



soldi &gt; l'infiltrato

di Alessandro Calderoni  
redazione@millionaire.it

# LA TRUFFA CORRE ON LINE

INTERNET, E-MAIL,  
BANCOMAT E CONTI  
VIRTUALI. LA FRODE  
È IN AGGUATO.  
ECCO COME DIFENDERSI

Avete un conto corrente on line? Fate acquisti in Rete? Volete rispondere a una e-mail arrivata dalla Nigeria? Usate con disinvoltura bancomat e carte di credito? Seguitemi, questo articolo fa per voi e potrebbe mettervi in guardia. Le frodi telematiche, truffe perpetrate grazie alle nuove tecnologie, sono in aumento. Si parla di tremila e 500 denunce nei primi tre mesi del 2007 fatte al Gat, il Nucleo Speciale Frodi Telematiche della Guardia di Finanza. Senza contare quelle pervenute nello stesso periodo alla Polizia Postale e quelle non denunciate. Ma vediamo quali sono i tecnoraggi più frequenti, grazie all'aiuto del colonnello delle Fiamme Gialle Umberto Rapetto, comandante del Gat, che all'argomento ha dedicato un libro (vedi riquadro a pag. 102).

## I classici raggiri

Nella top ten dei sistemi utilizzati per fregare la gente figurano termini stranieri ormai noti ai più. I *dialer* sono quei programmi che, scaricati, sono in grado di interrompere la connessione alla rete e instaurarne una nuova molto più costosa, con tariffazione da chiamata internazionale. «Possono essere molto silenziosi ma non invisibili» suggerisce Rapetto, che invita a con-

trollare le icone di connessione presenti sullo schermo. «Se non si può passare a una connessione a banda larga, che non richiede la composizione di un numero ogni volta, basta comunque innalzare il livello di sicurezza del proprio browser dalle opzioni del programma e chiedere al fornitore di linea telefonica di disabilitare le chiamate verso numeri ad alta tariffazione».

Un altro tormentone degli ultimi anni è il *phishing*, il sistema con cui i truffatori lanciano esche via e-mail, proponendosi in modo anche graficamente credibile come istituti di credito e chiedendo agli utenti le loro credenziali d'accesso ai conti on line, con la scusa di una procedura di aumento di sicurezza. Se l'utente clicca sul link contenuto nel messaggio di posta elettronica è rimandato a un falso sito, normalmente un clone di quello originale, ottenuto con un semplice software gratuito detto *spider* - e se vi inserisce *user id* e *password* cascando nella trappola, il suo conto corrente viene svuotato in meno di un attimo. Fine della fase uno. Fase due: come ripulire i soldi e dove farli finire? Ecco una nuova truffa e una nuova e-mail: qualcuno ti contatta offrendoti un lavoro come rappresentante commerciale per una determinata zona e proponendoti di ricevere denaro sul tuo conto corrente e di trattenerne ►►

**Dal 2005, ogni giorno, sono circa 8 milioni i tentativi di carpire dati e informazioni personali attraverso una e-mail**

**soldi** > l'infiltrato

►► una percentuale spendendo il resto con un servizio di *money transfer* tipo Western Union. «I soldi arrivano davvero e già nel momento in cui finiscono sul conto del cittadino per ripulirsi, l'ingenuo padre di famiglia o il ragazzino in cerca di arrotondamenti diventa suo malgrado partecipe di una grande operazione di riciclaggio e rischia il carcere. In pratica, i soldi che lui riceve sono quelli rubati dal conto on line di un altro truffato».

**Frodi nuove ma già note**

L'evoluzione del phishing si chiama *pharming* e si avvale di un escamotage tecnico per superare il buon senso e la diffidenza degli utenti ormai furbi. Il trucco consiste nel far credere all'internauta di essere davvero sul sito della sua banca, mentre è altrove. In pratica il pirata informatico attacca il *Dns*, cioè il computer che funge da centralinista per la Rete e collega l'indirizzo che digitiamo nel nostro browser ([www.eccetera](http://www.eccetera)) all'indirizzo numerico IP che contraddistingue la macchina su cui risiede il sito che vogliamo visitare. In caso di *pharming*, insomma, l'utente digita l'indirizzo corretto ma finisce ugualmente sul sito del truffatore.

«Nel 2004, un 19enne tedesco è riuscito a spostare migliaia di utenti dal sito EBay.de a un sito fasullo. Scoperto e arrestato, ha sostenuto che voleva soltanto divertirsi». Esistono comunque altri canali per il *pharming*, oltre all'attacco ai *Dns*. «Talora i truffatori inviano tramite e-mail un virus che cambia l'elenco dei siti cui l'utente si connette più spesso, per dirottarli a loro piacimento, o addirittura attaccano il server della banca per ricevere le connessioni regolari dei correntisti e rimpallarle su

un altro sito. Più spesso sfruttano la velocità con cui leggiamo sul monitor per sostituire alcune lettere con altre simili e deviarci verso siti non voluti. Il processo si chiama *mistyping* e accade per esempio al sito di pagamento on line Paypal, il cui link truffaldino fu inserito in alcune mail come Paypai: una sola lettera cambiata comportava il via alla truffa».

Ha meno di un anno di vita invece il cosiddetto *vishing*, un sistema col quale i truffatori inviano un messaggio di posta elettronica o un sms (sempre da parte di un pretestuoso istituto di credito o affine), invitando l'utente a chiamare un numero telefonico proprio per non incorrere in una truffa on line. «Rassicurato, il ricevente chiama e trova un risponditore telefonico che lo invita a digitare le cifre della sua carta di credito, la data di scadenza e il codice impresso sul retro. In pochi istanti, ha regalato a chissà chi il proprio denaro» aggiunge Repetto.

**Ti rubo l'identità e pure la password**

Negli Usa l'*identity theft*, il furto di identità, è molto diffuso. «Una delle cose prese di mira è il curriculum on line. Se metti in rete tutti i fatti tuoi sperando di trovare un lavoro, qualcuno può appropriarsi di ciò che dici di te, fingersi un tuo vecchissimo conoscente e ottenere favori o denaro. Quando non addirittura costruirsi un personaggio molto simile a te e agire in nome e per conto della tua persona. Basta che uno trovi on line nome, cognome, data di nascita, telefono, codice fiscale, residenza di una persona e può fargli di tutto». Per esempio, chiamare una compagnia te- ►►



**Umberto Rapetto  
colonnello  
hi tech**

Umberto Rapetto, classe 1959, due lauree (in Giurisprudenza e in Scienze della sicurezza economico-finanziaria), comandante del GAT, è uno dei quattro "esperti" nominati nel Comitato per la tutela della proprietà intellettuale presso la Presidenza del Consiglio dei Ministri. Repetto ha recentemente scritto un libro a quattro mani con la moglie Maria Teresa Lamberti, vicecaporedattore del Giornale Radio Rai, sulle frodi telematiche. Si intitola *Truffe.com* (Cairoeditore, 13 euro) e spiega come difendersi dalle frodi on line. Ha messo in piedi anche [www.rapetto.it](http://www.rapetto.it), il portale della sua famiglia. «Viviamo tutti in posti strani e lontani e questo è l'unico modo che abbiamo per tenerci in contatto. Così ho dedicato una pagina a mio fratello Vittorio, informatico vero, una a mia moglie, giornalista, una a mia figlia Barbara, ingegnere elettronico».

«Parole come *phishing, pharming, vishing* non vi dicono niente? Sono i nomi delle truffe del web. **Attenzione: qualcuno potrebbe cercarvi la fontana di Trevi. E magari riuscirci**»



