

Un crimine su 5 è commesso on line

2010-01-28 23:34:48



Secondo un interessante reportage redatto recentemente dagli esperti della Polizia di Stato, quasi un crimine su 5 non viene commesso nel mondo reale, ma si consuma fra i bit della rete telematica. Viaggi Fantasma, furto di identità digitale, estorsioni, riciclaggio, furti, rapine e quant'altro occorra, sono illeciti che hanno trovato su internet un loro fertile brodo di coltura.

Per questa ragione, molti agenti della PolPost lavorano da infiltrati per scoprire e arrestare gli autori di traffici turpi e pericolosi come quello di materiale pedopornografico, di terrorismo o di droga.

Questo il testo dell'utile report realizzato dagli esperti della Polizia Postale.

(per visualizzare l'articolo integrale recarsi su

http://poliziadistato.it/articolo/17734-Rischi_e_pericoli_del_web_come_difendersi) Nel sito della polizia sono presenti, inoltre, utili consigli ed approfondimenti in tema di carte di credito, phishing e strumenti di tutela contro le frodi on line.

Cosa consigliano gli esperti

Ma oltre questi casi più gravi e importanti ci sono molti altri tipi di truffe che ogni giorno possono ingannare gli utenti. E allora cosa si può fare per difendersi dai pericoli della Rete? Lo abbiamo chiesto agli esperti del Servizio di polizia postale e delle comunicazioni.

Phishing

Per non abboccare al "phishing" 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". Cosa vuol dire? "Significa 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 e-mail invitandovi a cambiare la vostra password, a entrare nella vostra banca o sul conto alla posta. Zireddu ribadisce: "nessuna banca o ufficio postale invia mail per verificare dati o comunicare con i clienti".

Viaggi fantasma

Nei periodi di vacanza, estate, Natale, Capodanno, numerose sono anche le finte offerte di viaggi che

Anti-Phishing Italia: il portale contro le truffe on-line

Un crimine su 5 è commesso on line

offrono pacchetti “last minute” di villaggi inesistenti o fatiscenti. È 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.

Social network e furti d’identità

Molti giovani oggi si impossessano della 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.

È 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.

“È molto facile su Internet sostituirsi a una persona e creare un profilo a suo nome sui social network” dice Stefano 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 poi non dovrebbero mettere fotografie che, una volta pubblicate, possono tranquillamente andare in giro sul web.

Gli esperti del Servizio polizia postale 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.

Fonte: Anti-Phishing Italia – www.anti-phishing.it