FARONOTIZIE.IT

Anno II - n° 15
Giugno 2007

Redazione e amministrazione:
Scesa Porta Laino, n. 33
87026 Mormanno (CS)
Tel. 0981 81819
Fax 0981 85700
redazione@faronotizie.it

Testata giornalistica registrata al Tribunale di Castrovillari n° 02/06 Registro Stampa (n.188/06 RVG) del 24 marzo 2006

Direttore responsabile
Giorgio Rinaldi

WEB & RISCHI

di Nicola Perrelli

Ormai è una certezza: le frodi on line sono in continuo aumento. Ad affermarlo è il risultato di un rapporto preparato da una società specializzata per conto di un pool di banche ed istituzioni finanziarie, i soggetti più esposti, per ovvi motivi, a tale tipo di truffa. Ma sono anche quelli che riescono meglio a difendersi grazie a sofisticati e costosi sistemi di difesa . E il privato cittadino? Ha poche ma importanti chance: mantenere sempre una buona dose di prudenza, una sana diffidenza e aggiornarsi di continuo sulle "novità" del settore.

Le forme al momento più diffuse e conosciute di frode sono: il *phishing*, il *pharming* e il *trojan horse*. Il primo è di fatto un vero e proprio furto di identità e deriva dal termine inglese *fishing* (pescare, in questo caso dati). Attraverso l'invio di e-mail, ma anche contatti telefonici, contenenti falsi messaggi confidenziali vengono richieste all'utente, ignaro dell'inganno, informazioni riservate riguardo a dati personali, come il numero della carta di credito, quello del c/c, i codici di accesso ai conti on line,ecc.. Il secondo, il *pharming*, sempre con l'inganno, ma questa volta meglio dissimulato, carpisce la buona fede dell'utente presentando una pagina web identica a quella ufficiale di siti di banche, assicurazioni,poste,ecc. In questo modo l'utente è convinto di trovarsi , ad esempio, nel sito della propria home banking e di compiere le normali operazioni sul proprio c/corrente on line. A questo punto, una volta digitati - id e password - il gioco è fatto.
Tramite un trojan horse, il terzo sistema di inganno, che consiste in un programma che permette l'accesso ad un altro utente, diventa possibile utilizzare i dati a scopi fraudolenti.
Ma non finisce qui. Le occasioni per cadere nella "rete" delle truffe sono davvero molte. A volte navigando in un sito basta cliccare su un banner con un logo che attrae, uno sfondo che piace e all'insaputa si scarica un programma, chiamato *dialer*, che crea automaticamente una connessione verso numeri telefonici che costano un occhio della testa. Come quelli che cominciano con il prefisso: 144, 163, 164, 166, 899 e di recente il 709. Peggio ancora se crea una connessione con prefissi satellitari e internazionali, in questo caso si può arrivare a pagare 3 euro per ogni minuto di navigazione, quindi 180 € all'ora!!

La situazione è insomma da allarme rosso. I c/c svuotati, le carte di credito clonate, i codici segreti violati e le bollette telefoniche a 4 e 5 cifre, restano all'ordine del giorno, nonostante l'impegno della Polizia Postale e delle Comunicazioni e le

continue esortazioni ad una maggiore attenzione da parte delle banche e istituiti finanziari.

La minaccia dei criminali informatici si è ormai capito non si combatte con leggi e disposizioni, sono necessari invece formazione e esperienza. Troppo spesso infatti le truffe vengono messe a segno per i programmi non sempre affidabili, troppo vulnerabili , ma anche e soprattutto per l'impreparazione e la scarsa attenzione dell'utente. E' bene allora , almeno per ciò che ha a che fare con i servizi finanziari che sono in definitiva quelli più colpiti e che per i danni che comportano sono anche quelli che fanno più "male", tenere a mente una serie di indicazioni per proteggersi da questo tipo di fregature che il web può regalare.
Bisogna intanto tenere presente che nel settore dei servizi finanziari identità e soldi sono "virtuali". Ci si autentica, come si dice nel gergo, con la propria password e si prelevano e spendono i soldi digitando i propri codici di sicurezza. Non c'è più insomma chi falsificando firme o forzando la cassaforte si appropria della nostra identità o dei nostri soldi, oggi si ci rubano molto probabilmente è per colpa nostra.

Password e codici vanno quindi custoditi con la massima attenzione. Il modo migliore e più sicuro per non perderli è quello di memorizzarli. Ma se proprio non ci si riesce, perché sono tanti, è del tutto sconsigliato trascriverli su blocchi notes, fogli e agende che stanno vicino al Pc e digitarli davanti ad altre persone. Mentre è buona regola quella di cambiarli di frequente e di disabilitare nei siti web il completamente automatico.

Analogo discorso per le Carte di credito, sempre più diffuse e utilizzate. Per mantenere un buon livello di sicurezza è opportuno non affidare la carta ad altri, non fornire il Pin e non perderla di vista al momento dei pagamenti. E' preferibile inoltre avere carte le cui società emittenti offrono l'utile servizio di *alert*, ossia l'avviso in tempo reale di avvenuta transazione. In questo modo si può intervenire immediatamente in caso di operazioni sospette. Fermo restando che è indispensabile controllare l'estratto conto periodico per contestare ,entro 60 giorni, eventuali spese mai effettuate.

Per gli acquisti su internet , prima di utilizzare la carta di credito è necessario verificare l'identità e la credibilità del sito. Come è opportuno appurare che il sito dove si intende fare acquisti utilizzi protocolli di sicurezza che permettano di identificare l'utente.

L’icona di un lucchetto, che compare durante la transazione, attesta che in quel momento la connessione è sicura. Affinché la transazione vada a buon fine serve solo il numero della carta di credito, l’eventuale codice posto sul retro e la relativa scadenza e nessun altro dato troppo personale.

Il livello di consapevolezza degli utenti connessi alla rete è quindi al momento l’unico vero strumento di difesa contro il dilagare delle attività delinquenziali su internet. Solo conoscendo il problema ci si può difendere. Del resto, prevenire è meglio che curare.