

Sempre in Alert

Aumentano sempre più le persone che comodamente da casa utilizzano la Rete per comprare o vendere oggetti, cercare una casa in affitto per le vacanze, una polizza assicurativa per la propria automobile e persino per trovare lavoro. Esigenze a cui il Web risponde con offerte commerciali sempre più diversificate, ma che vanno valutate con accortezza poiché potrebbero nascondere inganni o imbrogli. Ci riferiamo alle frodi informatiche messe in atto da criminali che utilizzano Internet come ambiente per cercare le proprie vittime. Un reato che rientra nella categoria più grande delle truffe informatiche (che è possibile denunciare presso tutte le forze di polizia del nostro Paese) sotto l'attenzione della Polizia Postale e delle Comunicazioni da molti anni. L'esperienza operativa di 20 Compartimenti e di 80 Sezioni, oltre al Portale del Commissariato on line, a cui giungono le segnalazioni degli utenti di tutta Italia, hanno permesso negli anni di maturare in questo settore una competenza professionale e una qualità di ascolto del cittadino in grado di creare una informazione efficace. «Il raggio è un reato oggi molto diffuso in Internet – spiega il primo dirigente Alessandra Belardini, direttore della seconda divisione del Servizio della polizia postale – ma attenzione a non demonizzare la Rete che amplifica quello che già esiste nella realtà e può presentare aspetti negativi, ma anche forme di sicurezza e garanzia. Se il truffatore seriale sceglie di muoversi nella dimensione del Web – prosegue – è perché quest'ultima gli consente più facilmente di crearsi un profilo falso, di poter offrire un prodotto ad un prezzo molto vantaggioso, di poter ottenere dati sensibili o documenti di identificazione da parte degli acquirenti che comunque avranno una percezione del danno economico solo molto tempo dopo». Per quanto riguarda l'e-commerce le situazioni a rischio possono essere: trovarsi di fronte a un «sito civetta» dove prodotti tecnologici o alla moda sono proposti a prezzi scontatissimi rispetto a quelli di mercato; che questi prodotti una volta comprati non arrivino mai, oppure non corrispondano a quelli scelti, e comunque sempre con il danno di vedersi prelevare quantità di denaro maggiori di quelle che pensavamo di risparmiare. «Sono imbrogli in cui possono cadere le persone sprovviste, ma anche i giovani che sono i principali acquirenti di prodotti tecnologici, abbigliamento, biglietti per concerti. Senza contare – prosegue la dirigente della Postale – che si sta ulteriormente abbassando l'età di chi acquista in Rete poiché oggi giorno anche un ragazzino di 9 anni può comprare in Internet il proprio gioco preferito, se utilizza le credenziali della carta di credito dei genitori già memorizzate nel sito». Sono i periodi a ridosso delle festività come Natale, Pasqua, quello dei saldi e delle vacanze estive ad essere «scelti» dai criminali per organizzare raggiri nel Web a danno dei consumatori più propensi all'acquisto e quindi anche all'affare. Mentre sono i prodotti tecnologici quelli sui quali più frequentemente si può essere ingannati (Iphone, gli Apple watch) eccetera) ma sono frequenti anche le truffe per chi cerca appartamenti in affitto a prezzi contenuti: «Questo tipo di raggio può riguardare case o ville non affittabili – prosegue il direttore della Seconda divisione – perché il proprietario ignora che la sua casa sia stata messa in un sito di annunci on line oppure perché non esiste. In questo caso in consiglio è di inserire l'immagine della casa a cui si è interessati su Google Maps, che tramite il servizio Street View consente di fare una verifica. È comunque raccomandabile, prima di versare una caparra, chiedere sempre il contatto telefonico che permetta di verificare le notizie del sito o di una agenzia pro loco in grado di fornire informazioni attendibili sulla richiesta di affitto». Altri suggerimenti degli esperti della Postale per acquistare in sicurezza in Internet riguardano la scelta di un motore di ricerca affidabile in cui esista la possibilità di verificare i feedback su un venditore; la valutazione del prezzo del prodotto che ci interessa che, se eccessivamente basso rispetto a quello proposto dal mercato è già un campanello di allarme di una possibile frode; l'utilizzo di una carta prepagata per limitare il danno economico oppure scegliere il pagamento in contrassegno. Inoltre, è bene fare attenzione, prima di fare qualsiasi acquisto, alle regole di vendita e recesso, poiché un sito con un sede legale fuori dal nostro Paese potrebbe seguire norme diverse. Tra le cautele tecnologiche da osservare, invece, l'utilizzo di un antivirus aggiornato nel proprio pc o smartphone, e accertarsi che i siti dove vogliamo comprare abbiano il lucchetto di sicurezza in alto a sinistra nella barra in alto degli indirizzi, a garanzia che le informazioni non possono essere condivise da nessuno, e naturalmente la raccomandazione di non inviare i propri documenti o dati bancari via e-mail se non si conosce l'identità del destinatario. Tra le recenti truffe on line, quella delle false offerte del lavoro. Ad architettarle criminali senza scrupoli che sfruttano la vulnerabilità di chi è in cerca di occupazione: si tratta di annunci di richiesta di corrieri o magazzinieri che prevedono, per i malcapitati che ci cadono, l'invio tramite e-mail dei documenti di identificazione e delle coordinate bancarie con il concreto rischio di ritrovarsi coinvolti, a propria insaputa, in acquisti di beni o in truffe e-commerce o in riciclaggio di denaro di provenienza illecita. «È un fenomeno ultimamente sotto la nostra attenzione grazie anche alla attività di scambio di informazioni sul territorio – racconta il vice questore Laura Patrizi, funzionario della seconda divisione della Postale – Può trattarsi di un annuncio di ricerca di personale in cui vengono fornite notizie verosimili, magari utilizzando nomi di aziende straniere e affermando di voler aprire una sede in Italia. La persona in cerca di occupazione viene indotta a inviare i propri documenti a questa fantomatica azienda, mettendo a rischio la riservatezza dei propri dati per poi essere impiegata nello svolgimento di una attività nel frattempo cambiata rispetto alla proposta iniziale. In un caso che abbiamo trattato – spiega la funzionaria – alcune persone contattate per fare i magazzinieri alla fine servivano per far transitare sui loro conti somme di denaro in parte destinate al loro compenso e in parte inviate su banche all'estero. È un settore che noi monitoriamo sempre con molta attenzione e nel quale le segnalazioni delle persone sono molto preziose, anche perché la tecnica di indagine è diversa rispetto alla tipologia di reato poiché può implicare la richiesta di collaborazione con le polizie di altri Paesi». Anche in questo caso il consiglio degli esperti della Postale è di inserire nel Web il telefono dell'azienda e l'annuncio di lavoro per verificare se, attraverso altre testimonianze, siamo caduti o rischiamo di cadere in una truffa. Altra frode che sta diffondendosi in Internet e a cui prestare attenzione, è quella delle polizze assicurative inesistenti: «In questo caso contrarre una falsa polizza causa un doppio danno – spiega Laura Patrizi – poiché, nel caso di un sinistro, entrambe le parti si ritrovano ad essere scoperte dal punto di vista della tutela assicurativa e quindi ci si trova ad essere truffati in due».

Commissariato di ps online A raccogliere le segnalazioni di cittadini che hanno subito frodi o sono stati vittime di raggiri, ma anche informare i cittadini con Alert sugli ultimi fenomeni pericolosi che girano nel Web il Portale del Commissariato on line. Creato nel 2013, ad oggi conta quasi 4 milioni di accessi mensili da parte dei cittadini che in esso possono trovare consigli per navigare in sicurezza nel Web. Negli anni si è sempre più perfezionato e arricchito di contenuti, come approfondimenti sugli argomenti di maggiore interesse.

quali l'antiterrorismo on line, il cyberbullismo, il diritto d'autore, il phishing, lo spamming, tanto per citarne alcuni ma anche campagne di informazione e utili vademecum. «Il Portale è nato per essere di aiuto agli utenti della Rete e spiega il vice commissario Roberto Giuli, responsabile del gruppo di lavoro del Commissariato on line e con il tempo siamo diventati un punto di riferimento per tanta gente che ci scrive per chiederci consigli e pareri; noi rispondiamo a tutti per e-mail mentre per i casi più critici contattiamo al telefono la persona. La maggior parte delle segnalazioni riguardano frodi informatiche e noi da parte nostra cerchiamo di dare indicazioni per un corretto utilizzo della Rete perché la formazione di una cultura della prevenzione in questo campo credo che sia fondamentale. È importante sapere e conclude Giuli che è bene denunciare appena ci si accorge di essere rimasti vittima di una truffa e che è possibile farlo anche dal proprio pc di casa sul sito del Commissariato on line. La denuncia però andrà ratificata entro entro 48 ore nell'ufficio di polizia più vicino»

I Consigli e-commerce del commissariato on line Porre attenzione al "feedback" assegnato al venditore. È preferibile che sia alto. In caso di primo acquisto, soprattutto su siti non conosciuti o su negozi on-line di recente costituzione valutare la possibilità di pagamento con modalità di contrassegno. Utilizzare il servizio di deposito a garanzia che permette all'acquirente di pagare una società che svolge il trasporto e, solo dopo l'avvenuta ricezione dell'oggetto, di autorizzare il pagamento al mittente. Il bonifico bancario è molto sicuro poiché si ha traccia di tutta la transazione. È necessario però recarsi presso la propria banca o ottenere un conto corrente on-line ed effettuare lo stesso tramite Internet. Chiedere al venditore più dati possibili così da avere una ragionevole certezza della identità della persona. Verificare tramite motore di ricerca, l'esistenza di segnalazioni da parte di altri utenti riguardanti il venditore/acquirente. Diffidare di prodotti venduti a prezzi estremamente vantaggiosi. È sempre consigliato acquistare e vendere nel territorio italiano in quanto la tutela legale è completa. Preferire l'utilizzo di carte prepagate che possono essere ricaricate in anticipo con la quantità di denaro da utilizzare. Dubitare di venditori che non forniscono utenze di telefoni fissi. Dubitare di chi fornisce indirizzi ubicati presso caselle postali. Evitare di fornire ove possibile dati personali e diffidare da richieste di ulteriori dati oltre quelli già forniti.

10/03/2020