COMUNICATO STAMPA

La Polizia di Stato scende in campo per la protezione dello shopping natalizio online. Dall'esperienza acquisita nella tutela dai rischi di truffe dalla Polizia Postale e delle Comunicazioni nasce una guida con consigli pratici e suggerimenti per acquistare in Rete con maggiore tranquillità

Roma, 17 dicembre 2019 – E' ormai iniziata la corsa agli ultimi acquisti dei regali di Natale!

Quale migliore occasione per fornire consigli utili ed evitare che lo shopping intenso finalizzato all'acquisto di doni per le persone a noi care, ci faccia incorrere in potenziali truffe, complice anche la ricerca di offerte a bassissimo costo ed i ristrettissimi tempi per gli acquisti.

Dall'esperienza acquisita nella tutela dai rischi di truffe on line, la Polizia Postale e delle Comunicazioni mette a disposizione una serie di informazioni per garantire la sicurezza in rete, la tutela dei dati personali, la protezione da frodi e rischi negli acquisti: temi caldi e particolarmente sentiti da chi utilizza Internet.

Il numero delle segnalazioni e denunce ricevute, sommate a quelle delle persone arrestate e denunciate ha richiamato l'attenzione della Polizia Postale e delle Comunicazioni che ha potenziato ogni utile strumento per indirizzare l'utenza ad un uso appropriato della Rete e dei pagamenti online e contrastare nel contempo le truffe messe in atto su Internet, anche attraverso la chiusura degli spazi virtuali.

Si tratta di consigli particolarmente utili all'avvicinarsi del **Natale e del Capodanno** quando il fenomeno delle truffe sembra acutizzarsi, complice anche la ricerca di offerte a bassissimo costo sia per la corsa ai regali sia per le case vacanza.

"Del resto, che la scelta di acquistare in rete sia legata anche alla possibilità di ottenere risparmi, oltre che alla comodità, non è una sorpresa: alcune ricerche confermano che il modello **dell'acquisto di impulso** legato a offerte speciali, ad esempio stock limitati o con prezzi scontati, si è talmente diffuso che anche i truffatori seriali riescono ad inserirsi con false vendite.

Nonostante ciò la stragrande maggioranza degli acquirenti online si affida alla Rete per gli acquisti, anche chi non è esperto a comprare in totale tranquillità.

Per questo motivo la Polizia Postale e delle Comunicazioni è scesa in campo con un opuscolo che offre alcuni utili consigli e pratici suggerimenti per muoversi tra i negozi online. Il vademecum sarà disponibile sul sito della Polizia di Stato, sul portale del Commissariato di P.S. on line e sulle relative pagine facebook e twitter.

L'ultima operazione effettuata dalla Polizia Postale ha messo in luce un complesso modus operandi che vedeva i criminali effettuare i furti della corrispondenza all'interno dei centri di smistamento di Poste Italiane, una volta impossessatisi delle lettere contenenti le carte di credito la banda metteva in atto la tecnica del Vishing (Neologismo anglosassone ottenuto dalla crasi tra le parole *voice* + *phishing*). Il gruppo dei "telefonisti" chiamava i vari Istituti emittenti delle carte e, presentandosi come Maresciallo o Ispettore delle Forze dell'ordine, affermava di aver appena sequestrato un consistente numero di carte di credito rinvenute in possesso a malviventi. Con fare perentorio e con la scusa di riconsegnare i titoli in sequestro, si faceva indicare il numero di telefono dei clienti.

"buon giorno carte di identità elettroniche… sono l'ispettore Maglione della Questura avrei bisogno di un accertamento anagrafico mi può aiutare??"

A questa seguiva una complessa attività di Social Engineering compiuta da esperti tecnici che provvedevano a reperire tutte le informazioni e gli ulteriori dati necessari. Una volta ottenuti i dati, l'organizzazione rivolgeva la sua abilità criminale proprio verso i clienti ai quali, spacciandosi per dipendenti della banca, paventava problemi connessi nell'attivazione del titolo riuscendo infine, con abilità persuasive, a farsi indicare il PIN dei titoli.

….la chiamo a riguardo la sua carta di credito, la chiamo dalla sede centrale amministrativa…….. in una settimana lavorativa gli arriverà la nuova carta dopodichè……sempre per raccomandata il nuovo codice PIN…….allora volevo solo alcune conferme perché abbiamo variato ….l'indirizzo……mi può confermare un recapito fisso???

Questi gli stralci di alcune intercettazioni telefoniche, da cui è emersa una capacità attoriale e di convincimento non comuni.

Tant'è che durante alcune conversazioni tra sodali questi si vantavano l'un l'altro delle eccellenti capacità di imitazione facendo a gara a chi era più bravo. La stessa persona era in grado di cambiare la propria voce anche passando dal femminile al maschile e con diversi accenti dal partenopeo al milanese.

Guida sicura per gli acquisti on line

1. Utilizzare software e browser completi ed aggiornati

Potrà sembrare banale, ma il primo passo per acquistare in sicurezza è avere sempre un buon antivirus aggiornato all'ultima versione sul proprio dispositivo informatico. Gli ultimi sistemi antivirus (gratuiti o a pagamento) danno protezione anche nella scelta degli acquisti su Internet. Per una maggiore sicurezza online, inoltre, è necessario aggiornare all'ultima versione disponibile il browser utilizzato per navigare perché ogni giorno nuove minacce possono renderlo vulnerabile.

2. Dare la preferenza a siti certificati o ufficiali

In rete è possibile trovare ottime occasioni ma quando un'offerta si presenta troppo conveniente rispetto all'effettivo prezzo di mercato del prodotto che si intende acquistare, allora è meglio verificare su altri siti. Potrebbe essere un falso o rivelarsi una truffa.

E' consigliabile dare la preferenza a negozi online di grandi catene già note perché oltre ad offrire sicurezza in termini di pagamento sono affidabili anche per quanto riguarda l'assistenza e la garanzia sul prodotto acquistato e sulla spedizione dello stesso.

In caso di siti poco conosciuti si può controllare la presenza di certificati di sicurezza quali TRUST e VERIFIED / VeriSign Trusted che permettono di validare l'affidabilità del sito web.

3. Un sito deve avere gli stessi riferimenti di un vero negozio!

Prima di completare l'acquisto verificare che il sito sia fornito di riferimenti quali un numero di Partiva IVA, un numero di telefono fisso, un indirizzo fisico e ulteriori dati per contattare l'azienda. Un sito privo di tali dati probabilmente non vuole essere rintracciabile e potrebbe avere qualcosa da nascondere. I dati fiscali sono facilmente verificabili sul sito istituzionale dell'Agenzia delle Entrate.

4. Leggere sempre i commenti e i feedback di altri acquirenti

Prima di passare all'acquisto del prodotto scelto è buona norma leggere i "feedback" pubblicati dagli altri utenti sul sito che lo mette in vendita. Anche le informazioni sull'attendibilità del sito attraverso i motori di ricerca, sui forum o sui social sono utilissime…

Le "voci" su un sito truffaldino circolano velocemente online!

5. Su smartphone o tablet utilizzare le app ufficiali dei negozi online

Se si sceglie di acquistare da grandi negozi online, il consiglio è quello di utilizzare le App ufficiali dei relativi negozi per completare l'acquisto. Questo semplice accorgimento permette di evitare i rischi di "passare" o "essere indirizzati" su siti truffaldini o siti clone che potrebbero catturare i dati finanziari e personali inseriti per completare l'acquisto.

6. Utilizzare soprattutto carte di credito ricaricabili

Per completare una transazione d'acquisto sono indispensabili pochi dati come numero di carta, data di scadenza della carta ed indirizzo per la spedizione della merce.
Se un venditore chiede ulteriori dati probabilmente vuole assumere informazioni personali (numero del conto, PIN o password) che, in quanto tali, dovete custodire gelosamente e non divulgare.
Al momento di concludere l'acquisto, la presenza del lucchetto chiuso in fondo alla pagina o di "https" nella barra degli indirizzi sono ulteriori conferme sulla riservatezza dei dati inseriti nel sito e della presenza di un protocollo di tutela dell'utente, ovvero i dati sono criptati e non condivisi.

7. Non cadere nella rete del phishing e/o dello smishing

…ovvero nella rete di quei truffatori che attraverso mail o sms contraffatti, richiedono di cliccare su un link al fine di raggiungere una pagina web trappola e sfruttando meccanismi psicologici come l'urgenza o l'ottenimento di un vantaggio personale, riusciranno a rubare informazioni personali quali password e numeri di carte di credito per scopi illegali.
L'indirizzo Internet a cui tali link rimandano differisce sempre, anche se di poco, da quello originale.

8. Un annuncio ben strutturato è più affidabile!

Leggi attentamente l'annuncio prima di rispondere: se ti sembra troppo breve o fornisce poche informazioni, non esitare a chiederne altre al venditore. Chiedi più informazioni al venditore sull'oggetto che vuoi acquistare e se le foto pubblicate sembrano troppo belle per essere vere, cerca in rete e scopri se sono state copiate da altri siti!

9. Non sempre…. è sempre un buon affare.

Diffida di un oggetto messo in vendita a un prezzo irrisorio, non sempre è un affare: accertati che non ci sia troppa differenza tra i prezzi proposti e quelli di mercato!

10. Non fidarsi….

Dubita di chi chiede di esser contattato al di fuori della piattaforma di annunci con e-mail ambigue ma anche di chi ha troppa fretta di concludere l'affare.