Prevenzione e contrasto alla criminalità informatica.

Queste le principali attività della Polizia Postale:

- reati relativi alla **pedopornografia** online e adescamento di minori sul web.
- reati contro la persona commessi sul web, **estorsioni a sfondo sessuale**, stalking, molestie e minacce sui social network.

Un fenomeno insidioso che ha fatto breccia tra i giovani e giovanissimi è rappresentato dagli stickers che consiste nella condivisione, su piattaforme di messaggistica istantanea, di adesivi digitali gratuiti, a contenuto offensivo, violento, discriminatorio, antisemita, nonché pedopornografico.

- contrasto al **revenge porn**, (la diffusione sul web di immagini o video privati a sfondo sessuale a scopi vendicativi e senza il consenso della persona ritratta).
- reati d'**incitamento all'odio**: condotte discriminatorie di genere, antisemite, xenofobe ecc.
- **cyber-crime**; la Postale svolge attività di prevenzione e contrasto degli **attacchi informatici**, nei confronti di infrastrutture critiche informatizzate di interesse nazionale e nei confronti di aziende di servizi pubblici essenziali.
- attività di contrasto dei fenomeni di radicalizzazione e **cyberterrorismo** e monitoraggio di spazi web.
- **financial cybercrime** (attività criminose analoghe a quelle tradizionali ma caratterizzate dall'uso di componenti tecnologiche informatiche, sia hardware che software).
- *Tra queste attività le più numerose sono le **truffe online** (vedasi consigli su come difendersi di seguito riportati).*

L' **attività di prevenzione** si svolge attraverso incontri educativi nelle scuole e attraverso la campagna itinerante "*Una vita da social*".

Segnalazioni

Le fattispecie di reati sopra elencate possono essere segnalate alla Polizia Postale e delle Comunicazioni all'indirizzo: www.commissariatodips.it

Topologia delle principali e più diffuse truffe online e come difendersi

Shopping con false identità

In crescita le **frodi creditizie** realizzate tramite **furto d'identità.** Come funziona? La truffa consiste, inizialmente, nell'ottenere dati personali e finanziari, copie fotografiche di documenti d'identità o bancari dalle potenziali vittime, anche attraverso raggiri come falsi annunci di lavoro o altro genere di inserzioni. Tali dati possono poi essere utilizzati per **richiedere prestiti o acquistare oggetti** on line. Il tutto a danno delle sfortunate vittime che, molto spesso, si rendono conto della truffa solo tempo dopo quando, per esempio, provano a richiedere un finanziamento ma gli viene negato per non aver

pagato le rate di quello attivato dai truffatori. In tal caso è necessario denunciare alle autorità e procedere con la richiesta di **disconoscimento dell'operazione.**

Bec Fraud e Ceo Fraud

Business e-mail compromise o Chief executive officer, sono questi alcuni dei nuovi tipi di **truffa** che vano a colpire in particolar modo le imprese. Infatti, attraverso di esse, i malviventi si inseriscono nelle comunicazioni commerciali tra aziende, o in quelle dei dirigenti di una stessa società e, con messaggi fasulli ma ritenuti credibili dai malcapitati, **dirottano somme ingenti** su conti corrente intestati ai truffatori.

Vishing

Spesso avete sentito parlare di **phishing**, oggi però gli orizzonti di questo genere di illecito si sono allargati arrivando al **vishing**, nato dall'unione tra i concetti di *voice e phishing.* Questa **nuova truffa** punta ad unire la conoscenza dei dati personali degli utenti con l'utilizzo di telefonate volte ad ingannarli. Sul cellulare o sulla casella di posta elettronica delle vittime arriva una notifica, apparentemente dalla propria banca, che segnala operazioni sospette relative al proprio conto. L'utente preoccupato dall'avviso clicca sull'indirizzo internet di un sito clone. Una volta lì riceve una telefonata (apparentemente credibile grazie all'uso di **un finto numero verde** della banca) in cui i truffatori si spacciano per solerti impiegati dell'istituto di credito che vogliono bloccare il furto quando in realtà, una volta ottenuti i codici di accesso, **autorizzano bonifici o pagamenti** alle spalle dell'ignara vittima.

Smishing e (SMS phishing) - Truffe sul bonus mobilità

A differenza delle campagne di spam via e-mail, lo smishing usa i messaggi di testo sui telefonini per attirare le vittime nella trappola ed estorcere informazioni personali, numeri di carte di credito e altri dati riservati. Si chiama infatti smishing (acronimo di SMS phishing) la variante di un attacco phishing che utilizza i messaggi SMS. Così come le campagne di phishing prevedono l'invio massiccio di e-mail esca, con lo smishing vengono inviati messaggi di testo con un tono urgente per richiedere informazioni riservate. Per difendersi da questi attacchi, è opportuno osservare che i messaggi malevoli di solito provengono da numeri di telefono insoliti. Chiaramente bisogna diffidare e non richiamare mai il numero, tantomeno fornire a sistemi vocali automatici i nostri dati personali. Ovviamente, per gli stessi motivi non bisogna mai cliccare sul link indicato nel messaggio, così come non bisogna aprire allegati provenienti da mittenti sospetti o sconosciuti.

Come difendersi

I consigli, oltre a prestare particolare attenzione, sono:

- quando si inseriscono i dati della propria **carta di credito su internet**, verificare prima la sicurezza del sito;
- non inviare a nessuno i propri codici di accesso al conto corrente. Gli istituti di credito ad esempio non richiedono mai via e-mail o per telefono le credenziali di accesso all'home-banking;
- prudenza e giudizio sono necessari nel momento in cui viene richiesto l'invio di copie di documenti;
- e infine, non scaricare mai allegati che arrivano tramite mail o sms se non si è sicuri circa l'identità del mittente;

- utilizzare password, specie nelle caselle e-mail, di almeno 12 caratteri alfanumerici, con lettere maiuscole e minuscole e con caratteri speciali (+ * $! & £).

Ultima modifica

Gio, 22/01/2026 - 18:10