stato, i Presidenti Giorgio Napolitano e Sergio Mattarella. Anche in campo internazionale l'iniziativa "Una Vita da Social" ha raggiunto risultati di altissimo livello, infatti la Commissione Europea ha selezionato la campagna di prevenzione itinerante della Polizia di Stato Italiana contro il cyberbullismo tra le migliori pratiche a livello europeo. Nel giorno in cui la Commissione Europea ha lanciato la "Digital Skills and Jobs Coalition", una iniziativa per ridurre il gap esistente sulle competenze digitali in Europa, è arrivata la decisione dell'Organo comunitario di riconoscere alla nota campagna della Polizia Postale e delle Comunicazioni un indubbio carattere di originalità ed innovazione. Una giuria indipendente, su input della Commissione Europea, ha selezionato tra 280 progetti mirati ad elevare le competenze digitali dei cittadini europei, l'iniziativa di successo della Polizia Postale italiana, individuandola come la più imponente ed incisiva campagna di sensibilizzazione mai realizzata da un Organismo di Polizia. La relativa pagina facebook di "Una Vita da Social", gestita direttamente dalla Polizia Postale e delle Comunicazioni, che rappresenta di fatto il diario di bordo, dove vengono pubblicati gli appuntamenti, le attività, i contributi eccellenti di tutte le tappe del tour e dove i giovani internauti possono riportare direttamente le loro impressioni ad ogni appuntamento ha ottenuto nel 2016 oltre 98.000 like. Inoltre, nel corso dell'anno, sono stati, realizzati numerosi incontri educativi su tutto il territorio nazionale raggiungendo circa 500.000 studenti, con i rispettivi genitori e insegnanti, e oltre 1.500 Istituti scolastici per i quali è stata messa a disposizione anche un'email dedicata:
progettoscuola.poliziapostale@interno.it

Consigli per un uso sicuro dei social network

L'uso dei social network è vietato ai minori di 13 anni ed è sconsigliato ai minori di 14: 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, 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 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 visibilità 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.

Come equipaggiare il computer e usarlo in sicurezza

- **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.
- **CONTROLLATE PERIODICAMENTE IL CONTENUTO DELL'HARD DISK** del computer.

- **USATE SOFTWARE "FILTRI"** con un elenco predefinito di siti da evitare. Verificate periodicamente che funzionino in modo corretto e tenete segreta la parola chiave.
- **LEGGETE 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.

9 Regole da tenere a mente

1 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.

2 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.

3 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.

4 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.

5 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).

6 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®.

7 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?

8 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.

9 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.

Alcuni utili consigli per i genitori

- **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 ragazzi

- **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 social network 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!

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.

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 entrata.

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. Affinché 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 effettuare 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.

Baiting | Prendere di mira utenti (user), nello specifico principianti (new user), in ambienti virtuali di gruppo (es: chat, game, forum), facendoli diventare oggetto di discussioni aggressive attraverso insulti e minacce per errori commessi dovuti all'inesperienza.

Bannare | Escludere un utente di Internet dall'accesso a una chat, a un forum, ecc., nel caso in cui questi abbia ripetutamente violato le regole delle netiquette.

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.

Bufala | Notizia falsa che circola sui social network e sul web.

Catfish | termine utilizzato per indicare chi assume online un'identità falsa perché appartenente ad un altro utente.

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.

Glossario

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.

Crashare | Indica il blocco o la terminazione improvvisa, non richiesta e inaspettata di un programma in esecuzione, oppure il blocco completo dell'intero computer. Si può estendere in qualsiasi situazione in cui qualcosa o qualcuno si blocca o si incastra.

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

Cyberbashing | specifica tipologia di Cyberbullismo che consiste nel videoregistrare un'aggressione fisica nella vita reale per poi pubblicarla online.

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 autoeseguibile 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 d'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.

Googlare | Cercare qualcosa su Google. Si può usare anche con il significato di cercare informazioni su qualcuno di cui si vuole conoscere dettagli personali.

Grooming | Lento adescamento online, tramite chat e social network, in cui un cyber predatore individua una giovane vittima, instaura una relazione dapprima amicale, poi confidenziale ed intima per poi sfruttarla a fini sessuali.

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. Purtroppo 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.

Hater | Utente di social network che, protetto da anonimato, commenta in maniera polemica e aggressiva post, immagini e video di altri utenti.

Hikikomori | Gravissima forma di ritiro sociale che consiste nel rifiuto di uscire di casa e svolgere le normali attività quotidiane. In queste situazioni i ragazzi utilizzano Internet come unico strumento per entrare in contatto con il mondo esterno.

Hoax (finte mail) | Un fenomeno legato al Phishing e al furto d'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.

Iger | È colui o colei che produce e pubblica foto o video per la piattaforma di Instagram. L'iger se ha successo può diventare una vera e propria celebrità.

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."

Mailbombing | Tipologia di attacco informatico che consiste nell'invio di una quantità di messaggi numericamente rilevanti, verso una stessa casella di posta elettronica. Ciò avviene tramite programmi denominati "mailbomber" che causano il rallentamento o il blocco del server di posta.

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 gratuito o un file da una rete peer to peer.

Meme | Vignetta umoristica diffusa sui social network: può essere una foto o un disegno, spesso l'immagine viene sovrascritta con un testo ironico.

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 utilizzare 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."

Postare | Pubblicare un post, una foto o un video sui social network.

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.

Selfie | E' un autoritratto realizzato attraverso una fotocamera digitale compatta, uno smartphone, un tablet o una webcam puntati verso sé stessi o verso uno specchio, e condiviso sui social network

Sexting | Atto di inviare fotografie e/o messaggi di testo sessualmente espliciti, sia attraverso telefoni cellulari, sia tramite mezzi informatici differenti.

Sextortion Scams | Truffa perpetrata ai danni di utenti internet ai quali, con l'illusione di un flirt o di una storia sentimentale, vengono estorte immagini erotiche usate poi come strumenti di ricatto.

Shazammare | Un termine derivato da Shazam, l'applicazione che riconosce qualsiasi canzone o programma tv.

Snappare | Inviare un messaggio tramite l'app Snapchat

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.

Spammare | È l'invio anche verso indirizzi generici, non verificati o sconosciuti, di messaggi ripetuti ad alta frequenza o a carattere di monotematicità tale da renderli indesiderati. Si può dire a livello colloquiale per intendere l'inviare messaggi o promuovere qualcosa con insistenza.

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.

Tabnabbing | Forma più raffinata di phishing. Si tratta di una truffa online che prende di mira le schede aperte (TAB) nel browser sostituendone il contenuto con una pagina identica, creata appositamente per indurre l'utente a inserire i propri dati personali che saranno poi copiati.

Taggare | Menzionare sui social network il profilo di un utente su foto o post.

Tinderizzare | Qualsiasi processo che ha che fare con la selezione veloce e basata solo su criteri visivi. Nasce da Tinder, l'app di dating che consente di scartare o approvare i profili dei potenziali partner in una manciata di secondi.

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 ese-

guendo il programma che contiene il Trojan, l'utente innesca il virus.

Trollare | Interagire con gli altri su web e social network tramite messaggi provocatori, irritanti, fuori tema o semplicemente senza senso, con l'obiettivo di disturbare la comunicazione e fomentare gli animi. Nel linguaggio comune assume la valenza di "prendere in giro", "ingannare per scherzo".

Twittare | Pubblicare un post sulla piattaforma Twitter.

Virale | Aggettivo per definire post, foto o video che sui social network collezionano un elevato numero di condivisioni.

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.

Webete | Il termine webete, composto da "web" ed "ebete", indica l'utente che assume comportamenti contrari alla "netiquette" con altri utenti.

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.

Whatsappare | Inviare messaggi tramite l'app WhatsApp.

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.

Youtuber | Lo youtuber è colui o colei che produce e pubblica video per la piattaforma di Youtube. Lo youtuber ha un proprio canale in cui pubblica con una certa costanza video di durata compresa tra i 5 e i 30 minuti in cui parla di un determinato argomento. Lo youtuber se ha successo può diventare una vera e propria celebrità.

Contatti

Compartimento Polizia Postale e delle Comunicazioni – ABRUZZO

Pescara, Via Ravenna n. 8, cap 65100
Centralino: tel. 085.4279750

SEZIONI

Chieti: Via Pescara n. 223
tel. 0871.584447

L'Aquila: S.S. 17 - Località Centi Colella
tel. 0862.579091

Teramo: Via San Benedetto in Chartullis n. 4, tel. 0861.439044

Compartimento Polizia Postale e delle Comunicazioni – BASILICATA

Potenza, Via Pasquale Grippo 27/29
cap 85100 - Centralino: tel. 0971.327364

SEZIONI

Matera: Via del Corso 15, tel. 0835.332722

Compartimento Polizia Postale e delle Comunicazioni – CALABRIA

Reggio Calabria, Via S. Anna, 2° tronco
cap 89100-centralino: tel. 0965.309011-49

SEZIONI

Catanzaro: Via dei Cardatori 14
tel. 0961.743923

Cosenza: Via Milelli, c/o poste vecchie
tel. 0984.687411

Crotone: Via della Menta snc
tel. 0962.9294521

Compartimento Polizia Postale e delle Comunicazioni – CAMPANIA

Napoli, Via delle Repubbliche Marinare n. 495, cap 80146
centralino: tel. 081.2433001

SEZIONI

Avellino: Via Amm. Ronca 13
tel. 0825.21074

Benevento: Via Traversa delle Poste 1
tel. 0824.50407

Caserta: Viale Lamberti 29
tel. 0823.527296

Salerno: Via Paradiso di Pastena 5
tel. 089.2572143

Compartimento Polizia Postale e delle Comunicazioni – EMILIA ROMAGNA

Bologna, Via Zanardi n. 28, cap 40132
centralino: tel. 051.6352611

SEZIONI

Ferrara: Via Bologna 690, tel. 0532.978348

Forlì: Via Bertini 11, tel. 0543.373360

Modena: Strada Nazionale Canaletto Sud 309, tel. 059.243064

Parma: Via Pastrengo 1, tel. 0521.219550

Piacenza: Via S. Antonino 38/40
tel. 0523.316442

Ravenna: Via Meucci 73, tel. 0544.284678

Reggio E.: Via Iori 8, tel. 0522.336420

Rimini: Largo Giulio Cesare 1
tel. 0541.634298

Compartimento Polizia Postale e delle Comunicazioni – FRIULI VENEZIA GIULIA

Trieste, Piazza Vittorio Veneto n. 1, cap 34100
centralino: tel. 040.6764589

SEZIONI

Gorizia: Via Corso Verde 33
tel. 0481.590258

Pordenone: Via S. Caterina 8
tel. 0434.222362

Udine: Via G. Marinelli 1/B
tel. 0432.223248

Compartimento Polizia Postale e delle Comunicazioni – LAZIO

Roma, Viale Trastevere n. 191, cap 00153
centralino: tel. 06.588831,
06.5813429, 5813608

SEZIONI

Frosinone: Via Vado del Tufo 67/A
tel. 0775.250756
Latina: Piazza Bonificatori 8
tel. 0773.449214
Rieti: Via Tancia 62, tel. 0746.270114
Viterbo: Via F. Ascenzi 9, tel. 0761.335499

Compartimento Polizia Postale e delle Comunicazioni – LIGURIA

Genova, Via Dante n. 4, cap 16100
centralino: tel. 010.540135

SEZIONI

Imperia: Via Spontone 39
tel. 0183.795502, 0183.710619
La Spezia: Piazza Verdi 1, tel. 0187.734074
Savona: Piazza Diaz 9, tel. 019.8414537

Compartimento Polizia Postale e delle Comunicazioni – LOMBARDIA

Milano, Via Moisè Loria n. 74, cap 20144
centralino: tel. 02.43333011
e-mail: poltel.mi@poliziadistato.it

SEZIONI

Bergamo: Via Matris Domini, 4
tel. 035.4532208
Brescia: Via della Posta 2, tel. 030.2912431
Como: Via E. Bossi 3, tel. 031.2763036
Cremona: Via Verdi, 1 tel. 0372.593588
Mantova: Via Pietro Nenni, 2
tel. 0376.327022
Pavia: Piazzale della Stazione, 21
tel. 0382.33950
Sondrio: Viale dell'Industria, 1
tel. 0342.545529
Varese: Via Milano, 11 tel. 0332.281402

Compartimento Polizia Postale e delle Comunicazioni – MARCHE

Ancona, Via Marconi n. 56, cap 60100
centralino: Tel. 071.4190330
e-mail: poltel.an@poliziadistato.it

SEZIONI

Ascoli Piceno: Largo S. Gallo, 2
tel. 0736.242305-06
Macerata: Piazza Oberdan, 1
tel. 0733.273012 – 0733273037-82-03-36
Pesaro: Strada dei Cacciatori snc.
tel. 0721.549719-20-21

Compartimento Polizia Postale e delle Comunicazioni – MOLISE

Campobasso, Via S. Giovanni n. 55
cap 86100,
centralino: tel. 0874.482100
e-mail: poltel.cb@poliziadistato.it

SEZIONI

Isernia: Via XXIV Maggio n. 243
tel. 0865.504324

Compartimento Polizia Postale e delle Comunicazioni – PIEMONTE

Torino, Corso Tazzoli n. 235, cap 10100
centralino: tel. 011.3014611
e-mail:
compartimento.polposta.to@pecps.interno.it

SEZIONI

Alessandria: Via Ghilini, 3
tel. 0131.302250
Aosta: Via Festaz 20, tel. 0165.276244
Asti: Via Verdi 17, tel. 0141.357270
Cuneo: Via Cavour 3, tel. 0171.460351
Biella: Via Sant'Eusebio, 5/A
tel. 015.3590685
Novara: Largo Costituente 4
tel. 0321.335257
Vercelli: Via S. Anna, 9 tel. 0161.264112

Compartimento Polizia Postale e delle Comunicazioni – PUGLIA

Bari, Via Amendola n. 116, cap 70100
centralino: tel. 080.5920611
e-mail: poltel.ba@poliziadistato.it

SEZIONI

Lecce: Piazzale Massari, 54
tel. 0832/244150

Foggia: Via Isonzo, 10 tel. 0881/722100

Taranto: Lungomare V. Emanuele III
c/o filiale P.T. - tel. 099/4554265

Brindisi: Piazza Vittorio Emanuele II, 5
tel. – 0831/523185

Compartimento Polizia Postale e delle Comunicazioni – SARDEGNA

Cagliari, Via Simeto n. 38, cap 09100
centralino: tel. 070.27665
e-mail: poltel.ca@poliziadistato.it

SEZIONI

Nuoro: Piazza Crispi, 1 tel. 0784/245238

Sassari: Via Brigata Sassari, 13
tel. 079/2821239

Oristano: Via Canepa n.1
tel. 0783/210143

Compartimento Polizia Postale e delle Comunicazioni – SICILIA OCCIDENTALE

Palermo, Via Roma n. 320, cap 90146
centralino: tel. 091.7535198
e-mail: poltel.pa@poliziadistato.it

SEZIONI

Agrigento: P.zza V. Emanuele, 7 - Palazzo Poste Italiane S.p.A. tel. 0922/551593

Caltanissetta: Via Leone XIII - Palazzo Poste Italiane S.p.A. tel. 0934/562153-5

Enna: contrada Baronessa snc
tel. 0935/562272

Trapani: P.zza V. Veneto nr.11, Palazzo Poste Italiane S.p.A. tel. 0923/434322

Compartimento Polizia Postale e delle Comunicazioni – SICILIA ORIENTALE

Catania, Via Beato Bernardo, 5, cap 95124
centralino: tel. 095/3520411
e-mail: poltel.ct@poliziadistato.it

SEZIONI

Siracusa: Viale Santa Panagia, 129
tel. 093/1498263

Messina: SS 114 Km. 5.200 Pistunina
tel. 090/6257295

Ragusa: Via Ercolano, 7 tel. 0932/235683

Compartimento Polizia Postale e delle Comunicazioni – TOSCANA

Firenze, Via della Casella n. 19, cap 50100
centralino: tel. 055.7876711
e-mail: poltel.fi@poliziadistato.it

SEZIONI

Grosseto: Viale Matteotti, 1
tel. 0564/448609 – 0564/448443

Livorno: Piazza Benamozegh, 3
tel. 0586/276467-8

Massa: Via Carducci, 40, tel. 0585/255491
0585/259248 - 0585/259252

Siena: Viale Achille Sclavo, 4
tel. 0577/276645 - 0577/276652

Pisa: Via Emilia, 370/a - tel. 050/3162431

Arezzo: Via G. Monaco, 34
tel. 0575/332431–2

Pistoia: Via Pratese, 49 tel. 0573/970726

Lucca: Via Piaggia c/o C.P.O.
tel. 0583/457807

Prato: c/o Sezione Polizia Stradale
tel. 0574/614540

Compartimento Polizia Postale e delle Comunicazioni – TRENTINO ALTO ADIGE

Trento, Via Vannetti n. 15, cap 38100
centralino: tel. 0461.232462
e-mail: poltel.tn@poliziadistato.it

SEZIONI

Bolzano: Via Resia n.190 tel. 0471/531413

Compartimento Polizia Postale e delle Comunicazioni – UMBRIA

Perugia, Via M. Angeloni n. 72, cap 06124
centralino: tel. 075.5001703
e-mail: poltel.pg@poliziadistato.it

SEZIONI

Terni: Via Bramante, 5
tel. 0744/201305 – 0744/201390

Compartimento Polizia Postale e delle Comunicazioni – VENETO

Venezia, Via Torino n. 88, cap 30174
centralino: tel. 041/2907311
e-mail: poltel.ve@poliziadistato.it

SEZIONI

Belluno: Via Vittorio Veneto n.250
tel. 0437931776

Padova: Via della Ricerca Scientifica, 5
tel. 049/656456

Rovigo: Piazza Caffaratti, 1
tel. 0425/420225

Treviso: Piazza Vittoria, 1
tel. 0422/653301

Verona: Piazzale Guardini, snc
tel. 045/9273293

Vicenza: Contra' S. Maria Nova, 4
tel. 0444/338551

Finito di stampare nel mese di aprile 2017
da Tipografia Facciotti - Roma
www.tipografiafacciotti.com

www.poliziadistato.it
www.commissariatodips.it