BANCA
SISTEMA
WWW.BANCASISTEMA.IT

DECALOGO ABI LAB PER I CLIENTI

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

2. È 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 di informazioni personali per motivi non ben specificati (es. scadenza, smarrimento, problemi tecnici);
   - fanno uso di toni "intimidatori", ad esempio minacciando 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 una e-mail contenente richieste di questo tipo, non rispondete alla e-mail stessa, ma informate subito la vostra banca tramite il *call center* o recandovi in filiale.

4. Non cliccate su *link* presenti in e-mail sospette, in quanto questi collegamenti potrebbero condurvi a un sito contraffatto, difficilmente distinguibile dall'originale. Anche se sulla barra degli indirizzi del *browser* viene visualizzato l'indirizzo corretto, non vi fidate: è possibile infatti per un *hacker* visualizzare nella barra degli indirizzi del vostro *browser* un indirizzo diverso da quello nel quale realmente vi trovate. Diffidate inoltre di e-mail con indirizzi *web* molto lunghi, contenenti caratteri inusuali, quali in particolare @.

5. Quando inserite dati riservati in una pagina *web*, assicuratevi che si tratti di una pagina protetta: queste pagine sono riconoscibili in quanto l'indirizzo che compare nella barra degli indirizzi del browser comincia con "https://" e non con "http://" e nella parte in basso a destra della pagina è presente un lucchetto. In proposito si sottolinea la necessità di stabilire l'autenticità della connessione 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 vi viene chiesto di inserire i vostri codici di accesso all'*home banking*: ad esempio, se questi vengono chiesti non tramite una pagina del sito, ma tramite *pop-up* (una finestra aggiuntiva di dimensioni ridotte). In questo caso, contattate la vostra banca tramite il *call center* o recandovi in filiale.

7. Controllate regolarmente gli estratti conto del vostro conto corrente e delle carte di credito per assicurarvi che le transazioni 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* e scaricabili gratuitamente degli aggiornamenti (cosiddette *patch*) che incrementano la sicurezza di questi programmi. Sui siti di queste 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 che i siti di phishing tentano spesso di installare sul computer della vittima codice malevolo atto a carpire le informazioni personali in un secondo momento, attivandosi nel momento in cui vengono digitate. Si può impedire tale operazione tenendo sempre aggiornato il *software antivirus* presente sul proprio computer.

10. *Internet* è un po' come il mondo reale: come non dareste a uno sconosciuto il codice PIN del vostro bancomat, allo stesso modo occorre essere estremamente diffidenti nel consegnare i vostri dati riservati senza essere sicuri dell'identità di chi li sta chiedendo. In caso di dubbio, rivolgetevi allavostra banca!