

IVG

Il crimine “trasloca” sul web, allarme della Postale: 1 reato su 5 è in rete

di **Redazione**

29 Dicembre 2009 - 10:51



[thumb:1175:1]Fino a qualche anno fa i furti, la violenza e le truffe erano considerati reati da “strada”, ma adesso, nell’era di internet, la rotta sembra decisamente essere cambiata. E’ sempre più preoccupante infatti il fenomeno dei reati perpetrati usando il web. Furti d’identità, scippi virtuali, phishing, Facebook e altri social network utilizzati per danneggiare una persona o per inneggiare alla violenza, e ancora, notizia recente, per fare apologia della camorra.

A lanciare l’allarme è la Polizia Postale che ha perfino pubblicato sul sito della Polizia di Stato (www.poliziadistato.it) una serie di consigli e suggerimenti per non cadere vittime del “lato oscuro di internet” e per proteggersi dalle insidie che si nascondono nel mondo “parallelo” della rete. Pare infatti che ormai un crimine su cinque venga commesso in Rete e gli agenti della Postale, oltre duemila quelli impegnati su questo fronte, in molti casi lavorano da infiltrati, soprattutto per scoprire e arrestare gli autori di traffici turpi e pericolosi come quello di materiale pedopornografico, di terrorismo o di droga.

Ma accanto ai reati più gravi, ci sono molti altri tipi di truffe che ogni giorno possono ingannare gli utenti. Per non abboccare al phishing, ad esempio, fenomeno con il quale si sfruttano le vulnerabilità dei sistemi per installare virus che rubano codici segreti (il più recente si chiama “Zeus bot” che carpisce i dati sensibili) la cosa più importante, dice il vice questore aggiunto Stefano Zireddu, “è avere sempre sul computer antivirus aggiornati e utilizzare una navigazione protetta”.

“Bisogna per esempio disabilitare, quando è possibile, quegli accessori del browser, come ad esempio i java script, che spesso vengono sfruttati per rubare le informazioni”. Altra cosa fondamentale è non cliccare mai su un link che arriva per email invitandovi a cambiare la vostra password, a entrare nella vostra banca o sul conto alla posta. Nessuna banca o ufficio postale invia mail per verificare dati o comunicare con i clienti” ribadisce Zireddu.

C'è poi il fronte dei cosiddetti "viaggi fantasma". Nei periodi di vacanza, estate, Natale, Capodanno, numerose sono anche le finte offerte di viaggi che offrono pacchetti last minute di villaggi inesistenti o fatiscenti. E' successo proprio pochi giorni fa, ad esempio, che un truffatore aveva affittato via web, contemporaneamente a più locatari, una baita a Cortina d'Ampezzo per le vacanze di Natale.

Ma l'inganno è stato scoperto in tempo dai poliziotti. "Questo può succedere anche se si affitta una casa vacanza da un giornale di annunci di privati", sostengono gli uomini della polizia postale. Non è tanto un problema di Internet quanto di incauto acquisto. In questi casi, così come per qualsiasi acquisto in Rete, è importante avere alcune cautele basilari: verificare il contesto in cui avviene l'inserzione, vedere cioè se il sito o la società che gestisce la vendita è affidabile o meno.

Se si tratta di privati che inseriscono annunci su siti di compravendita verificare le credenziali del venditore. In genere chi commercia abitualmente in modo corretto ha dei giudizi di valore che attestano la sua serietà. Sarebbe comunque sempre meglio, come cautela di buon senso, non inviare tutti i soldi subito: magari inviare solo una caparra e poi pagare il resto del soggiorno quando si arriva sul posto e dopo aver verificato che è tutto a posto.

Un'attenzione particolare è poi dedicata ai social network e ai furti d'identità. Molti giovani oggi, spiega la Polizia Postale, si impossessano dell'identità di una persona per diffamarla, denigrarla o peggio ancora distribuire password e numeri di telefono. Succede quando ci si vuole vendicare di un fidanzato o di una fidanzata che ci ha lasciato, ma anche per un semplice scherzo. E' possibile però anche che qualcuno si impossessi dell'identità di persone più o meno note per creare profili che li mettono in cattiva luce o per utilizzare il nome della personalità in questione per ricevere benefici o compiere atti illeciti screditando il suo nome.

"E' molto facile su Internet sostituirsi a una persona e creare un profilo a suo nome sui social network -spiega Zireddu -. Per cautelarsi la prima regola, anche se sembra contraddittoria per chi usa i social network, è quella di non fornire dati personali sensibili: indirizzo, data di nascita, luogo di lavoro o scuola frequentata e così via. Più informazioni si danno più è facile per un altro spacciarsi per noi". I ragazzini, consiglia ancora la Polizia Postale, non dovrebbero poi mettere fotografie che, una volta pubblicate, possono tranquillamente andare in giro sul web.

Gli esperti del Servizio Polizia Postale, inoltre, ricordano che la sostituzione di persona, così come l'accesso abusivo ai sistemi informatici, o l'utilizzo non autorizzato del sistema e ancora la detenzione di codici e password sono tutti reati previsti del codice penale e punibili con la reclusione.