Phishing: riservatezza dei codici di accesso al servizio

Ovvero come catturare illegalmente “codice utente” e “password”

Il meccanismo è semplice: consiste nel ricevere una comunicazione, apparentemente da parte della Banca del cliente (nella maggior parte dei casi tramite la posta elettronica), nella quale vengono richiesti i dati personali tramite un modulo incluso nella e-mail stessa o tramite un collegamento (link) ad una pagina internet.

Come giustificazione a questa comunicazione, vengono riportate problematiche tecniche non meglio precisate.

Compilando tale modulo, l’ignaro cliente finisce per svelare “codice utente” e “password” che possono essere così utilizzati dai pirati informatici per compiere operazioni illegali.

Il fenomeno è particolarmente insidioso perché i messaggi, nella maggior parte dei casi, sembrano effettivamente inviati da Banche molto note, in modo tale da non sollevar sospetti nel destinatario.

Sfuggire a questi “attacchi” è, di contro, piuttosto semplice.

Di seguito, alcune indicazioni di carattere generale:

1. gli Istituti di Credito non richiedono mai utenze, password o dati personali tramite messaggi di posta elettronica

2. non rispondere mai a queste e-mail: nel dubbio, contattare la Banca che dichiara di averVi inviato la comunicazione

3. qualora il messaggio contenga allegati o un collegamento (link) ad una pagina internet, non aprire né l’allegato né cliccare sul collegamento anche su sollecitazioni ad entrare nel sito della Banca per urgenti comunicazioni, in quanto potrebbero condurre entrambi ad un sito contraffatto.

4. diffidare ancor di più se il messaggio contiene argomenti intimidatori: per esempio, in caso di mancata risposta, sospensione del “codice utente”.