

## **FRODI**

Negli ultimi tempi stanno variando i sistemi di "hackeraggio": si è passati da tentativi volti a scardinare semplicemente la sicurezza per carpire informazioni protette ad azioni volte a trarre vantaggio economico tramite sottrazione di fondi; queste azioni prevedono il furto dell'identità elettronica.

E' molto diffusa una modalità di truffa on-line (nota come "phishing") che, senza violare i sistemi di sicurezza della Banca, punta a catturare in modo fraudolento i codici di accesso all'Internet Banking dei clienti.

Ciò avviene attraverso l'invio di una e-mail, che sembra provenire dalla banca stessa, ad un elenco di indirizzi creato in modo casuale dai truffatori. In tale e-mail si richiede di accedere ad un link (che sembra riportare al sito ufficiale di tale banca) e di inserire i propri codici di accesso, adducendo generici motivi di sicurezza. In realtà, seguendo le istruzioni riportate, il cliente si collega al sito del truffatore e ad esso trasmette le informazioni personali inserite.

In altri casi, le e-mail contengono un allegato che, se aperto, installa sul computer un programma per permettere al truffatore di accedere alle informazioni riservate presenti sul pc del cliente oppure di "vedere" quello che il cliente sta digitando sulla tastiera del proprio computer (fenomeno noto come "key logging"). In alcuni casi tali programmi "trojan" permettono di far puntare il pc a siti non ufficiali anche digitando l'indirizzo corretto (fenomeno noto come "pharming").

In nessuno di questi casi si è in presenza di violazione informatica dei siti della banca poiché l'obiettivo è accedervi regolarmente con i codici sottratti.

Si suggerisce di prestare attenzione ad eventuali anomalie rispetto alle modalità consuete con cui viene richiesto l'inserimento dei dati personali; è altresì consigliabile di controllare sempre l'autenticità della connessione mediante il controllo accurato del nome del sito.

Occorre non dare mai seguito a messaggi o telefonate che richiedano l'immissione o comunicazione della user, password o pin. In caso di dubbi è possibile contattare la filiale di riferimento.

Si raccomanda, infine, di non aderire in rete ad iniziative volte ad ottenere la messa a disposizione del proprio conto corrente, con finalità di transito di somme la cui origine potrebbe essere illecita.