PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 8 - numero 1441 di martedì 21 marzo 2006

PISHING: UN'INVASIONE

Si moltiplicano i tentativi di dirottare i clienti di banche on line verso siti truffa grazie all'invio di e-mail subdole che possono far credere di essere di fronte a reali richieste del proprio istituto di credito. Il caso Bancoposta.

In questi giorni si stanno moltiplicando gli invii di e-mail subdole che cercano di dirottare i clienti di banche on line verso siti truffa per carpire i codici segreti di accesso, il cosiddetto "pishing". Grazie all'invio di messaggi sempre più raffinati (vedere i primi esempi "sgrammaticati" in PuntoSicuro n. 1321), i destinatari possono credere di essere di fronte a reali richieste del proprio istituto di credito.

In particolare numerosi sono gli invii destinati agli utenti del servizio Bancoposta di Poste Italiane.

Il comportamento più sicuro in questi casi è ignorare il messaggio in arrivo e verificare direttamente nel sito già conosciuto (in questo caso www.poste.it) se ci sono in atto richieste particolari nei confronti dei clienti. In ogni caso, mai cliccare sul messaggio, e soprattutto non inserire i propri codici personali!

Messaggi truffa simili sono stati inviati anche a nome di Visa: in questo caso chiedendo "Proteggi la tua carta Visa online con una password personale, Visa assicura che solamente tu potrai utilizzare la tua carta Visa on line, abilita la tua carta di credito alle ultime misure di sicurezza Visa.com, segui il link riportato per abilitare la tua carta di credito alle transazioni autenticate protette dal protocollo SSL3 e dalla tua password personale".

Invii anche a nome di Banca Intesa: "Egregio Cliente, ci sono stati segnalati probabili tentativi di utilizzo abusivo della sua carta di credito (o di addebito improprio sul suo conto corrente); è possibile che qualcuno sia riuscito ad impadronirsi di liste di dati sensibili; la invitiamo a comunicarci immediatamente il codice della sua carta di credito (o la sua userid e password di accesso al servizio di home banking), per consentirci le opportune verifiche".

In quest'ultimo messaggio, per rendere più efficace il messaggio, è stata inserita anche una "velata" minaccia: "In assenza di un suo riscontro, ci vedremo costretti, nel suo interesse, a bloccare l'operatività della sua carta (o del suo conto corrente annullando nel contempo le chiavi di accesso)".

Per ulteriori notizie e consigli su come difendersi da questo e da altri tentativi di truffa si possono consultare i siti della Polizia di Stato e dell'associazione no-profit Anti-Phishing Italia.
