Resoconto attività 2022
della Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica

Nel 2022 la Polizia Postale è stata chiamata a far fronte a continue e sempre più evolute sfide investigative sulle macro-aree di competenza, in particolare negli ambiti della prevenzione e contrasto alla pedopornografia online, della protezione delle infrastrutture critiche di rilevanza nazionale, del financial cybercrime e di quelle relative alle minacce eversivo-terroristiche, riconducibili sia a forme di fondamentalismo religioso che a forme di estremismo politico ideologico, anche in contesti internazionali.

CENTRO NAZIONALE PER IL CONTRASTO ALLA PEDOPORNOGRAFIA ONLINE (C.N.C.P.O.)

In uno scenario nel quale la continua evoluzione tecnologica influenza ogni azione del nostro vivere quotidiano, lo sforzo della Polizia Postale e delle Comunicazioni nell'anno 2022 è stato costantemente indirizzato alla prevenzione e al contrasto della criminalità informatica in generale, con particolare riferimento ai reati in danno di minori.

Il **Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.)** nel 2022 ha confermato il suo ruolo di punto di riferimento e di coordinamento nazionale dei **Centri Operativi Sicurezza Cibernetica – COSC** della Polizia Postale nella lotta alla pedofilia e pornografia minorile online.

L'analisi dei dati relativi all'anno di riferimento ha confermato la lieve diminuzione dei casi trattati già evidenziata nella rilevazione di medio termine. La flessione negativa dei dati è stata riscontrata anche in riferimento al numero delle segnalazioni provenienti da organismi internazionali attivi nella protezione dei minori in rete. L'impegno profuso dalla Specialità si è concentrato nel reprimere episodi di particolare gravità, con l'effetto rilevabile di evidenziare un maggior numero di individui sottoposti a pene detentive.

Nell'ambito poi delle segnalazioni relative alla pubblicazione di contenuti pedopornografici su social network, si è evidenziato un fenomeno per il quale veniva intaccata

la reputazione dei vari titolari di profili social attraverso la pubblicazione di materiale scabroso di natura pedopornografica con accessi abusivi massivi a profili privati di ignari cittadini e di persone dotate di rilevanza mediatica, politica o di altra natura.

La fine dell'emergenza sanitaria, con la progressiva ripresa delle attività nella direzione di un recupero della normalità, potrebbe aver contribuito a ridurre l'isolamento sociale, facendo rilevare nel 2022 una riduzione della circolazione globale di materiale pedopornografico su circuiti internazionali, che non ha però inciso sull'attività di contrasto. Infatti, **è stato registrato un aumento dei soggetti individuati e deferiti per violazioni connesse ad abusi in danno di minori**.

In particolare, nell'ambito dell'attività di contrasto coordinata dal Centro sono stati trattati complessivamente **4.542 casi**, che hanno consentito di indagare **1.463 soggetti**, di cui **149 tratti in arresto** per reati connessi alla materia degli abusi tecnomediati in danno di minori, con un aumento di persone tratte in arresto di circa il **+8%** rispetto allo stesso periodo dell'anno precedente.

Per quanto concerne l'attività di prevenzione svolta dal C.N.C.P.O. attraverso una continua e costante attività di monitoraggio della rete, sono stati visionati **25.696** siti, di cui **2.622** inseriti in black list e oscurati, in quanto presentavano contenuti pedopornografici.

PEDOPORNOGRAFIA E ADESCAMENTO ONLINE	**2021**	**2022***	**Variazione percentuale**
Persone indagate	1.419	1.463	**+3%**
Siti in Black List	2.543	2.622	**+3%**
* - dati rilevati il 27/12/2022			

Adescamento online

Nel periodo di riferimento sono stati trattati **424** casi per adescamento online: anche quest'anno la fascia dei preadolescenti (età 10-13 anni) è quella più coinvolta in interazioni sessuali tecnomediate, **229** rispetto al totale.

Continua a preoccupare il lento incremento dei casi relativi a bambini adescati di età inferiore ai 9 anni, trend che è diventato più consistente a partire dalla pandemia. Social network e videogiochi online sono i luoghi di contatto tra minori e adulti più frequentemente teatro delle interazioni nocive, a riprova ulteriore del fatto che il rischio si concretizza con maggiore probabilità quando i bambini e i ragazzi si esprimono con spensieratezza e fiducia, nei linguaggi e nei comportamenti tipici della loro età.

Cyberbullismo

Si registra una leggera flessione anche dei casi di cyberbullismo che può essere interpretata come effetto della normalizzazione delle abitudini dei ragazzi: non si può escludere che il ritorno ad una vita sociale priva di restrizioni abbia avuto un'influenza positiva sulla qualità delle interazioni sociali, delle relazioni tra coetanei e che la costanza dell'opera di

sensibilizzazione svolta dalla Polizia Postale, presso le strutture scolastiche, abbia mantenuto alta l'attenzione degli adulti e dei ragazzi stessi sulla necessità di agire responsabilmente e correttamente in rete.

Nel periodo di riferimento sono stati trattati **323** casi di cyberbullismo.

CYBERBULLISMO	**2021**	**2022***
Casi trattati vittime 0-9 anni	27	17
Casi trattati vittime 10-13 anni	112	87
Casi trattati vittime 14-17 anni	319	219
TOTALE	**458**	**323**
* - dati rilevati il 27/12/2022		

	2021	**2022***
Minori denunciati per Cyberbullismo	117	128
* - dati rilevati il 27/12/2022		

Sextortion

È un fenomeno che di solito colpisce gli adulti in modo violento e subdolo, fa leva su piccole fragilità ed esigenze personali, minacciando, nel giro di qualche click, la tranquillità delle persone.

Recentemente le **sextortion** stanno interessando sempre più spesso vittime minorenni, con effetti lesivi potenziati: la vergogna che i ragazzi provano impedisce loro di chiedere aiuto ai genitori o ai coetanei di fronte ai quali si sentono colpevoli di aver ceduto e di essersi fidati di perfetti e "avvenenti" sconosciuti.

La sensazione di sentirsi in trappola che sperimentano le vittime è amplificata spesso dalla difficoltà che hanno nel pagare le somme di denaro richieste. Nel corso dell'anno sono stati trattati **130 casi,** la maggior parte dei quali nella fascia **14-17 anni,** più spesso in danno di vittime maschili.

CENTRO NAZIONALE ANTICRIMINE PER LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE (C.N.A.I.P.I.C.)

Nell'esercizio della propria missione istituzionale, il Servizio Polizia Postale e delle Comunicazioni - Organo del Ministero dell'interno per la sicurezza delle telecomunicazioni garantisce, fra l'altro, ai sensi dell'art. 7 bis DL 144 del 2005 e del DM 15 agosto 2017 - Direttiva sul riordino dei comparti di Specialità delle Forze di Polizia – la protezione delle infrastrutture critiche informatizzate del Paese.

Nell'attuale e particolare contesto internazionale, l'*escalation* delle tensioni geopolitiche connesse al conflitto in Ucraina continua ad avere significativi riverberi anche in materia di sicurezza cibernetica. Risultano, infatti, in corso campagne massive a livello internazionale dirette verso infrastrutture critiche, sistemi finanziari e aziende operanti in settori strategici quali comunicazione e difesa, tra le quali figurano campagne di *phishing*, diffusione di *malware* distruttivi (specialmente *Ransomware*), attacchi Ddos, campagne di disinformazione e *leak* di database. Inoltre, alcuni tra i più pericolosi gruppi di hacker criminali hanno deciso di schierarsi a favore della Russia, altri con l'Ucraina, prendendo di fatto parte al conflitto nel c.d. "dominio cibernetico".

In tal senso, come noto, il conflitto russo-ucraino ha comportato una recrudescenza nell'attività di attori ostili, connotati per l'esecuzione di attacchi ransomware – volti a paralizzare servizi e sistemi critici mediante la cifratura dei dati contenuti – campagne DDoS, volti a sabotare la funzionalità di risorse online e, soprattutto, attacchi di tipo ATP (Advanced Persistent Threat), condotti da attori ostili di elevato expertise tecnico, in grado di penetrare i sistemi più strategici mediante tecniche di social engineering o sfruttamento di vulnerabilità, al fine di garantirsi una persistenza silente all'interno dei sistemi a scopo di spionaggio o successivo danneggiamento.

La proliferazione di gruppi ostili, si è attuata poi mediante il ricorso a crew hacker di c.d. *crime as a service*, ordinariamente attive nel fornire supporto tecnologico ad attori criminali ed oggi sempre più contigue a gruppi di ascendenza statuale.

In particolare, il Servizio polizia postale ha implementato l'attività informativa e di monitoraggio ad ampio spettro, esteso anche al *dark web*, attivando canali di diretta interlocuzione dedicati allo scenario in atto con Europol, oltre che con Interpol e FBI, con l'obiettivo di elevare il livello di attenzione con particolare riguardo al settore economico/finanziario, tradizionalmente oggetto di interesse da parte di compagini criminali con connotazione *state sponsored*.

Il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC), attraverso dedicati *alert* ha diffuso indicatori di compromissione e avvisi di informazione di sicurezza alle infrastrutture informatiche dicasteriali, alle infrastrutture critiche nazionali e ai potenziali *target* di azioni ostili, individuati attraverso la permanente attività informativa assicurata dal Centro.

I Centri Operativi per la Sicurezza Cibernetica della Polizia Postale hanno svolto adeguati servizi di monitoraggio e analisi, condividendo ogni evidenza utile in relazione al quadro internazionale in parola.

L'attività del CNAIPIC del Servizio Polizia Postale e delle Comunicazioni, oltre agli approfondimenti investigativi, si è tradotta nell'analisi tecnica della minaccia, volta all'elaborazione di informazioni di sicurezza preventiva, nonché nel supporto operativo alle infrastrutture attaccate, che hanno contribuito al ritorno alla piena operatività dei sistemi informatici colpiti.

Attacchi infrastrutture critiche ad istituzioni, aziende e privati	**2021**	**2022***	**Variazione percentuale**
Attacchi rilevati	**5.434**	**12.947**	**+138%**
Persone indagate	**187**	**332**	**+78%**
Alert diramati	**110.524**	**113.226**	**+2%**
Richieste di cooperazione HTC	**60**	**77**	**+28%**

* - dati rilevati il 27/12/2022

SEZIONE OPERATIVA

Nell'ambito delle competenze della Polizia Postale si segnala il rafforzamento dell'attività di prevenzione attraverso il monitoraggio attivo della rete e un'articolata attività di contrasto alle **truffe online** con **3541 persone deferite all'Autorità Giudiziaria**, in particolare nel settore dell'e-commerce e *market place.*

Truffe OnLine	**2021**	**2022***	**Variazione percentuale**
Casi trattati	15.083	15.508	**+3%**
Persone indagate	3.403	3.541	**+4%**
Somme sottratte	€ 73.245.740	€ 115.457.921	**+58%**
* - dati rilevati il 27/12/2022			

Nell'ambito delle truffe sul web anche nel corso del 2022, importante l'incremento degli illeciti legati al fenomeno del **trading online** (**3.020** ***i casi trattati, 130 le persone)***, con l'aumento del numero di portali che propongono programmi speculativi, apparentemente redditizi, e l'utilizzo di tecniche molto sofisticate per contattare le vittime. L'attività investigativa, qualora la denuncia sia tempestiva, prevede l'immediata attivazione dei canali di Cooperazione Internazionale di Polizia, con la richiesta del blocco urgente delle somme versate e l'espletamento di accertamenti sui flussi finanziari normalmente destinati all'estero.

Proprio per dare maggior impulso alle indagini che vedono coinvolti cittadini stranieri, la Sezione Operativa della Polizia Postale, nel corso dell'anno 2022, ha attivato **260 richieste di cooperazione internazionale** attraverso il canale Europol che, in più di un'occasione, si sono rivelate determinanti per l'individuazione degli autori dei reati investigati.

Particolare attenzione è rivolta inoltre ai fenomeni del **revenge porn, con *244 casi trattati (di cui 34 in danno di minori) e 71 persone denunciate*** e delle **truffe romantiche,** con ***442 casi trattati (di cui 4 in danno di minori) e 103 persone denunciate***, spesso sommersi in quanto caratterizzati da un forte coinvolgimento emotivo che induce la vittima a non denunciare.

Sono stati **15** i casi di ***Codice Rosso*** che hanno visto la Polizia Postale impegnata attivamente nel contrasto dei reati contro la persona commessi attraverso la rete.

Reati contro la persona perpetrati OnLine[1]	**2021**	**2022***
Casi trattati	10.297	9.278

Persone indagate	1.693	1.167

[1] – *Stalking* / diffamazione online / minacce / *revenge porn* / molestie / sextortion / illecito trattamento dei dati / sostituzione di persona / hate speech / propositi suicidari
* - dati rilevati il 27/12/2022

Specifiche iniziative sono state rivolte all'attività di prevenzione e contrasto al fenomeno degli atti intimidatori nei confronti della categoria dei giornalisti e servizi di monitoraggio dei canali di diffusione, costituiti da siti web, piattaforme di digitali, profili e pagine presenti sui social network più noti (Facebook, Twitter, Instagram, Telegram, Pinterest e Youtube), finalizzati ad arginare la diffusione del linguaggio d'odio (hate speech).

La Sezione Operativa è stata impegnata anche nell'individuazione di proposte di vendita online di prodotti contraffatti o all'utilizzo illecito di segni distintivi dei marchi registrati, per la tutela del c.d. *italian sounding.*

Il monitoraggio di siti e spazi *web* (blog, gruppi social e siti dedicati) dediti a giochi e scommesse clandestine è un'altra attività operativa particolarmente seguita dalla Polizia Postale e delle Comunicazioni, sia per contrastare la diffusione irregolare o illegale, che per tutelare gli interessi dei consumatori, specie se minori d'età: numerosi sono i siti con sedi legali presso paesi esteri, che operano in Italia anche se privi della prevista autorizzazione per poter esercitare legalmente la raccolta di scommesse.

Nel corso del 2022 sono state implementate anche le attività di monitoraggio relative alla vendita online di tabacchi, sigarette elettroniche e liquidi da inalazione in rete, su siti sprovvisti delle relative autorizzazioni da parte dell'Agenzia delle Dogane e Monopoli.

In ultimo, ma comunque di primaria importanza, è stata l'attività rivolta all'individuazione di quelle persone che, sfruttando principalmente la cassa di risonanza che i social media offrono, hanno manifestato intenti suicidari in conseguenza dei quali sono state attivate tutte le procedure necessarie per la salvaguardia delle persone coinvolte con l'ausilio degli uffici di polizia competenti territorialmente (***64 le segnalazioni veicolate attraverso il Commissariato di P.S. OnLine e 51 gli interventi eseguiti sul territorio dalla Polizia Postale e delle Comunicazioni*** *).*

SEZIONE CYBERTERRORISMO

Nel corso degli ultimi anni, il continuo e vertiginoso incremento dell'utilizzo delle piattaforme di comunicazione online, social network e di applicazioni di messaggistica istantanea, ha determinato un'allarmante diffusione di contenuti propagandistici riconducibili al terrorismo, ad una platea pressoché illimitata, sia di matrice islamista (*jihadista, ISIS, Al Qaeda, Al Shabaab* ed altre articolazioni locali), sia di formazioni suprematiste di estrema destra (neonazismo, neofascismo, tifoserie strutturate), nonché di estrema sinistra (movimenti di lotta armata, anarco/insurrezionalisti, antagonisti).

Cyberterrorismo[1]	2021	2022*
Casi trattati	1.321	1.193
Persone indagate	80	66
Spazi virtuali monitorati	126.998	173.306

[1]- Estremismo internazionale religioso / estremismo razziale, antagonista ed anarchico
* - dati rilevati il 27/12/2022

In tale ambito, la Polizia Postale garantisce sia l'esecuzione di una costante attività di monitoraggio investigativo della rete e dei canali di messaggistica istantanea, per l'identificazione e il deferimento all'Autorità Giudiziaria dei responsabili della diffusione dei contenuti illeciti, sia un costante scambio informativo con la Direzione Centrale della Polizia di Prevenzione competente in materia di contrasto al terrorismo.

Trattandosi, in particolare, di un fenomeno di carattere transnazionale, sia per la natura internazionale del fenomeno che per la stessa connaturata struttura della rete, risulta imprescindibile l'attivazione efficiente degli strumenti della cooperazione sovranazionale, soprattutto per la condivisione di informazioni che, collegate a situazioni peculiari interne, riescono ad apportare un indiscusso valore aggiunto alle attività di prevenzione messe in atto dalle diverse forze di polizia nazionali.

In ambito europeo, proprio al fine di garantire la cooperazione internazionale, il Servizio Polizia Postale e delle Comunicazioni rappresenta il punto di contatto nazionale dell'Internet Referral Unit (IRU) di Europol, Unità preposta a ricevere dai Paesi Membri le segnalazioni relative ai contenuti terroristici diffusi in rete e di orientarne l'attività.

In tale ambito, l'attività di monitoraggio del web effettuata dalla Specialità ha permesso di riscontrare, in primis, come la diffusione di contenuti propagandistici jihadisti, nel corso del tempo, abbia subito un sensibile peggioramento "qualitativo", determinato sia dal ridimensionamento del Califfato sul territorio, sia dalle perdite di tecnici e social media manager cui era devoluto l'incarico di gestire la propaganda, nonché per l'utilizzo sempre più frequente dell'Intelligenza Artificiale sulle principali piattaforme web, per la scansione (e rimozione) dei contenuti pubblicati dagli utenti.

In analogia a quanto sin qui evidenziato con riferimento alla propaganda jihadista, anche nell'ambito dei fenomeni di radicalizzazione online legati all'ideologia neofascista e xenofo/razziale, il web si conferma lo strumento strategico per la diffusione della propaganda delle ideologie estremiste e violente, nonché per il reclutamento di nuovi combattenti, il finanziamento, lo scambio di comunicazioni riservate nella pianificazione degli attentati e di rivendicazione degli stessi.

Appare opportuno evidenziare come il movimento "suprematista" si basi su una importante attività di propaganda di dottrine ideologiche come il neonazismo, il razzismo, l'identitarismo e l'etnocentrismo, che avviene soprattutto all'interno di piattaforme di comunicazione online "riservate", diverse dai principali social network.

La costante attività di monitoraggio informativo ed investigativo ha permesso di accertare come nel corso degli ultimi mesi si sia stato registrato un notevole incremento dei trend e delle discussioni all'interno di chat in diverse piattaforme; si passa dai tradizionali gruppi Facebook (molti dei quali risultano essere già stati bloccati) a social meno noti, come Reddit, fino a piattaforme come 8chan, vk.com (Vkontakte), nonché Telegram, privilegiando tutte quelle piattaforme che per la propria policy garantiscono l'anonimato e rendono più complicata l'identificazione degli autori dei messaggi.

Alla luce di quanto premesso, appare opportuno evidenziare come gli operatori della Specialità abbiano intensificato le attività di monitoraggio proprio in tali contesti e, in raccordo con la Direzione Centrale della Polizia di Prevenzione, abbiano avviato numerose attività investigative, con il deferimento alle competenti Autorità Giudiziarie dei soggetti identificati – anche attraverso attività sotto copertura e perquisizioni – quali autori dei messaggi connotati dalla discriminazione razziale, etnica e religiosa.

FINANCIAL CYBERCRIME

L'anno 2022 ha vissuto, subendoli, gli strascichi dell'emergenza sanitaria da Covid19, che ha comportato il cambiamento radicale di alcune abitudini di vita consolidate. La sostituzione della socializzazione diretta con quella telematica e lo svolgimento dell'attività lavorativa non in presenza, imposti dall'avvio della pandemia fin dal 2020, si sono, in parte, stabilizzati, aprendo la strada a nuove consuetudini: molte aziende hanno proseguito con forme di telelavoro e *smartworking*, contribuendo a incrementare la frequenza di navigazione in rete da parte dei soggetti adulti anche attraverso *devices* quali *tablet*, *smartphone*, pc molto spesso utilizzati anche per scopi personali a scapito della sicurezza.

Nel solco di questi cambiamenti si è registrato un aumento dei reati informatici che ha raggiunto livelli altissimi, mettendo in luce come il crimine post pandemia nel nostro Paese stia cambiando radicalmente.

Il settore del *financial cybercrime* rappresenta un bacino molto remunerativo ed appetibile sfruttato da molte organizzazioni criminali, anche estere, come veicolo per finanziare le proprie attività illecite, il più delle volte attraverso l'utilizzo di sofisticate tecniche di *social engineering* per manipolare le vittime e indurle a fornire informazioni riservate.

Le conseguenze di un attacco riuscito possono essere drammatiche e avere effetti devastanti non solo su singoli utenti o investitori, ma anche con riverberi negativi per ciò che concerne piccole e medie imprese, con ingenti perdite economiche e danni d'immagine difficilmente quantificabili.

Nel settore del contrasto al *financial cybercrime*, il fenomeno dei "*money mules*" rappresenta senz'altro una delle modalità più frequenti e consolidate per realizzare frodi online: con la funzione di "teste di legno" cibernetiche, personalità di dubbia moralità si prestano ad essere l'ultimo anello della catena attraverso il quale i criminali monetizzano i proventi del reato. La diffusione di questa modalità e il numero dei soggetti che si prestano a svolgere tale funzione criminale sono in costante crescita e rappresentano ormai una realtà criminale quasi endemica in tutto il mondo.

Anche il 2022, inoltre, è stato caratterizzato dalla crescita dell'interesse per le ***Cryptovalute***: i cittadini italiani, anche con bassa scolarizzazione informatica, sono sempre più frequentemente attratti dagli investimenti in ***Cryptovalute***, con la speranza di realizzare i facili e veloci guadagni pubblicizzati.

Quello delle *Cryptovalute* costituisce un mondo eterogeneo e virtuale, peraltro, non dissimile da quello reale. In tale contesto sono realizzate attività investigative finalizzate a fermare i tentativi di *phishing* verso i ***Wallet*** che le contengono: i truffatori informatici agganciano le vittime attraverso richieste di natura tecnica, su chat ufficiali o semi ufficiali, con la promessa di risolvere i loro problemi gestionali previa cessione delle chiavi private, che permettono la movimentazione delle Crypto (cd. SEED), in realtà queste consentono ai malfattori di prendere il pieno possesso del *Wallet* e di impadronirsi del contenuto.

Forte anche l'impegno per contrastare il fenomeno del riciclaggio perpetrato attraverso la conversione delle somme frodate in *Cryptovalute*, sono state infatti coordinate dal Servizio Polizia Postale diverse attività investigative che hanno visto truffe informatiche ad alto contenuto tecnico conosciute come le BEC, le CEO fraud, *Vishing*, *phishing* tentare di realizzare i proventi criminali inviando le somme sottratte tramite bonifico bancario ad *exchange* di *cryptovalute* non collaborativi con la Polizia, convertendo la valuta ufficiale in *Bitcoin* o *Ethereum*. Tale procedimento consente facilmente lo spostamento e spacchettamento delle somme, in attesa di fare *cashout*.

Per tale ragione è stata intensificata la collaborazione con le grandi società di Exchange di Crypto per i report operativi e per il congelamento delle somme sottratte, così come è stata intensificata anche l'analisi delle transazioni *Crypto* con la collaborazione degli specialisti di Europol.

La mancanza di confini geografici in Internet consente sempre più frequentemente la formazione di gruppi criminali con nazionalità eterogenee ed è questo che caratterizza ormai quasi l'intero panorama dei reati commessi attraverso le nuove tecnologie.

In Italia sono state **frodate 156 grandi, medie e piccole imprese**, per un ammontare complessivo di **oltre 20 milioni di euro** di profitti illeciti, dei quali oltre **4 milioni** sono stati recuperati in seguito all'intervento della Polizia Postale e delle Comunicazioni.

In merito ai fenomeni di *phishing, smishing e vishing,* tecniche utilizzate per carpire illecitamente dati personali e bancari, per operare sui sistemi di *home banking*, sono state **identificate ed indagate 853 persone (+9% rispetto all'anno precedente).**

Frodi Informatiche	**2021**	**2022***	**Variazione percentuale**
Persone indagate	779	853	**+9%**
Somme sottratte	€ 33.258.422	€ 38.678.134	**+16%**
* - dati rilevati il 22/12/2022			

COMMISSARIATO DI P.S. ONLINE

L'uso crescente delle nuove tecnologie ha reso necessario lo sviluppo e il potenziamento di nuovi strumenti di comunicazione che consentissero alla Polizia di Stato di mettersi in contatto diretto con gli utenti del *web*.

In tale ottica, il portale del Commissariato di PS online ha permesso al cittadino, abituato ormai a utilizzare la rete internet per svolgere le principali attività quotidiane, di rivolgersi agli agenti della Polizia Postale in qualsiasi momento e ovunque si trovi. Attraverso il computer, l'utente può segnalare comportamenti che giudica illeciti e chiedere aiuto per superare difficoltà e problematiche, anche nei casi in cui potrebbe essere fonte di disagio rappresentarle di persona.

La facilità con cui il cittadino ha interagito con la piattaforma dedicata, ha reso possibile raccogliere le segnalazioni di quegli utenti che, mossi da spirito altruistico e di collaborazione, si sono rivolti alla Polizia Postale in un'ottica di sicurezza partecipata - nella sua declinazione online - fornendo utili evidenze su fenomeni emergenti potenzialmente lesivi, così contribuendo, in termini di efficace prevenzione, ad evitare che altri internauti potessero cadere nelle trappole della Rete.

L'esigenza di innalzare al massimo i livelli dell'azione preventiva ha imposto di introdurre una nuova sezione, dedicata agli *alert*, dove vengono raccolti e pubblicati gli "avvisi agli utenti" che, proprio perché costantemente aggiornati e facilmente raggiungibili, costituiscono un efficace strumento di autotutela messo a disposizione del cittadino.

Tra i fenomeni riscontrati con maggior frequenza nell'anno 2022 annoveriamo, a titolo esemplificativo, i furti di *account social*, le estorsioni a sfondo sessuale, il *phishing* ai danni di correntisti di istituti bancari, le proposte di falsi investimenti online, nonché falsi siti di vendita di quei prodotti che, in un determinato contesto temporale, risultano essere maggiormente richiesti sul mercato.

Sul sito, inoltre, giungono segnalazioni da parte di utenti che si trovano in situazioni di pericolo o che minacciano gesti estremi; in tali circostanze, ai poliziotti della sala operativa del Commissariato di PS online è richiesto un tempestivo e coordinato intervento che coinvolge gli uffici territoriali delle Questure interessate dall'evento.

Gli interventi finalizzati alla prevenzione di **intenti suicidari** da parte di utenti dei vari social network, segnalati attraverso il Commissariato di P.S. online **sono stati 64.**

L'analisi delle oltre **100.000** segnalazioni ricevute dal sito del Commissariato di PS online nell'anno 2022, ha evidenziato che in molti casi gli internauti sconoscono e/o non adottano quelle piccole e necessarie accortezze di *cyber hygiene* che consentirebbero loro di prevenire e limitare la maggior parte degli attacchi informatici e il perpetrarsi di attività delittuose.

Per questo motivo, è stata introdotta sul sito una specifica sezione con cui vengono veicolate al cittadino pillole di sicurezza informatica, funzionali a ridurre al minimo i rischi legati all'uso di dispositivi informatici.

La popolarità del sito è avvalorata dal numero degli accessi che sono stati, nel periodo di riferimento, oltre **42.200.000**.

Nella costante ricerca di nuove e incisive strategie di comunicazione per fornire ad un'utenza sempre più ampia, si è passati da una comunicazione verso il cittadino a una interazione con il cittadino.

ATTIVITA' DI PREVENZIONE

La Polizia Postale se da un lato svolge un'incisiva attività di repressione dei reati informatici, dall'altro lato svolge un'importante azione preventiva a tutela dei minori, soprattutto per quanto concerne il fenomeno del cyberbullismo e di tutte le forme di prevaricazione online, fenomeni che destano grande allarme sociale.

Tra le iniziative educative si riporta il coinvolgente format teatrale itinerante e in streaming **#cuoriconnessi** che ha coinvolto oltre 270mila studenti sul territorio nazionale.

Di rilievo è anche la campagna educativa itinerante di sensibilizzazione e prevenzione sui rischi e pericoli legati ad un uso non corretto della rete internet da parte dei minori denominata *Una vita da social*.

L'iniziativa, arrivata quest'anno alla sua X edizione, ha coinvolto oltre **2milioni e 8oomila studenti,** attraverso il truck didattico multimediale della Polizia Postale, e ha proseguito la sua attività itinerante in Italia e all'estero.

Il progetto si cala nella filosofia dei giovani interlocutori, interagendo con un linguaggio comunicativo semplice ma esplicito, adatto a tutte le fasce di età, coinvolgendo così dai più piccoli ai docenti ai genitori, con la finalità di combattere la violenza e la prevaricazione dei giovani bulli.

L'impegno profuso dagli specialisti della Polizia Postale nell'azione di sensibilizzazione e informazione ha consentito, nell'anno appena trascorso, di realizzare incontri con docenti e genitori in oltre 2.800 istituti scolastici e di coinvolgere oltre **820mila** studenti.

ATTIVITA' DI FORMAZIONE INNOVAZIONE E RICERCA NEL SETTORE DELLE TECNOLOGIE ICT E DI REALIZZAZIONE DEL CERT MINISTERO DELL'INTERNO

Nel corso dell'anno 2022, la Polizia Postale e delle Comunicazioni ha proseguito nell'attività di collaborazione con diverse Istituzioni Scientifiche ed Enti di Ricerca volta ad individuare e valorizzare nuove tecniche e metodologie di lavoro nel contesto info-investigativo. In tal senso, di significativa rilevanza è la pianificazione di percorsi formativi di settore, con particolare riferimento alle tecnologie emergenti (5G, blockchain, IoT, AI) ed al complesso mondo dei sistemi criptati ed al loro dilagante utilizzo criminale.

Di assoluta importanza è stata l'attività di progettazione ed alta formazione specialistica finalizzata all'avvio del CERT (Computer Emergency Response Team) – Ministero Interno. Tale costituendo organismo, che opererà sotto l'egida della nuova Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica, sarà chiamato a svolgere un'efficace attività di presidio e risposta interdipartimentale contro incidenti informatici, coordinando le attività di contenimento e ripristino, per la prevenzione e la gestione degli attacchi cibernetici, delle reti e dei sistemi informativi del Ministero dell'Interno.

Si è dato avvio ad una formazione specialista di altissimo profilo a beneficio degli operatori già impegnati nello specifico contesto.