RELAZIONE DEL VICE COMANDANTE DELLA POLIZIA LOCALE DI PONTE S. NICOLO'

Nella relazione presentata dalla Vicecomandante Giulia Lunardi, ha spiegato i pericoli che si incorrono in auto, con altri mezzi di circolazione e a piedi da parte di alcuni giovani con la loro imprudenza, le persone che sono sottoposte all'assunzione di medicinali che possono rallentare le reazioni attive in un traffico congestionato oppure con un'età avanzata in cui i riflessi per un naturale percorso della vita rallentano.
Ha poi ricordato la documentazione che bisogna sempre avere a seguito (carta di circolazione dell'auto, patente, assicurazione) per essere in regola e non incorrere in multe in caso di un controllo da parte delle forze dell'ordine (Vigili, Carabinieri, Polizia, ecc.)
Ha poi accennato alle truffe che soprattutto gli anziani possono incorrere essendo loro più fragili e circuibili da chi mette in atto quanto scritto sopra.

TRUFFE ONLINE (VIA SMARTPHONE O COMPUTER): LE PIÙ DIFFUSE,
COME DIFENDERSI

Come avvengono le truffe online e quali sono gli strumenti che possiamo adottare per difenderci?
Internet, email, sms, app e social network, WhatsApp: oggi più che mai disponiamo di strumenti e canali che offrono molteplici opportunità, ma che possono esporci anche a qualche rischio.
TRUFFE ONLINE: il **phishing** (furto dati sensibili) che mira al furto dei dati personali.
E' una particolare tipologia di truffa realizzata sulla rete Internet attraverso l'inganno degli utenti. Si concretizza principalmente attraverso messaggi di posta elettronica ingannevoli:
Attraverso una e-mail, solo apparentemente proveniente da istituti finanziari (banche o società emittenti di carte di credito) o da siti web che richiedono l'accesso previa registrazione (web-mail, ecc.). Il messaggio invita, riferendo problemi di registrazione o di altra natura, a fornire i propri riservati dati di accesso al servizio. Solitamente nel messaggio, per rassicurare falsamente l'utente, è indicato un **(link) collegamento (esempio: www.nonfarlomai.it, www.nonfarlomai.com)** che rimanda solo apparentemente al sito web dell'istituto di credito o del servizio a cui si è registrati. In realtà il sito a cui ci si collega è stato allestito "**con l'inganno**" identico a quello originale. Qualora l'utente inserisca i propri dati riservati, **questi saranno nella disponibilità dei criminali.**
Diversi utenti hanno segnalato di aver ricevuto comunicazioni, da parte di un sedicenti servizi istituzionali, relative a problemi nell'esecuzione di bonifici. "Non siamo in grado di effettuare il bonifico perché ci risulta che i dati registrati nel sistema non sono stati aggiornati": questo l'avviso contenuto nella email, seguito dall'invito ad aggiornare i propri dati personali, tramite un **link (collegamento)**, per poter ricevere il fantomatico bonifico da parte dell'Istituto. Evitte di cliccare (aprire) questi **link (collegamento).**
Sono stati segnalati, inoltre, tentativi di truffa tramite email che invitano a scaricare bollettini di versamento precompilati o **link (collegamenti)** cliccabili per ricevere il rimborso di contributi versati in eccesso. Bisogna sempre diffidare di queste comunicazioni in quanto gli Istituti, per motivi di sicurezza, non inviano mai messaggi di posta elettronica contenenti allegati da **scaricare** o **link cliccabili**.
Non solo email. È necessario fare attenzione anche agli SMS che inducono ad aprire un **link (collegamento)** per aggiornare la propria posizione nei servizi istituzionali.

TRUFFE TELEFONICHE

Gli utenti possono anche ricevere una telefonata nel corso della quale un **finto operatore** telefonico chiede di conoscere i dati relativi alla propria posizione nell'ambito di soggetti di diritto privato, come società o associazioni.

Falsi funzionari
I tentativi di raggiro avvengono, inoltre, da parte di **falsi funzionari** che possono presentarsi anche presso la propria abitazione. Tutte le **istituzioni pubbliche** non inviano incaricati presso il domicilio degli utenti e assistiti.

PRESTITI E PUBBLICITÀ INGANNEVOLE
Esistono società, non correlate e non riconducibili alle **istituzioni pubbliche**, Si tratta di società d'intermediazione finanziaria che pubblicizzano, tramite SMS, prestiti sponsorizzati come "convenzionati" con l'Istituto, i cui siti non rimandano affatto ai benefici erogati istituzionalmente ai propri iscritti o pensionati.

Consigli utili

È importante ricordare che nessun ente acquisisce in alcun caso, telefonicamente o via email ordinaria, le coordinate bancarie o altri dati che permettano di risalire a informazioni finanziarie. Inoltre, tutte le informazioni sulle prestazioni sono consultabili esclusivamente accedendo al sito istituzionale.
È, quindi, necessario:

- non dare seguito a richieste che arrivino per email non certificata, telefono o tramite il porta a porta;
- diffidare di qualsiasi persona dichiari di essere un incaricato o funzionario di **istituzioni pubbliche** e sostenga di dover effettuare accertamenti di varia natura;
- prestare la massima attenzione alle comunicazioni che si ricevono, non cliccare sui **link (collegamento)**di email di origine dubbia e verificare sempre l'indirizzo di provenienza.

Come difendersi dalle truffe online

- Il principale, se non l'unico, scudo contro le truffe online è sicuramente il buon senso, unito al giusto grado di dubbio. Quando riceviamo una richiesta di amicizia sospetta, che non ha amicizie in comune con noi, che condivide pochissimi contenuti e mostra poche immagini è bene dubitare.
- Lo stesso vale per le altre tipologie di truffa telematica. Nessuno, infatti, offre facili guadagni a fronte di piccoli corrispettivi. Se qualcuno ci propone un sistema per fare facili guadagni e migliorare in poco tempo la nostra condizione economica ci troviamo certamente di fronte a una truffa online o nella migliore delle ipotesi di fronte a qualcuno che vuole solo venderci un prodotto di dubbia validità.
- Nel caso dell'acquisto di prodotti online è invece bene diffidare di piattaforme sconosciute e affidarsi invece a quelle più conosciute che offrono diversi livelli di protezione dell'acquisto. Anche su tali piattaforme è bene però valutare l'affidabilità del venditore attraverso le recensioni degli altri utenti e la reputazione che ne emerge. Per quanto riguarda l'acquisto di prodotti firmati la scelta migliore rimane sempre quella di recarsi in negozio o di acquistare sugli **store (magazzini)** ufficiali.

IL NUOVO TIPO DI TRUFFA CREATO CON L'INTELLIGINZA ARTIFICIALE (RIPRODUZIONE DELLA VOCE DI UN VOSTRO PARENTE O AMICO)

Rispondete a una chiamata di un vostro parente, che vi spiega affannosamente di essere rimasto coinvolto in un terribile incidente stradale. Per non finire in carcere, ha bisogno che gli inviate immediatamente dei soldi. Riuscite a percepire la sua disperazione mentre vi implora la sua richiesta. **Anche se la voce e il numero di telefono sembrano proprio quelli del vostro familiare**, avete la sensazione che ci sia qualcosa di strano. Decidete di riagganciare e di richiamarlo subito. Ma a questo punto, la persona all'altro capo del telefono vi dice di non sapere di cosa stiate parlando. Congratulazioni: siete appena scampati a una **chiamata truffa realizzata da un'intelligenza artificiale**.

Grazie al miglioramento delle capacità degli strumenti di AI generativa, **creare audio falsi ma convincenti** in grado di replicare la voce delle persone è **sempre più facile ed economico**. Questi cloni vocali AI sono addestrati su clip audio reali e possono essere regolati in modo da imitare la voce di quasi chiunque. I modelli più recenti sono addirittura in grado di parlare numerose lingue.

Chiudete la chiamata e richiamate

ESEMPI da cancellare immediatamente senza nemmeno aprirli per curiosità

Come noterete dall'esempio accanto questo **sms** richiede di chiamare un numero di uno smartphone, causa rottura del proprio, bene il numero non è altro che un link (collegamento) che attiverà una app utile a perpetuare la frode rubandovi i dati sensibili inseriti nel vostro smartphone (rubrica telefonica, foto, messaggi, e quello più importante abbiate salvato nell'app NOTE i dati della vostra banca)

Come noterete dall'esempio accanto questo messaggio spedito o via sms o via WhatsApp chiedi di bloccare un **link (collegamento)** per togliere l'associazione ad un nuovo dispositivo (smartphone) rilevato a Lugano

Come noterete dall'esempio accanto questo messaggio spedito o via sms o via WhatsApp chiedi premere su un **link (collegamento)** sottoforma di numero **telefonico** per salvare il figlio da un arresto

Come noterete dall'esempio accanto questo messaggio spedito o via sms o via WhatsApp chiedi di verificare attraverso un **link (collegamento)** l'anomalia sul **conto corrente postale**

Anche siti sicuri come quello sotto rappresentato della Polizia di Stato, o altre forze dell'Ordine, se non siete proprio interessati, è meglio cancellarli o telefonare alla Polizia di Stato se hanno veramente emesso una allerta di truffe.