IL DECALOGO ABI PER I CLIENTI (*)

ABI Lab, grazie all'attività della Centrale d'allarme per attacchi informatici, il cui compito è quello di arginare l'evoluzione del fenomeno fraudolento del furto d'identità elettronica tramite Internet, ha diffuso due decaloghi comportamentali diretti rispettivamente alle banche e alla clientela.

Qui di seguito riportiamo il secondo, in una versione aggiornata ed integrata con ulteriori contromisure aggiuntive.

1. Diffidate di qualunque e-mail richieda l'inserimento di dati riservati riguardanti codici di carte di pagamento, chiavi di accesso al servizio di home banking o informazioni personali. La vostra Banca non richiederà mai tali informazioni via e-mail.

2. E' possibile riconoscere le truffe via e-mail con qualche piccola attenzione. Generalmente queste e-mail:

- non sono personalizzate e contengono un messaggio generico di richiesta informazioni personali per motivi non ben specificati; o fanno uso di toni "intimidatori", per esempio minacciano la sospensione dell'account in caso di mancata risposta da parte dell'utente;
- promettono remunerazione immediata a seguito della verifica delle proprie credenziali di identificazione;
- non riportano una data di scadenza per l'invio delle informazioni.

3. Nel caso in cui riceviate un'e-mail con richieste di questo tipo, non rispondete ma informate subito la vostra Banca.

4. Non cliccate su link presenti in e-mail sospette, in quanto potrebbero condurvi a un sito contraffatto, difficilmente distinguibile dall'originale. Diffidate, inoltre, di e-mail con indirizzi web molto lunghi, contenenti caratteri inusuali, oppure sequenze casuali di caratteri.

5. Quando inserite dati riservati in una pagina web, assicuratevi che si tratti di una pagina protetta: l'indirizzo comincia con "https://" e non con "http://" e nella parte in basso a destra è presente un lucchetto. Al riguardo, si sottolinea la necessità di stabilire l'autenticità della connessione sicura facendo doppio click sul lucchetto in basso a destra e verificando la correttezza delle informazioni di rilascio e validità che compaiono per il relativo certificato digitale.

6. Diffidate se improvvisamente cambia la modalità con la quale è richiesto d'inserire i vostri codici di accesso all'home banking: per esempio, se questi sono chiesti non tramite una pagina del sito, ma tramite pop-up; in questo caso contattate la vostra Banca.

7. Controllate regolarmente gli estratti conto del conto corrente e delle carte di credito per assicurarvi che le operazioni riportate siano quelle realmente effettuate. In caso contrario, contattate la Banca e/o l'emittente della carta di credito.

8. Le aziende produttrici dei browser rendono periodicamente disponibili on-line, scaricabili gratuitamente, degli aggiornamenti (patch) che migliorano la sicurezza di questi programmi. Sui siti di tali aziende è anche possibile verificare che il vostro browser sia aggiornato; in caso contrario, è consigliabile scaricare e installare le patch.

9. Sia le e-mail sia i siti di phishing tentano spesso di installare sul computer della vittima un "codice malevolo" atto a carpire le informazioni personali in un secondo momento, attivandosi nel quando sono digitate. Si può impedire tale operazione tenendo sempre aggiornato il software antivirus.

In caso di dubbio, rivolgetevi alla vostra Banca!

(*) ABI LAB È IL CENTRO DI RICERCA E SVILUPPO DELLE TECNOLOGIE PER LA BANCA, PROMOSSO DALL'ASSOCIAZIONE BANCARIAITALIANA IN UN'OTTICA DI COOPERAZIONE TRA BANCHE E INTERMEDIARI FINANZIARI, PARTNER TECNOLOGICI E ISTITUZIONI. MAGGIORI INFORMAZIONI SONO DISPONIBILI SUL SITO WWW.ABILAB.IT